

**UNIVERZITET SINGIDUNUM
BEOGRAD
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE**

MAGISTARSKI RAD

**Analiza bezbednosnih karakteristika IKE
protokola za razmenu ključeva na Internetu**

MENTOR:

Prof. dr Mladen Veinović

STUDENT: Zoran Antić

BROJ INDEKSA: II-1/2004

Beograd, 2026.

Članovi komisije:

Prof. dr Mladen Veinović, mentor

Prof. dr Aleksandar Jevremović

Prof. dr Zoran Banjac, viši naučni saradnik

Datum odbrane magistarskog rada : _____

Zahvalnica:

Svom mentoru, prof. dr Mladenu Veinoviću, dugujem najiskreniju zahvalnost za dragoceno stručno vođstvo, podsticaj i poverenje koje mi je ukazao tokom naučno-istraživačkog rada i pisanja ove magistarske teze. Njegovi saveti i smernice predstavljali su siguran oslonac u svakoj fazi rada, a naučna posvećenost i istinski posvećen pristup mentorstvu kojim je pratio ovo istraživanje čine profesora Veinovića izuzetnim uzorom kome težim u sopstvenom naučnoistraživačkom radu.

Članovima komisije, prof. dr Aleksandru Jevremoviću i prof. dr Zoranu Banjcu, zahvaljujem na vremenu i pažnji posvećenoj oceni ove teze.

Univerzitetu Singidunum i Departmanu za poslediplomske studije zahvalan sam na pruženoj prilici za usavršavanje i sticanje novih znanja tokom magistarskih studija.

Posebnu zahvalnost, na kraju, dugujem svojoj porodici — na razumevanju, strpljenju i podršci koju su mi pružali tokom čitavog perioda studiranja.

Ovaj rad predstavlja plod višegodišnjeg truda, učenja i profesionalnog usavršavanja, i istovremeno je snažan podsticaj da nastavim dalje naučnoistraživačko usavršavanje u oblasti bezbednosti i kriptografske zaštite komunikacionih sistema, verujući da je ovo tek prvi korak u dugoročnoj posvećenosti nauci.

Rezime:

Predmet ovog istraživanja predstavljaju bezbednosne karakteristike Internet Key Exchange (IKE), protokola za razmenu kriptografskih ključeva u okviru IPsec arhitekture. Cilj rada bio je da se analiziraju projektantski principi, bezbednosni mehanizmi i evolucija IKE protokola od verzije IKEv1 do savremene arhitekture IKEv2, kao i da se sagleda njihov značaj u zaštiti informaciono-komunikacionih sistema. Istraživanje je zasnovano na integrisanom procesno-komparativnom metodološkom pristupu kojim su objedinjeni tehnički, implementacioni, hardverski, organizacioni i operativni aspekti bezbednosti. Kroz analizu IPsec arhitekture, mehanizama autentifikacije, razmene kriptografskih ključeva, upravljanja bezbednosnim asocijacijama i životnog ciklusa bezbednosnih mehanizama utvrđeno je da se bezbednost savremenih VPN sistema ne može posmatrati isključivo kroz primenu pojedinačnih kriptografskih algoritama, već kao rezultat njihovog koordinisanog delovanja u okviru jedinstvene bezbednosne arhitekture. Rezultati istraživanja potvrđuju da Internet Key Exchange Version 2 predstavlja značajan kvalitativni iskorak u odnosu na IKEv1, kako u pogledu projektantske arhitekture, tako i u oblasti interoperabilnosti, upravljanja kriptografskim ključevima i otpornosti na savremene bezbednosne pretnje. Naučni doprinos rada ogleda se u razvoju integrisanog procesno-komparativnog modela za procenu bezbednosnih karakteristika IKE protokola, koji omogućava sveobuhvatnije sagledavanje bezbednosti savremenih informaciono-komunikacionih sistema.

Ključne reči: Internet Key Exchange (IKE), IKEv1, IKEv2, IPsec, razmena kriptografskih ključeva, bezbednosna arhitektura, VPN, Security Association (SA), upravljanje kriptografskim ključevima, informaciono-komunikacioni sistemi.

Sadržaj:

1. Uvod.....	1
1.1. Predmet istraživanja	4
1.2. Cilj istraživanja	6
1.3. Naučni problem i hipoteze istraživanja.....	7
1.4. Metodologija istraživanja.....	9
1.5. Struktura magistarskog rada.....	11
2. Teorijsko-analiitička osnova kriptografske razmene ključeva.....	14
2.1. Istorijski razvoj razmene kriptografskih ključeva	14
2.2. Nastanak kriptografije sa javnim ključem kao prekretnica u razvoju bezbedne razmene kriptografskih ključeva	21
2.3 Diffie–hellman algoritam za razmenu kriptografskih ključeva – teorijske, matematičke i bezbednosne osnove	23
2.3.1. Teorijska osnova i naučno-istraživačka analiza nastanka diffie–hellman algoritma za razmenu kriptografskih ključeva	25
2.3.2. Izbor diffie–hellman grupa : implementacioni i konfiguracioni izazovi kao determinante bezbednosnih karakteristika ikev1 i ikev2 protokola	29
2.3.3. Funkcije za izvođenje kriptografskog materijala kao osnova bezbedne arhitekture internet key exchange protokola	31
2.4. Entropija, generatori slučajnih brojeva i nonce vrednosti kao osnova bezbedne razmene kriptografskih ključeva	33
2.4.1. Entropija i kvalitet slučajnosti kao fundamentalni preduslov bezbednosti internet key exchange protokola	33
2.5. Perfect forward secrecy i upravljanje životnim ciklusom kriptografskih ključeva kao osnova dugoročne bezbednosti internet key exchange protokola.....	34
3. Arhitektura ipsec protokola kao osnova za uspostavljanje digitalnog poverenja i funkcionisanje internet key exchange (ike) protokola	37
3.1. Teorijska osnova nastanka ipsec arhitekture	37
3.2. Ipsec kao procesno organizovana bezbednosna arhitektura.....	39
3.2.1. Teorijska osnova procesnog pristupa ipsec arhitekturi	39
3.2.2. Ipsec kao integrisani bezbednosni proces	39
3.2.3. Proces uspostavljanja digitalnog poverenja	39
3.2.4. Bezbednosni značaj procesnog modela za internet key exchange	40
3.3. Security policy database (spd) kao polazna tačka procesa uspostavljanja digitalnog poverenja	41
3.3.1. Teorijska osnova security policy database	41
3.3.2. Security policy database kao proces donošenja bezbednosnih odluka	41
3.3.3. Bezbednosni značaj security policy database.....	41
3.3.4. Implementacioni i konfiguracioni izazovi.....	42

3.3.5. Procesni značaj security policy database u ipsec arhitekturi.....	42
3.4. Internet key exchange kao centralni procesni mehanizam ipsec arhitekture	43
3.4.1. Teorijska osnova uloge internet key exchange protokola	43
3.4.2. Internet key exchange kao procesna veza između bezbednosne politike i zaštićene komunikacije	43
3.4.3. Uloga internet key exchange u procesu uspostavljanja digitalnog poverenja.....	44
3.4.4. Implementacioni i konfiguracioni izazovi.....	44
3.4.5. Procesni značaj internet key exchange u ipsec arhitekturi	44
3.5. Security association (sa) kao operativna realizacija digitalnog poverenja u ipsec arhitekturi	47
3.5.1. Teorijska osnova security association mehanizma.....	47
3.5.2. Security association kao rezultat procesa uspostavljanja digitalnog poverenja	47
3.5.3. Značaj (sa) security association.....	48
3.5.4. Životni ciklus security association	48
3.6. Security association database (sad) kao mehanizam upravljanja aktivnim stanjem digitalnog poverenja	49
3.6.1. Teorijska osnova security association database	49
3.6.2. Security association database kao operativni mehanizam upravljanja poverenjem.....	49
3.6.3. Uloga security association database	50
3.6.4. Životni ciklus digitalnog poverenja.....	51
3.6.5. Implementacioni i konfiguracioni izazovi.....	51
3.6.6. Procesni značaj security association database.....	51
3.7. Authentication header (ah) kao mehanizam očuvanja integriteta procesa digitalnog poverenja	52
3.7.1. Teorijska osnova authentication header mehanizma.....	52
3.7.2. Authentication header kao zaštita integriteta uspostavljenog poverenja	52
3.7.3. Značaj authentication header protokola	52
3.7.4. Implementacioni i konfiguracioni izazovi.....	53
3.7.5. Bezbednosni značaj authentication header mehanizma	53
3.8. Encapsulating security payload (esp) kao centralni operativni mehanizam zaštite digitalnog poverenja	54
3.8.1. Teorijsko-kriptografska osnova encapsulating security payload mehanizma.....	59
3.8.2. Esp kao operacionalizacija digitalnog poverenja	59
3.8.3. Implementaciono-bezbednosna dimenzija	60
3.8.4. Savremeni izazovi primene esp mehanizma	60
4. Bezbednosne karakteristike internet key exchange version 1 (ikev1) protokola kroz procesnu analizu faza, modova i mehanizama upravljanja bezbednosnim asocijacijama	61

4.1. Bezbednosne karakteristike faze 1 ikev1 protokola – uspostavljanje ike security association	64
4.2. Main mode – detaljna analiza bezbednosnih karakteristika	65
4.3. Aggressive mode – detaljna analiza bezbednosnih karakteristika	66
4.4. Komparativna analiza main mode i aggressive mode	70
4.5. Bezbednosne karakteristike faze 2 ikev1 protokola quick mode i uspostavljanje ipsec security association	71
4.6. Metode autentifikacije u ikev1 protokolu i njihov bezbednosni značaj	73
4.7. Kriptografski algoritmi u ikev1 protokolu i njihov bezbednosni značaj	76
4.8. Životni ciklus security association i upravljanje bezbednosnim asocijacijama	80
4.9. Rekeying mehanizmi i kontinuitet bezbednosti	81
4.10. Savremene napredne persistentne pretnje (advanced persistent threat – apt) u slučaju ikev1	83
4.11. Savremeni značaj analize ikev1 protokola u uslovima postepene migracije ka ikev2	85
5. Razvoj ikev2 protokola kroz procesnu analizu arhitekture, bezbednosnih mehanizama i evolucije u odnosu na ikev1 protokol	88
5.1. Evolucija bezbednosne arhitekture: istorijski razvoj, razlozi za nastanak i standardizacija internet key exchange (ikev2) protokola	89
5.1.1. Kritička analiza evolucije bezbednosne arhitekture: projektna unapređenja implementirana u ikev2 protokolu	90
5.2. Arhitektura i funkcionalni model ikev2	92
5.3. Uspostavljanje ike_sa: proces razmene poruka i uspostavljanje digitalnog poverenja	97
5.4. Child_sa mehanizam i upravljanje ključevima	101
5.4.1. Arhitektura child_sa mehanizma, životni ciklus i upravljanje kriptografskim ključevima	101
5.4.2. Rekeying, create_child_sa mehanizam i bezbednosni značaj upravljanja životnim ciklusom kriptografskih ključeva	102
5.5. Bezbednosni mehanizmi ikev2	104
5.5.1. Integrisana arhitektura autentifikacije, tajnosti i integriteta u ikev2 protokolu	104
5.6. Napredne funkcionalnosti ikev2	107
5.6.1. Mobilnost, interoperabilnost i adaptivnost ikev2 u savremenim mrežnim okruženjima	107
5.6.2. Interoperabilnost, proširivost i evolutivna arhitektura ikev2 protokola	108
5.7. Bezbednosne ranjivosti ikev2	110
5.7.1. Teorijski model bezbednosnih ranjivosti ikev2 protokola	110
5.7.2. Implementacione ranjivosti, cve analiza i bezbednosni izazovi praktičnih implementacija ikev2	113
5.7.3. Integrisani model upravljanja bezbednosnim komponentama ikev2: endpoint	

bezbednost, višeslojna zaštita i perspektive razvoja	115
5.8. Komparativna analiza bezbednosne arhitekture, upravljanja ključevima i operativnih karakteristika ikev1 i ikev2	116
5.9. Kritička evaluacija ikev2 u savremenim vpn sistemima	119
5.10. Naučno-istraživačka sinteza i perspektive daljeg razvoja	121
6. Savremeni bezbednosni izazovi ike protokola	123
6.1. Analiza bezbednosnih karakteristika i ranjivosti ike implementacija	123
6.2. Analiza poznatih cve ranjivosti u kontekstu ipsec, ikev1 i ikev2	125
6.3. Naučno-istraživačka klasifikacija cve ranjivosti ike implementacija i analiza uzročno-posledičnih veza.....	127
6.4. Metodološki okvir za izbor reprezentativnih cve ranjivosti i analiza obrazaca nastanka bezbednosnih propusta.....	130
6.5. Komparativna analiza reprezentativnih cve ranjivosti, metodološka sinteza i implikacije za bezbednost ike implementacija.....	132
6.6. Rop i byovd tehnika eksploatacije sa ipsec/ikev1/ikev2	134
6.6.1. Predmet, ciljevi i metodologija istraživanja rop/byovd rizika	134
6.7. Ipsec arhitektura: ah, esp i security association u kontekstu rop i byovd tehnika eksploatacije	136
6.7.1. Cve-2026-33824 — windows ike extension (ikeext).....	138
6.7.2. Cve-2025-9242 — watchguard fireware os (ikev2).....	138
6.7.3. Rop niz u fortios ssl-vpn/ipsec stack-u (cve-2022-42475, cve-2023-27997, cve-2024-21762).....	139
6.7.4. Mehanizam byovd tehnike: zloupotreba modela poverenja u potpisane drajvere	140
6.8. Objedinjena cve tabela i povezanost sa rop/byovd tehnikama.....	142
6.8.1. Metodologija sistematizacije.....	142
6.8.2. Komparativna i trend analiza	145
6.8.3. Ograničenja sistematizacije.....	145
6.8.4. Implikacije za procenu rizika mrežne infrastrukture.....	146
6.9. Pregled konkretnih ranjivih hardverskih uređaja	146
6.9.1. Fortinet fortigate (fortios).....	147
6.9.2. Watchguard firebox (fireware os)	147
6.9.3. Ivanti connect secure, policy secure i zta gateway.....	147
6.9.4. Check point security gateway	148
6.9.5. Windows server: ike extension (ikeext) hostovi	148
6.10. Postkvantna kriptografija i granica njene zaštite.....	149
6.10.1. Rfc 9370 i ml-kem integracija u ikev2 protokolu	149
6.10.2. Mogućnost zaobilaženja ili narušavanja pqc zaštite primenom pop i byovd tehnika	150

6.10.3. Formulacija centralnog nalaza: nezavisnost slojeva kao strukturno svojstvo.....	151
6.11. Post-kvantna kriptografija u ike sistemima	152
7. Zaključak	157
7.1. Potvrđivanje glavne hipoteze kroz procesni pristup	157
7.2. Testiranje pomoćnih hipoteza	159
7.3. Lateralno kretanje nakon inicijalnog pristupa: rop eksploatacija.....	160
7.4. Byovd napadi i lateralno kretanje.....	163
7.5. Sinteza originalnih analitičkih doprinosa	165
7.6. Ograničenja istraživanja i pravci budućih istraživanja	166
Literatura	168
2009.....	168
2010. Uvodi ECP grupe 19-21 zasnovane na NIST krivama.....	171
2017. Zabranjuje Diffie-Hellman grupe manje od 2048 bita za IKEv2.....	171
<i>Fragmentation.</i> " 2014. Mehanizam fragmentacije IKE poruka; implementaciona osjetljivost dokumentovana kroz CVE zapise.	172
2015. Fleksibilnija autentifikacija digitalnim potpisom u IKEv2.	172
2007. Profil sertifikata (PKI) za upotrebu u IKE protokolu.	172
PRILOG "A"	175
PRILOG "B"	176

Spisak slika

Slika 1. Prikaz komponenti Windows NTOS kernel executive-a i njihove interakcije sa korisničkim i kernel modom	18
Slika 2. Konceptualni model transformacije zajedničke tajne (Diffie-Hellman/ECDH) u višeslojnu bezbednosnu arhitekturu savremenih kriptografskih IPSec/IKE sistem.....	28
Slika 3. Konceptualni prikaz adaptivnog <i>Defense-in-Depth</i> modela zaštite IKEv2/IPsec protokola, sa pripadajućim vektorima napada i kontrolnim mehanizmom	46
Slika 4. Uporedni prikaz strukture IP paketa kod primene AH i ESP mehanizama zaštite IPsec protokola, u transportnom i tunelskom modu rada.....	55
Slika 5. Integrirani prikaz komponenti bezbedne IP komunikacije u okviru IPsec protokola, od kriptografske zaštite do upravljanja rizikom i odgovora na incidente	62

Spisak tabela

Tabela 1. Procesni pristup detekciji napada	15
Tabela 2. Nivoi pristupa operativnom sistemu.....	16
Tabela 3. Status kriptografskih algoritama prema RFC preporukama.....	20
Tabela 4. Komparativna analiza Diffie–Hellman grupa	24
Tabela 5. AH vs ESP – bezbednosne karakteristike	57
Tabela 6. Transport Mode vs Tunnel Mode	58
Tabela 7. Komparativna analiza IKEv1 i IKEv2	69
Tabela 8. Mehanizmi zaobilaženja kriptografske zaštite	84
Tabela 9. Lawful Hacking tehnike kao vektor na IPsec/IKE	112
Tabela 10. Objedinjena CVE tabela — ROP-eksploataбилne i autentifikacione ranjivosti IKE/IPSEC infrastrukture.....	143
Tabela 11. BYOVD dražveri dokumentovani u kompromitacijama VPN/IPSEC infrastrukture	144
Tabela 12. Objedinjeni dvofazni procesni lanac napada.....	144

1. Uvod

Razvoj informaciono-komunikacionih tehnologija doveo je do intenzivne digitalizacije društva, u kojoj se gotovo svi procesi zasnivaju na kontinuiranoj razmeni podataka između geografski distribuiranih informaciono-komunikacionih sistema. Takva transformacija nije uticala isključivo na način razmene informacija, već je bezbednost digitalnih komunikacija učinila jednim od osnovnih preduslova funkcionisanja savremenog društva [20].

Kontinuirani razvoj informaciono-komunikacionih tehnologija uslovio je eksponencijalni rast broja korisnika informaciono-komunikacionih sistema, kao i kompleksnost veza koje se svakodnevno uspostavljaju između korisnika, računarskih sistema, mrežnih uređaja, *cloud* platformi i drugih distribuiranih informacionih resursa. Paralelno sa povećanjem obima digitalne komunikacije raste i broj procesa razmene kriptografskih ključeva, čime se istovremeno povećava i složenost bezbednosnih izazova povezanih sa uspostavljanjem i očuvanjem digitalnog poverenja između učesnika u procesu komunikacije [38].

Savremeni informaciono-komunikacioni sistemi izloženi su sve sofisticiranijim oblicima napada koji ne ciljaju isključivo kriptografske algoritme, već čitav proces uspostavljanja bezbedne komunikacije, uključujući pregovaranje bezbednosnih parametara, autentifikaciju komunikacionih učesnika, upravljanje kriptografskim ključevima i implementaciju komunikacionih protokola. Takav razvoj bezbednosnih pretnji zahteva da se proces razmene kriptografskih ključeva posmatra kao jedan od najvažnijih elemenata ukupne bezbednosne arhitekture informaciono-komunikacionog sistema [44].

Bezbednost digitalnih komunikacija započinje mnogo pre prve razmenjene korisničke poruke – ona započinje pouzdanom verifikacijom digitalnog identiteta učesnika u procesu komunikacije, uspostavljanjem međusobnog digitalnog poverenja i bezbednom razmenom kriptografskih ključeva, čime se stvaraju osnovni preduslovi za uspostavljanje zaštićenog komunikacionog kanala.

Internet Key Exchange (IKE) protokol ne uspostavlja samo kriptografski zaštićeni komunikacioni kanal, već uspostavlja digitalno poverenje između prethodno verifikovanih digitalnih identiteta učesnika u komunikaciji, čime omogućava bezbednu razmenu kriptografskih ključeva i predstavlja temelj bezbednosti IPsec komunikacije [2].

Matematička otpornost kriptografskih algoritama na kriptozanalizu predstavlja neophodnu, ali ne i dovoljnu pretpostavku bezbedne komunikacije. Ostvareni nivo zaštite informaciono-komunikacionog sistema ne određuje isključivo izbor kriptografskih algoritama, već međusobno sadejstvo arhitekture komunikacionog protokola, bezbednosne aspekte i kompleksnost procesa autentifikacije (*password* vs *MFA*), upravljanja kriptografskim ključevima, uspostavljanja sigurnosnih asocijacija, kvalitet implementacije bezbednosnih mehanizama, pravilne konfiguracije informaciono-komunikacionog sistema i kontinuiranog nadzora rada informaciono-komunikacionog sistema u cilju detekcije zloupotreba (*insajderi koji predstavljaju pretnju po bezbednost i resurse informacionog sistema*) i u cilju pravovremene detekcije anomalija (*eksfiltracija podataka i neovlašćen pristup*). Posledično, kompromitacija procesa razmene kriptografskih ključeva može ugroziti celokupnu bezbednosnu arhitekturu sistema, čak i u situacijama kada primenjeni kriptografski algoritmi ispunjavaju najviše bezbednosne standard [47].

Upravo u tom kontekstu posebno mesto zauzima *Internet Key Exchange* (IKE) protokol kao centralni mehanizam za uspostavljanje digitalnog poverenja u okviru IPsec arhitekture.

Njegova funkcija nije ograničena na razmenu kriptografskih ključeva između komunikacionih učesnika, već obuhvata pregovaranje bezbednosnih parametara, autentifikaciju identiteta, generisanje zajedničkog kriptografskog materijala, uspostavljanje i upravljanje *Security Association* (SA), kao i obezbeđivanje uslova za bezbedno funkcionisanje kriptografski zaštićenih komunikacionih kanala. Na taj način *Internet Key Exchange* (IKE) predstavlja protokol za uspostavljanje digitalnog poverenja između komunikacionih entiteta kroz autentifikaciju identiteta, razmenu kriptografskih ključeva i upravljanje sigurnosnim asocijacijama. Osnovni normativni dokument koji definiše arhitekturu IPsec protokola, uključujući *Security Policy Database* (SPD), *Security Association Database* (SAD), *Security Association* (SA) i osnovne principe zaštite IP komunikacije. Predstavlja temelj za razumevanje uloge *Internet Key Exchange* (IKE) protokola u okviru IPsec arhitekture (RFC 4301). I pored činjenice da su osnovni principi IKE protokola standardizovani kroz RFC dokumente i predstavljaju predmet brojnih stručnih analiza, savremeno bezbednosno okruženje karakterišu nove tehnološke okolnosti koje zahtevaju ponovnu naučnu evaluaciju bezbednosnih mehanizama zaštite informaciono-komunikacionih sistema [2].

Ostvarena (*realizovana*) bezbednost *Internet Key Exchange* (IKE) protokola ne određuje se trenutkom uspešno završene razmene kriptografskih ključeva, već sposobnošću da u realnom operativnom okruženju dugoročno očuva poverenje, otpornost/rezistentnost na vektore napada i bezbednost komunikacije uprkos promenljivim tehnološkim i bezbednosnim uslovima. Iako su osnovni principi *Internet Key Exchange* (IKE) protokola normativno definisani kroz međunarodne RFC dokumente i specificirane NIST publikacije i standarde, njihova praktična primena odvija se u informaciono-komunikacionim okruženjima koja karakterišu kontinuirane tehnološke promene, povećanje kompleksnosti mrežnih infrastruktura i evolucija bezbednosnih pretnji. Posledično, procena bezbednosnih karakteristika IKE protokola ne može biti ograničena isključivo na analizu formalnog dizajna, već mora obuhvatiti i način implementacije, konfiguracije, upravljanja kriptografskim ključevima i interakcije sa drugim komponentama bezbednosne arhitekture. Savremeni informaciono-komunikacioni sistemi zahtevaju da *Internet Key Exchange* (IKE) protokol ne obezbeđuje samo bezbednu razmenu kriptografskih ključeva, već i visok nivo bezbednosne otpornosti (*rezilientnosti*, *rezistentnosti*) procesa uspostavljanja i održavanja digitalnog poverenja u uslovima promenljivog i dinamičnog bezbednosnog okruženja [51].

Razvoj informaciono-komunikacionih tehnologija, računarskih mreža, *cloud* infrastrukture, mobilnih platformi i distribuiranih informacionih sistema značajno je promenio bezbednosno okruženje u kojem se uspostavljaju i održavaju savremene digitalne komunikacije. Povećanje broja međusobno povezanih uređaja, informacionih sistema i komunikacionih sesija dovelo je do eksponencijalnog rasta broja procesa razmene kriptografskih ključeva, ali istovremeno i do povećanja broja potencijalnih bezbednosnih rizika kojima su ti procesi izloženi (*primer su državno-sponzorisani akteri, akteri u sferi subverzivne aktivnosti i industrijska špiunaža*). Posledično, bezbednost procesa razmene kriptografskih ključeva postala je jedno od najznačajnijih pitanja savremene informacione bezbednosti [23].

Savremene visokotehnološke pretnje po bezbednost informaciono-komunikacionih sistema sve ređe su usmerene isključivo na kompromitaciju kriptografskih algoritama. Naprotiv, napadači teže dugotrajnoj infiltraciji i ostvarivanju pristupa sistemu putem instalacije malicioznih softvera, koriste ranjivosti implementacije, nepravilnu konfiguraciju informaciono-komunikacionih sistema, kompromitaciju krajnjih uređaja putem funkcionalno izmenjenog *firmware*-a, zloupotrebu privilegovanih naloga, kompromitaciju infrastrukture javnih ključeva, kao i propuste u upravljanju životnim ciklusom kriptografskih ključeva [1].

Internet Key Exchange (IKE) protokol razvijen je upravo sa ciljem da obezbedi bezbedno uspostavljanje kriptografski zaštićene komunikacije kroz autentifikaciju učesnika u procesu komunikacije, pregovaranje bezbednosnih parametara, bezbednu razmenu kriptografskih ključeva i uspostavljanje sigurnosnih asocijacija u okviru IPsec arhitekture. Međutim, savremeno bezbednosno okruženje karakterišu kontinuirane tehnološke promene, razvoj novih arhitektura, povećana upotreba distribuiranih informacionih sistema i stalna evolucija visokotehnoloških pretnji i aktivnosti državno-sponzorisanih hakerskih grupa koje raspolažu znatno većim kapacitetima za napad na infrastrukturu of vitalnog značaja za nacionalnu bezbednost. Zbog toga, procena bezbednosnih karakteristika IKE protokola ne može biti ograničena isključivo na analizu normativnog dizajna IKE protokola, već je od ključnog značaja obuhvatiti i način implementacije, konfiguracije, upravljanja kriptografskim ključevima i interakcije sa drugim komponentama bezbednosne arhitekture informaciono-komunikacionog sistema. Polazeći od navedenog, predmet ovog istraživanja nije samo analiza funkcionalnih karakteristika *Internet Key Exchange* (IKE) protokola, već sveobuhvatna višekriterijumska analiza faktora koji određuju njegovu ostvarenu/realizovanu bezbednost u savremenom operativnom okruženju. Takav pristup omogućava da se IKE posmatra ne samo kao protokol za razmenu kriptografskih ključeva, već kao centralni mehanizam uspostavljanja i održavanja digitalnog poverenja između verifikovanih komunikacionih entiteta u okviru IPsec arhitekture [2].

Bezbednost *Internet Key Exchange* (IKE) protokola ne proizlazi iz uspešno realizovane razmene kriptografskih ključeva kao izolovanog događaja, već iz sposobnosti IKE protokola da tokom celokupnog životnog ciklusa komunikacije očuva verifikovani digitalni identitet komunikacionih učesnika, međusobno digitalno poverenje i bezbednosnu otpornost informaciono-komunikacionog sistema u uslovima kontinuirano promenljivog okruženja pretnji [53. RFC 2409], [54. RFC 4306].

Dosadašnja istraživanja *Internet Key Exchange* (IKE) protokola najvećim delom bila su usmerena na analizu arhitekture IKE protokola, razmene poruka, primenjenih kriptografskih algoritama i funkcionalnih karakteristika pojedinih verzija protokola. Takav pristup predstavlja neophodnu osnovu za razumevanje rada IKE protokola, ali sam po sebi nije dovoljan za sveobuhvatnu procenu bezbednosnih karakteristika u savremenom informaciono-komunikacionom okruženju [36].

Savremeno bezbednosno okruženje karakterišu kontinuirana evolucija sajber pretnji, razvoj distribuiranih informacionih sistema, primena *cloud/multicloud* infrastrukture (*cloud/multicloud infrastruktura može u cilju redudantnosti da bude u vlasništvu više kompanija koje imaju različite bezbednosne politike, takođe postoji i kontekst jurisdikcije i procedure prikupljanja po prirodi volatilnih digitalnih dokaza u slučaju bezbednosnih incidenata*), virtualizovanih okruženja i mobilnih komunikacionih platformi, kao i sve izraženija međuzavisnost informaciono-komunikacionih sistema. U takvim uslovima bezbednost procesa razmene kriptografskih ključeva ne može se posmatrati kao izolovana funkcija jednog protokola, već kao sastavni deo složenog procesa sa aspekta bezbednosti [2].

Polazeći od navedenih činjenica, predmet ovog istraživanja nije ograničen na analizu tehničkih karakteristika *Internet Key Exchange* (IKE) protokola, već obuhvata sistematsku analizu svih faktora koji utiču na njegovu bezbednost tokom celokupnog životnog ciklusa komunikacije. Posebna pažnja posvećena je međusobnim odnosima između autentifikacije digitalnog identiteta, razmene kriptografskih ključeva, upravljanja *Security Association* (SA), implementacije, konfiguracije, upravljanja kriptografskim ključevima i savremenih bezbednosnih mehanizama koji zajedno određuju nivo otpornosti procesa uspostavljanja digitalnog poverenja.

Konceptualni model prikazan na Slici 1 predstavlja metodološki okvir ovog istraživanja. Model ilustruje međusobnu povezanost digitalnog identiteta, autentifikacije, *Internet Key Exchange* (IKE) protokola, razmene kriptografskih ključeva, *Security Association* (SA), IPsec zaštite komunikacije i digitalnog poverenja, uz istovremeni prikaz faktora koji doprinose bezbednosti, faktora koji je mogu ugroziti i procesa kontinuiranog upravljanja bezbednošću. Na taj način konceptualni model ne predstavlja opis rada jednog protokola, već vizuelnu sintezu istraživačkog pristupa koji će biti razvijan kroz sva naredna poglavlja ove magistarske teze. *Internet Key Exchange* (IKE) protokol u ovom istraživanju posmatra se kao centralni mehanizam uspostavljanja i održavanja digitalnog poverenja, pri čemu stvarni nivo njegove bezbednosti proizlazi iz integrisanog dejstva kriptografskih, protokolnih, implementacionih, konfiguracionih i operativnih faktora koji zajedno određuju otpornost savremenih informaciono-komunikacionih sistema [40].

IKE bibliografija obuhvata širok spektar literature, primer su međunarodni standardi *Internet Engineering Task Force* (IETF), preporuke *National Institute of Standards and Technology* (NIST), međunarodni ISO/IEC standardi i brojna naučna istraživanja detaljno definišu arhitekturu, funkcionalne karakteristike i bezbednosne mehanizme *Internet Key Exchange* (IKE) protokola, u dostupnoj literaturi uočava se nedostatak jedinstvenog metodološkog okvira koji na integrisan način povezuje kriptografske, protokolne, implementacione, konfiguracione, operativne, identitetske i organizacione faktore u proceni bezbednosti procesa razmene kriptografskih ključeva. Upravo identifikacija i prevazilaženje tog metodološkog jaza predstavlja centralni naučni problem istraživanja u okviru ove magistarske teze. Analiza dostupne međunarodne literature pokazuje da su *Internet Key Exchange* (IKE) protokol i IPsec arhitektura detaljno normativno definisani u RFC dokumentima i predmet brojnih naučnih istraživanja. Međutim, u dostupnoj literaturi ne uočava se jedinstven metodološki okvir koji u procesu procene ostvarenog nivoa bezbednosti razmene kriptografskih ključeva na integrisan način povezuje kriptografske, protokolne, implementacione, konfiguracione, operativne, identitetske i organizacione faktore. Upravo identifikacija i prevazilaženje tog metodološkog jaza predstavlja polazište ovog istraživanja i osnov za razvoj autorskog integrisanog procesnog modela analize bezbednosnih karakteristika *Internet Key Exchange* (IKE) protokola [38].

1.1. Predmet istraživanja

Predmet istraživanja u okviru ove magistarske teze predstavlja sveobuhvatna analiza bezbednosnih karakteristika *Internet Key Exchange* (IKE) protokola kao centralnog bezbednosnog protokola IPsec arhitekture za uspostavljanje, razmenu i upravljanje kriptografskim ključevima preko Interneta. Istraživanje je usmereno na identifikaciju, analizu i višekriterijumsku evaluaciju svih faktora koji utiču na bezbednost procesa razmene kriptografskih ključeva, pri čemu se IKE protokol posmatra ne samo kao mehanizam za uspostavljanje kriptografski zaštićenog komunikacionog kanala, već i kao ključni element uspostavljanja i održavanja digitalnog poverenja između komunikacionih entiteta [2],[18],[19].

Predmet istraživanja obuhvata analizu arhitekture IPsec sistema, bezbednosnih karakteristika IKEv1 i IKEv2 protokola, mehanizama autentifikacije, razmene kriptografskih ključeva, upravljanja *Security Association* (SA), primene *Diffie–Hellman* i *Elliptic Curve Diffie–Hellman* algoritama, upravljanja životnim ciklusom kriptografskih ključeva, *Perfect Forward Secrecy* (PFS), infrastrukture javnih ključeva (PKI), kao i analizu savremenih bezbednosnih pretnji koje mogu ugroziti proces uspostavljanja bezbedne komunikacije [46].

Pored analize normativno definisanih karakteristika IKE protokola, istraživanje obuhvata i kritičku evaluaciju implementacionih, konfiguracionih i operativnih faktora koji neposredno utiču na realizovani nivo bezbednosti procesa razmene kriptografskih ključeva. Posebna pažnja posvećena je analizi međusobnih odnosa između kriptografskih mehanizama, bezbednosne arhitekture, implementacije protokola, upravljanja digitalnim identitetom, upravljanja kriptografskim ključevima i savremenih bezbednosnih mehanizama koji zajedno određuju otpornost informaciono-komunikacionih sistema na savremene sajber pretnje [11].

Normativnu osnovu istraživanja čine međunarodni standardi i preporuke koje definišu IPsec arhitekturu, *Internet Key Exchange* (IKE) protokol, upravljanje kriptografskim ključevima, digitalni identitet i savremene principe upravljanja informacionom bezbednošću. Poseban značaj imaju RFC dokumenti *Internet Engineering Task Force* (IETF), publikacije *National Institute of Standards and Technology* (NIST), međunarodni standardi ISO/IEC iz oblasti upravljanja informacionom bezbednošću, preporuke *International Telecommunication Union – Telecommunication Standardization Sector* (ITU-T), kao i smernice *European Union Agency for Cybersecurity* (ENISA), koje zajedno predstavljaju normativnu i stručnu osnovu za analizu bezbednosnih karakteristika *Internet Key Exchange* (IKE) protokola.

Jedan od ciljeva istraživanja jeste formulisanje autorskog integrisanog konceptualnog modela za analizu bezbednosnih karakteristika *Internet Key Exchange* (IKE) protokola, kojim se u jedinstven metodološki okvir analiziraju kriptografski, protokolni, implementacioni, konfiguracioni, operativni i organizacioni aspekti i kontekst koji određuju ostvareni nivo bezbednosti u procesa razmene kriptografskih ključeva (*uzimajući u obzir karakteristike okruženja informaciono-komunikacionog sistema i znanja/resursa sa kojima raspolažu akteri i hakerske grupe*). Model obuhvata analizu normativno definisanih bezbednosnih mehanizama, implementacionih i konfiguracionih izazova, upravljanja digitalnim identitetom i kriptografskim ključevima, kao i kompleksnih vektora napada, uključujući kompromitaciju krajnjih uređaja, lawful hacking metode, eksploataciju implementacionih ranjivosti, *Return-Oriented Programming* (ROP) tehnike, zloupotrebu privilegija, *insider threat* scenarije, napade na infrastrukturu javnih ključeva (PKI), kompromitaciju komunikacionih krajnjih tačaka i druge faktore koji mogu uticati na bezbednost procesa uspostavljanja i održavanja digitalnog poverenja. Cilj istraživanja nije samo identifikacija pojedinačnih ranjivosti, već razvoj integrisanog analitičkog okvira koji omogućava sistematsku procenu njihove međusobne povezanosti, uticaja na bezbednost procesa razmene kriptografskih ključeva i doprinosa ukupnoj bezbednosnoj otpornosti informaciono-komunikacionih sistema [11], [13].

Procesni pristup u ovom istraživanju predstavlja osnovni metodološki okvir za razumevanje, analizu, praćenje, upravljanje i kontinuirano unapređenje bezbednosti procesa razmene kriptografskih ključeva tokom celokupnog životnog ciklusa komunikacije. Za razliku od tradicionalnog statičkog pristupa, koji bezbednost najčešće posmatra kroz analizu pojedinačnih kriptografskih algoritama ili protokolnih mehanizama, procesni pristup omogućava sagledavanje međusobnih zavisnosti između svih faza uspostavljanja, održavanja i kriptografske zaštite komunikacije.

Pristup obuhvata kontinuirani monitoring procesa, detekciju anomalija, identifikaciju odstupanja od očekivanog ponašanja, pravovremeno otkrivanje kompromitacije bezbednosti, prepoznavanje obrazaca koji mogu ukazivati na pokušaje eksfiltracije podataka, otkrivanje dugotrajnih i prikrivenih *Advanced Persistent Threat* (APT) kampanja, analizu aktivnosti insajdera, kao i procenu otpornosti informaciono-komunikacionog sistema na savremene vektore napada.

Istovremeno, procesni pristup omogućava integraciju kriptografskih, protokolnih, implementacionih, konfiguracionih, operativnih, identitetskih i organizacionih aspekata u jedinstveni analitički okvir, čime se prevazilaze ograničenja tradicionalnih statičkih analiza *Internet Key Exchange* (IKE) protokola i stvaraju uslovi za analizu i procenu stanja bezbednosti.

1.2. Cilj istraživanja

Osnovni cilj ovog istraživanja jeste sprovođenje sistematske, sveobuhvatne i višekriterijumske analize bezbednosnih karakteristika *Internet Key Exchange* (IKE) protokola za razmenu kriptografskih ključeva preko Interneta, sa ciljem utvrđivanja faktora koji određuju stvarni nivo bezbednosti procesa uspostavljanja, održavanja i zaštite kriptografski zaštićenih komunikacija u savremenim informaciono-komunikacionim sistemima. Istraživanje je usmereno ka prevazilaženju isključivo protokolno orijentisanog pristupa i razvoju integrisanog analitičkog okvira koji bezbednost IKE protokola posmatra kao rezultat međusobnog dejstva više grupa međusobno povezanih faktora.

Polazeći od činjenice da savremene sajber pretnje sve ređe kompromituju kriptografske algoritme direktnim kriptanalitičkim napadima, a sve češće iskorišćavaju implementacione propuste, nepravilnu konfiguraciju, kompromitaciju krajnjih uređaja, zloupotrebu privilegija i operativne slabosti informaciono-komunikacionih sistema, cilj istraživanja jeste da se bezbednost *Internet Key Exchange* (IKE) protokola sagleda kroz jedinstven metodološki okvir koji prevazilazi granice tradicionalne analize komunikacionog protokola.

Jedan od ključnih ciljeva magistarske teze jeste formulisanje autorskog integrisanog konceptualnog modela za analizu bezbednosnih karakteristika *Internet Key Exchange* (IKE) protokola, kojim se u jedinstvenu metodološku celinu objedinjuju kriptografski, protokolni, implementacioni, konfiguracioni, operativni, identitetski i organizacioni faktori koji zajedno određuju stvarni nivo bezbednosti procesa razmene kriptografskih ključeva.

Takav model ne predstavlja zamenu za postojeće međunarodne standarde, već njihovu sistematsku integraciju i naučno utemeljenu interpretaciju u kontekstu savremenog bezbednosnog okruženja.

U okviru istraživanja posebna pažnja biće posvećena analizi međusobnog dejstva sledećih kategorija faktora:

- **kriptografskih i kriptanalitički aspekata**, uključujući *Diffie–Hellman* i *Elliptic Curve Diffie–Hellman* mehanizme razmene ključeva, funkcije za izvođenje ključeva (PRF i KEYMAT), *Perfect Forward Secrecy* (PFS), izbor i primenu kriptografskih algoritama i upravljanje životnim ciklusom kriptografskih ključeva,
- **protokolnih aspekata razmene kriptografskih ključeva**, koji obuhvataju arhitekturu IPsec sistema, IKEv1 i IKEv2 protokole, uspostavljanje i upravljanje *Security Association* (SA), IKEv2 *Cookie* mehanizam, *Replay Protection* i druge bezbednosne mehanizme definisane međunarodnim standardima,
- **aspekt implementacije**, uključujući analizu programskih grešaka, implementacionih ranjivosti evidentiranih u CVE bazama podataka, konfiguracionih propusta, kao i tehnika eksploatacije implementacionih slabosti, primer *Return-Oriented Programming* (ROP), *memory corruption* i drugih oblika napada usmerenih na softverske implementacije mrežnih uređaja i bezbednosnih servisa,
- **operativnih faktora**, koji obuhvataju upravljanje kriptografskim ključevima,

monitoring, evidentiranje bezbednosnih događaja (*logging*), SIEM, SOAR, NDR/XDR platforme, analizu mrežnog saobraćaja, Threat Intelligence i kontinuirano praćenje bezbednosnog stanja informaciono-komunikacionih sistema,

- **identitetskih faktora**, uključujući infrastrukturu javnih ključeva (PKI), digitalne sertifikate, upravljanje digitalnim identitetom, autentifikaciju komunikacionih entiteta i očuvanje digitalnog poverenja,
- **značaj i ulogu aktivne odbrane informaciono-komunikacionog sistema (uključujući i odbranu od državno sponzorisanih aktera)**, koji obuhvataju *lawful hacking* metode u zakonom dozvoljenim okvirima, digitalnu forenziku, detekciju kompromitovanih krajnjih uređaja, insider threat analizu, odgovor na incidente i druge mehanizme aktivne zaštite informaciono-komunikacionih sistema,
- **organizacionih faktora**, uključujući primenu *Zero Trust* principa, upravljanje informacionim rizicima, bezbednosne politike, upravljanje konfiguracijama, kontinuirano unapređenje bezbednosti i razvoj organizacione otpornosti.

Cilj istraživanja nije samo identifikacija pojedinačnih ranjivosti niti izolovana analiza pojedinačnih komponenti *Internet Key Exchange* (IKE) protokola, već razumevanje njihovih uzročno-posledičnih odnosa i međusobnog uticaja na bezbednost procesa razmene kriptografskih ključeva. Poseban akcenat stavljen je na razlikovanje ranjivosti samog protokola od ranjivosti njegove implementacije, konfiguracije i operativnog okruženja, čime se obezbeđuje metodološki preciznija i naučno utemeljenija analiza.

Konačni cilj istraživanja jeste razvoj integrisanog analitičkog pristupa koji omogućava da se bezbednosne karakteristike *Internet Key Exchange* (IKE) protokola sagledaju kao rezultat sinergijskog dejstva kriptografskih, protokolnih, implementacionih, konfiguracionih, operativnih i organizacionih faktora. Na taj način istraživanje nastoji da doprinese unapređenju metodološkog okvira za analizu bezbednosti procesa razmene kriptografskih ključeva, povezujući međunarodne standarde, savremena naučna saznanja i praktične bezbednosne izazove u jedinstvenu naučno-istraživačku celinu.

Polazeći od ovako definisanog cilja, istraživanje ne posmatra *Internet Key Exchange* (IKE) protokol kao izolovani komunikacioni mehanizam, već kao centralni element uspostavljanja, očuvanja i kontinuiranog unapređenja digitalnog poverenja, pri čemu stvarni nivo njegove bezbednosti proizlazi iz integrisanog dejstva kriptografskih, protokolnih, implementacionih, konfiguracionih, operativnih, identitetskih i organizacionih faktora koji zajedno određuju otpornost savremenih informaciono-komunikacionih sistema.

1.3. Naučni problem i hipoteze istraživanja

Savremeni informaciono-komunikacioni sistemi zasnivaju svoje funkcionisanje na bezbednoj razmeni podataka između velikog broja međusobno povezanih komunikacionih entiteta. U takvom okruženju *Internet Key Exchange* (IKE) protokol predstavlja centralni mehanizam za uspostavljanje kriptografski zaštićene komunikacije kroz autentifikaciju komunikacionih učesnika, razmenu kriptografskih ključeva i upravljanje sigurnosnim asocijacijama u okviru IPsec arhitekture. Međutim, razvoj informaciono-komunikacionih tehnologija, promena bezbednosnog okruženja i pojava novih vektora napada ukazuju da procena bezbednosti IKE protokola ne može biti zasnovana isključivo na analizi njegovih normativno definisanih karakteristika.

Osnovni naučni problem ovog istraživanja proizlazi iz potrebe da se utvrdi na koji način

međusobno dejstvo kriptografskih, protokolnih, implementacionih, konfiguracionih, operativnih, identitetskih i organizacionih faktora određuje stvarni nivo bezbednosti procesa razmene kriptografskih ključeva u savremenim informaciono-komunikacionim sistemima. U skladu sa tim, istraživanje polazi od pretpostavke da bezbednost *Internet Key Exchange* (IKE) protokola predstavlja rezultat složenog i dinamičkog sistema međusobno povezanih faktora, a ne isključivo primene snažnih kriptografskih algoritama.

Savremeni informaciono-komunikacioni sistemi zasnivaju svoju bezbednost na uspostavljanju pouzdanog digitalnog poverenja između komunikacionih entiteta. U okviru IPsec arhitekture *Internet Key Exchange* (IKE) protokol predstavlja centralni mehanizam za autentifikaciju učesnika komunikacije, razmenu kriptografskih ključeva, uspostavljanje i upravljanje *Security Association* (SA), kao i omogućavanje poverljive, integritetom zaštićene i autentifikovane komunikacije preko javnih računarskih mreža. Iako su osnovni bezbednosni mehanizmi IKE protokola normativno definisani kroz RFC dokumente *Internet Engineering Task Force* (IETF), savremeno bezbednosno okruženje ukazuje da stvarni nivo bezbednosti informaciono-komunikacionih sistema zavisi od znatno šireg spektra faktora od onih koji su definisani samim protokolom.

Naučni problem ovog istraživanja proizlazi iz činjenice da tradicionalni pristupi analizi *Internet Key Exchange* (IKE) protokola dominantno posmatraju njegove kriptografske i protokolne karakteristike, dok se implementacione, konfiguracione, operativne, identitetske i organizacione dimenzije bezbednosti često analiziraju odvojeno ili imaju sekundarni značaj. Takav pristup otežava sagledavanje međusobnih uzročno-posledičnih odnosa između različitih faktora koji zajednički određuju stvarni nivo bezbednosti procesa razmene kriptografskih ključeva.

Polazeći od navedenog problema, ovo istraživanje zasniva se na procesnom pristupu kao osnovnom metodološkom okviru za analizu bezbednosnih karakteristika *Internet Key Exchange* (IKE) protokola. Procesni pristup omogućava da se razmena kriptografskih ključeva posmatra kao dinamičan i kontinuiran životni ciklus koji obuhvata uspostavljanje komunikacije, autentifikaciju, upravljanje *Security Association* (SA), upravljanje kriptografskim ključevima, kontinuirani monitoring, detekciju anomalija, analizu bezbednosnih događaja, odgovor na incidente i kontinuirano unapređenje bezbednosti. Na taj način bezbednost IKE protokola ne posmatra se kao statička osobina jednog komunikacionog protokola, već kao rezultat međusobnog dejstva svih procesa koji učestvuju u uspostavljanju i očuvanju digitalnog poverenja.

Poseban značaj procesnog pristupa ogleda se u njegovoj sposobnosti da omogući kontinuirano praćenje životnog ciklusa bezbedne komunikacije, identifikaciju odstupanja od očekivanih obrazaca ponašanja, detekciju anomalija, rano otkrivanje pokušaja eksfiltracije podataka, identifikaciju dugotrajnih *Advanced Persistent Threat* (APT) kampanja, analizu aktivnosti insajdera, korelaciju bezbednosnih događaja i procenu ukupne otpornosti informaciono-komunikacionog sistema na savremene vektore napada. Istovremeno, procesni pristup omogućava integraciju podataka prikupljenih kroz monitoring, SIEM, SOAR, NDR/XDR platforme, Threat Intelligence izvore, digitalnu forenziku i lawful hacking aktivnosti koje se sprovode u skladu sa važećim pravnim okvirom, čime se stvara sveobuhvatnija osnova za procenu bezbednosnog stanja sistema.

Polazeći od tako definisanog naučnog problema postavljena je sledeća glavna hipoteza istraživanja u okviru ove magistarske teze:

Glavna hipoteza: Bezbednost procesa razmene kriptografskih ključeva putem *Internet Key Exchange* (IKE) protokola ne zavisi isključivo od kriptografske otpornosti primenjenih algoritama, već predstavlja rezultat integrisanog dejstva karakteristika samog protokola,

kriptografskih, implementacionih, konfiguracionih, operativnih, identitetskih i organizacionih faktora koji se mogu pouzdano analizirati primenom integrisanog procesnog pristupa.

U cilju provere glavne hipoteze definisane su sledeće pomoćne hipoteze:

- **H1.** Kriptografski mehanizmi *Internet Key Exchange* (IKE) protokola predstavljaju neophodan, ali ne i dovoljan uslov za ostvarivanje visokog nivoa bezbednosti procesa razmene kriptografskih ključeva.
- **H2.** Implementacione ranjivosti, konfiguracioni propusti i eksploatacija softverskih slabosti mogu značajno ugroziti bezbednost procesa razmene kriptografskih ključeva bez kompromitovanja samih kriptografskih algoritama.
- **H3.** Primena procesa kontinuiranog monitoringa, detekcije anomalija, logovanje pristupa resursima informaciono-komunikacionog sistema i analize bezbednosnih događaja i odgovora na incidente omogućava ranije otkrivanje kompromitacije bezbednosti u odnosu na tradicionalne statičke modele analize.
- **H4.** Integrisana primena infrastrukture javnih ključeva (PKI), upravljanja digitalnim identitetom, upravljanja kriptografskim ključevima, Security Association (SA), Perfect Forward Secrecy (PFS), Zero Trust principa i savremenih sistema za detekciju i odgovor na incidente doprinosi povećanju bezbednosne otpornosti informaciono-komunikacionih sistema.
- **H5.** Integrisani procesni pristup omogućava metodološki potpuniju i naučno utemeljeniju analizu bezbednosnih karakteristika *Internet Key Exchange* (IKE) protokola od pristupa zasnovanih isključivo na analizi pojedinačnih kriptografskih ili protokolnih mehanizama.

Provera postavljenih hipoteza biće izvršena kroz teorijsku analizu međunarodnih standarda i preporuka (*IETF RFC*, *NIST*, *ISO/IEC*, *ENISA* i *ITU-T*), kritičku analizu naučne literature, komparativnu analizu *Internet Key Exchange* verzija IKEv1 i IKEv2, analizu savremenih bezbednosnih pretnji i ranjivosti, kao i sintezu rezultata u okviru autorskog integrisanog konceptualnog i procesnog modela analize bezbednosnih karakteristika *Internet Key Exchange* (IKE) protokola.

1.4. Metodologija istraživanja

Metodologija ovog istraživanja zasniva se na interdisciplinarnom i integrisanom naučno-istraživačkom pristupu kojim se bezbednosne karakteristike *Internet Key Exchange* (IKE) protokola analiziraju kroz međusobno povezane kriptografske, protokolne, implementacione, konfiguracione, operativne, identitetske i organizacione dimenzije. Polazeći od složenosti savremenih informaciono-komunikacionih sistema i dinamične prirode sajber pretnji, istraživanje prevazilazi tradicionalni pristup usmeren isključivo na analizu pojedinačnih bezbednosnih mehanizama i zasniva se na procesnom sagledavanju celokupnog životnog ciklusa razmene kriptografskih ključeva.

Normativnu osnovu istraživanja čine međunarodni standardi i preporuke *Internet Engineering Task Force* (IETF), uključujući RFC dokumente koji definišu IPsec arhitekturu i *Internet Key Exchange* (IKE) protokol, publikacije *National Institute of Standards and Technology* (NIST) iz oblasti upravljanja kriptografskim ključevima, digitalnog identiteta i upravljanja sajber bezbednošću, međunarodni standardi ISO/IEC iz oblasti sistema upravljanja informacionom bezbednošću, preporuke International Telecommunication Union – *Telecommunication*

Standardization Sector (ITU-T), smernice *European Union Agency for Cybersecurity (ENISA)*, relevantni IEEE standardi, kao i drugi međunarodno priznati normativni i stručni izvori koji predstavljaju teorijsku i stručnu osnovu istraživanja.

U metodološkom smislu istraživanje objedinjuje više komplementarnih naučnih metoda. Primijenjena je metoda analize sadržaja međunarodnih standarda, stručne i naučne literature, komparativna metoda radi poređenja bezbednosnih karakteristika IKEv1 i IKEv2 protokola, metoda kritičke evaluacije radi identifikacije prednosti, ograničenja i bezbednosnih izazova postojećih rešenja, kao i metoda naučne sinteze kojom se rezultati pojedinačnih analiza objedinjuju u jedinstven teorijski okvir.

Posebno mesto u metodologiji zauzima procesni pristup, koji predstavlja osnovni metodološki okvir ovog istraživanja. Procesni pristup omogućava da se *Internet Key Exchange (IKE)* protokol ne posmatra kao izolovani komunikacioni mehanizam, već kao sastavni deo kontinuiranog procesa uspostavljanja, održavanja i zaštite digitalnog poverenja. Takav pristup omogućava analizu međusobnih zavisnosti između pojedinačnih faza komunikacije, kontinuirani monitoring procesa, detekciju anomalija, identifikaciju odstupanja od očekivanih obrazaca ponašanja, rano otkrivanje kompromitacije bezbednosti, analizu pokušaja ekfiltracije podataka, detektovanje dugotrajnih *Advanced Persistent Threat (APT)* kampanja, analizu aktivnosti insajdera, kao i procenu otpornosti informaciono-komunikacionih sistema na kompleksne vektore napada i izuzetno složen bezbednosni izazov sa aspekta zaštite nacionalne bezbednosti jer su akteri najčešće državno-sponzorisanе hakerske grupe(koji uključuju ROP (Return-Oriented Programming) i BYOVD (Bring Your Own Vulnerable Driver)).

Metode kompromitacije koje imaju karakteristiku efikasnog ostvarivanja neovlašćenog pristupa često ne napadaju kriptografske algoritme poput *Internet Key Exchange (IKE)* protokola, već zaobilaze njihovu zaštitu kompromitacijom krajnjih uređaja, implementacije ili operativnog okruženja, čime se omogućava pristup podacima pre njihovog šifrovanja ili nakon njihovog dešifrovanja. Savremeno bezbednosno okruženje karakteriše razvoj metoda koje ne nastoje da kompromituju kriptografske algoritme niti da izvrše kriptanalizu *Internet Key Exchange (IKE)* ili *IPsec* protokola. Umesto toga, napadači sve češće primenjuju tehnike kojima se zaobilazi kriptografska zaštita kompromitacijom krajnjih uređaja, eksploatacijom implementacionih ranjivosti, zloupotrebom privilegije pristupa (*kredencijala lica koja su zaposlena i čiji podaci za logovanje su u posedu napadača*) ili kompromitacijom operativnog okruženja. Takav pristup omogućava pristup podacima u njihovom izvornom obliku (engl. *plaintext*), odnosno pre procesa šifrovanja ili nakon procesa dešifrovanja, čime se zaobilaze bezbednosni mehanizmi zasnovani na kriptografskoj zaštiti komunikacionog kanala. Upravo zbog toga savremena analiza bezbednosnih karakteristika *Internet Key Exchange (IKE)* protokola mora, pored kriptografskih i protokolnih aspekata, obuhvatiti i implementacione, operativne i organizacione faktore koji određuju ukupnu otpornost informaciono-komunikacionog sistema.

Primeri su :

- ROP (Return-Oriented Programming), jeste tehnika eksploatacije memorijskih ranjivosti.
- BYOVD (Bring Your Own Vulnerable Driver), jeste tehnika kojom se zloupotrebljava ranjiv ili legitimno potpisan drajver u cilju eskalacije privilegija ili zaobilaznja bezbednosnih mehanizama.

Oba primera zaobilaze kriptografsku zaštitu, primenjuju se legalno (uz nalog suda), u okviru softvera za LAWFUL HACKING , uglavnom je softver izraelske proizvodnje jer imaju

najbolje stručnjake, većim delom bivše pripadnike obaveštajne strukture specijalizovane za visokotehnološki aspekt obaveštajno/kontraobaveštajnog delovanja) ali su korišćeni i od strane hakera sa visokospecijalizovanim poznavanjem ofanzivne bezbednosti.

Metodologija istraživanja obuhvata i analizu implementacionih, konfiguracionih i operativnih aspekata bezbednosti, uključujući razmatranje implementacionih ranjivosti evidentiranih u CVE bazama podataka, konfiguracionih propusta, eksploatacije softverskih slabosti, kompromitacije krajnjih uređaja, kao i savremenih lawful hacking metoda koje u zakonom dozvoljenim okvirima omogućavaju pristup zaštićenim komunikacijama kompromitacijom implementacije ili komunikacionih krajnjih tačaka, a ne kriptanalizom samog *Internet Key Exchange* (IKE) protokola.

Konačna faza istraživanja zasniva se na integraciji rezultata dobijenih primenom navedenih metoda u autorski konceptualni, procesni i analitički model analize bezbednosnih karakteristika *Internet Key Exchange* (IKE) protokola. Time se omogućava sistematsko povezivanje teorijskih saznanja, međunarodnih standarda, primera najbolje prakse i savremenih bezbednosnih praksi prema tipu aktera i karakteristikama vektora napada i praktičnih bezbednosnih izazova u jedinstven metodološki okvir, čime se obezbeđuje sveobuhvatnija procena stvarnog nivoa bezbednosti procesa razmene kriptografskih ključeva u savremenim informaciono-komunikacionim sistemima.

Metodologija primenjena u ovom istraživanju zasniva se na pretpostavci da se stvarna bezbednost procesa razmene kriptografskih ključeva može pouzdano proceniti samo integrisanom primenom normativne, teorijske, komparativne, procesne i analitičke metode, pri čemu procesni pristup predstavlja centralni metodološki okvir koji objedinjuje sve faze istraživanja u jedinstvenu naučno-istraživačku celinu. Polazeći od definisanog naučnog problema, postavljenih ciljeva i hipoteza, kao i primenjene metodologije istraživanja, ova magistarska teza nastoji da pruži sistematsku i naučno utemeljenu analizu bezbednosnih karakteristika *Internet Key Exchange* (IKE) protokola. Kroz integraciju međunarodnih standarda, savremenih bezbednosnih praksi, procesa upravljanja kriptografskim ključevima i autorskog procesnog modela analize, istraživanje nastoji da doprinese unapređenju metodološkog okvira za procenu bezbednosti procesa razmene kriptografskih ključeva u savremenim informaciono-komunikacionim sistemima.

1.5. Struktura magistarskog rada

U cilju preglednosti i lakšeg praćenja naučno-istraživačkog toka, magistarski rad je organizovana u šest tematski povezanih poglavlja, čiji redosled odražava logičku progresiju od teorijsko-analitičkih osnova, preko analize arhitekture protokola i bezbednosnih mehanizama IKE protokola, do sistematizacije savremenih bezbednosnih izazova *Internet Key Exchange* (IKE) protokola. Svako naredno poglavlje nadograđuje se na nalaze prethodnog, čime se ostvaruje dosledna primena procesnog pristupa u okviru metodologije istraživanja.

Drugo poglavlje, naslovljeno „Teorijsko-analitička osnova kriptografske razmene ključeva“, uspostavlja fundamentalnu teorijsku podlogu neophodnu za razumevanje bezbednosnih mehanizama analiziranih u narednim poglavljima. Poglavlje obuhvata istorijski razvoj razmene kriptografskih ključeva i nastanak kriptografije sa javnim ključem, detaljnu matematičku i bezbednosnu analizu Diffie–Hellman algoritma, uključujući izbor kriptografskih grupa kao determinante bezbednosnih karakteristika IKEv1 i IKEv2 protokola, funkcije za izvođenje kriptografskog materijala (PRF, SKEYSEED, KEYMAT), značaj

entropije i nonce vrednosti, kao i koncept Perfect Forward Secrecy i upravljanje životnim ciklusom kriptografskih ključeva. Ovo poglavlje predstavlja neophodan teorijsko-analički preduslov za sva naredna poglavlja, budući da se IKE protokol ne može razumeti izolovano od matematičkih i kriptografskih principa na kojima počiva [2].

Treće poglavlje, „Arhitektura IPsec protokola kao osnova za uspostavljanje digitalnog poverenja i funkcionisanje *Internet Key Exchange* (IKE) protokola", prelazi sa čisto kriptografskog na nivo analize arhitekture protokola. Poglavlje sistematizuje IPsec arhitekturu kao procesno organizovanu bezbednosnu celinu i detaljno analizira njene sastavne komponente — *Security Policy Database* (SPD) kao polaznu tačku procesa uspostavljanja digitalnog poverenja, *Internet Key Exchange* kao centralni procesni mehanizam, *Security Association* (SA) kao operativnu realizaciju digitalnog poverenja, *Security Association Database* (SAD) kao mehanizam upravljanja aktivnim stanjem poverenja, te *Authentication Header* (AH) i *Encapsulating Security Payload* (ESP) kao mehanizme očuvanja integriteta i zaštite podataka. Ovim poglavljem uspostavlja se procesni okvir unutar kojeg se, u narednim poglavljima, analiziraju konkretne verzije IKE protokola.

Četvrto poglavlje sprovodi sveobuhvatnu procesnu analizu bezbednosnih karakteristika *Internet Key Exchange Version 1* (IKEv1) protokola kroz analizu faza, modova i mehanizama upravljanja bezbednosnim asocijacijama. Analiza obuhvata Fazu 1 protokola i uspostavljanje *IKE Security Association*, detaljno poređenje *Main Mode* i *Aggressive Mode* režima razmene poruka, metode autentifikacije (*Pre-Shared Key*, digitalni sertifikati i infrastrukturu javnih ključeva), Fazu 2 i *Quick Mode* mehanizam, kriptografske algoritme primenjene u IKEv1 protokolu, upravljanje životnim ciklusom *Security Association* i *rekeying* mehanizme, savremene napredne persistentne pretnje (APT) relevantne za IKEv1 infrastrukturu, kao i savremeni značaj analize IKEv1 protokola u uslovima postepene migracije ka IKEv2. Poglavlje služi kao komparativna osnova za analizu IKEv2 protokola sprovedenu u narednom poglavlju.

Peto poglavlje, „Razvoj IKEv2 protokola kroz procesnu analizu arhitekture, bezbednosnih mehanizama i evolucije u odnosu na IKEv1 protokol", predstavlja direktan nastavak i produbljenje analitičkog okvira uspostavljenog u prethodnom poglavlju. Poglavlje razmatra istorijski razvoj i projektantska unapređenja implementirana u IKEv2 protokolu, arhitekturu i funkcionalni model protokola sa posebnim osvrtom na hijerarhijski odnos *IKE_SA* i *CHILD_SA* bezbednosnih asocijacija, proces uspostavljanja *IKE_SA*, mehanizme upravljanja *CHILD_SA* asocijacijama i *rekeying* procese, integrisanu arhitekturu bezbednosnih mehanizama (autentifikacija, tajnost, integritet), napredne funkcionalnosti (mobilnost, interoperabilnost), teorijski model bezbednosnih ranjivosti i pregled dokumentovanih implementacionih propusta, kao i komparativnu analizu bezbednosne arhitekture IKEv1 i IKEv2 protokola. Poglavlje se zaokružuje kritičkom evaluacijom IKEv2 protokola u savremenim VPN sistemima i naučno-istraživačkom sintezom.

Šesto poglavlje, posvećeno savremenim bezbednosnim izazovima IKE protokola, predstavlja sintezu i praktičnu nadogradnju teorijsko-protokolarne analize sprovedene u prethodnim poglavljima. Poglavlje obuhvata sistematsku analizu poznatih CVE ranjivosti u kontekstu IPsec, IKEv1 i IKEv2 implementacija, naučno-istraživačku klasifikaciju tih ranjivosti i analizu uzročno-posledičnih veza, metodološki okvir za izbor reprezentativnih slučajeva, analizu ROP (*Return-Oriented Programming*) i BYOVD (*Bring Your Own Vulnerable Driver*) tehnika eksploatacije dokumentovanih na konkretnim hardverskim uređajima, kao i analizu odnosa postkvantne kriptografije prema memorijsko-izvršnom riziku savremenih

IKE/IPsec implementacija. Ovo poglavlje predstavlja empirijsko težište magistarskog rada, u kojem se teorijski i naučno-istraživački nalazi iz primene IKE protokola (*u okviru prethodnih poglavlja*) sučeljavaju sa dokumentovanim, stvarnim bezbednosnim incidentima.

Magistarski rad u zaključku, sintezi sprovedenog istraživanja, u kojoj se sumiraju ključni nalazi svakog poglavlja, proverava stepen potvrđenosti postavljene glavne i pomoćnih hipoteza definisanih u odeljku 1.3, i formuliše zaključna razmatranja o naučnom doprinosu istraživanja, njegovim ograničenjima i pravcima budućih istraživanja u oblasti bezbednosti protokola za razmenu kriptografskih ključeva. Na ovaj način, struktura magistarskog rada u celini odražava dosledan prelazak od opšte teorijske osnove, preko analize arhitekture IPsec i IKE protokola i analize konkretnih verzija IKE protokola (uključujući i analize softverskih implementacija IKE protokola), do sinteze savremenih bezbednosnih izazova i konačnih naučnih zaključaka, čime se ostvaruje sistematičan i metodološki utemeljen odgovor na naučni problem i hipoteze istraživanja formulisane u ovom uvodnom poglavlju.

2. Teorijsko-analička osnova kriptografske razmene ključeva

2.1. Istorijski razvoj razmene kriptografskih ključeva

Razvoj savremenih informaciono-komunikacionih sistema je povezan sa razvojem kriptografije kao naučne discipline čiji je osnovni cilj zaštita tajnosti, integriteta, autentičnosti i raspoloživosti informacija tokom njihove obrade, skladištenja i prenosa podataka. Međutim, istorijski razvoj kriptografije pokazuje da bezbednost komunikacije nikada nije zavisila isključivo od otpornosti na kriptanalitičke napade u slučaju primenjenih kriptografskih algoritama, već pre svega od mogućnosti bezbedne razmene kriptografskih ključeva između komunikacionih učesnika. Upravo zbog toga problem razmene ključeva predstavlja jedno od centralnih pitanja razvoja savremene primenjene kriptografije i osnovni preduslov za nastanak protokola kao što je *Internet Key Exchange* (IKE). U najranijim fazama razvoja kriptografije zaštita informacija zasnivala se gotovo isključivo na simetričnim kriptografskim sistemima. Kod ovakvih sistema isti tajni ključ koristi se i za šifrovanje i za dešifrovanje podataka. Ograničenja simetrične kriptografije i problem bezbedne distribucije kriptografskih ključeva su bili ključni pokretači razvoja moderne kriptologije kao nauke [34].

Analiza razvoja kriptografskih sistema pokazuje da su prvi modeli zaštite informacija gotovo isključivo bili zasnovani na primeni simetrične kriptografije, pri čemu se isti tajni ključ koristio za šifrovanje i dešifrovanje podataka. Ovakav pristup predstavljao je logično rešenje u periodu kada su komunikacioni sistemi bili ograničeni na mali broj učesnika i unapred uspostavljene odnose poverenja između korisnika takvih sistema tajne komunikacije. U takvim uslovima razmena zajedničkog tajnog ključa mogla se realizovati neposrednim kontaktom ili korišćenjem fizički zaštićenih kanala komunikacije, zbog čega pitanje distribucije ključeva nije predstavljalo dominantan bezbednosni problem za razliku od savremenih informacionih sistema i činjenice da informacione tehnologije predstavljaju izuzetno važan element od višestrukog značaja za nacionalnu bezbednost (*bezbednosne službe, sistemi odbrane, kontrola granica i međunarodna policijska saradnja, komunikacija i koordinacija službi bezbednosti na nacionalnom nivou jer službe odlikuje raspolaganje različitim kapacitetima delovanja u incidentnim situacijama itd*) [20].

Međutim, ubrzani razvoj računarskih mreža i transformacija lokalnih komunikacionih sistema u globalno povezane informaciono-komunikacione infrastrukture suštinski su promenili bezbednosni kontekst primene simetrične kriptografije. Povećanjem broja korisnika, geografskom disperzijom komunikacionih učesnika i korišćenjem Interneta za prenos podataka, tradicionalni model zasnovan na prethodno razmenjenom zajedničkom tajnom ključu postao je sve teže održiv. Problem zaštite komunikacije više nije bio ograničen na otpornost primenjenog algoritma, već se premestio na pitanje bezbednog uspostavljanja zajedničkog kriptografskog poverenja između komunikacionih strana koje se međusobno ne poznaju i koje komuniciraju preko potencijalno kompromitovanog komunikacionog kanala [31].

Tabela 1. Procesni pristup detekciji napada

Faza procesa	Cilj	Izvori telemetrije	Analitičke aktivnosti	Rezultat
1. Prikupljanje informacija o incidentu	Prikupiti relevantne bezbednosne događaje.	VPN logovi, sistemski logovi, mrežni uređaji, EDR.	Centralizacija i vremenska sinhronizacija zapisa i analiza karakteristika digitalnih dokaza u cilju obezbeđivanja digitalnih dolaza (volatilnost i problem jurisdikcije)	Konzistentan skup podataka.
2. Korelacija	Povezati događaje iz više izvora, utvrditi rokove za obezbeđenje digitalnih dokaza u cilju rekonstrukcije bezbednosnog incidenta.	SIEM, NDR, EDR, identitetski sistemi.	Korelacija prema više kriterijuma (prema vremenu nastanka, korisniku i uređaju).	Identifikovan i obrasci ponašanja. (otkrivanje insajdera koji pristupaju resursima IKT sistema za koji nemaju pravo pristupa)
3. Detekcija anomalija	Uočiti odstupanja od uobičajenog rada IKT sistema.	Telemetrija sistema i mreže.	Pravila, statistička analiza i modeli detekcije.	Generisanje upozorenja.
4. Procena rizika	Odrediti značaj identifikovanog događaja.	Rezultati korelacije i kontekst sistema.	Klasifikacija prema uticaju i verovatnoći.	Prioritet za obradu.
5. Odgovor na incident	Smanjiti uticaj događaja.	SOC, SIEM, SOAR, administrativne procedure.	Izolacija, analiza i sanacija.	Ograničen uticaj incidenta.
6. Kontinuirano unapređenje	Unapređenje procesa detekcije bezbednosnih incidenata.	Rezultati analiza i naučene lekcije.	Ažuriranje pravila, procedura i konfiguracija.	Veća otpornost sistema.

Napomena: Tabela prikazuje procesni model detekcije napada sa naglaskom na prikupljanje telemetrije, korelaciju događaja, analizu anomalija, procenu rizika i kontinuirano unapređenje bezbednosnih kontrola u IPsec/IKE okruženju.

Izvor: Autor, na osnovu autorskog procesnog modela razvijenog u okviru ovog istraživanja, uz oslanjanje na NIST SP 800-61 Rev. 2 (Computer Security Incident Handling Guide) i NIST SP 800-137 (Information Security Continuous Monitoring)

Podaci u tabeli 1. ukazuju da šestofazni procesni model detekcije napada, koji operacionalizuje procesni pristup primenjen kroz čitavo ovo istraživanje na konkretan, ciklično strukturiran tok bezbednosnog monitoringa IPsec/IKE okruženja. Model počinje prikupljanjem bezbednosnih događaja iz heterogenih izvora telemetrije (*VPN i sistemski logovi, mrežni uređaji, EDR*), nakon čega sledi korelacija tih događaja kroz SIEM, NDR i identitetske sisteme radi povezivanja naizgled izolovanih zapisa u prepoznatljive obrasce ponašanja. Ova dva inicijalna koraka predstavljaju neophodan preduslov za sve naredne faze, budući da kvalitet i konzistentnost prikupljenih podataka direktno određuje pouzdanost kasnije detekcije anomalija i procene rizika.

Sa aspekta operativnog toka, tabela 1 ukazuje da se proces ne završava generisanjem upozorenja u fazi detekcije anomalija, već se nastavlja kroz procenu rizika, koja klasifikuje identifikovani događaj prema uticaju i verovatnoći, i odgovor na incident, koji putem SOC, SIEM i SOAR platformi ograničava posledice kompromitacije. Poslednja faza, kontinuirano unapređenje, zatvara ciklus tako što naučene lekcije iz prethodnih incidenata transformiše u ažurirana pravila, procedure i konfiguracije, čime se povećava otpornost sistema na buduće, slične obrasce napada. Ova cikličnost potvrđuje centralnu metodološku tezu ovog istraživanja — da bezbednost IPsec/IKE infrastrukture ne predstavlja statičko stanje koje se jednom uspostavlja, već kontinuiran proces čije faze uzajamno zavise jedna od druge i zajedno formiraju zatvorenu petlju unapređenja bezbednosne otpornosti [3],[11].

Tabela 2. Nivoi pristupa operativnom sistemu

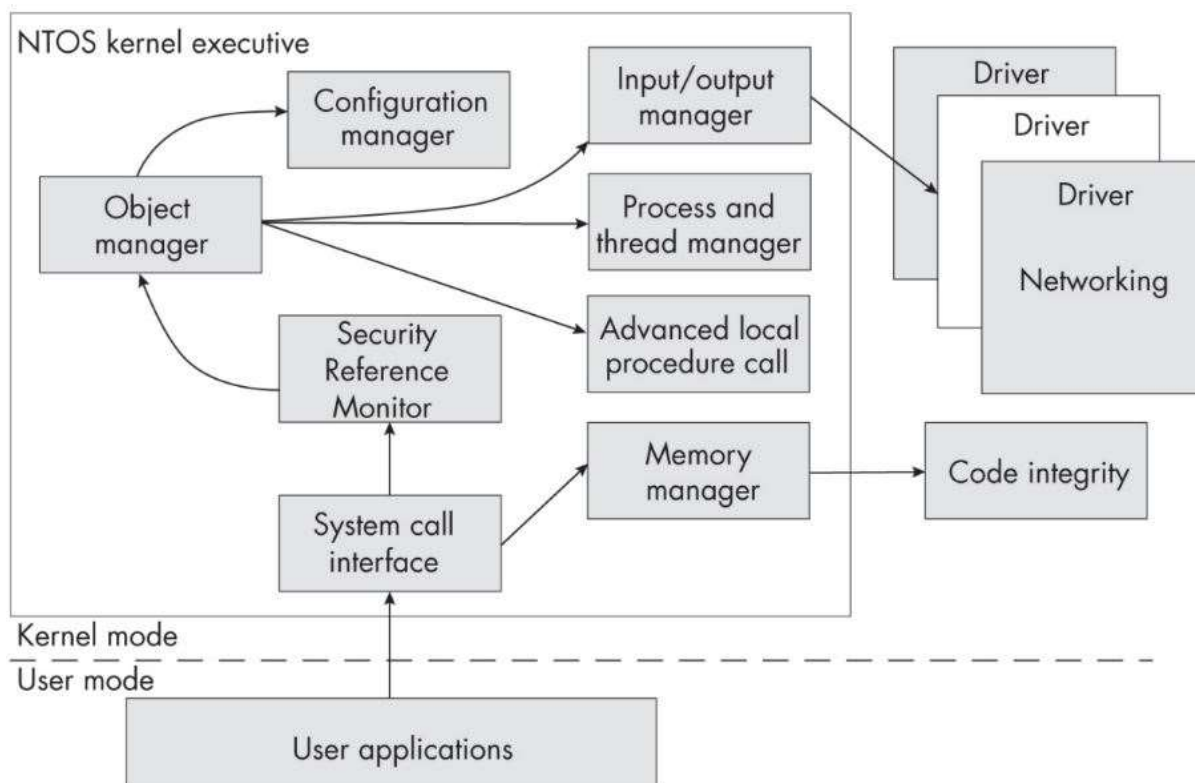
Nivo	Karakteristike	Primeri komponenti	Bezbednosni značaj / kontrole
Korisnički režim (User Mode)	Izvršavanje aplikacija sa ograničenim privilegijama.	VPN klijent, pregledač, poslovne aplikacije.	Kompromitacija utiče na procese i podatke korisnika. Kontrola pristupa je neophodna mera zaštite IKT sistema (logovanje pristupa), EDR, ažuriranja aplikacija.
Kernel režim (Kernel Mode)	Najviši nivo privilegija operativnog sistema.	Kernel, sistemski drajveri, upravljački moduli.	Greške ili kompromitacija mogu uticati na ceo infomaciono-komunikacioni sistem. Integritet kernela, kontrola drajvera, zaštita memorije predstavljaju neke od mera zaštite IKT sistema.
Hipervizor	Upravlja virtuelnim mašinama i izolacijom resursa.	Hyper-V, VMware ESXi, KVM.	Kompromitacija može uticati na više virtuelnih sistema. Sigurna konfiguracija, kontrola pristupa, ažuriranja (<i>security update</i>).
Firmware / UEFI	Softver koji inicijalizuje hardver pre pokretanja sistema.	UEFI, BIOS, firmware uređaja.	Može uticati na kompromitaciju stanja bezbednosti pri pokretanju sistema. Secure Boot, verifikacija integriteta firmware-a.
Hardver	Fizička osnova računarskog sistema.	CPU, TPM, memorija, mrežni adapteri itd.	Predstavlja osnovu bezbednosnog lanca poverenja. TPM, fizička zaštita, bezbedno upravljanje uređajima. (neophodno je proveriti da li se kriptografski ključevi nalaze na back-up kopijama podataka i kako su definisane procedure u okviru bezbednosnih politika)

Napomena: Tabela prikazuje hijerarhiju nivoa pristupa operativnom sistemu i njihov značaj za zaštitu IPsec/IKE okruženja. Viši nivoi privilegija zahtevaju strože bezbednosne kontrole zbog potencijalno većeg uticaja na celokupan sistem.

Izvor: Autor, na osnovu opšteprihvaćenih principa bezbednosnog inženjerstva (koncept lanca poverenja – Chain of Trust, Trusted Computing Group – TPM specifikacije) i NIST SP 800-147 (BIOS Protection Guidelines)

Podaci u prikazanoj tabeli 2 prikazuju hijerarhiju privilegija u savremenim informaciono-komunikacionim sistemima, počevši od korisničkog režima (*User Mode*), preko kernel režima i hipervizora, do firmware/UEFI sloja i, na najnižem nivou, hardverske osnove sistema. Ova struktura direktno objašnjava zašto tehnike poput BYOVD, predstavljaju ozbiljnu pretnju po bezbednost informaciono-komunikacionog sistema (omogućava napadaču da ostvari pristup kernel-u operativnog sistema), vektor napada zaobilazi mere zaštite i bezbednosne mehanizme.

Na slici 1 prikazan je Windows kernel executive koji predstavlja centralni deo operativnog sistema koji se izvršava u privilegovanom, kernel modu, i čija je osnovna funkcija posredovanje između korisničkih aplikacija i hardverskih resursa sistema. Arhitektura ovog sloja zasniva se na skupu međusobno povezanih komponenti, od kojih Object manager ima centralnu ulogu u upravljanju *kernel* objektima i koordinaciji sa ostalim modulima, uključujući *Configuration manager*, *Input/output manager*, Process and thread manager i Advanced local procedure call (ALPC) interfejs. Bezbednosnu kontrolu pristupa sistemskim resursima obezbeđuje Security Reference Monitor, dok Code integrity komponenta, povezana sa Memory managerom, vrši verifikaciju digitalnih potpisa modula i drajvera pre njihovog učitavanja u kernel prostor. Komunikacija između korisničkog i kernel moda odvija se isključivo preko System call interface-a, čime se uspostavlja jasna i kontrolisana granica privilegija između ove dve celine sistema. Upravo ova arhitektonska karakteristika koncentracija kritičnih bezbednosnih funkcija unutar ograničenog broja kernel komponenti čini polaznu tačku za razumevanje mehanizma BYOVD (*Bring Your Own Vulnerable Driver*) napada, budući da učitavanje legitimno potpisanog, ali ranjivog drajvera omogućava napadaču da zaobiđe proveru sprovedenu od strane *Code integrity* komponente i ostvari izvršavanje proizvoljnog koda sa privilegijama kernela. U cilju razumevanja arhitekture na kojoj počivaju BYOVD tehnike eksploatacije, neophodno je sagledati unutrašnju strukturu Windows kernel executive-a i način na koji njegove komponente međusobno komuniciraju. U tu svrhu, u nastavku je prikazan model arhitekture Windows kernela, preuzet i prilagođen prema Forshaw-u (2024). Poznavanje osnovnih komponenti Windows kernel executive-a uključujući Object manager, Security Reference Monitor i Memory manager predstavlja preduslov za razumevanje mehanizama putem kojih se izvršavaju napadi na informaciono-komunikacione sisteme putem instalacije ranjivih (i digitalno potpisanih) drajvera i na taj način se realizuje privilegovan pristup sistemu.



Slika 1. Prikaz komponenti Windows NTOS kernel executive-a i njihove interakcije sa korisničkim i kernel modom

Izvor: Preuzeto i prilagođeno iz: Forshaw, 2024

Model ilustruje jasnu podjelu između korisničkog i kernel moda, pri čemu se pristup svim kritičnim resursima sistema: procesima, memoriji, uređajima i mrežnim komponentama ostvaruje isključivo kroz kontrolisane interfejs NTOS kernel executive-a. Ova činjenica objašnjava zašto kompromitacija bilo koje komponente unutar kernel moda, uključujući i putem ranjivog drajvera, ima kritične bezbednosne posledice po ceo sistem. Prikazana arhitektura ukazuje na to da svi zahtevi korisničkih aplikacija prolaze kroz System call interface pre nego što dospeju do ključnih komponenti kernel moda (Object managera, Security Reference Monitora i Memory managera) koje zajednički kontrolišu pristup sistemskim resursima. Ovakva centralizovana arhitektura znači da drajver koji uspe da ostvari izvršavanje koda u kernel modu, zaobilazeći redovan put kroz System call interface i Security Reference Monitor i na taj način stiče praktično neograničen pristup sistemu, što predstavlja osnovu za BYOVD tehnike eksploatacije analizirane u nastavku rada.

Sa aspekta zaštite IPsec/IKE komponenti, tabela ukazuje da bezbednost ovih protokola, bez obzira na njihovu kriptografsku ispravnost, u krajnjoj liniji zavisi od integriteta čitavog lanca poverenja koji počinje na nivou hardvera (CPU, TPM) i firmware-a (UEFI, Secure Boot), a završava se na nivou korisničkog procesa u kome se IKE/IPsec komunikacija stvarno izvršava. Ukoliko je bilo koji niži nivo ovog lanca kompromitovan, na primer, putem manipulacije firmware-om ili zloupotrebe ranjivog drajvera na kernel nivou, kriptografska zaštita uspostavljena na višem, aplikativnom nivou postaje irelevantna, jer napadač stiče mogućnost pristupa podacima nezavisno od primenjenih algoritama. Ova zavisnost potvrđuje da sveobuhvatna bezbednosna procena IKE/IPsec infrastrukture mora obuhvatiti čitavu vertikalnu privilegiju, od hardverskog korena poverenja do aplikativnog sloja, umesto da se ograniči isključivo na analizu protokolarnih i kriptografskih mehanizama.

Ovakva promena bezbednosne paradigme predstavlja jednu od najznačajnijih prekretnica u istoriji primenjene kriptografije. Matematička otpornost simetričnih algoritama na kriptanalizu može biti izuzetno visoka, ali je ukupna bezbednost sistema i dalje zavisi od načina na koji je zajednički ključ distribuiran. Drugim rečima, bezbednost komunikacionog sistema determinisana je njegovom najslabijom komponentom. Ukoliko bi proces distribucije ključa bio kompromitovan, bezbednost celokupnog sistema bila bi narušena bez obzira na kvalitet primenjenog algoritma za šifrovanje. Time se potvrđuje jedno od osnovnih načela savremene informacione bezbednosti, prema kojem ukupna otpornost sistema na vektore napada ne zavisi isključivo od pojedinačnih bezbednosnih mehanizama, već od njihove međusobne povezanosti i pouzdanosti celokupnog bezbednosnog procesa, implementacije mera zaštite, detekcije bezbednosnih incidenata i kompromitacije kriptografskih ključeva[45].

Poseban izazov predstavljao je problem skalabilnosti sistema zasnovanih na simetričnoj kriptografiji. U okruženju sa malim brojem korisnika upravljanje kriptografskim ključevima bilo je relativno jednostavno. Međutim, u slučajevima kada je broj učesnika u komunikaciji veći distribucija kriptografskih ključeva predstavlja izuzetno složen proces, dolazi do eksponencijalnog povećanja broja potrebnih tajnih kriptografskih ključeva. Takva arhitektura značajno komplikuje administraciju sistema, povećava mogućnost ljudske greške, otežava pravovremenu zamenu kriptografskih ključeva i povećava verovatnoću kompromitacije poverljivih informacija. Posledično, problem upravljanja kriptografskim ključevima prerasta iz tehničkog pitanja u strateški bezbednosni izazov koji zahteva razvoj potpuno novih metodoloških i tehničko-tehnoloških rešenja [47].

Navedeni problemi posebno dolaze do izražaja u savremenim informaciono-komunikacionim sistemima koji karakterišu visok stepen decentralizacije, *(infrastruktura je raspoređena u više jurisdikcija i izložena vektorima napada u kompleksnom geopolitičkom i geostrateški specifičnom okruženju gde akteri imaju agendu koju nastoje realizovati, reprezentativan slučaj za takvu vrstu aktivnosti je Harvest now, decrypt later (HNDL))*, zatim dinamičko uspostavljanje komunikacionih sesija i veliki broj heterogenih uređaja koji međusobno razmenjuju podatke preko Interneta.

U takvom okruženju praktično je nemoguće unapred distribuirati zajedničke tajne ključeve svim potencijalnim komunikacionim partnerima, niti je moguće dugoročno održavati tajnost kriptografskih ključeva bez odgovarajućih mehanizama za automatizovano upravljanje životnim ciklusom kriptografskim materijalom. Ova činjenica jasno pokazuje da problem razmene kriptografskih ključeva nije bio rezultat slabosti algoritama u domenu simetrične kriptografije kao matematičkog koncepta, već posledica promenjenih funkcionalnih i bezbednosnih zahteva koje je nametnuo razvoj globalnih računarskih mreža [50].

Tabela 3. Status kriptografskih algoritama prema RFC preporukama

Algoritam	Namena	Status prema RFC preporukama	Napomena
DES	Šifrovanje	Zastareo / ne preporučuje se	Nedovoljna dužina ključa
3DES	Šifrovanje	Ograničena upotreba	Postepeno se napušta
AES-CBC	Šifrovanje	Dozvoljen	Široko podržan
AES-GCM	AEAD (šifrovanje + integritet)	Preporučen	Visoke performanse i savremena preporuka
ChaCha20-Poly1305	AEAD	Preporučen	Pogodan za uređaje bez AES akceleracije
HMAC-SHA-1	Integritet / autentifikacija	Ograničena upotreba	Zamenjuje se jačim SHA-2 varijantama
HMAC-SHA-256	Integritet / PRF	Preporučen	Najčešći izbor
HMAC-SHA-384	Integritet / PRF	Preporučen	Viši nivo bezbednosti
HMAC-SHA-512	Integritet / PRF	Preporučen	Pogodan za visoke bezbednosne zahteve

Napomena: Status algoritama predstavlja sintezu preporuka iz relevantnih RFC dokumenata za IPsec/IKE (uključujući RFC 8247, RFC 8221 i povezana ažuriranja). Pri izboru algoritama uvek treba primenjivati najnovije važeće RFC preporuke.

Izvor: Autor, na osnovu sinteze relevantnih RFC i NIST/FIPS dokumenata (RFC 8247, RFC 8221, RFC 4106, FIPS 197, FIPS 180-4, FIPS 198-1).

Tabela 3 sistematizuje status devet kriptografskih algoritama korišćenih u IPsec/IKE arhitekturi prema aktuelnim RFC preporukama, razvrstanih u tri funkcionalne kategorije — algoritme za šifrovanje, AEAD (*Authenticated Encryption with Associated Data*) mehanizme i algoritme za proveru integriteta i izvođenje ključeva (PRF). Podaci jasno ukazuju na jasnu evolucijsku putanju: DES se smatra zastarelim usled nedovoljne dužine ključa, dok se 3DES, kao njegov prelazni naslednik, postepeno napušta iz upotrebe. Sličan obrazac uočava se i kod HMAC-SHA-1 algoritma, čija se upotreba ograničava u korist savremenijih SHA-2 varijanti (HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512), koje RFC preporuke tretiraju kao preporučene bez izuzetka.

Sa aspekta savremene primene, tabela 3 ističe AES-GCM i ChaCha20-Poly1305 kao preporučene AEAD algoritme, koji objedinjavanjem funkcija šifrovanja i provere integriteta u jednoj kriptografskoj operaciji predstavljaju efikasniju i bezbedniju alternativu tradicionalnom pristupu odvojene primene šifre i HMAC mehanizma. Značajno je istaći da ChaCha20-Poly1305 predstavlja posebno pogodno rešenje za uređaje bez hardverske AES akceleracije, čime se otvara prostor za fleksibilan izbor algoritma prema karakteristikama konkretne implementacione platforme. Ova dinamika potvrđuje da izbor kriptografskih algoritama u IPsec/IKE sistemima ne predstavlja jednokratnu odluku, već zahteva kontinuirano usklađivanje sa najnovijim RFC preporukama, s obzirom na to da se status pojedinačnih algoritama menja usled napretka kriptanalize i razvoja računarskih kapaciteta.

Iz navedenih razloga naučna zajednica postepeno menja istraživački fokus. Umesto razvoja sve složenijih algoritama za šifrovanje, pažnja se usmerava na rešavanje problema uspostavljanja bezbednog kriptografskog poverenja između komunikacionih učesnika. Time proces razmene ključeva postaje centralni predmet istraživanja, dok upravljanje kriptografskim ključevima prerasta u jednu od najvažnijih komponenti ukupne bezbednosti

informaciono-komunikacionog sistema. Ovakva promena istraživačke paradigme predstavlja osnov za nastanak moderne kriptografije sa javnim ključem i razvoj prvih protokola koji omogućavaju uspostavljanje zajedničke tajne preko komunikacionog kanala koji se unapred ne smatra bezbednim (*usled prisutnosti aktera državnog i subdržavnog nivoa i u zavisnosti od kapaciteta kojima akteri raspolažu u cilju kompromitacije bezbednosti informaciono-komunikacionog sistema koji je meta vektora napada*) [5], [52; RFC 2408.], [53; RFC 2409].

Posmatrano iz perspektive savremene informacione bezbednosti, upravo se u ovoj razvojnoj fazi može uočiti početak transformacije kriptografije iz discipline usmerene isključivo na zaštitu sadržaja poruka u disciplinu koja upravlja celokupnim procesom uspostavljanja digitalnog poverenja. Bezbednost komunikacije više se ne meri samo snagom algoritma za šifrovanje, već kvalitetom procesa generisanja, razmene, validacije, obnove i opoziva kriptografskih ključeva. Time upravljanje kriptografskim ključevima postaje sastavni deo bezbednosne arhitekture informaciono-komunikacionog sistema, a ne samo jedna od aktivnosti administratora sistema informacione bezbednosti [1],[2].

Sa stanovišta razvoja *Internet Key Exchange* protokola, navedena transformacija ima fundamentalni značaj. IKE nije projektovan kao mehanizam za šifrovanje podataka, već kao protokol čija je osnovna funkcija bezbedno uspostavljanje kriptografskog poverenja između komunikacionih strana kroz pregovaranje bezbednosnih parametara, autentifikaciju učesnika i generisanje zajedničkog kriptografskog materijala. Drugim rečima, IKE predstavlja odgovor na višedecenijski istraživački problem bezbedne distribucije kriptografskih ključeva u otvorenim mrežnim okruženjima kao što je Internet. Razumevanje ograničenja simetrične kriptografije predstavlja neophodan teorijsko-analički preduslov za razumevanje razloga zbog kojih su razvijeni savremeni protokoli za razmenu ključeva i zbog čega upravo proces uspostavljanja kriptografskog poverenja predstavlja jedan od najznačajnijih elemenata ukupne bezbednosti informaciono-komunikacionih sistema. Analiza istorijskog razvoja simetrične kriptografije pokazuje da ključni izazov nije predstavljala matematička otpornost algoritama na kriptooanalizu, već bezbedno uspostavljanje i održavanje zajedničkog poverenja između komunikacionih učesnika. Upravo problem distribucije i upravljanja ključevima predstavljao je osnovni pokretač razvoja moderne kriptografije sa javnim ključem i kasnijeg nastanka protokola za razmenu kriptografskih ključeva.

Posmatrano iz perspektive *Internet Key Exchange* protokola, može se zaključiti da njegova bezbednosna vrednost proizlazi upravo iz sposobnosti da sistematski rešava problem koji je decenijama predstavljao najveće ograničenje tradicionalnih simetričnih kriptografskih sistema. Time se potvrđuje da se bezbednosne karakteristike IKE protokola ne mogu razumeti bez prethodne analize evolucije procesa upravljanja kriptografskim ključevima i razvoja koncepta digitalnog poverenja u savremenim informaciono-komunikacionim sistemima [2], [31],[38].

2.2. Nastanak kriptografije sa javnim ključem kao prekretnica u razvoju bezbedne razmene kriptografskih ključeva

Naučno-istraživačka analiza razvoja kriptografije pokazuje da su ograničenja simetričnih kriptografskih sistema predstavljala osnovni pokretač jedne od najznačajnijih tehnoloških i teorijskih promena u istoriji informacione bezbednosti. Problem bezbedne distribucije zajedničkog tajnog ključa nije bio moguće trajno rešiti daljim unapređenjem postojećih simetričnih algoritama, budući da se suština problema nalazila u bezbednom uspostavljanju poverenja između komunikacionih učesnika koji međusobno komuniciraju preko otvorenih i

potencijalno kompromitovanih komunikacionih mreža. Upravo ova činjenica dovela je do razvoja potpuno nove istraživačke paradigme, poznate kao kriptografija sa javnim ključem, koja je suštinski promenila način razumevanja bezbedne komunikacije u savremenim informaciono-komunikacionim sistemima [42].

Razvoj kriptografije sa javnim ključem predstavlja jednu od najznačajnijih naučnih prekretnica u oblasti primenjene kriptografije, jer je prvi put omogućio da se problem razmene kriptografskih ključeva posmatra nezavisno od potrebe za prethodno uspostavljenim zajedničkim tajnim ključem. Ovim pristupom uvedena je nova koncepcija digitalnog poverenja zasnovana na primeni para međusobno matematički povezanih ključeva – javnog i privatnog. Za razliku od tradicionalnih simetričnih sistema, kod kojih kompromitacija procesa distribucije ključa neposredno ugrožava bezbednost komunikacije, novi model omogućava javnu distribuciju jednog dela kriptografskog materijala bez narušavanja poverljivosti privatnog ključa. Time se prvi put ostvaruje mogućnost uspostavljanja bezbedne komunikacije između subjekata koji se prethodno nisu poznavali niti su razmenili zajedničku tajnu [2].

Posmatrano sa metodološkog aspekta, nastanak kriptografije sa javnim ključem označava prelazak sa koncepta zaštite podataka na koncept upravljanja digitalnim poverenjem. Dok je tradicionalna kriptografija prvenstveno bila usmerena na očuvanje poverljivosti sadržaja komunikacije, nova paradigma uvodi znatno širi bezbednosni okvir u kojem autentifikacija učesnika, razmena ključeva, potvrda identiteta i uspostavljanje sigurnosnih odnosa postaju sastavni elementi jedinstvenog bezbednosnog procesa. Ovakav pristup predstavlja osnov za razvoj savremenih komunikacionih protokola u kojima bezbednost nije rezultat izolovanog algoritma, već koordinisanog delovanja više međusobno povezanih bezbednosnih mehanizama [13].

Poseban značaj ove promene ogleda se u činjenici da je prvi put omogućeno rešavanje problema koji je decenijama predstavljao osnovno ograničenje razvoja globalnih računarskih mreža. Razvoj Interneta, elektronskog poslovanja, distribuiranih informacionih sistema i međusobno povezanih mrežnih uređaja zahtevao je mehanizam kojim bi se bezbedno uspostavljalo poverenje između velikog broja komunikacionih učesnika bez potrebe za fizičkom razmenom tajnih ključeva. Kriptografija sa javnim ključem omogućila je upravo takvu transformaciju, stvarajući preduslove za razvoj protokola koji danas predstavljaju osnovu bezbedne komunikacije na Internetu [2],[9].

Analiza uzročno-posledičnih veza jasno pokazuje da se razvoj ove nove paradigme nije dogodio slučajno niti isključivo kao rezultat matematičkog napretka. Naprotiv, nastanak kriptografije sa javnim ključem predstavlja direktan odgovor na rastuće zahteve savremenih informaciono-komunikacionih sistema za skalabilnim, fleksibilnim i automatizovanim upravljanjem kriptografskim materijalom i digitalnim poverenjem. Što su komunikacione mreže postajale složenije, a broj učesnika veći, to je postajala izraženija potreba za modelom koji omogućava bezbednu razmenu ključeva bez prethodno uspostavljenog poverljivog komunikacionog kanala. Upravo iz te potrebe razvijeni su matematički koncepti koji će kasnije omogućiti razvoj prvih praktičnih protokola za razmenu kriptografskih ključeva [2], [31].

Sa stanovišta *Internet Key Exchange* protokola, značaj ove istorijske prekretnice prevazilazi njen teorijski doprinos. Celokupna arhitektura IKE zasniva se na principima koje je uspostavila kriptografija sa javnim ključem: mogućnosti bezbednog uspostavljanja

zajedničkog kriptografskog materijala preko nepouzdanog komunikacionog kanala, autentifikaciji učesnika u komunikaciji i dinamičkom upravljanju kriptografskim ključevima tokom životnog ciklusa komunikacione sesije. Bez primene ovih principa razvoj IKE protokola, a samim tim ni savremenih VPN sistema zasnovanih na IPsec arhitekturi, ne bi bio moguć u obliku u kojem danas postoji [52; RFC 2408.], [53. RFC 2409], [55; RFC 7296].

Sa aspekta informacione bezbednosti može se zaključiti da kriptografija sa javnim ključem nije predstavljala samo novu klasu algoritama, već novu filozofiju projektovanja bezbednih informaciono-komunikacionih sistema. Fokus se trajno pomera sa zaštite pojedinačne poruke na projektovanje bezbednih procesa uspostavljanja poverenja, upravljanja identitetima, razmene kriptografskih ključeva i očuvanja dugoročne otpornosti informaciono-komunikacionih sistema na vektore napada. Upravo zbog toga razvoj kriptografije sa javnim ključem predstavlja ne samo istorijsku prekretnicu u razvoju kriptografije, već i teorijsku osnovu svih savremenih protokola za razmenu kriptografskih ključeva, uključujući *Internet Key Exchange* protokol koji predstavlja predmet ovog istraživanja [2],[74; RFC 9370].

Analiza razvoja kriptografije sa javnim ključem potvrđuje da je rešavanje problema bezbedne distribucije kriptografskih ključeva predstavljalo ključni uslov za razvoj savremenih informaciono-komunikacionih sistema. Uvođenjem digitalnog poverenja stvoreni su teorijski i tehnološki preduslovi za razvoj protokola koji omogućavaju bezbednu razmenu kriptografskih ključeva preko otvorenih komunikacionih mreža. Posmatrano iz perspektive *Internet Key Exchange* protokola, upravo ova promena predstavlja osnovnu prekretnicu koja omogućava razumevanje njegovih bezbednosnih karakteristika, budući da se IKE zasniva na principima koje je uspostavila kriptografija sa javnim ključem i razvija ih u okviru integrisanog procesa autentifikacije, razmene ključeva i upravljanja sigurnosnim asocijacijama [42].

2.3 Diffie–hellman algoritam za razmenu kriptografskih ključeva – teorijske, matematičke i bezbednosne osnove

Primena *Diffie–Hellman* algoritma u protokolima kao što su IKE, TLS, SSH, *WireGuard*, *Signal*, QUIC, WPA3 i brojnim drugim savremenim komunikacionim sistemima potvrđuje da ovaj mehanizam predstavlja jedan od fundamentalnih stubova moderne kriptografije. Iako pojedini protokoli koriste različite implementacione varijante, uključujući klasični *Diffie–Hellman*, *Elliptic Curve Diffie–Hellman (ECDH)* ili njegove optimizovane oblike kao što su X25519 i Curve448, osnovni princip ostaje isti – bezbedno uspostavljanje zajedničkog kriptografskog materijala preko komunikacionog kanala koji se unapred ne smatra bezbednim (izložen je presretanju paketa, izmeni paketa i čitavom spektru vektora napada). Ova široka primena potvrđuje da značaj *Diffie–Hellman* algoritma prevazilazi okvire pojedinačnog algoritma i predstavlja jedan od najvažnijih koncepata savremene primenjene kriptografije [31],[82; SP 800-56A Rev. 3].

Tabela 4. Komparativna analiza Diffie–Hellman grupa

DH grupa	Tip	Veličina	Nivo bezbednosti	Status primene	Napomena
MODP 1024 (Grupa 2)	Klasični DH	1024 bita	Nedovoljan	Ne preporučuje se	Zastareo , nedovoljan stepen zaštite može prouzrokovati kompromitaciju stanja bezbednosti
MODP 2048 (Grupa 14)	Klasični DH	2048 bita	Dobar	Široko podržan	Minimalna preporučena veličina
MODP 3072 (Grupa 15)	Klasični DH	3072 bita	Veoma dobar	Preporučen	Viši nivo otpornosti
MODP 4096 (Grupa 16)	Klasični DH	4096 bita	Vrlo visok	Preporučen	Povećani računarski zahtevi
ECP 256 (Grupa 19)	ECDH	256 bita	Visok	Preporučen	Veoma dobar odnos bezbednosti i performansi
ECP 384 (Grupa 20)	ECDH	384 bita	Vrlo visok	Preporučen	Za okruženja sa višim bezbednosnim zahtevima
ECP 521 (Grupa 21)	ECDH	521 bit	Izuzetno visok	Specijalizovana primena	Najveći nivo bezbednosti uz veće hardverske zahteve

Napomena: Tabela predstavlja komparativni pregled najčešće korišćenih Diffie–Hellman grupa u IPsec/IKE okruženju. Savremene implementacije preporučuju najmanje MODP grupu 14 (2048 bita), dok ECDH grupe pružaju viši nivo bezbednosti uz manji računarski i komunikacioni overhead.

Izvor: Autor, na osnovu sinteze relevantnih RFC i NIST dokumenata (RFC 3526, RFC 5903, RFC 8247, NIST SP 800-56A Rev. 3).

Tabela 4 sistematizuje sedam Diffie-Hellman grupa korišćenih u savremenim IPsec/IKE implementacijama, razvrstanih prema dva fundamentalno različita matematička pristupa — klasičnoj modularnoj eksponencijaciji (MODP grupe) i eliptičkim krivama (ECP/ECDH grupe). Podaci jasno ukazuju na direktnu korelaciju između veličine grupe i ostvarenog nivoa bezbednosti u okviru MODP porodice: dok se MODP 1024 (Grupa 2) smatra nedovoljno bezbednom i ne preporučuje se za primenu, MODP 2048 (Grupa 14) predstavlja minimalno prihvatljivu veličinu prema savremenim RFC preporukama, dok MODP 3072 i MODP 4096 pružaju viši, odnosno vrlo visok nivo otpornosti na kriptanalizu, ali uz proporcionalno povećane računarske zahteve.

Sa aspekta praktične primene, tabela posebno ističe prednost ECDH grupa (ECP 256, ECP 384, ECP 521) u odnosu na klasične MODP grupe tj. ekvivalentan ili viši nivo otpornosti na kriptanalitičke napade ECDH grupe postižu primenom parametara znatno manjeg obima, čime se bitno redukuje procesorsko opterećenje i obim podataka razmenjenih tokom pregovaranja, za razliku od zahtevnijeg MODP pristupa. ECP 256 (Grupa 19) izdvaja se kao grupa sa najboljim odnosom bezbednosti i performansi za opštu primenu, dok ECP 521 (Grupa 21), uprkos izuzetno visokom nivou bezbednosti, ostaje rezervisan za specijalizovane

scenarije sa povišenim bezbednosnim zahtevima usled većih računarskih zahteva. Ova tabela time potvrđuje da savremeni trend u izboru Diffie-Hellman parametara ide u pravcu postepenog napuštanja MODP grupa u korist ECDH mehanizama, koji nude povoljniji kompromis između kriptografske otpornosti i operativne efikasnosti.

2.3.1. Teorijska osnova i naučno-istraživačka analiza nastanka diffie–hellman algoritma za razmenu kriptografskih ključeva

Razvoj kriptografije sa javnim ključem predstavlja jednu od najznačajnijih naučnih prekretnica u istoriji informacione bezbednosti, dok se uvođenje *Diffie–Hellman* mehanizma za razmenu kriptografskih ključeva smatra događajem koji je suštinski promenio dotadašnje razumevanje bezbedne komunikacije u otvorenim računarskim mrežama. Do pojave ovog koncepta problem bezbedne razmene zajedničkog tajnog ključa predstavljao je osnovno ograničenje praktične primene simetrične kriptografije u distribuiranim informaciono-komunikacionim sistemima. Bez obzira na visok nivo matematičke otpornosti algoritama za šifrovanje, bezbednost komunikacije ostajala je uslovljena mogućnošću bezbedne distribucije zajedničkog tajnog ključa između komunikacionih učesnika. Upravo rešavanje ovog problema predstavlja osnovni naučni doprinos Diffie–Hellman paradigme i razlog zbog kojeg ona zauzima centralno mesto u razvoju savremene primenjene kriptografije [31],[2].

Suštinska vrednost Diffie–Hellman koncepta ne ogleda se isključivo u razvoju novog matematičkog algoritma, već u promeni načina razmišljanja o uspostavljanju digitalnog poverenja. Umesto polaska od pretpostavke da komunikacioni učesnici unapred raspolažu zajedničkom tajnom, uvedena je nova paradigma prema kojoj se zajednički kriptografski materijal može generisati tokom same komunikacije, čak i kada se razmena odvija preko komunikacionog kanala koji se unapred smatra nepouzdanim ili podložnim nadzoru. Ovakva promena istraživačke paradigme predstavlja jedan od najvažnijih teorijskih doprinosa savremenoj kriptografiji, budući da omogućava razdvajanje problema razmene ključeva od problema zaštite sadržaja komunikacije [31].

Naučno posmatrano, *Diffie–Hellman* mehanizam uvodi novu bezbednosnu logiku u kojoj poverenje između komunikacionih učesnika nije posledica prethodno razmenjene tajne, već rezultat pažljivo projektovanog matematičkog procesa. Time se bezbednost više ne zasniva na tajnosti postupka razmene, već na složenosti matematičkih problema čije efikasno rešavanje nije poznato savremenim računarskim metodama u okviru odgovarajućih bezbednosnih parametara ali će biti neophodno uvesti nove mehanizme zaštite usled primene kvantnih računara. Upravo ova činjenica predstavlja jednu od osnovnih karakteristika moderne kriptografije: bezbednost sistema ne proizlazi iz tajnosti algoritma, već iz javno poznatih matematičkih principa čija praktična kompromitacija zahteva računarske resurse koji prevazilaze realne mogućnosti napadača. Sa metodološkog stanovišta posebno je značajno uočiti da *Diffie–Hellman* ne predstavlja algoritam za šifrovanje podataka. Njegova osnovna funkcija jeste uspostavljanje zajedničke kriptografske tajne koja će kasnije biti iskorišćena za generisanje sesijskih kriptografskih ključeva namenjenih zaštiti komunikacije primenom simetričnih algoritama. Ovakva podela funkcionalnosti predstavlja jednu od osnovnih karakteristika savremenih bezbednosnih protokola. Proces uspostavljanja poverenja odvaja se od procesa zaštite sadržaja komunikacije, čime se omogućava razvoj fleksibilnih i modularnih bezbednosnih arhitektura koje se mogu prilagođavati različitim operativnim zahtevima [2],[31].

Posebnu pažnju zaslužuje činjenica da se bezbednost *Diffie–Hellman* mehanizma zasniva na jasno definisanim matematičkim pretpostavkama. Za razliku od tradicionalnog pristupa u kojem se bezbednost postiže fizičkom zaštitom ključeva ili komunikacionih kanala, ovde se otpornost sistema temelji na teškoći rešavanja odgovarajućih matematičkih problema. Ovakav pristup omogućio je razvoj kriptografskih sistema čija bezbednost može biti predmet formalne matematičke analize, čime je kriptografija dobila čvršću naučnu osnovu i postala disciplina u kojoj se bezbednosne tvrdnje mogu procenjivati kroz precizno definisane matematičke modele [60; RFC 3526].

Analizirajući razvoj savremenih informaciono-komunikacionih sistema može se zaključiti da je *Diffie–Hellman* paradigma omogućila rešavanje problema koji je decenijama ograničavao razvoj distribuiranih mreža. Pojava Interneta, elektronskih servisa, *cloud* infrastruktura, mobilnih komunikacija i virtuelnih privatnih mreža zahtevala je mehanizam kojim će veliki broj međusobno nepoznatih komunikacionih učesnika moći dinamički da uspostavi zajednički kriptografski materijal bez prethodne razmene tajnih informacija. Upravo zbog toga *Diffie–Hellman* nije značajan samo kao istorijska inovacija, već kao osnova na kojoj su kasnije razvijeni brojni bezbednosni protokoli, uključujući *Internet Key Exchange* protokol, koji predstavlja centralni predmet istraživanja ove magistarske teze. Posmatrano iz perspektive bezbednosne arhitekture IKE protokola, značaj *Diffie–Hellman* mehanizma daleko prevazilazi njegovu matematičku funkcionalnost. U okviru IKE procesa razmene ključeva ovaj mehanizam predstavlja početnu fazu uspostavljanja digitalnog poverenja između komunikacionih učesnika. Bez uspešno realizovanog procesa zajedničkog generisanja kriptografskog materijala nije moguće bezbedno formirati sigurnosne asocijacije (SA), nije moguće generisati sesijske ključeve niti obezbediti tajnost i integritet komunikacije. Drugim rečima, *Diffie–Hellman* predstavlja prvi algoritam sa takvim karakteristikama i jedan od najvažnijih koraka u višefaznom procesu uspostavljanja bezbedne IPsec komunikacije [60; RFC 3526].

Sa stanovišta ovog istraživanja posebno je važno naglasiti da analiza *Diffie–Hellman* mehanizma ne može ostati ograničena na matematičku formulaciju algoritma. Njegove bezbednosne karakteristike zavise od pravilnog izbora parametara, kvaliteta implementacije, adekvatne konfiguracije i načina na koji je integrisan u širu arhitekturu IKE protokola. Zbog toga će u nastavku ovog poglavlja biti izvršena detaljna analiza matematičkih osnova *Diffie–Hellman* razmene kriptografskih ključeva, bezbednosnih pretpostavki na kojima se zasniva njegova otpornost, kao i implementacionih i konfiguracionih faktora koji određuju njegovu praktičnu bezbednost u savremenim informaciono-komunikacionim sistemima [2].

Jedna od osnovnih karakteristika savremene primenjene kriptografije jeste činjenica da njena bezbednost nije zasnovana na tajnosti algoritama (*tajni kriptografski algoritmi predstavljaju algoritme gde programski kod nije dostupan analizi slabosti algoritma, obaveštajne službe najčešće koriste jake javno dostupne algoritme ili u određenim slučajevima tzv privatne algoritme gde nije publikovan programski kod konkretnog algoritma*), već na matematičkim problemima čije rešavanje prevazilazi praktične računarske mogućnosti napadača u okviru definisanih bezbednosnih parametara. *Diffie–Hellman* mehanizam predstavlja jedan od najznačajnijih primera takvog pristupa, budući da svoju bezbednost zasniva na pažljivo odabranim matematičkim strukturama koje omogućavaju zajedničko generisanje kriptografske tajne bez njenog direktnog prenosa preko komunikacionog kanala. Na taj način ostvaruje se fundamentalni cilj moderne razmene ključeva – uspostavljanje zajedničkog kriptografskog materijala između učesnika u procesu komunikacije koji komuniciraju preko otvorene i potencijalno neprijateljske mreže [44].

Matematička osnova Diffie–Hellman mehanizma zasniva se na osobinama modularne aritmetike i eksponenciranja u konačnim grupama. Upravo ove matematičke strukture omogućavaju izvođenje operacija koje su efikasne u smeru generisanja zajedničke tajne, dok je njihovo obrnuto rešavanje, pri odgovarajućem izboru parametara, računarski izuzetno složeno. Ovakva asimetrija između lakoće izvođenja i težine obrnutog problema predstavlja jedno od osnovnih načela savremene kriptografije i omogućava izgradnju bezbednosnih sistema čija otpornost proizlazi iz formalno definisanih matematičkih pretpostavki [60; RFC 3526].

Na slici 2. prikazan je konceptualni model transformacije zajedničke tajne. Model objedinjuje fazu uspostavljanja zajedničke tajne (Diffie-Hellman/ECDH), proces izvođenja ključeva i njihovu funkcionalnu specijalizaciju u okviru jedinstvene analitičke celine. Kako bi se jasnije prikazao proces od uspostavljanja zajedničke tajne do formiranja kompletne bezbednosne arhitekture komunikacionog kanala, u nastavku je predstavljen konceptualni model koji objedinjuje kriptografsku razmenu, proces izvođenja ključeva i njihovu funkcionalnu podelu. Model ilustruje kako jedna zajednička tajna, dobijena Diffie-Hellman ili ECDH razmenom, predstavlja polaznu tačku za formiranje bezbednosnih mehanizama u okviru višeslojne zaštite informaciono-komunikacionog sistema.

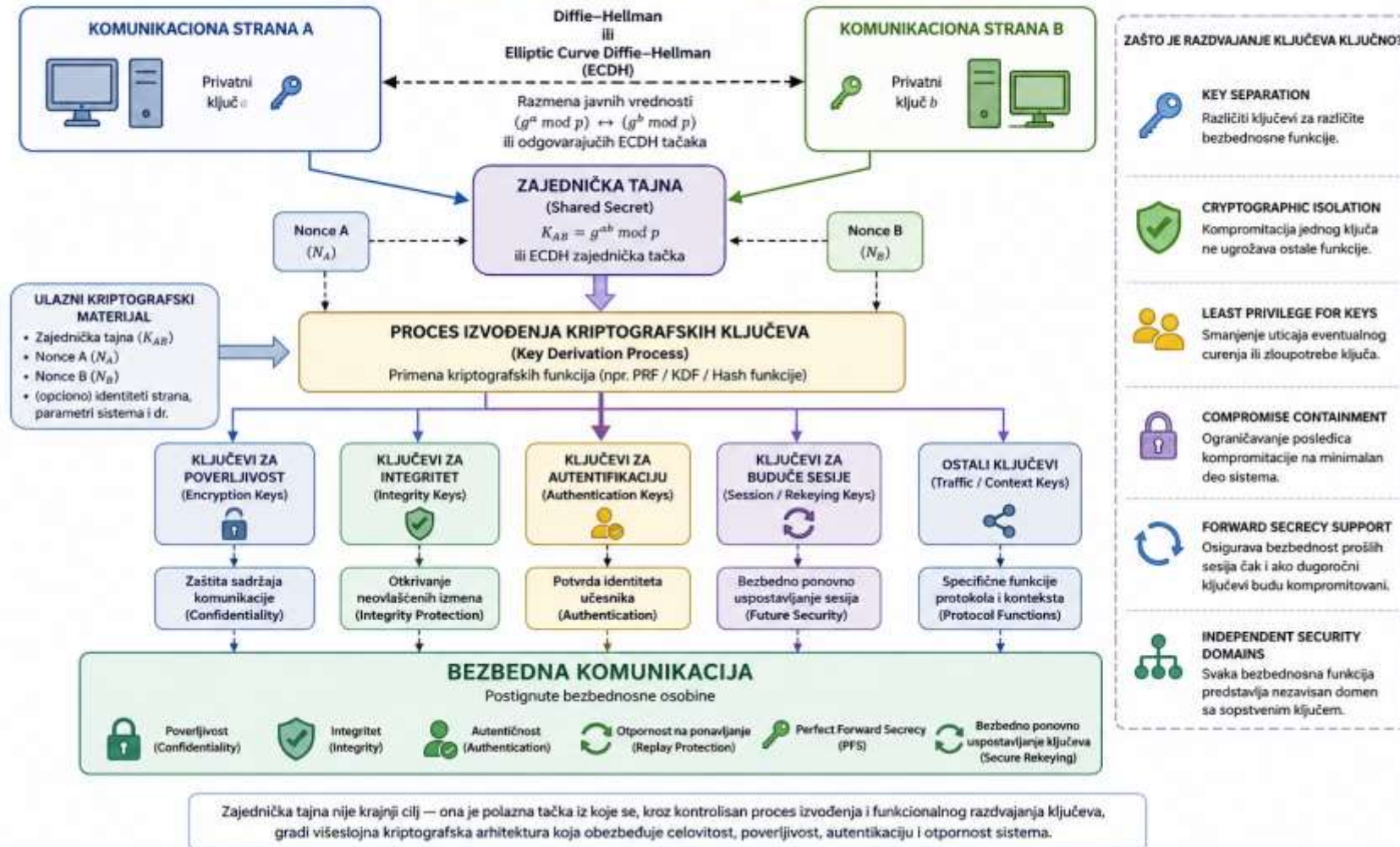
Centralni bezbednosni oslonac *Diffie–Hellman* mehanizma predstavlja problem diskretnog logaritma. U teorijskom smislu, ovaj problem podrazumeva da je, za odgovarajuće izabrane parametre, praktično neizvodljivo odrediti privatnu vrednost učesnika samo na osnovu javno dostupnih podataka i poznatih matematičkih parametara sistema. Upravo zbog toga komunikacioni učesnici mogu razmenjivati javne vrednosti preko otvorene komunikacione mreže bez neposrednog otkrivanja zajedničke tajne koja će biti izvedena lokalnim izračunavanjem na svakoj strani komunikacije [5].

Poseban naučni značaj ovog koncepta ogleda se u činjenici da bezbednost sistema nije zasnovana na skrivanju postupka razmene vrednosti neophodnih u slučaju primene *Diffie–Hellman algoritma*. Naprotiv, kompletan algoritamski postupak može biti javno poznat, dok se otpornost sistema zasniva isključivo na tajnosti privatnih vrednosti i matematičkoj složenosti rešavanja diskretnog logaritma. Time *Diffie–Hellman* algoritam u potpunosti reprezentuje *Kerckhoffsov* princip, prema kojem bezbednost kriptografskog sistema mora zavisiti isključivo od zaštite tajnog ključa, a ne od tajnosti algoritma ili implementacije. Ovaj princip predstavlja jedno od osnovnih načela savremene kriptografije i nalazi se u osnovi projektovanja gotovo svih današnjih bezbednosnih protokola.

Analiza matematičkih osnova Diffie–Hellman mehanizma pokazuje da izbor bezbednosnih parametara predstavlja jedan od najvažnijih faktora njegove ukupne otpornosti. Veličina konačne grupe, izbor generatora pseudoslučajnih kriptovarijabli i odgovarajuće karakteristike korišćenih matematičkih struktura neposredno određuju složenost potencijalnog napada i nivo bezbednosti koji sistem može pružiti. Iz tog razloga savremeni bezbednosni standardi definišu preporučene parametre koji omogućavaju odgovarajući nivo zaštite u odnosu na raspoložive računarske kapacitete i očekivani životni vek kriptografskih ključeva [2],[10].

KONCEPTUALNI MODEL TRANSFORMACIJE ZAJEDNIČKE TAJNE U BEZBEDNOSNU ARHITEKTURU SAVREMENIH KRIPTOGRAFSKIH SISTEMA

Jedna zajednička tajna – temelj za više nezavisnih bezbednosnih funkcija



Slika 2. Konceptualni model transformacije zajedničke tajne (Diffie-Hellman/ECDH) u višeslojnu bezbednosnu arhitekturu savremenih kriptografskih IPsec/IKE sistem

Iz prikazanog modela proizlazi da se bezbednosne funkcije: tajnost, integritet, autentičnost, neporecivost i anti-replay zaštita izvede iz jedinstvene zajedničke tajne kroz kontrolisan proces derivacije kriptografskih ključeva. Ovakav pristup omogućava da se svaka bezbednosna funkcija oslanja na nezavisan ključ, čime se ograničava stepen kompromitacije informaciono-komunikacionog sistema u slučaju kompromitacije bilo kog pojedinačnog ključa.

Sa aspekta *Internet Key Exchange* protokola, izbor *Diffie–Hellman* parametara predstavlja mnogo više od tehničke konfiguracione odluke. Neadekvatno odabrane grupe ili zastareli parametri mogu značajno umanjiti otpornost na kriptanalitičke napade procesa razmene ključeva u celosti i time ugroziti bezbednost IPsec komunikacije. Nasuprot tome, pravilnim izborom savremenih *Diffie–Hellman* grupa omogućava se uspostavljanje visokog nivoa kriptografske otpornosti na vektore napada, očuvanje poverljivosti sesijskih ključeva i stvaranje preduslova za ostvarivanje svojstva *Perfect Forward Secrecy*, koje predstavlja jedan od osnovnih bezbednosnih ciljeva savremenih VPN sistema [2],[26].

Posebno je značajno naglasiti da matematička otpornost *Diffie–Hellman* mehanizma sama po sebi nije dovoljna za garantovanje ukupne bezbednosti informaciono-komunikacionog sistema. Praktična bezbednost zavisi od pravilne implementacije algoritma, kvaliteta generatora pseudoslučajnih brojeva, zaštite privatnih vrednosti, adekvatnog upravljanja životnim ciklusom ključeva i pravilne integracije ovog mehanizma u širu arhitekturu bezbednosnog protokola. Ovakav zaključak potvrđuje osnovnu istraživačku tezu ovog rada, prema kojoj se bezbednosne karakteristike *Internet Key Exchange* protokola mogu objektivno procenjivati jedino kroz integrisanu analizu matematičkih, implementacionih, konfiguracionih i procesnih aspekata njegove primene. [60; RFC 3526].

Matematičke osnove *Diffie–Hellman* mehanizma predstavljaju teorijski stub savremenih sistema za razmenu kriptografskih ključeva. Njegova bezbednost proizlazi iz formalno definisanih matematičkih problema, dok njegova praktična efikasnost zavisi od pravilnog izbora parametara, kvalitetne implementacije i adekvatne integracije u bezbednosnu arhitekturu komunikacionog sistema. Posmatrano iz perspektive *Internet Key Exchange* protokola, *Diffie–Hellman* nije samo algoritam za razmenu ključeva, već osnovni mehanizam uspostavljanja digitalnog poverenja između komunikacionih učesnika. Upravo zbog toga analiza njegovih matematičkih osnova predstavlja neophodan teorijsko-analički preduslov za razumevanje bezbednosnih karakteristika IKE protokola i njegove uloge u zaštiti savremenih informaciono-komunikacionih sistema [53; RFC 2409].

2.3.2. Izbor diffie–hellman grupa : implementacioni i konfiguracioni izazovi kao determinante bezbednosnih karakteristika ikev1 i ikev2 protokola

Nakon uspostavljanja teorijskih i matematičkih osnova *Diffie–Hellman* mehanizma, neophodno je izvršiti detaljnu analizu faktora koji određuju njegovu praktičnu bezbednost u savremenim informaciono-komunikacionim sistemima. Iako matematička otpornost *Diffie–Hellman* paradigme predstavlja neophodan preduslov za bezbednu razmenu kriptografskih ključeva, iskustva iz praktične primene pokazuju da ukupni nivo bezbednosti u velikoj meri zavisi od pravilnog izbora kriptografskih parametara, kvaliteta implementacije, konfiguracije protokola i načina upravljanja životnim ciklusom kriptografskog materijala. Drugim rečima, matematička teorija predstavlja osnovu bezbednosti, ali tek njena pravilna implementacija omogućava ostvarivanje projektovanog nivoa zaštite u realnim operativnim uslovima.

Jedan od najznačajnijih elemenata praktične primene *Diffie–Hellman* mehanizma jeste izbor odgovarajuće *Diffie–Hellman* grupe. U okviru IKE protokola, pojam grupe označava unapred definisane matematičke parametre koji određuju strukturu u kojoj se realizuje razmena kriptografskih ključeva. Izbor grupe neposredno utiče na nivo kriptografske otpornosti, računarsku složenost izvođenja operacija, interoperabilnost između različitih implementacija i ukupne performanse procesa uspostavljanja sigurnosnih asocijacija. Zbog toga izbor *Diffie–Hellman* grupe ne predstavlja isključivo tehničku konfiguracionu odluku, već strateški bezbednosni parametar koji može značajno uticati na otpornost celokupnog Ipsec (IKEv1 ili IKEv2) sistema [2],[31],[77; SP 800-77 Rev. 1.].

Razvoj računarskih tehnologija pokazao je da bezbednost pojedinih *Diffie–Hellman* grupa nije trajna kategorija. Parametri koji su u jednom periodu predstavljali adekvatan nivo zaštite mogu, usled povećanja procesorske snage, razvoja novih metoda analize i otkrivanja slabosti algoritama ili napretka metoda kriptanalize, postati nedovoljni za zaštitu savremenih informaciono-komunikacionih sistema. Ova činjenica ukazuje da procena bezbednosti *Diffie–Hellman* grupa mora biti dinamičan proces koji prati razvoj računarskih tehnologija i aktuelnih pretnji po informacionu bezbednost kao i analizu kompleksne strukture vektora napada državno sponzorisanih aktera jer državno-sponzorisani akteri raspolažu najvećim kapacitetima. Iz tog razloga međunarodni standardi periodično revidiraju preporuke u vezi sa minimalnim neophodnim karakteristikama grupa i prihvatljivim bezbednosnim parametrima.

Posebnu pažnju zaslužuje analiza zastarelih *Diffie–Hellman* grupa koje su bile projektovane u periodu kada raspoloživi računarski kapaciteti nisu omogućavali izvođenje složenijih kriptanalitičkih napada. Danas se smatra da upotreba takvih grupa može predstavljati značajan bezbednosni rizik, naročito u sistemima koji štite informacije visoke vrednosti ili podatke čija poverljivost mora biti očuvana tokom dužeg vremenskog perioda. Posledično, savremeni pristup projektovanju bezbednih informaciono-komunikacionih sistema podrazumeva kontinuirano praćenje preporuka standardizacionih tela i pravovremenu zamenu zastarelih kriptografskih parametara savremenijim rešenjima [31].

Pored izbora grupa, jedan od ključnih faktora bezbednosti predstavlja kvalitet implementacije *Diffie–Hellman* mehanizma. U praksi je više puta potvrđeno da kompromitacija bezbednosti često nije posledica slabosti matematičkog modela, već implementacionih grešaka koje omogućavaju napadaču iskorišćavanje nepravilnosti u radu softvera ili hardvera. Neadekvatna validacija javnih vrednosti, nepravilno generisanje privatnih parametara, upotreba generatora slučajnih brojeva niskog kvaliteta ili neodgovarajuće upravljanje memorijom mogu značajno umanjiti nivo zaštite koji teorijski obezbeđuje *Diffie–Hellman* mehanizam. Ovakvi primeri potvrđuju da između matematičke bezbednosti algoritma i praktične bezbednosti implementacije postoji suštinska razlika koja mora biti predmet posebne naučno-istraživačke analize. Konfiguracija IKE protokola predstavlja dodatni sloj koji neposredno utiče na efikasnost primene *Diffie–Hellman* razmene ključeva. Proces pregovaranja bezbednosnih parametara mora obezbediti da obe komunikacione strane koriste međusobno kompatibilne i dovoljno bezbedne kriptografske *Diffie–Hellman* grupe. U slučaju prihvatanja zastarelih ili nedovoljno bezbednih grupa može doći do smanjenja ukupnog nivoa zaštite komunikacije, iako ostali elementi bezbednosne arhitekture funkcionišu u skladu sa projektovanim zahtevima. Zbog toga konfiguraciona politika ne sme biti zasnovana isključivo na interoperabilnosti, već prvenstveno na proceni bezbednosnog rizika i primeni savremenih kriptografskih preporuka [31].

Analiza razvoja IKE protokola pokazuje da je upravo potreba za unapređenjem bezbednosti i performansi predstavljala jedan od glavnih razloga za široku primenu *Elliptic Curve Diffie–Hellman* (ECDH) mehanizma. Primenom eliptičkih krivih omogućeno je ostvarivanje ekvivalentnog ili višeg nivoa bezbednosti uz znatno drugačije kriptografske parametre, što rezultuje manjom potrošnjom procesorskih resursa, manjim komunikacionim opterećenjem i efikasnijim izvršavanjem kriptografskih operacija. Ovakve karakteristike imaju poseban značaj u savremenim informaciono-komunikacionim sistemima koji obuhvataju mobilne uređaje, *IoT* infrastrukturu, *cloud* okruženja i druge sisteme sa ograničenim računarskim resursima. Sa aspekta bezbednosnih karakteristika IKEv1 i IKEv2 protokola može se zaključiti da izbor *Diffie–Hellman* grupe predstavlja jedan od najznačajnijih faktora koji određuju otpornost procesa razmene kriptografskih ključeva. Međutim, taj izbor ne može se posmatrati izolovano. Stvarni bezbednosni efekat izbora *Diffie–Hellman* grupe zavisi od kvaliteta implementacije politike bezbednosti informaciono-komunikacionog sistema u celosti, pravilne konfiguracije, bezbednog generisanja slučajnih vrednosti, odgovarajućeg upravljanja životnim ciklusom ključeva i kontinuiranog prilagođavanja bezbednosnih parametara razvoju novih tehnoloških i kriptanalitičkih mogućnosti. Ovakav zaključak potvrđuje osnovnu istraživačku tezu ovog rada da bezbednost *Internet Key Exchange* protokola predstavlja rezultat međusobnog delovanja više tehničkih, organizacionih i procesnih faktora, a ne isključivo matematičke otpornosti pojedinačnih kriptografskih algoritama [2].

Analiza izbora *Diffie–Hellman* grupa pokazuje da bezbednost razmene kriptografskih ključeva ne zavisi samo od teorijskih svojstava algoritma, već od pravilnog izbora parametara, kvaliteta implementacije i konfiguracije protokola. Upravo zbog toga savremena procena bezbednosnih karakteristika IKEv1 i IKEv2 mora obuhvatiti integrisanu analizu matematičkih, implementacionih i operativnih aspekata primene *Diffie–Hellman* mehanizma. Takav pristup omogućava objektivnije razumevanje stvarnog nivoa zaštite koji IKE može obezbediti u savremenim informaciono-komunikacionim sistemima i predstavlja osnov za dalje razmatranje evolucije ka *Elliptic Curve Diffie–Hellman* mehanizmu.

2.3.3. Funkcije za izvođenje kriptografskog materijala kao osnova bezbedne arhitekture internet key exchange protokola

Proces razmene kriptografskih ključeva predstavlja samo početnu fazu uspostavljanja bezbedne komunikacije između učesnika u informaciono-komunikacionom sistemu. Iako primena *Diffie–Hellman* ili *Elliptic Curve Diffie–Hellman* mehanizma omogućava komunikacionim stranama da nezavisno izračunaju identičnu zajedničku tajnu, ta vrednost se u savremenim bezbednosnim protokolima ne koristi neposredno za zaštitu korisničkih podataka. Umesto toga, zajednička tajna predstavlja ulazni kriptografski materijal iz kojeg se, primenom posebno projektovanih funkcija za izvođenje ključeva, generiše čitav skup međusobno nezavisnih kriptografskih ključeva namenjenih različitim bezbednosnim funkcijama. Upravo ovaj proces predstavlja jednu od najvažnijih karakteristika arhitekture *Internet Key Exchange* protokola i jedan od osnovnih razloga njegove visoke bezbednosne otpornosti [82; SP 800-56A Rev. 3].

Savremeni pristup projektovanju kriptografskih protokola zasniva se na principu funkcionalne razdvojenosti kriptografskih ključeva. Umesto korišćenja jedinstvenog ključa za više različitih bezbednosnih funkcija, uvodi se koncept izvođenja specijalizovanih kriptografskih ključeva namenjenih autentifikaciji, proveru integriteta, zaštiti tajnosti komunikacije i upravljanju sigurnosnim asocijacijama. Ovakav pristup značajno smanjuje mogućnost da kompromitacija jednog ključa dovede do ugrožavanja ostalih bezbednosnih funkcija sistema [2],[18],[31].

Centralnu ulogu u ovom procesu imaju pseudonasumične funkcije (*Pseudo-Random Functions* – PRF). Njihova osnovna funkcija jeste determinističko izvođenje novih kriptografskih vrednosti iz zajedničke tajne i dodatnih ulaznih parametara, pri čemu dobijeni izlaz mora posedovati visok stepen kriptografske nepredvidivosti. U teorijskom smislu, PRF predstavlja mehanizam kojim se ograničena količina početnog kriptografskog materijala transformiše u skup novih vrednosti pogodnih za različite bezbednosne namene. Na taj način zajednička tajna dobijena *Diffie–Hellman* razmenom postaje početna tačka za izgradnju kompletne bezbednosne arhitekture komunikacione sesije [2],[31].

Sa aspekta *Internet Key Exchange* protokola, posebno mesto zauzima koncept SKEYSEED-a. Ova vrednost predstavlja osnovni kriptografski temelj iz kojeg se dalje izvode svi ostali ključevi neophodni za funkcionisanje IKE i IPsec arhitekture. Njegov značaj proizlazi iz činjenice da omogućava logičko razdvajanje procesa razmene zajedničke tajne od procesa generisanja operativnih kriptografskih ključeva. Time se postiže dodatni nivo bezbednosti, budući da zajednička tajna ostaje posredno povezana sa ključevima koji se koriste u praktičnoj komunikaciji, dok se stvarna zaštita podataka ostvaruje korišćenjem izvedenih vrednosti [2]. Na osnovu SKEYSEED vrednosti generiše se KEYMAT – skup kriptografskih ključeva namenjenih različitim funkcijama u okviru IKE i IPsec komunikacije.

Prikazani koncept omogućava da svaki bezbednosni mehanizam koristi zaseban ključ, prilagođen svojoj konkretnoj funkciji. Posledično, autentifikacija, zaštita integriteta, šifrovanje korisničkog saobraćaja i upravljanje sigurnosnim asocijacijama realizuju se korišćenjem međusobno nezavisnih kriptografskih vrednosti. Ovakva arhitektura značajno povećava otpornost sistema na različite vrste napada i predstavlja jedan od osnovnih razloga zbog kojih se IKE smatra jednim od najbezbednijih protokola za uspostavljanje kriptografskog poverenja. Analiza bezbednosnih karakteristika procesa izvođenja ključeva pokazuje da njegova efikasnost zavisi od više međusobno povezanih faktora. Kvalitet zajedničke tajne dobijene primenom DH ili ECDH mehanizma, izbor odgovarajuće pseudonasumične funkcije, kvalitet ulaznih parametara, pravilna implementacija i zaštita izvedenih ključeva predstavljaju elemente koji zajedno određuju stvarni nivo bezbednosti komunikacione sesije. Ovakav zaključak potvrđuje da bezbednost procesa razmene ključeva ne završava trenutkom generisanja zajedničke tajne, već se nastavlja kroz pažljivo projektovan proces izvođenja i upravljanja kriptografskim materijalom [2],[54; RFC 4306].

Posebno je značajno naglasiti da proces izvođenja ključeva predstavlja važan element ostvarivanja principa kriptografske izolacije. Kompromitacija pojedinačnog izvedenog ključa ne mora nužno dovesti do kompromitacije ostalih ključeva niti zajedničke tajne iz koje su izvedeni. Ovakva osobina značajno povećava otpornost sistema na parcijalne kompromitacije i omogućava efikasnije upravljanje bezbednosnim incidentima. Upravo zbog toga savremeni standardi za projektovanje bezbednosnih protokola naglašavaju potrebu za strogo definisanim procedurama izvođenja, upotrebe i zamene kriptografskih ključeva [31].

Posmatrano sa aspekta *Internet Key Exchange* protokola, PRF, SKEYSEED i KEYMAT ne predstavljaju pomoćne funkcije, već centralne komponente koje povezuju razmenu ključeva sa praktičnom zaštitom komunikacije. Bez njihovog pravilnog funkcionisanja nije moguće uspostaviti sigurnosne asocijacije, generisati sesijske ključeve niti obezbediti poverljivost, integritet i autentičnost IPsec komunikacije. Njihova analiza stoga predstavlja neophodan teorijsko-analitički korak ka razumevanju unutrašnje arhitekture IKEv1 i IKEv2 protokola [2].

Proces izvođenja kriptografskih ključeva predstavlja jednu od najznačajnijih faza savremenih protokola za razmenu ključeva, budući da omogućava transformaciju zajedničke tajne u skup funkcionalno specijalizovanih kriptografskih vrednosti. Primena PRF funkcija, SKEYSEED-a i KEYMAT-a potvrđuje da bezbednost Internet Key Exchange protokola ne proizlazi samo iz kvaliteta mehanizma razmene ključeva, već iz pažljivo projektovanog procesa upravljanja kriptografskim materijalom tokom čitavog životnog ciklusa komunikacione sesije. Upravo ovakav višeslojni pristup predstavlja jedan od ključnih razloga zbog kojih IKE ostvaruje visok nivo bezbednosti u savremenim informaciono-komunikacionim sistemima [2],[60; RFC 3526].

2.4. Entropija, generatori slučajnih brojeva i nonce vrednosti kao osnova bezbedne razmene kriptografskih ključeva

2.4.1. Entropija i kvalitet slučajnosti kao fundamentalni preduslov bezbednosti internet key exchange protokola

Analiza savremenih kriptografskih sistema pokazuje da bezbednost procesa razmene kriptografskih ključeva ne zavisi isključivo od matematičke otpornosti primenjenih algoritama, već u značajnoj meri i od kvaliteta ulaznih kriptografskih vrednosti koje učestvuju u procesu njihovog generisanja. U tom kontekstu, entropija predstavlja jedan od osnovnih pojmova savremene primenjene kriptografije, budući da određuje stepen nepredvidivosti podataka koji se koriste za generisanje privatnih ključeva, *nonce* vrednosti, inicijalizacionih parametara i drugih elemenata od kojih zavisi bezbednost čitavog komunikacionog procesa. Posmatrano iz perspektive *Internet Key Exchange* protokola, kvalitet entropije predstavlja jedan od temeljnih preduslova za bezbedno uspostavljanje digitalnog poverenja između učesnika u procesu komunikacije [2].

U teorijskom smislu, entropija predstavlja meru neizvesnosti ili slučajnosti raspoloživih podataka. Što je nivo entropije viši, to je veća nepredvidivost generisanih vrednosti i manja verovatnoća da napadač može rekonstruisati ili predvideti kriptografski materijal koji će biti korišćen tokom procesa razmene ključeva.

Upravo zbog toga savremeni kriptografski sistemi posebnu pažnju posvećuju kvalitetu izvora slučajnosti iz kojih se generišu privatni parametri, budući da kompromitacija ovog procesa može dovesti do narušavanja bezbednosti bez obzira na formalnu otpornost primenjenih algoritama. Jedan od ključnih elemenata obezbeđivanja dovoljnog nivoa entropije predstavlja upotreba kvalitetnih generatora slučajnih brojeva. Njihova osnovna funkcija jeste proizvodnja vrednosti koje poseduju visok stepen statističke slučajnosti i nepredvidivosti. U savremenim informaciono-komunikacionim sistemima generatori slučajnih brojeva često koriste kombinaciju različitih fizičkih izvora entropije, kao što su vremenske varijacije rada procesora, hardverski generatori slučajnosti, elektronski šum ili drugi teško predvidivi fizički procesi. Na taj način smanjuje se mogućnost da napadač predvidi generisane vrednosti i kompromituje proces razmene kriptografskih ključeva [38].

Sa aspekta *Internet Key Exchange* protokola, posebno mesto zauzimaju **nonce** vrednosti. *Nonce* predstavlja jedinstvenu, slučajnu vrednost (primena u vremenski ograničenom intervalu) koja se koristi tokom procesa razmene poruka radi obezbeđivanja višeg stepena bezbednosti informaciono-komunikacionog sistema, sprečavanja ponovne upotrebe prethodnih komunikacionih poruka i povećanja entropije procesa generisanja zajedničkog kriptografskog materijala. Za razliku od dugoročnih kriptografskih ključeva, *nonce* nema funkciju trajne zaštite podataka, već doprinosi bezbednosti same procedure uspostavljanja

komunikacione sesije. Pravilna primena omogućava razlikovanje svake nove razmene ključeva od prethodnih sesija, čime se značajno povećava otpornost sistema na različite oblike aktivnih napada. Jedna od najvažnijih bezbednosnih funkcija *nonce* vrednosti jeste zaštita od napada ponovnim emitovanjem poruka (*replay* napada). U odsustvu jedinstvenih *nonce* vrednosti napadač bi mogao da presretne legitimnu komunikaciju i kasnije ponovo emituje prethodno zabeležene poruke sa ciljem neovlašćenog uspostavljanja komunikacione sesije. Uvođenjem jedinstvenih *nonce* vrednosti svaka komunikaciona sesija dobija sopstveni identitet, dok se prethodno korišćene poruke mogu pouzdano prepoznati kao nevažeće. Time *nonce* postaje važan element očuvanja integriteta procesa razmene ključeva i sprečavanja zloupotrebe legitimnih komunikacionih tokova [2].

Posebnu pažnju zaslužuje analiza posledica nedovoljne entropije ili ponovne upotrebe *nonce* vrednosti. Savremena praksa pokazala je da značajan broj bezbednosnih incidenata nije bio posledica slabosti osnovnih kriptografskih algoritama, već nepravilnog generisanja slučajnih vrednosti ili njihovog ponovnog korišćenja. Nedovoljna entropija može omogućiti napadaču smanjenje prostora mogućih vrednosti, olakšati izvođenje napada zasnovanih na pretpostavkama ili čak dovesti do kompromitacije privatnih kriptografskih ključeva. Slično tome, ponovna upotreba *nonce* vrednosti može narušiti bezbednosne pretpostavke pojedinih kriptografskih mehanizama i ugroziti tajnost ili integritet komunikacije. Ovi primeri potvrđuju da kvalitet procesa generisanja slučajnih vrednosti predstavlja jednako važan bezbednosni faktor kao i izbor samih kriptografskih algoritama [31].

Analiza bezbednosnih karakteristika IKEv1 i IKEv2 pokazuje da se entropija i *nonce* ne mogu posmatrati kao izolovani tehnički parametri. Njihov značaj proizlazi iz njihove uloge u celokupnom procesu uspostavljanja digitalnog poverenja. Kvalitet ulaznih slučajnih vrednosti neposredno utiče na kvalitet zajedničke tajne, kvalitet izvedenih ključeva, otpornost procesa autentifikacije i pouzdanost sigurnosnih asocijacija (SA). Zbog toga projektovanje bezbednog IKE sistema mora obuhvatiti ne samo izbor odgovarajućih kriptografskih algoritama, već i obezbeđivanje pouzdanih izvora entropije, pravilno upravljanje *nonce* vrednostima i kontinuirano praćenje kvaliteta procesa generisanja slučajnih brojeva. Entropija, generatori slučajnih brojeva i *nonce* vrednosti predstavljaju fundamentalne elemente savremene kriptografske arhitekture. Njihova funkcija nije ograničena na generisanje slučajnih podataka, već obuhvata očuvanje nepredvidivosti procesa razmene ključeva, sprečavanje ponovne upotrebe komunikacionih poruka i povećanje otpornosti informaciono-komunikacionih sistema na različite oblike kriptanalitičkih i aktivnih mrežnih napada. Posmatrano iz perspektive *Internet Key Exchange* protokola, kvalitet entropije predstavlja jedan od osnovnih preduslova bezbednog funkcionisanja celokupnog procesa razmene kriptografskih ključeva, potvrđujući da se bezbednost IKE ne zasniva isključivo na izboru algoritama, već na kvalitetu svih komponenti koje učestvuju u procesu uspostavljanja i održavanja digitalnog poverenja [2].

2.5. Perfect forward secrecy i upravljanje životnim ciklusom kriptografskih ključeva kao osnova dugoročne bezbednosti internet key exchange protokola

Razvoj savremenih informaciono-komunikacionih sistema pokazuje da bezbednost razmene kriptografskih ključeva ne može biti posmatrana kao jednokratni događaj ograničen na trenutak uspostavljanja komunikacione sesije. Naprotiv, bezbednost predstavlja kontinuirani proces koji obuhvata generisanje, razmenu, izvođenje, korišćenje, rotaciju, obnovu i bezbedno uklanjanje kriptografskog materijala tokom čitavog životnog ciklusa komunikacije. Ovakav

pristup predstavlja jednu od osnovnih karakteristika savremene kriptografske arhitekture i posebno dolazi do izražaja u projektovanju *Internet Key Exchange* protokola, gde dugoročna otpornost sistema zavisi od pravilnog upravljanja kriptografskim ključevima, a ne samo od njihove inicijalne razmene [2],[42].

Jedan od najznačajnijih bezbednosnih principa koji proističe iz ovakvog pristupa jeste ***Perfect Forward Secrecy (PFS)***. Suština ovog principa ogleda se u tome da kompromitacija dugoročnih autentifikacionih ključeva ne sme omogućiti naknadnu kompromitaciju sesijskih ključeva korišćenih u prethodno uspostavljenim komunikacionim sesijama. Drugim rečima, svaka komunikaciona sesija mora posedovati sopstveni, nezavisno generisan kriptografski materijal, tako da kompromitacija jednog elementa bezbednosne arhitekture ne dovodi do kompromitacije celokupne istorije komunikacije. Ovakva osobina predstavlja jedan od najvažnijih pokazatelja otpornosti savremenih protokola za razmenu kriptografskih ključeva [31], [64; RFC 8221].

Teorijski posmatrano, *Perfect Forward Secrecy* predstavlja evoluciju koncepta digitalnog poverenja. Dok su raniji modeli bezbedne komunikacije bili zasnovani na dugoročnim zajedničkim tajnama, savremeni pristup uvodi dinamičko generisanje sesijskih ključeva za svaku novu komunikacionu sesiju. Primena efemernih *Diffie–Hellman* i *Elliptic Curve Diffie–Hellman* vrednosti omogućava da se zajednička tajna generiše nezavisno za svaku sesiju, čime se značajno smanjuju posledice eventualne kompromitacije dugoročnih autentifikacionih ključeva. Na taj način PFS ne predstavlja dodatnu bezbednosnu funkciju, već temeljni princip projektovanja savremenih sistema za razmenu kriptografskih ključeva [2].

Poseban značaj ovog principa dolazi do izražaja u arhitekturi IKEv2 protokola. Uspostavljanje novih *Security Association* putem efemernih DH ili ECDH razmena omogućava da svaka nova komunikaciona sesija bude kriptografski nezavisna od prethodnih. Posledično, čak i u slučaju kasnije kompromitacije privatnog autentifikacionog ključa, prethodno razmenjeni podaci ostaju zaštićeni, budući da sesijski ključevi nisu izvedeni direktno iz dugoročnih poverljivih vrednosti. Ovakva arhitektura predstavlja jedan od ključnih razloga zbog kojih se *Perfect Forward Secrecy* smatra standardnim bezbednosnim zahtevom u savremenim VPN sistemima. Međutim, ostvarivanje *Perfect Forward Secrecy* predstavlja samo jednu fazu mnogo šireg procesa upravljanja životnim ciklusom kriptografskih ključeva. Savremena kriptografija polazi od pretpostavke da svaki ključ prolazi kroz jasno definisane faze: generisanje, distribuciju, aktivnu upotrebu, periodičnu rotaciju, obnovu, opoziv i konačno bezbedno uništavanje. Svaka od ovih faza nosi sopstvene bezbednosne rizike i zahteva odgovarajuće organizacione, tehničke i proceduralne mere zaštite. Zbog toga upravljanje ključevima ne predstavlja administrativnu aktivnost, već integralni deo bezbednosnog upravljanja informaciono-komunikacionim sistemom [2],[29].

Sa procesnog aspekta, pravilno upravljanje životnim ciklusom ključeva predstavlja mehanizam kojim se održava kontinuitet digitalnog poverenja. Rotacija ključeva ograničava vreme njihove aktivne upotrebe i smanjuje potencijalne posledice kompromitacije. *Rekeying* omogućava periodično uspostavljanje novih sesijskih ključeva bez prekida komunikacije, dok opoziv i bezbedno uklanjanje kompromitovanih ili zastarelih ključeva sprečavaju njihovu dalju zloupotrebu. Posmatrano sistemski, ove aktivnosti čine zatvoren bezbednosni ciklus koji omogućava kontinuirano održavanje visokog nivoa zaštite [2].

Analiza savremenih bezbednosnih incidenata potvrđuje da kompromitacija informaciono-komunikacionih sistema često nije posledica slabosti osnovnih kriptografskih algoritama, već nedostataka bezbednosne politike i propusta u specificiranju procedura upravljanja životnim ciklusom ključeva. Dugotrajna upotreba istih ključeva, neblagovremena rotacija, neadekvatno čuvanje tajnih vrednosti ili nepostojanje procedura za opoziv kompromitovanih ključeva (*PKI sistemi*, *CRL liste*) mogu značajno umanjiti bezbednosne karakteristike sistema, čak i kada su korišćeni algoritmi matematički otporni. Ovakvi primeri potvrđuju osnovnu istraživačku tezu ovog rada da se bezbednost *Internet Key Exchange* protokola mora procenjivati kroz integrisanu analizu algoritama, implementacije, konfiguracije i upravljanja kriptografskim materijalom [22], [48].

Posebnu dimenziju ove analize predstavljaju savremeni izazovi koje donosi razvoj kvantnog računarstva. Kvantni algoritmi mogli bi u budućnosti uticati na bezbednosne pretpostavke na kojima se zasnivaju klasični *Diffie–Hellman* i *Elliptic Curve Diffie–Hellman* mehanizmi. Iz tog razloga međunarodna stručna zajednica intenzivno razvija postkvantne algoritme za razmenu ključeva i hibridne modele koji kombinuju postojeće mehanizme sa novim postkvantnim rešenjima. Takav pristup omogućava postepenu tranziciju ka novoj generaciji kriptografskih sistema uz očuvanje interoperabilnosti i kontinuiteta rada postojećih informaciono-komunikacionih infrastruktura. Time se potvrđuje da upravljanje životnim ciklusom ključeva podrazumeva ne samo operativno održavanje postojećih mehanizama, već i njihovu plansku evoluciju u skladu sa razvojem novih tehnoloških i bezbednosnih izazova [2].

Analiza teorijskih osnova razmene kriptografskih ključeva potvrđuje da se bezbednost *Internet Key Exchange* protokola ne može objasniti niti procenjivati analizom pojedinačnih algoritama. Istorijski razvoj kriptografije, nastanak *Diffie–Hellman* paradigme, evolucija ka *Elliptic Curve Diffie–Hellman* mehanizmu, funkcije za izvođenje ključeva, značaj entropije, nonce vrednosti i *Perfect Forward Secrecy* predstavljaju međusobno povezane elemente jedinstvene bezbednosne arhitekture. Svaki od ovih elemenata doprinosi uspostavljanju, održavanju i zaštiti digitalnog poverenja između komunikacionih učesnika [19].

Na osnovu sprovedene teorijsko-analitičke analize može se zaključiti da bezbednosne karakteristike *Internet Key Exchange* protokola proizlaze iz sinergijskog delovanja matematičkih modela, kvaliteta implementacije, pravilne konfiguracije, upravljanja životnim ciklusom kriptografskih ključeva i procesnog upravljanja bezbednošću informaciono-komunikacionog sistema. Upravo ovakav integrisani pristup predstavlja metodološku osnovu ovog istraživanja i polaznu tačku za naredna poglavlja, u kojima će biti izvršena detaljna analiza IPsec arhitekture, IKEv1 i IKEv2 protokola [23], [35].

3. Arhitektura ipsec protokola kao osnova za uspostavljanje digitalnog poverenja i funkcionisanje internet key exchange (ike) protokola

U prethodnom poglavlju izvršena je teorijsko-analiitička analiza osnovnih kriptografskih mehanizama koji omogućavaju bezbednu razmenu kriptografskih ključeva preko otvorenih komunikacionih mreža. Analizirani su istorijski razvoj kriptografije sa javnim ključem, *Diffie-Hellman* i *Elliptic Curve Diffie-Hellman* mehanizmi, funkcije za izvođenje kriptografskog materijala, značaj entropije, *Perfect Forward Secrecy* i upravljanje životnim ciklusom kriptografskih ključeva. Time je uspostavljena teorijska osnova za razumevanje procesa uspostavljanja digitalnog poverenja između strana u procesu komunikacije.

Digitalno poverenje koje realizujemo razmenom kriptografskih ključeva ima praktičnu vrednost koju dobija u procesu integracije u sistem mera zaštite informaciono-komunikacionog sistema i na taj način omogućava zaštitu mrežnog saobraćaja. Upravo iz tog razloga predmet ovog poglavlja nije analiza pojedinačnih mrežnih protokola, već analiza IPsec arhitekture kao sistemskog okvira koji omogućava implementaciju kriptografskih mehanizama u zaštiti komunikacije na mrežnom sloju OSI modela. U tom kontekstu *Internet Key Exchange* predstavlja centralni mehanizam za uspostavljanje, održavanje i obnavljanje digitalnog poverenja kroz pregovaranje bezbednosnih parametara, upravljanje *Security Association* mehanizmima i kontinuirano održavanje bezbednosti komunikacije [2],[74; RFC 9370].

3.1. Teorijska osnova nastanka ipsec arhitekture

Razvoj savremenih informaciono-komunikacionih sistema tokom poslednjih decenija XX veka doveo je do intenzivnog povezivanja računarskih mreža na globalnom nivou. Nastankom Interneta kao univerzalne komunikacione infrastrukture ostvarene su brojne tehnološke, ekonomske i društvene prednosti, ali su istovremeno nastali i novi bezbednosni izazovi. Prvobitna arhitektura TCP/IP modela projektovana je u periodu kada bezbednost nije predstavljala primarni projektantski zahtev, već je dominantan cilj bio omogućavanje pouzdane interoperabilnosti između različitih računarskih sistema. Posledično, osnovni Internet protokoli nisu sadržali ugrađene mehanizme za obezbeđivanje tajnosti, integriteta, autentifikacije i zaštite od neovlašćenih izmena mrežnog saobraćaja [15].

Kako je Internet prerastao akademsku i istraživačku mrežu i postao globalna infrastruktura za poslovnu, državnu i vojnu komunikaciju, postalo je očigledno da postojeća mrežna arhitektura ne može obezbediti odgovarajući nivo zaštite osetljivih podataka.[31] Informacije koje su se prenosile preko javnih komunikacionih mreža bile su izložene presretanju, neovlašćenim izmenama, lažnom predstavljanju komunikacionih učesnika i različitim oblicima aktivnih mrežnih napada. Ovakvi bezbednosni izazovi ukazali su na potrebu za razvojem standardizovane arhitekture koja će omogućiti zaštitu komunikacije nezavisno od aplikacija koje koriste mrežne servise [5],[38],[39]. Analiza istorijskog razvoja mrežne bezbednosti pokazuje da je nastanak IPsec arhitekture bio rezultat potrebe za sistemskim rešavanjem fundamentalnih bezbednosnih problema Interneta. Za razliku od aplikacionih mehanizama zaštite, koji obezbeđuju sigurnost samo za pojedinačne servise, IPsec uvodi zaštitu na mrežnom sloju, čime omogućava jedinstven model bezbednosti za sve aplikacije koje koriste IP komunikaciju. Ovakav pristup predstavljao je značajnu promenu u filozofiji projektovanja bezbednosnih sistema, jer je bezbednost prvi put integrisana u samu mrežnu arhitekturu [31].

Osnovni cilj razvoja IPsec arhitekture bio je uspostavljanje standardizovanog okvira koji omogućava ostvarivanje četiri osnovna bezbednosna svojstva: tajnost podataka, zaštitu integriteta, autentifikacije komunikacionih učesnika i zaštite od ponovnog emitovanja legitimnih komunikacionih poruka. Međutim, IPsec nije projektovan kao pojedinačni protokol koji rešava svaki od ovih problema zasebno. Naprotiv, razvijen je kao modularna arhitektura sastavljena od međusobno povezanih mehanizama koji zajedničkim delovanjem ostvaruju željeni nivo zaštite [15].

Ovakva arhitektonska filozofija predstavlja jednu od najvažnijih karakteristika IPsec sistema. Bezbednost nije koncentrisana u jednoj komponenti, već proizlazi iz koordinisanog rada više međusobno zavisnih mehanizama. Upravo zbog toga analiza IPsec-a zahteva sistemski pristup koji prevazilazi opis pojedinačnih protokola i obuhvata međusobne odnose svih elemenata bezbednosne arhitekture. Jedna od ključnih karakteristika razvoja IPsec arhitekture jeste prelazak sa posmatranja bezbednosti kao skupa izolovanih kriptografskih funkcija na koncept integrisanog procesa upravljanja digitalnim poverenjem. U takvom modelu razmena ključeva predstavlja samo početnu fazu, nakon koje slede pregovaranje bezbednosnih parametara, uspostavljanje *Security Association*, zaštita mrežnog saobraćaja, kontinuirano praćenje stanja komunikacije i periodična obnova kriptografskog materijala. Svaka od ovih aktivnosti predstavlja sastavni deo jedinstvenog procesa čiji je cilj očuvanje bezbednosti komunikacije tokom čitavog njenog trajanja kriptografski zaštićenog komunikacionog kanala između entiteta u procesu komunikacije [2].

Sa metodološkog stanovišta, ovakav pristup omogućava da se IPsec posmatra kao dinamička bezbednosna arhitektura, a ne kao skup statičkih mrežnih protokola. Time se otvara mogućnost za analizu međusobnih uzročno-posledičnih veza između bezbednosnih politika, procesa autentifikacije, upravljanja kriptografskim ključevima i operativnog funkcionisanja informaciono-komunikacionog sistema. Upravo ova procesna perspektiva predstavlja osnovnu metodološku polaznu tačku ovog istraživanja [19]. Sa aspekta naučno-istraživačke analize u okviru ove magistarske teze, razvoj IPsec arhitekture ima poseban značaj jer predstavlja okruženje u kojem *Internet Key Exchange* ostvaruje svoju punu funkcionalnost. Kriptografski algoritmi analizirani u prethodnom poglavlju dobijaju praktičnu vrednost tek kada postanu deo arhitekture koja omogućava njihovu koordinisanu primenu u zaštiti mrežne komunikacije. *Internet Key Exchange* upravo zbog toga ne predstavlja izolovan protokol za razmenu ključeva, već centralni upravljački mehanizam koji omogućava uspostavljanje, održavanje i obnovu digitalnog poverenja unutar IPsec sistema [2].

Analiza razvoja IPsec arhitekture potvrđuje da njeno nastajanje nije predstavljalo samo odgovor na potrebu za uvođenjem novih kriptografskih algoritama, već rezultat evolucije bezbednosne paradigme koja je bezbednost počela da posmatra kao integrisani proces. Projektovanjem modularne arhitekture koja povezuje bezbednosne politike, razmenu ključeva, *Security Association* mehanizme i zaštitu mrežnog saobraćaja uspostavljen je sistem sposoban da kontinuirano održava digitalno poverenje između komunikacionih učesnika. Upravo zbog toga IPsec predstavlja mnogo više od mrežnog protokola – IPsec predstavlja procesno organizovanu bezbednosnu arhitekturu u kojoj *Internet Key Exchange* ima centralnu ulogu u upravljanju životnim ciklusom digitalnog poverenja [53; RFC 2409].

3.2. Ipsec kao procesno organizovana bezbednosna arhitektura

3.2.1. Teorijska osnova procesnog pristupa ipsec arhitekturi

Savremeni informaciono-komunikacioni sistemi karakterišu visok stepen međusobne povezanosti, distribuirana obrada podataka i kontinuirana razmena informacija između velikog broja heterogenih mrežnih čvorova[16]. U takvom okruženju bezbednost se više ne može posmatrati kao statična osobina pojedinačnih protokola ili kriptografskih algoritama, već kao dinamičan proces koji obuhvata donošenje bezbednosnih odluka, upravljanje kriptografskim materijalom, autentifikaciju komunikacionih učesnika, zaštitu mrežnog saobraćaja i kontinuirano prilagođavanje promenama u operativnom okruženju. Upravo zbog toga IPsec arhitekturu nije metodološki opravdano analizirati kao skup međusobno nezavisnih komponenti, već kao integrisani proces čiji je osnovni cilj uspostavljanje i održavanje digitalnog poverenja. Tradicionalni pristup proučavanju IPsec-a najčešće podrazumeva zasebnu analizu njegovih sastavnih elemenata, kao što su *Authentication Header* (AH), *Encapsulating Security Payload* (ESP), *Security Association* (SA), *Security Policy Database* (SPD) i *Security Association Database* (SAD). Iako ovakav pristup omogućava detaljno razumevanje funkcionalnosti pojedinačnih mehanizama, on često ne prikazuje njihove međusobne zavisnosti niti objašnjava način na koji zajedničkim delovanjem ostvaruju bezbednosne ciljeve sistema. Posledično, analiza ostaje na nivou opisivanja arhitektonskih komponenti, bez sagledavanja procesa koji omogućava koordinisanu primenu svih komponenti sistema informacione bezbednosti [23].

3.2.2. Ipsec kao integrisani bezbednosni proces

Sa aspekta ovog istraživanja, IPsec predstavlja procesno organizovanu bezbednosnu arhitekturu u kojoj svaka komponenta učestvuje u jasno definisanoj fazi uspostavljanja, održavanja i obnove digitalnog poverenja. Proces započinje definisanjem bezbednosnih politika kojima se određuje način zaštite različitih kategorija mrežnog saobraćaja. Nakon toga sledi analiza komunikacionih zahteva i donošenje odluke da li je potrebno uspostaviti novu sigurnosnu asocijaciju (SA) ili koristiti postojeću. Ukoliko bezbednosna politika zahteva novu zaštićenu komunikaciju, primenom *Internet Key Exchange* protokola koji pregovara bezbednosne parametre, autentifikuje komunikacione strane i uspostavlja zajednički kriptografski materijal. Tek nakon uspešnog završetka ovog procesa moguće je formirati *Security Association* i primenom kriptografskih algoritama zaštititi korisnički mrežni saobraćaj. Proces zaštite se vrši primenom odgovarajućih IPsec mehanizama [77; SP 800-77 Rev. 1.].

Security Policy Database ne može ostvariti zaštitu bez pregovaranja bezbednosnih parametara. *Internet Key Exchange* ne može uspostaviti sigurnosnu asocijaciju bez prethodno definisanih politika bezbednosti. *Security Association* nema praktičnu funkciju ukoliko nije povezana sa bazom u kojoj se čuvaju njeni parametri, niti *Encapsulating Security Payload* može zaštititi podatke bez prethodno uspostavljenih kriptografskih ključeva. Stvarna bezbednost proizlazi iz njihove međusobne koordinacije, odnosno iz procesa koji povezuje sve navedene komponente u jedinstvenu funkcionalnu celinu IPsec-a [10].

3.2.3. Proces uspostavljanja digitalnog poverenja

Jedan od osnovnih doprinosa procesnog pristupa jeste mogućnost da se digitalno poverenje posmatra kao dinamička kategorija. Poverenje između komunikacionih učesnika ne nastaje automatski uspostavljanjem komunikacione veze, već prolazi kroz niz međusobno povezanih faza. Najpre se definišu bezbednosni zahtevi i na osnovu politike bezbednosti strana u komunikaciji se usaglašavaju mehanizmi kriptografske zaštite.

Nakon toga se vrši autentifikacija identiteta komunikacionih strana, razmena kriptografskih

ključeva i generisanje sigurnosnih asocijacija. U narednoj fazi ostvaruje se zaštita mrežnog saobraćaja, dok završne faze obuhvataju nadzor aktivnih sesija, periodičnu obnovu kriptografskog materijala i bezbedno upravljanje sigurnosnim asocijacijama (SA). Na taj način digitalno poverenje postaje proces koji traje tokom životnog ciklusa komunikacije.

Posebna vrednost ovakvog pristupa ogleda se u mogućnosti identifikovanja kritičnih tačaka procesa. Svaka faza predstavlja potencijalnu tačku bezbednosnog rizika. Nepravilno definisana bezbednosna politika može dovesti do neadekvatnog nivoa zaštite. Greške tokom autentifikacije mogu omogućiti neovlašćeni pristup. Slabosti u upravljanju *Security Association* mehanizmima mogu ugroziti kontinuitet bezbedne komunikacije, dok nedostatak periodične obnove kriptografskih ključeva povećava rizik od njihove kompromitacije. Procesna analiza omogućava sistematsko identifikovanje ovih tačaka i procenu njihovog uticaja na ukupnu otpornost/resizstentost na vektore napada usmerene ka informaciono-komunikacionom sistemu [23].

3.2.4. Bezbednosni značaj procesnog modela za internet key exchange

Posmatrano iz perspektive *Internet Key Exchange* protokola, procesni model IPsec arhitekture posebno dobija na značaju. *Internet Key Exchange* nije samo mehanizam za razmenu kriptografskih ključeva, već centralni koordinacioni proces koji povezuje bezbednosne politike, autentifikaciju, upravljanje *Security Association* mehanizmima i zaštitu mrežnog saobraćaja. Njegova funkcija nije ograničena na početnu razmenu ključeva, već obuhvata kontinuirano održavanje digitalnog poverenja kroz obnovu sesijskih ključeva, pregovaranje novih sigurnosnih asocijacija i prilagođavanje promenama u bezbednosnom okruženju. Ovakav pristup potvrđuje da se bezbednosne karakteristike IKE protokola mogu objektivno procenjivati jedino u kontekstu celokupne IPsec arhitekture[2].

Savremena literatura uglavnom analizira IPsec kroz funkcionalnu klasifikaciju protokola, log datoteka pristupa korisnika informaciono-komunikacionog sistema i baza podataka (za koje je neophodno formulisati stepen tajnosti). Takav pristup je neophodan za razumevanje pojedinačnih komponenti, ali nije dovoljan za razumevanje njihovog zajedničkog delovanja. Procesni model omogućava prelazak sa statičke analize komponenti na analizu njihove međusobne interakcije tokom čitavog životnog ciklusa bezbedne komunikacije. Time se otvara mogućnost preciznijeg identifikovanja uzročno-posledičnih veza između bezbednosnih politika, upravljanja kriptografskim ključevima, uspostavljanja *Security Association* mehanizama i zaštite mrežnog saobraćaja. Upravo ovakav metodološki pristup predstavlja jednu od osnovnih istraživačkih vrednosti ove magistarske teze.

Analiza IPsec arhitekture iz procesne perspektive pokazuje da bezbednost ne proizlazi iz pojedinačnih protokola ili algoritama, već iz koordinisanog rada svih komponenti sistema koje učestvuju u procesu uspostavljanja i održavanja digitalnog poverenja. Bezbednosne politike, *Internet Key Exchange*, *Security Association*, baze bezbednosnih parametara i mehanizmi zaštite mrežnog saobraćaja predstavljaju međusobno povezane faze jedinstvenog bezbednosnog procesa. Posmatranje IPsec-a kao procesno organizovane bezbednosne arhitekture omogućava potpunije razumevanje uloge IPsec-a u zaštiti informaciono-komunikacionih sistema i predstavlja metodološku osnovu za detaljnu analizu njegovih pojedinačnih komponenti u nastavku ovog poglavlja.

3.3. Security policy database (spd) kao polazna tačka procesa uspostavljanja digitalnog poverenja

3.3.1. Teorijska osnova security policy database

Savremena arhitektura IPsec protokola zasniva se na pretpostavci da bezbedna komunikacija ne može biti rezultat isključivo primene kriptografskih algoritama, već mora predstavljati posledicu unapred definisanih bezbednosnih pravila (*formulisanih u politici bezbednosti i primenom opšteprihvaćenih standardizovanih procedura koje su pokazale rezultate kao primeri najbolje prakse*) koja određuju način zaštite mrežnog saobraćaja. U tom kontekstu *Security Policy Database* (SPD) predstavlja jedan od osnovnih elemenata IPsec arhitekture, budući da definiše skup bezbednosnih politika kojima se određuje način obrade svakog mrežnog paketa pre nego što započne proces njegove zaštite. Posmatrano iz funkcionalne perspektive, SPD predstavlja centralni mehanizam donošenja bezbednosnih odluka kojim se uspostavlja veza između poslovnih bezbednosnih zahteva i njihove tehničke implementacije u okviru IPsec sistema [2].

U kontekstu informacione bezbednosti i bezbednosnih nauka, *Security Policy Database* se opisuje kao skup pravila koja određuje da li će određeni mrežni saobraćaj biti zaštićen primenom IPsec mehanizama, prosleđen bez zaštite ili odbačen. Međutim, ovakav opis predstavlja samo funkcionalni prikaz njene uloge. Sa aspekta ovog istraživanja, SPD se posmatra kao početna faza procesa uspostavljanja digitalnog poverenja, budući da upravo u okviru bezbednosnih politika nastaje odluka da li određena komunikacija zahteva kriptografsku zaštitu i pod kojim uslovima će ona biti realizovana [77; SP 800-77 Rev. 1.].

3.3.2. Security policy database kao proces donošenja bezbednosnih odluka

Procesni pristup omogućava da se *Security Policy Database* analizira kao dinamički mehanizam odlučivanja, a ne kao pasivna baza konfiguracionih podataka. Svaki pokušaj uspostavljanja komunikacije predstavlja ulazni događaj koji pokreće proces procene definisanih bezbednosnih pravila. Na osnovu unapred definisanih selektora, kao što su izvorna i odredišna IP adresa, transportni protokol, broj porta ili druge karakteristike komunikacije, sistem određuje odgovarajući način obrade mrežnog saobraćaja [57; RFC 4301].

Ovakav pristup predstavlja prvu fazu procesa uspostavljanja digitalnog poverenja. Ukoliko bezbednosna politika zahteva zaštitu komunikacije, pokreće se naredna faza procesa koja podrazumeva aktiviranje *Internet Key Exchange* protokola radi pregovaranja bezbednosnih parametara i uspostavljanja odgovarajuće *Security Association*. Ukoliko zaštita nije predviđena definisanom politikom, komunikacija se odvija bez aktiviranja IPsec mehanizama ili se u potpunosti odbacuje. Time *Security Policy Database* postaje mehanizam koji određuje da li će proces uspostavljanja digitalnog poverenja uopšte biti pokrenut [31].

3.3.3. Bezbednosni značaj security policy database

Kvalitet definisanih bezbednosnih politika neposredno određuje nivo zaštite informaciono-komunikacionog sistema. Neadekvatno definisana pravila mogu omogućiti prenos osetljivih podataka bez kriptografske zaštite, izazvati neuspešno pregovaranje *Security Association* ili dovesti do nepotrebnog opterećenja mrežnih resursa primenom zaštite tamo gde ona nije potrebna. Posledično, bezbednosne politike predstavljaju jedan od ključnih faktora koji određuju ukupnu otpornost IPsec arhitekture. Sa bezbednosnog aspekta, značaj *Security Policy Database* daleko prevazilazi kontekst informacione bezbednosti i ima ulogu u klasifikaciji i kriptografskoj zaštiti mrežnog saobraćaja.

Posebnu pažnju zaslužuje činjenica da Security Policy Database predstavlja mesto na kojem se tehničke konfiguracije neposredno povezuju sa organizacionim bezbednosnim zahtevima. Poslovna pravila, regulatorni zahtevi, klasifikacija podataka i procena rizika transformišu se u konkretna pravila koja određuju način zaštite mrežnog saobraćaja. Na taj način SPD predstavlja vezu između strateškog upravljanja bezbednošću i operativnog funkcionisanja IPsec sistema [27].

3.3.4. Implementacioni i konfiguracioni izazovi

Efikasnost *Security Policy Database* u velikoj meri zavisi od implementacije i pravilne konfiguracije. Definisanje bezbednosnih politika zahteva preciznu identifikaciju komunikacionih tokova, pravilnu klasifikaciju stepena tajnosti podataka i odgovarajuću procenu bezbednosnih rizika i analizu vektora napada. Preteviše restriktivne politike bezbednosti mogu prouzrokovati prekid legitimne komunikacije i smanjiti raspoloživost sistema, dok previše liberalna pravila mogu omogućiti zaobilazanje mehanizama kriptografske zaštite. Zbog toga konfiguracija *Security Policy Database* predstavlja kontinuirani proces koji mora pratiti promene u informaciono-komunikacionom okruženju, poslovnim zahtevima organizacije, značaj za zaštitu nacionalne bezbednosti i aktuelnim bezbednosnim pretnjama (*neophodnost analize geopolitičkih i geostrateških aspekata informacione bezbednosti u konkretnom slučaju primenom adekvatne metodologije*) [24].

Savremeni informaciono-komunikacioni sistemi dodatno usložnjavaju ovaj proces zbog dinamičkih *cloud* okruženja, virtualizovanih mrežnih funkcija, mobilnih korisnika i distribuiranih servisa. U takvim uslovima bezbednosne politike moraju biti dovoljno fleksibilne da omoguće prilagođavanje promenama, ali istovremeno dovoljno restriktivne da očuvaju projektovani nivo zaštite. Ovakav balans predstavlja jedan od najvažnijih izazova savremenog upravljanja IPsec arhitekturom [28],[93; BSI TR-02102-3].

3.3.5. Procesni značaj security policy database u ipsec arhitekturi

Posmatrano kroz procesni model razvijen u ovom radu, *Security Policy Database* predstavlja početnu tačku čitavog procesa uspostavljanja digitalnog poverenja. Upravo u ovoj fazi donosi se odluka da li određena komunikacija zahteva zaštitu, koji će bezbednosni mehanizmi biti primenjeni i da li će biti pokrenut *Internet Key Exchange* protokol. Sve naredne faze procesa – autentifikacija, razmena kriptografskih ključeva, uspostavljanje *Security Association*, zaštita mrežnog saobraćaja i periodična obnova bezbednosnih parametara – neposredno zavise od odluka donetih u okviru *Security Policy Database*. Na taj način SPD ne predstavlja samo konfiguracionu bazu podataka, već prvi korak u procesu izgradnje digitalnog poverenja. Njena funkcija nije ograničena na definisanje pravila, već obuhvata iniciranje celokupnog bezbednosnog procesa kojim se ostvaruje zaštita mrežne komunikacije [2].

Analiza dostupne stručne i naučne literature pokazuje da se *Security Policy Database* najčešće opisuje kroz njenu tehničku strukturu i funkcionalne karakteristike. Takav pristup omogućava razumevanje načina rada ovog mehanizma, ali ne objašnjava njegov značaj u ukupnoj bezbednosnoj arhitekturi IPsec sistema. Procesni model razvijen u ovom radu omogućava proširenje tradicionalnog pristupa posmatranjem *Security Policy Database* kao centralnog mehanizma donošenja bezbednosnih odluka kojim započinje proces uspostavljanja digitalnog poverenja. Na taj način se uspostavlja jasna uzročno-posledična veza između definisanih bezbednosnih politika, *Internet Key Exchange* protokola i zaštite mrežnog saobraćaja. *Security Policy Database* predstavlja mnogo više od baze bezbednosnih pravila. Ona predstavlja početnu fazu procesa uspostavljanja digitalnog poverenja u okviru IPsec arhitekture. Definisanjem bezbednosnih politika određuje se način zaštite mrežnog saobraćaja, inicira se rad *Internet Key Exchange* protokola i stvaraju uslovi za uspostavljanje *Security*

Association mehanizama. Posmatranje SPD kroz procesni model omogućava potpunije razumevanje njegove uloge u bezbednosnoj arhitekturi IPsec sistema i potvrđuje osnovnu tezu ovog rada da se bezbednost *Internet Key Exchange* protokola može objektivno analizirati jedino kroz integrisanu analizu svih faza procesa uspostavljanja, održavanja i obnove digitalnog poverenja [29].

3.4. Internet key exchange kao centralni procesni mehanizam ipsec arhitekture

3.4.1. Teorijska osnova uloge internet key exchange protokola

Analiza savremene IPsec arhitekture pokazuje da bezbednost mrežne komunikacije ne zavisi isključivo od bezbednosnih karakteristika primenjenih kriptografskih algoritama (*sa napomenom da je neophodan prijelaz na kriptografske algoritme koji prema specifikaciji štite od kriptoolitičkih napada primenom kvantnih računara i u okviru IPSec je već uspostavljen vremenski okvir za takvo unapređenje zaštite informaciono-komunikacionih sistema*), već od sposobnosti sistema da na pouzdan, standardizovan i dinamičan način uspostavi, održava i obnavlja međusobno poverenje između komunikacionih učesnika. Upravo u tom kontekstu *Internet Key Exchange* (IKE) predstavlja centralni procesni mehanizam IPsec arhitekture. Njegova osnovna funkcija nije ograničena na razmenu kriptografskih ključeva, već obuhvata koordinaciju svih aktivnosti koje prethode uspostavljanju zaštićene komunikacije i omogućavaju njeno bezbedno održavanje tokom čitavog životnog ciklusa.

Tradicionalni prikaz IKE protokola najčešće ga definiše kao protokol za pregovaranje Security Association parametara i razmenu kriptografskih ključeva. Takvo određenje jeste tačno, ali ne obuhvata njegov stvarni značaj u okviru IPsec arhitekture. Posmatrano iz perspektive ovog istraživanja, Internet Key Exchange predstavlja centralni upravljački proces koji povezuje bezbednosne politike, autentifikaciju komunikacionih učesnika, razmenu kriptografskog materijala, uspostavljanje Security Association mehanizama i njihovo kontinuirano održavanje. Na taj način IKE postaje ključni element procesa uspostavljanja digitalnog poverenja [92; BSI TR-02102-1],[93; BSI TR-02102-3].

3.4.2. Internet key exchange kao procesna veza između bezbednosne politike i zaštićene komunikacije

U prethodnom potpoglavlju pokazano je da *Security Policy Database* predstavlja početnu tačku procesa donošenja bezbednosnih odluka. Međutim, definisana bezbednosna politika sama po sebi ne može obezbediti zaštitu mrežnog saobraćaja. Potrebno je uspostaviti mehanizam koji će definisane bezbednosne zahteve pretvoriti u konkretne kriptografske parametre i operativne bezbednosne odnose između komunikacionih učesnika. Upravo tu funkciju ostvaruje *Internet Key Exchange*. Nakon što *Security Policy Database* utvrdi da određeni komunikacioni tok zahteva zaštitu primenom IPsec mehanizama, *Internet Key Exchange* pokreće proces pregovaranja između strana koje imaju za cilj uspostavljanje kriptografski zaštićene komunikacije. Tokom ovog procesa usaglašavaju se kriptografski algoritmi, autentifikacioni mehanizmi, *Diffie–Hellman* ili *Elliptic Curve Diffie–Hellman* parametri, funkcije za izvođenje ključeva, vremensko trajanje Security Association i drugi bezbednosni elementi neophodni za uspostavljanje zaštićene komunikacije. Time IKE predstavlja vezu i operacionalizaciju između definisanih bezbednosnih politika i njihove praktične realizacije [60; RFC 3526.].

3.4.3. Uloga internet key exchange u procesu uspostavljanja digitalnog poverenja

Procesni model razvijen u ovom radu omogućava da se *Internet Key Exchange* posmatra kao centralna faza procesa uspostavljanja digitalnog poverenja. Dok *Security Policy Database* određuje potrebu za zaštitom komunikacije, *Internet Key Exchange* omogućava da komunikacione strane potvrde svoj identitet, usaglasе bezbednosne parametre i zajednički uspostave kriptografski materijal koji će biti korišćen tokom komunikacije.

Posebna vrednost ovog pristupa ogleda se u činjenici da poverenje nije unapred zadato, niti proizlazi isključivo iz posjedovanja odgovarajućih kriptografskih ključeva. Proces uspostavljanja poverenja nastaje kao rezultat jasno definisanog procesa pregovaranja, autentifikacije i zajedničkog donošenja bezbednosnih odluka (*odabirom skupa kriptografskih algoritama koji je otporan na kriptoolizmu i podržanih politikama bezbednosti strana koje uspostavljaju kriptografski zaštićenu komunikaciju*). Na taj način digitalno poverenje predstavlja dinamičku kategoriju koja se kontinuirano uspostavlja, proverava i obnavlja tokom trajanja komunikacije [38].

3.4.4. Implementacioni i konfiguracioni izazovi

Efikasnost *Internet Key Exchange* protokola neposredno zavisi od kvaliteta implementacije i pravilne konfiguracije. Neadekvatno definisani kriptografski algoritmi, upotreba zastarelih *Diffie–Hellman* grupa, nepravilna konfiguracija autentifikacionih mehanizama ili neodgovarajuće upravljanje *Security Association* parametrima mogu značajno umanjiti bezbednosne karakteristike čitavog IPsec sistema. Zbog toga konfiguracija IKE protokola predstavlja jedan od najosetljivijih elemenata ukupne bezbednosne arhitekture.

Dodatni izazov predstavlja potreba za očuvanjem interoperabilnosti između različitih implementacija IPsec sistema. *Internet Key Exchange* mora omogućiti uspešno pregovaranje između uređaja različitih proizvođača, pri čemu istovremeno mora očuvati visok nivo bezbednosti i otpornosti na savremene napade. Ovakvi zahtevi potvrđuju da se bezbednost IKE protokola ne može posmatrati odvojeno od njegove implementacije i operativnog okruženja [42].

3.4.5. Procesni značaj internet key exchange u ipsec arhitekturi

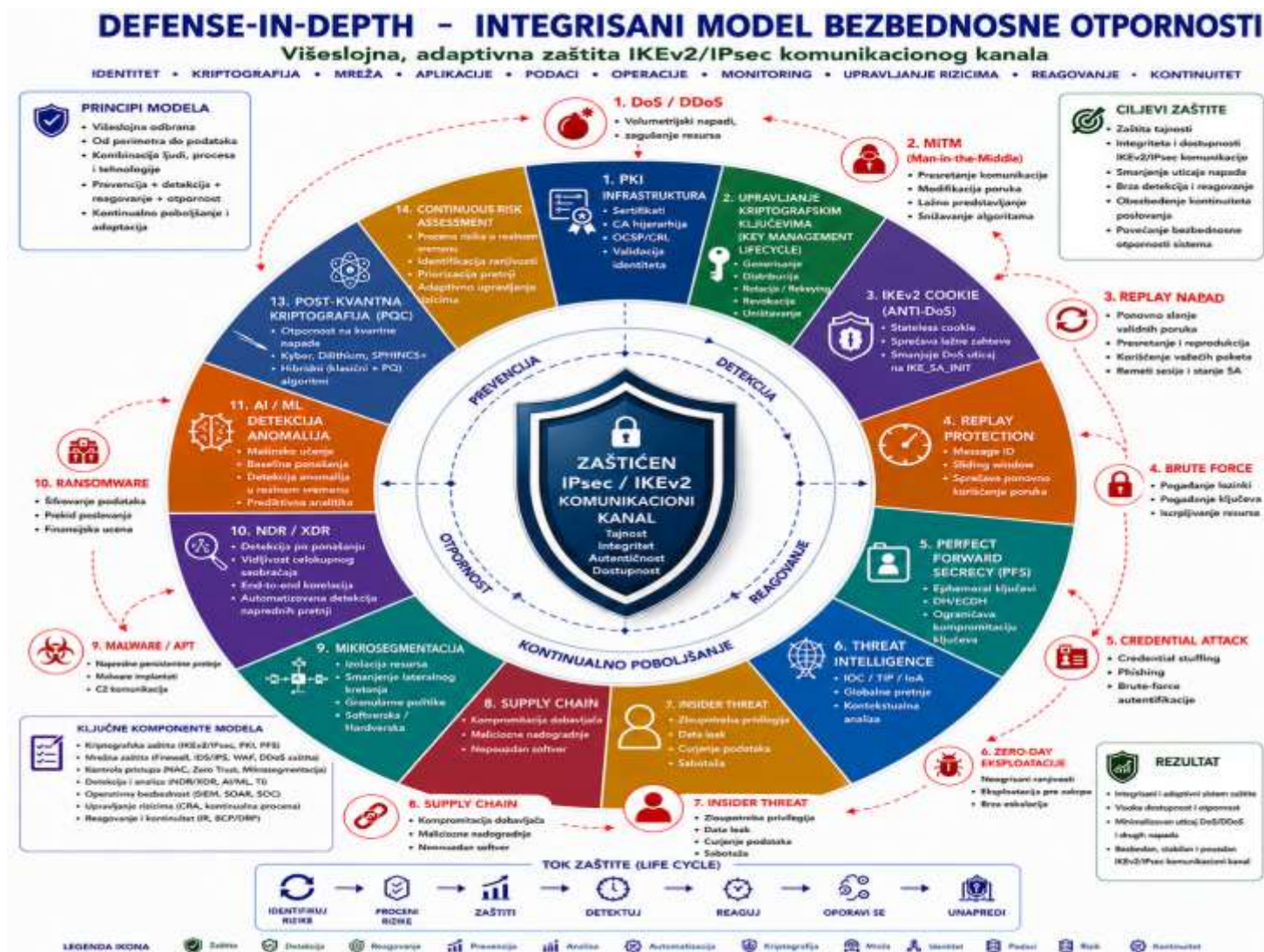
Posmatrano kroz procesni model razvijen u ovom istraživanju, *Internet Key Exchange* predstavlja centralnu koordinacionu tačku celokupne IPsec arhitekture. On povezuje rezultate procesa donošenja bezbednosnih odluka sa praktičnom realizacijom zaštićene komunikacije. Nakon što *Security Policy Database* definiše potrebu za zaštitom određenog komunikacionog toka, *Internet Key Exchange* preuzima upravljanje procesom autentifikacije, razmene kriptografskih ključeva, uspostavljanja *Security Association* i pripreme sistema za bezbedan prenos podataka. Sve naredne faze zaštite mrežnog saobraćaja neposredno zavise od uspešnosti ovog procesa [2].

Posebno je značajno istaći da funkcija *Internet Key Exchange* ne prestaje uspostavljanjem prve *Security Association*. Tokom čitavog trajanja komunikacije IKE učestvuje u obnovi bezbednosnih parametara, ponovnom pregovaranju *Security Association*, rotaciji ključeva i prilagođavanju promenama u bezbednosnom okruženju. Na taj način *Internet Key Exchange* postaje mehanizam koji omogućava kontinuitet digitalnog poverenja.

Savremena stručna literatura najčešće naglašava kriptografske funkcije *Internet Key Exchange* protokola. Međutim, takav pristup ne prikazuje njegovu centralnu ulogu u koordinaciji svih bezbednosnih procesa unutar IPsec arhitekture. Procesna analiza razvijena naučno-

istraživačkim radom u okviru ove magistarske teze pokazuje da *Internet Key Exchange* predstavlja mnogo više od protokola za razmenu ključeva. IKE koordinira međusobno povezane aktivnosti koje obuhvataju donošenje bezbednosnih odluka, autentifikaciju, upravljanje kriptografskim materijalom, uspostavljanje i održavanje *Security Association* mehanizama i očuvanje kontinuiteta bezbedne komunikacije. Upravo ovakav pristup omogućava objektivnije razumevanje njegovog stvarnog značaja u savremenim informaciono-komunikacionim sistemima [53; RFC 2409].

U cilju sistematizacije višeslojnih mehanizama zaštite IKE/IPsec komunikacionog kanala, u nastavku je prikazan integrisani model bezbednosne otpornosti zasnovan na konceptu odbrane u dubinu (*Defense-in-Depth*). Model objedinjuje četrnaest bezbednosnih domena sa pripadajućim kategorijama pretnji, ciljevima zaštite i fazama upravljanja rizikom u okviru jedinstvene analitičke celine.



Slika 3. Konceptualni prikaz adaptivnog *Defense-in-Depth* modela zaštite IKEv2/IPsec protokola, sa pripadajućim vektorima napada i kontrolnim mehanizmima

Kao što se vidi na slici, model je strukturiran oko centralnog cilja zaštite — poverljivosti, integriteta, autentičnosti i dostupnosti IKEv2/IPsec komunikacije — dok su četrnaest bezbednosnih domena raspoređeni po principu prevencije, detekcije, reagovanja i kontinuiranog poboljšanja. Svakom domenu je pridružena odgovarajuća kategorija pretnji (od DoS/DDoS napada do ROP/BYOVd vektora napada), čime se uspostavlja direktna veza između konkretnog vektora napada i bezbednosnih mehanizama zaštite(mehanizmi zaštite treba da poseduju komplementarnost i koordinisan rad u slučaju bezbednosnog incidenta).

Internet Key Exchange predstavlja centralni procesni mehanizam IPsec arhitekture koji povezuje bezbednosne politike sa praktičnom realizacijom zaštićene mrežne komunikacije. Njegova uloga prevazilazi razmenu kriptografskih ključeva i obuhvata koordinaciju svih aktivnosti neophodnih za uspostavljanje, održavanje i obnovu digitalnog poverenja između komunikacionih učesnika. Detaljna višekriterijumska i multidisciplinarna analiza *Internet Key Exchange* protokola kroz primenu procesnog pristupa omogućava bolje razumevanje arhitekture IKE protokola, bezbednosnih mehanizama u okviru protokola i predstavlja osnov za analizu značaja i pravilnog specificiranja kriterijuma uspostavljanja *Security Association* mehanizma kao sledeće faze procesa praktične realizacije digitalnog poverenja u okviru IPsec sistema. *Security Association* nije skup tehničkih parametara, već operativna realizacija digitalnog poverenja koje je uspostavljeno putem *Internet Key Exchange* protokola [2].

3.5. Security association (sa) kao operativna realizacija digitalnog poverenja u ipsec arhitekturi

3.5.1. Teorijska osnova security association mehanizma

Savremena arhitektura IPsec protokola zasniva se na principu da bezbedna komunikacija može biti ostvarena tek nakon što učesnici usaglasе zajedničke bezbednosne parametre koji će biti korišćeni tokom prenosa podataka. Rezultat ovog procesa predstavlja ***Security Association (SA)***, koja definiše skup kriptografskih i operativnih parametara neophodnih za zaštitu konkretnog komunikacionog toka. U tradicionalnoj stručnoj literaturi *Security Association* najčešće se definiše kao logička jednosmerna veza koja sadrži informacije o algoritmima, kriptografskim ključevima, identifikatorima, vremenu važenja i drugim parametrima potrebnim za funkcionisanje IPsec mehanizama. Međutim, takav pristup predstavlja prvenstveno tehnički opis, koji ne objašnjava njen stvarni značaj u ukupnoj bezbednosnoj arhitekturi [77; SP 800-77 Rev. 1.].

Sa aspekta ovog naučnog istraživanja, *Security Association* predstavlja mnogo više od skupa konfiguracionih parametara. SA predstavlja operativnu i praktičnu realizaciju digitalnog poverenja koje je prethodno uspostavljeno kroz proces pregovaranja *Internet Key Exchange* protokola. Tek nakon uspešno završene autentifikacije, razmene kriptografskih ključeva i usaglašavanja bezbednosnih politika moguće je formirati *Security Association*, čime digitalno poverenje dobija svoju konkretnu operativnu formu [15].

3.5.2. Security association kao rezultat procesa uspostavljanja digitalnog poverenja

Procesni model razvijen u ovom radu omogućava da se *Security Association* posmatra kao logičan rezultat svih prethodnih faza procesa uspostavljanja digitalnog poverenja. *Security Policy Database* određuje potrebu za zaštitom komunikacije. *Internet Key Exchange* pregovara bezbednosne parametre, potvrđuje identitet komunikacionih učesnika i omogućava zajedničko generisanje kriptografskog materijala. *Security Association* predstavlja završni rezultat ovog procesa, budući da objedinjuje sve prethodno usaglašene elemente u jedinstven operativni bezbednosni kontekst [2], [53; RFC 2409].

Na taj način *Security Association* ne nastaje automatski niti predstavlja statičan skup podataka. Njeno formiranje predstavlja završetak procesa izgradnje međusobnog poverenja između komunikacionih strana. Svaka aktivna *Security Association* potvrđuje da su komunikacioni učesnici uspešno završili proces autentifikacije, usaglasili bezbednosne politike i prihvatili zajedničke kriptografske parametre koji omogućavaju bezbedan prenos podataka [2].

3.5.3. Značaj (sa) security association

Posmatrano iz perspektive IPsec arhitekture, *Security Association* predstavlja centralnu vezu između procesa pregovaranja bezbednosnih parametara i procesa zaštite mrežnog saobraćaja. Dok *Internet Key Exchange* upravlja uspostavljanjem poverenja, upravo *Security Association* omogućava njegovu praktičnu primenu. Svi mehanizmi zaštite koje ostvaruju *Authentication Header* i *Encapsulating Security Payload* koriste parametre definisane u okviru odgovarajuće *Security Association*. Zbog toga se može zaključiti da bez aktivne *Security Association* nije moguće ostvariti nijednu od osnovnih bezbednosnih funkcija IPsec sistema [10].

Poseban značaj *Security Association* ogleda se u njenoj ulozi u razdvajanju procesa pregovaranja od procesa zaštite podataka. Pregovaranje bezbednosnih parametara predstavlja složen i računski zahtevan proces koji se realizuje prema specificiranim okolnostima (*vreme trajanja konekcije ili količina podataka u prenosu*) nakon toga dolazi do obnove parametara kriptografski zaštićene sesije, dok se zaštita mrežnog saobraćaja odvija kontinuirano. Formiranjem *Security Association* omogućava se da se jednom uspostavljeni bezbednosni parametri koriste tokom trajanja komunikacione sesije bez potrebe za ponavljanjem kompletnog procesa pregovaranja pri svakom prenosu podataka [15].

3.5.4. Životni ciklus security association

Jedna od najvažnijih karakteristika *Security Association* jeste njen dinamički životni ciklus. Za razliku od statičkih konfiguracionih elemenata, *Security Association* prolazi kroz jasno definisane faze: inicijalno uspostavljanje, aktivnu upotrebu, periodično obnavljanje (*rekeying*), zamenu novom *Security Association* i konačno bezbedno uklanjanje nakon isteka perioda važenja. Ovakav pristup omogućava očuvanje kontinuiteta digitalnog poverenja uz istovremeno ograničavanje vremena upotrebe pojedinačnih kriptografskih ključeva [2].

Posebno je značajno istaći da životni ciklus *Security Association* neposredno prati životni ciklus kriptografskih ključeva analiziran u prethodnom poglavlju. Na taj način se potvrđuje metodološka povezanost između teorijsko-kriptografskih osnova razmene ključeva i njihove praktične implementacije u okviru IPsec arhitekture. *Security Association* predstavlja operativni okvir u kojem se realizuje upravljanje kriptografskim materijalom tokom čitavog trajanja komunikacione sesije [38].

Efikasnost *Security Association* mehanizma zavisi od pravilnog upravljanja njenim parametrima tokom čitavog životnog ciklusa. Neadekvatno definisano vreme trajanja *Security Association*, nepravilna sinhronizacija između komunikacionih učesnika ili neblagovremena obnova bezbednosnih parametara mogu dovesti do prekida komunikacije ili smanjenja nivoa zaštite tj. do kompromitacije tajnosti komunikacije. Pored toga, kompromitacija procesa upravljanja *Security Association* može omogućiti napadaču da ugrozi bezbednost komunikacije bez direktnog kompromitovanja osnovnih kriptografskih algoritama. Ovakve okolnosti potvrđuju da ukupna otpornost IPsec sistema zavisi podjednako od kvaliteta upravljanja *Security Association* kao i od matematičke otpornosti primenjenih algoritama.

U okviru procesnog modela razvijenog u ovom radu, *Security Association* predstavlja fazu u kojoj digitalno poverenje prelazi iz logičkog u operativni oblik. Dok su prethodne faze procesa

bile usmerene na pregovaranje, autentifikaciju i generisanje zajedničkog kriptografskog materijala, *Security Association* omogućava da rezultati tih aktivnosti budu neposredno primenjeni u zaštiti mrežnog saobraćaja. Na taj način ona predstavlja centralnu operativnu tačku celokupne IPsec arhitekture i neophodan preduslov za funkcionisanje svih narednih bezbednosnih mehanizama [2].

Analiza savremene literature pokazuje da se *Security Association* pretežno opisuje kao tehnički mehanizam koji definiše parametre potrebne za zaštitu mrežnog saobraćaja. Takav pristup pruža važne informacije o njenoj strukturi, ali ne prikazuje njenu ulogu u ukupnom procesu uspostavljanja digitalnog poverenja. Procesna analiza sprovedena u ovom radu omogućava drugačije metodološko tumačenje. *Security Association* se ne posmatra kao pasivni skup parametara, već kao operativna realizacija poverenja koje je uspostavljeno između učesnika u komunikaciji. Time se uspostavlja jasna uzročno-posledična veza između bezbednosnih politika, rada *Internet Key Exchange* protokola i praktične zaštite mrežnog saobraćaja [44].

Security Association predstavlja centralni operativni element IPsec arhitekture u kojem se materijalizuje digitalno poverenje uspostavljeno tokom procesa pregovaranja *Internet Key Exchange* protokola. Njena funkcija prevazilazi čuvanje tehničkih parametara, budući da omogućava praktičnu realizaciju svih bezbednosnih odluka donetih tokom prethodnih faza procesa. Analizom procesa uspostavljanja *Security Association* kao operativne realizacije digitalnog poverenja potvrđuje se osnovna teza ovog rada da bezbednost *Internet Key Exchange* protokola proizlazi iz koordinisanog delovanja bezbednosnih politika, kriptografskih mehanizama, procesa pregovaranja i upravljanja životnim ciklusom *Security Association*. Upravo ovakav procesni pristup omogućava potpunije razumevanje funkcionisanja IPsec arhitekture i predstavlja osnov za analizu narednog mehanizma – ***Security Association Database (SAD)***, koja omogućava upravljanje aktivnim stanjem uspostavljenog digitalnog poverenja [2].

3.6. Security association database (sad) kao mehanizam upravljanja aktivnim stanjem digitalnog poverenja

3.6.1. Teorijska osnova security association database

Bezbedna mrežna komunikacija ne završava se uspostavljanjem *Security Association*. Naprotiv, trenutkom formiranja *Security Association* započinje nova faza bezbednosnog procesa koja podrazumeva kontinuirano upravljanje svim parametrima neophodnim za održavanje zaštićene komunikacije. U okviru IPsec arhitekture ovu funkciju ostvaruje ***Security Association Database (SAD)***, koja predstavlja centralni mehanizam za upravljanje aktivnim sigurnosnim asocijacijama i njihovim operativnim stanjem [56; RFC 9395], [65; RFC 8247].

U stručnoj literaturi *Security Association Database* opisuje se kao baza podataka u kojoj se čuvaju informacije o svim aktivnim *Security Association*. Takvo određenje obuhvata njenu tehničku funkciju, ali ne prikazuje njen stvarni značaj u okviru celokupne IPsec arhitekture. Sa aspekta naučno-istraživačkog rada u okviru ove magistarske teze, *Security Association Database* predstavlja dinamički mehanizam upravljanja aktivnim stanjem digitalnog poverenja, budući da omogućava kontrolu, održavanje i ažuriranje svih bezbednosnih parametara tokom trajanja komunikacione sesije [2].

3.6.2. Security association database kao operativni mehanizam upravljanja poverenjem

Procesni model razvijen u ovom radu polazi od pretpostavke da digitalno poverenje nije statična kategorija. Nakon uspešno uspostavljene *Security Association* neophodno je obezbediti da svi njeni parametri ostanu dostupni, konzistentni i sinhronizovani tokom čitavog trajanja komunikacije. Upravo ovu funkciju ostvaruje *Security Association Database* [2].

SAD omogućava čuvanje i upravljanje informacijama koje određuju način zaštite konkretnog komunikacionog toka. Među informacijama se nalaze identifikatori *Security Association*, primenjeni kriptografski algoritmi, izvedeni sesijski ključevi, parametri autentifikacije, vremenski period važenja sigurnosne asocijacije, brojači sekvenci i drugi elementi neophodni za pravilno funkcionisanje IPsec mehanizama. Međutim, značaj SAD nije u samom skladištenju ovih podataka, već u činjenici da omogućava njihovu operativnu upotrebu tokom svake faze zaštićene komunikacije [87; FIPS 140-3].

3.6.3. Uloga security association database

Analizirano sa aspekta arhitekture IPSec-a, *Security Association Database* predstavlja vezu između procesa uspostavljanja *Security Association* i procesa zaštite mrežnog saobraćaja (realizacije kriptozastite). Nakon što *Internet Key Exchange* uspešno završi pregovaranje i uspostavi *Security Association*, svi relevantni bezbednosni parametri prenose se u *Security Association Database*. Od tog trenutka *Authentication Header* i *Encapsulating Security Payload* koriste informacije iz SAD prilikom zaštite svakog pojedinačnog IP paketa.

Na ovaj način *Security Association Database* postaje centralna operativna komponenta IPsec arhitekture. Ona obezbeđuje da svi mehanizmi zaštite koriste specificirane (*na osnovu politika bezbednosti*) i međusobno usklađene bezbednosne parametre, čime se ostvaruje konzistentnost zaštite tokom čitavog trajanja komunikacije. Bez ovakvog mehanizma kontinuirano korišćenje *Security Association* bilo bi praktično neizvodljivo realizovati iz više razloga (*primer je duže vreme korišćenje istog kriptografskog ključa zbog činjenice da se napadaču koji prisluskuje mrežni saobraćaj daje velika količina podataka koji jesu u kriptografski zaštićenoj formi ali neminovno dovode do nižeg stepena zaštite IKT sistema jer kriptoo analizom može da se dođe do "otvorenog teksta"*) [85; SP 800-57 Part 1 Rev. 5].

Dijagram predstavlja konceptualni model izrađen za potrebe istraživanja, zasnovan na sistematskoj analizi relevantnih RFC dokumenata (RFC 2401, RFC 2408, RFC 2409 i pratećih specifikacija), relevantne stručne literature i rezultata sprovedene integrativne procesno-strukturne analize IKEv1 protokola. Model objedinjuje deset ključnih dimenzija arhitekture protokola, objedinjuje regulatorni okvir, modalitete uspostavljanja *Security Association* i kriptografskih mehanizama, pa sve do životnog ciklusa SA i sumarnih bezbednosnih karakteristika i ima ilustrativno-metodološku funkciju, sa ciljem sistematizovanog prikaza logičkih odnosa između funkcionalnih komponenti protokola i njihove međusobne uslovljenosti. (Prilog "A" u radu).

Sa bezbednosnog aspekta, SAD predstavlja veoma važnu komponentu sistema informacione bezbednosti. Integritet SAD direktno određuje bezbednost celokupne IPsec komunikacije jer sadrži simetrične ključeve za enkripciju i autentifikaciju u otvorenom (ili minimalno zaštićenom) obliku unutar operativne memorije kernela ili IPsec modula. Iz tog razloga, kontrola pristupa SAD-u mora biti strogo ograničena isključivo na IPsec podsistem, uz onemogućavanje bilo kakvog neovlašćenog čitanja ili izmene zapisa od strane drugih procesa. Ova karakteristika direktno korespondira sa bezbednosnim izazovima analiziranim u poglavlju posvećenom savremenim vektorima napada na IKE infrastrukturu – tehnike poput ROP (Return-Oriented Programming) i BYOVD (Bring Your Own Vulnerable Driver) eksploatacije koji ciljaju memorijski prostor kernela i privilegovane drajvere kako bi zaobišle kontrolu pristupa i izvršile čitanje ili manipulaciju SAD zapisa, čime bi se kompromitovali aktivni kriptografski ključevi bez potrebe za razbijanjem samog kriptografskog algoritma. Ova činjenica potvrđuje da robusnost IKE/IPsec infrastrukture ne zavisi isključivo od jačine primenjenih kriptografskih primitiva, već u jednakoj meri i od bezbednosti operativnog okruženja u kojem se SAD nalazi.

3.6.4. Životni ciklus digitalnog poverenja

Jedna od osnovnih karakteristika *Security Association Database* jeste njena uloga u upravljanju životnim ciklusom aktivnog digitalnog poverenja. Tokom trajanja komunikacione sesije bezbednosni parametri nisu nepromenljivi. Vreme važenja *Security Association* se približava isteku, dolazi do rotacije ključeva, pokreću se novi procesi pregovaranja, a pojedine sigurnosne asocijacije bivaju zamenjene novim. *Security Association Database* omogućava da se sve ove promene realizuju kontrolisano i bez narušavanja kontinuiteta bezbedne komunikacije [2]. Poseban značaj ima upravljanje prelaskom između stare i nove *Security Association* tokom procesa *rekeying*-a. U tom periodu sistem mora obezbediti istovremeno postojanje više sigurnosnih asocijacija uz očuvanje konzistentnosti bezbednosnih parametara i neprekidnost komunikacije. Upravo zbog toga *Security Association Database* predstavlja jedan od ključnih mehanizama očuvanja kontinuiteta digitalnog poverenja.

3.6.5. Implementacioni i konfiguracioni izazovi

Efikasnost *Security Association Database* neposredno zavisi od kvaliteta implementacije i pravilnog upravljanja sadržajem. Neusklađenost parametara između komunikacionih strana, neblagovremeno uklanjanje zastarelih *Security Association* ili nepravilno upravljanje procesom obnove sigurnosnih asocijacija mogu izazvati prekid komunikacije ili smanjenje nivoa zaštite. Poseban izazov predstavljaju distribuirana i virtualizovana okruženja, u kojima veliki broj istovremenih *Security Association* zahteva visoko efikasne mehanizme upravljanja i sinhronizacije. Sa bezbednosnog aspekta, kompromitacija procesa upravljanja SAD može imati ozbiljne posledice po bezbednost informaciono-komunikacionog sistema. Čak i ukoliko osnovni kriptografski algoritmi ostanu matematički nekompromitovani, greške u upravljanju aktivnim *Security Association* mogu omogućiti neadekvatnu primenu bezbednosnih parametara, prekid kontinuiteta zaštite ili povećanje površine napada. Ovakve okolnosti potvrđuju da otpornost na vektore napada u slučaju IPsec arhitekture zavisi ne samo od kvaliteta u kontekstu kriptografske zaštite, već i od pouzdanosti procesa upravljanja aktivnim stanjem digitalnog poverenja [2].

3.6.6. Procesni značaj security association database

U okviru procesnog modela razvijenog u ovom istraživanju, *Security Association Database* predstavlja fazu upravljanja uspostavljenim digitalnim poverenjem. Dok *Security Policy Database* definiše potrebu za zaštitom, *Internet Key Exchange* uspostavlja poverenje, a *Security Association* ga operacionalizuje, *Security Association Database* omogućava njegovo kontinuirano održavanje tokom trajanja komunikacione sesije. Time se uspostavlja logičan sled procesa u kojem svaka komponenta IPsec arhitekture ostvaruje jasno definisanu funkciju u životnom ciklusu digitalnog poverenja [77; SP 800-77 Rev. 1].

Ovakav pristup omogućava da se *Security Association Database* posmatra kao aktivni upravljački mehanizam, a ne kao pasivna baza podataka. Njena osnovna funkcija jeste očuvanje konzistentnosti, kontinuiteta i pouzdanosti bezbednosnih parametara koji omogućavaju pravilno funkcionisanje svih ostalih komponenti IPsec sistema [31].

Većina dostupne literature *Security Association Database* opisuje kroz njenu tehničku strukturu i sadržaj. Takav pristup pruža korisne informacije o organizaciji podataka, ali ne objašnjava njenu ulogu u ukupnom procesu funkcionisanja IPsec arhitekture. Procesni model razvijen u okviru ove magistarske teze dovodi do zaključka da *Security Association Database* predstavlja mehanizam kojim se upravlja aktivnim stanjem digitalnog poverenja i obezbeđuje kontinuitet zaštite tokom čitavog životnog ciklusa komunikacije. Time se dodatno potvrđuje osnovna istraživačka teza da se bezbednosne karakteristike *Internet Key Exchange* protokola mogu pravilno razumeti jedino kroz analizu međusobno povezanih procesa (*primer su ROP-return oriented programming vektori napada koje koriste državno sponzorisane hakerske grupe*), a ne

izolovanih isključivo analizom komponenti sistema informacione bezbednosti [18]. *Security Association Database* predstavlja centralni operativni mehanizam za upravljanje aktivnim stanjem digitalnog poverenja u okviru IPsec arhitekture. Njena funkcija prevazilazi skladištenje parametara *Security Association*, budući da omogućava njihovo kontinuirano održavanje, ažuriranje i primenu tokom čitavog životnog ciklusa komunikacije. Posmatranjem *Security Association Database* kroz procesni model razvijen u ovom radu potvrđuje se da bezbednost IPsec sistema ne zavisi isključivo od kvaliteta kriptografskih algoritama ili uspešno uspostavljene *Security Association*, već i od sposobnosti sistema da tokom vremena pouzdano upravlja uspostavljenim digitalnim poverenjem. Upravo zbog toga *Security Association Database* predstavlja neizostavni element integrisane bezbednosne arhitekture IPsec protokola [2].

3.7. Authentication header (ah) kao mehanizam očuvanja integriteta procesa digitalnog poverenja

3.7.1. Teorijska osnova authentication header mehanizma

Jedan od osnovnih zahteva savremenih informaciono-komunikacionih sistema jeste mogućnost pouzdane provere da sadržaj prenetih podataka nije izmenjen tokom komunikacije i da zaista potiče od legitimnog komunikacionog učesnika. U okviru IPsec arhitekture ovu funkciju ostvaruje **Authentication Header (AH)**, čiji je osnovni cilj zaštita integriteta i autentičnosti IP paketa. Za razliku od mehanizama koji obezbeđuju poverljivost šifrovanjem sadržaja komunikacije, *Authentication Header* omogućava proveru da podaci nisu neovlašćeno modifikovani i da komunikacija potiče od autentifikovanog izvora [58; RFC 4302.].

Tradicionalna stručna literatura *Authentication Header* definiše kao IPsec protokol koji obezbeđuje zaštitu integriteta, autentifikaciju izvora podataka i zaštitu od napada ponovnim emitovanjem (*replay attack*), pri čemu ne pruža zaštitu poverljivosti sadržaja komunikacije. Iako je ovakav opis funkcionalno tačan, on ne prikazuje njegovu širu ulogu u ukupnoj bezbednosnoj arhitekturi IPsec sistema. U okviru ovog istraživanja *Authentication Header* posmatra se kao mehanizam očuvanja integriteta procesa digitalnog poverenja koji je prethodno uspostavljen primenom *Internet Key Exchange* protokola i operacionalizovan kroz *Security Association* [2].

3.7.2. Authentication header kao zaštita integriteta uspostavljenog poverenja

Proces uspostavljanja digitalnog poverenja završen je tek kada komunikacione strane uspešno pregovaraju bezbednosne parametre, autentifikuju identitet i uspostave odgovarajuću *Security Association*. Međutim, poverenje koje je jednom uspostavljeno mora biti primenom bezbednosnih mehanizama u stanju bezbednosti tokom perioda trajanja komunikacije. Upravo tu funkciju ostvaruje *Authentication Header* [58; RFC 4302.].

Posmatrano kroz procesni model razvijen u ovom radu, *Authentication Header* predstavlja mehanizam koji kontinuirano proverava da li se komunikacija odvija u skladu sa parametrima definisanim tokom procesa uspostavljanja poverenja. Svaka neovlašćena izmena zaštićenog IP paketa predstavlja narušavanje integriteta procesa i ukazuje na mogućnost kompromitacije komunikacije. Time *Authentication Header* ne štiti samo podatke, već i pouzdanost procesa koji omogućava njihovu bezbednu razmenu [31].

3.7.3. Značaj authentication header protokola

Sa aspekta arhitekture IPsec-a *Authentication Header* predstavlja komponentu koja neposredno koristi parametre definisane u okviru *Security Association* i kojima upravlja *Security Association Database*. Na osnovu tih parametara izračunavaju se vrednosti za proveru integriteta svakog pojedinačnog IP paketa. Primenom u procesu zaštite komunikacija *Authentication Header*

predstavlja neposrednu vezu između procesa upravljanja bezbednosnim parametrima i njihove praktične primene tokom prenosa podataka preko nebezbednog komunikacionog kanala (*infrastruktura se nalazi u više jurisdikcija, postoji mogućnost prisluškivanja i trajnog arhiviranja mrežnog saobraćaja ukoliko se radi o metama od posebnog interesa za napadače*). Arhitektonska povezanost potvrđuje da *Authentication Header* nema samostalnu funkciju. Njegovo pravilno funkcionisanje zavisi od kvaliteta rada prethodnih faza procesa – bezbednosnih politika definisanih u *Security Policy Database*, uspešnog pregovaranja *Internet Key Exchange* protokola i pravilnog upravljanja *Security Association* parametrima [20].

3.7.4. Implementacioni i konfiguracioni izazovi

Praktična primena *Authentication Header* mehanizma pokazuje da njegova efikasnost zavisi od pravilnog izbora algoritama za proveru integriteta, tačne implementacije zaštite od *replay* napada i odgovarajuće sinhronizacije između komunikacionih učesnika. Nepravilna konfiguracija može dovesti do odbacivanja legitimnih paketa ili, suprotno tome, omogućiti prihvatanje neovlašćeno izmenjenih komunikacionih poruka. Pored toga, *Authentication Header* štiti i određene delove IP zaglavlja koji se ne menjaju tokom prenosa. Upravo zbog ove osobine njegova primena u okruženjima koja koriste **Network Address Translation (NAT)** postaje ograničena, budući da NAT menja pojedine elemente IP zaglavlja, čime se narušava validnost provere integriteta. Ova implementaciona karakteristika predstavlja jedan od razloga zbog kojih je u savremenim VPN implementacijama dominantnu ulogu preuzeo *Encapsulating Security Payload*, posebno u kombinaciji sa *NAT Traversal* mehanizmima [2], [59; RFC 4303].

3.7.5. Bezbednosni značaj authentication header mehanizma

Bezbednosni doprinos *Authentication Header* protokola ne ogleda se isključivo u zaštiti od neovlašćenih izmena podataka. Njegova funkcija obuhvata očuvanje poverenja u ispravnost komunikacionog procesa. Svaki uspešno verifikovan paket potvrđuje da komunikacija i dalje odgovara bezbednosnim parametrima uspostavljenim tokom rada *Internet Key Exchange* protokola. Na taj način *Authentication Header* omogućava kontinuiranu proveru da uspostavljeno digitalno poverenje nije narušeno tokom prenosa podataka [2].

Posebno je značajna njegova uloga u zaštiti od *replay* napada. Korišćenjem sekvencijalnih brojeva i odgovarajućih mehanizama verifikacije sprečava se ponovno emitovanje prethodno legitimnih komunikacionih poruka, čime se dodatno štiti integritet procesa digitalnog poverenja i smanjuje mogućnost manipulacije komunikacijom. Analiza stručne literature pokazuje da se *Authentication Header* najčešće opisuje kao protokol za zaštitu integriteta i autentifikaciju IP paketa. Takav pristup je tehnički ispravan, ali ostavlja po strani njegovu ulogu u ukupnoj arhitekturi procesa uspostavljanja digitalnog poverenja. Procesna analiza sprovedena u ovom naučno-istraživačkom radu omogućava analizu više aspekata informacione bezbednosti. *Authentication Header* predstavlja mehanizam kojim se proverava očuvanost poverenja uspostavljenog prethodnim fazama procesa. Na taj način njegova funkcija prevazilazi zaštitu pojedinačnih paketa i postaje sastavni deo kontinuiranog upravljanja bezbednošću komunikacije [5].

Authentication Header predstavlja mehanizam očuvanja integriteta procesa digitalnog poverenja u okviru IPsec arhitekture. Njegova osnovna funkcija nije ograničena na proveru integriteta IP paketa, već obuhvata kontinuiranu potvrdu da komunikacija i dalje odgovara bezbednosnim parametrima uspostavljenim tokom procesa pregovaranja *Internet Key Exchange* protokola. Analizom *Authentication Header* kroz procesni model razvijen u ovom radu potvrđuje se da bezbednost IPsec sistema proizlazi iz koordinisanog delovanja bezbednosnih politika, procesa uspostavljanja poverenja, upravljanja *Security Association* mehanizmima i kontinuirane provere integriteta komunikacije. Upravo ovakav pristup predstavlja osnov za narednu analizu

Encapsulating Security Payload protokola, koji će pokazati na koji način se uspostavljeno i očuvano digitalno poverenje primenjuje radi ostvarivanja poverljivosti i celovite zaštite mrežnog saobraćaja. ESP predstavlja operativni mehanizam kojim se digitalno poverenje, uspostavljeno primenom IPsec i *Internet Key Exchange* i operacionalizovano putem *Security Association*, transformiše u bezbednosni mehanizam primenom kriptografije u cilju zaštite mrežnog saobraćaja obezbeđivanjem tajnosti, integriteta i autentifikacije podataka.

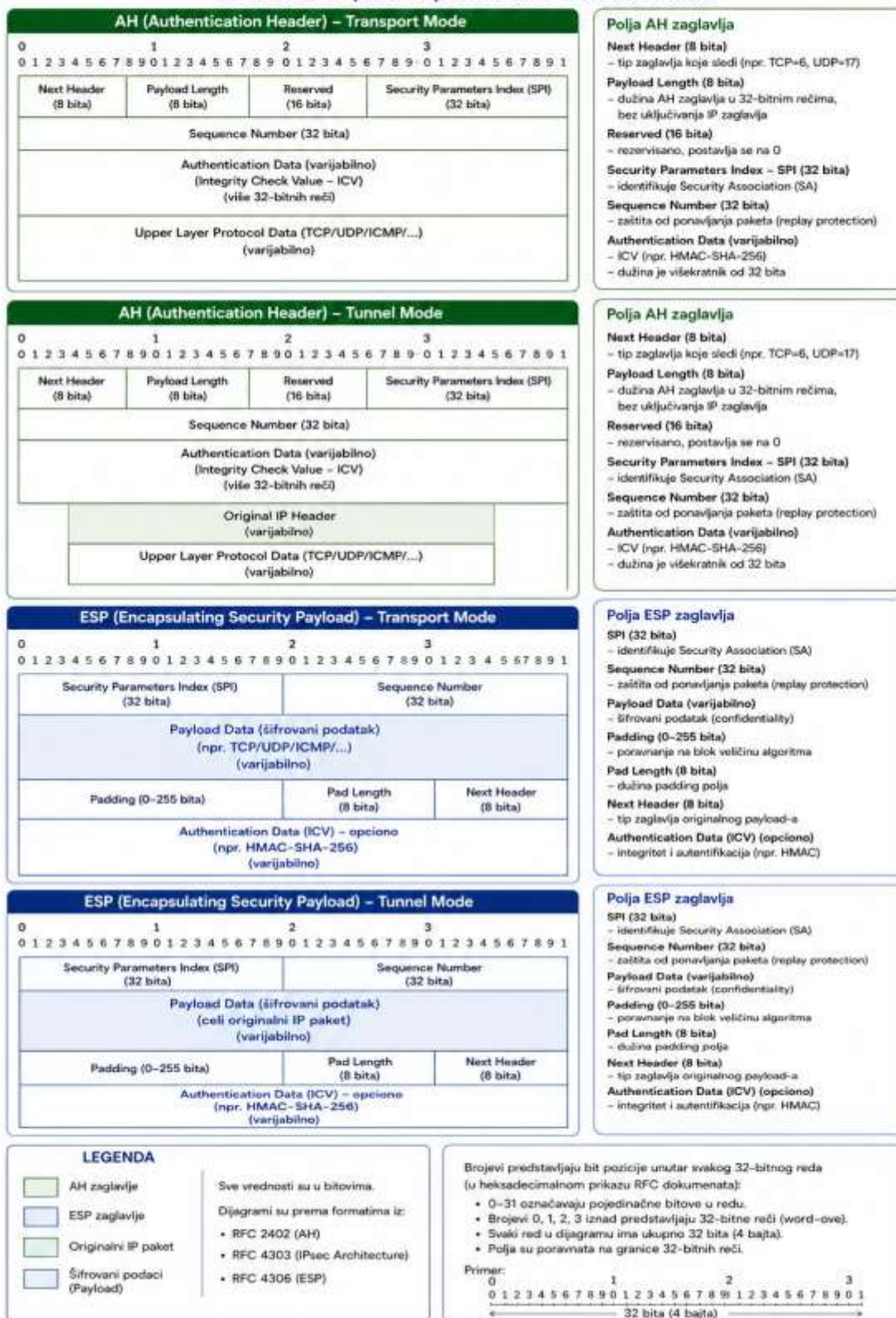
3.8. Encapsulating security payload (esp) kao centralni operativni mehanizam zaštite digitalnog poverenja

Encapsulating Security Payload (ESP) predstavlja osnovni protokol IPsec arhitekture namenjen zaštiti podataka tokom njihovog prenosa preko nepouzdatih komunikacionih mreža. Iako IPsec obuhvata dva osnovna protokola, *Authentication Header* (AH) i *Encapsulating Security Payload* (ESP), savremena praksa pokazuje da upravo ESP predstavlja dominantan mehanizam zaštite u gotovo svim implementacijama virtuelnih privatnih mreža (VPN), državnih informacionih sistema, finansijskih institucija, industrijskih komunikacionih mreža i kritične informacione infrastrukture. Razlog za ovakav status proizlazi iz činjenice da ESP objedinjeno obezbeđuje tajnost podataka, zaštitu integriteta, autentifikaciju izvora komunikacije i zaštitu od *replay napada*, pri čemu istovremeno omogućava kompatibilnost sa savremenim mrežnim tehnologijama, uključujući NAT-T (*Network Address Translation-Traversal*).

AH i ESP predstavljaju dva osnovna bezbednosna protokola u okviru IPsec arhitekture, koji se međusobno razlikuju kako po obimu pružene zaštite, tako i po strukturi zaglavlja koje dodaju IP paketu. Radi preciznog razumevanja ovih razlika, u nastavku je prikazana bitovska struktura AH i ESP zaglavlja u transportnom i tunelskom modu rada, prema relevantnim RFC specifikacijama. Razumevanje tačne strukture AH i ESP zaglavlja predstavlja preduslov za analizu bezbednosnih mehanizama koje ovi protokoli obezbeđuju, uključujući zaštitu integriteta, autentičnosti i tajnost podataka.

IPSec – AH vs ESP

Struktura IP paketa prema RFC dokumentima



Slika 4. Uporedni prikaz strukture IP paketa kod primene AH i ESP mehanizama zaštite IPsec protokola, u transportnom i tunelskom modu rada

Uporednom analizom prikazanih struktura uočava se da ESP zaglavlje, za razliku od AH, sadrži polja Padding i Pad Length neophodna za usklađivanje dužine podataka sa blok veličinom primenjenog algoritma šifrovanja, dok polje Authentication Data ostaje opciono kod oba moda ESP-a. Ovakva razlika u strukturi direktno odražava različite bezbednosne ciljeve dva protokola. AH ima za fokus isključivo integritet i autentičnost (ne obezbeđuje tajnost) , dok ESP objedinjuje tajnost podataka sa mogućnošću dodatne autentifikacije podataka. Kao što se vidi na slici, osnovna razlika između AH i ESP zaglavlja ogleda se u obimu zaštite koju svaki protokol pruža. Razlika između transportnog i tunelskog moda dodatno se ogleda u tretmanu originalnog IP zaglavlja, koje se u tunelskom modu enkapsulira i, u slučaju ESP-a, šifrjuje zajedno sa ostatkom paketa.

Sa aspekta procesa uspostavljanja digitalnog poverenja, ESP ne predstavlja izolovani kriptografski mehanizam, već centralnu operativnu komponentu koja omogućava da rezultati prethodno izvršenog IKE pregovaranja budu praktično primenjeni tokom prenosa korisničkih podataka. Internet Key Exchange (IKEv1 ili IKEv2) uspostavlja bezbednosne asocijacije (Security Associations – SA), pregovara kriptografske algoritme i generiše odgovarajući kriptografski materijal, dok ESP predstavlja operativni mehanizam koji taj materijal koristi za zaštitu svakog pojedinačnog IP paketa. Na taj način ostvaruje se jasna funkcionalna podela između kontrolne ravni (*Control Plane*), kojoj pripada IKE protokol, i ravni podataka (*Data Plane*), u kojoj dominantnu ulogu ima upravo ESP.

Pored zaštite tajnosti, ESP obezbeđuje i integritet podataka, čime omogućava detekciju svake neovlašćene izmene sadržaja paketa tokom prenosa. Integritet se ostvaruje primenom autentifikacionih mehanizama, pri čemu savremeni AEAD (*Authenticated Encryption with Associated Data*) algoritmi, kao što je AES-GCM, objedinjeno realizuju šifrovanje i proveru integriteta bez potrebe za dodatnim autentifikacionim algoritmom. Ovakav pristup smanjuje procesno opterećenje uređaja, povećava performanse komunikacije i istovremeno unapređuje ukupni nivo bezbednosti.

Treći važan aspekt predstavlja autentifikacija porekla podataka, odnosno potvrđivanje da zaštićeni paket zaista potiče od legitimnog komunikacionog partnera. Iako se međusobna autentifikacija učesnika primarno ostvaruje tokom IKE faze, ESP obezbeđuje kontinuitet tog poverenja tokom čitavog životnog ciklusa bezbednosne asocijacije. Time se sprečava uspešno ubacivanje lažnih paketa od strane neovlašćenih aktera i održava konzistentnost bezbednosnog konteksta uspostavljenog tokom inicijalnog pregovaranja.

Jedna od ključnih karakteristika ESP protokola jeste implementacija zaštite od *replay* napada. Svakom paketu pridružuje se jedinstveni sekvencijalni broj, dok primalac održava odgovarajući „*sliding window*“ mehanizam kojim razlikuje legitimne pakete od prethodno presretnutih i ponovo poslatih paketa. Na taj način napadač ne može jednostavno reprodukovati ranije zabeležen saobraćaj kako bi izazvao neovlašćene akcije ili narušio bezbednosne funkcije i procese informaciono-komunikacionog sistema. *Replay* zaštita predstavlja posebno značajnu komponentu zaštite VPN infrastrukture, jer omogućava očuvanje integriteta procesa komunikacije čak i u prisustvu aktivnog mrežnog napadača.

ESP podržava dva osnovna moda rada: *Transport Mode* i *Tunnel Mode*. U transportnom modu zaštićen je isključivo korisnički sadržaj originalnog IP paketa, dok originalno IP zaglavlje ostaje vidljivo mrežnoj infrastrukturi. Ovaj režim rada najčešće se koristi u komunikaciji između dva krajnja računarska sistema. Nasuprot tome, tunelski mod predstavlja dominantan način rada u savremenim VPN implementacijama. U ovom režimu kompletan originalni IP paket enkapsulira

se unutar novog IP paketa, pri čemu se štiti kako korisnički sadržaj, tako i originalno IP zaglavlje. Time se dodatno povećava nivo zaštite komunikacije i otežava analiza mrežnog saobraćaja od strane potencijalnih napadača.

Sa aspekta procesnog pristupa, ESP ne treba posmatrati isključivo kao mehanizam šifrovanja, već kao centralnu operativnu komponentu bezbednosnog procesa. Efikasnost njegove primene zavisi od kvaliteta prethodno uspostavljenih bezbednosnih asocijacija, pravilnog izbora kriptografskih algoritama, bezbednog upravljanja ključevima, odgovarajuće konfiguracije uređaja, kontinuiranog monitoringa rada sistema i pravovremenog odgovora na bezbednosne incidente. Drugim rečima, ukupna bezbednosna otpornost IPsec infrastrukture ne proizlazi samo iz matematičke otpornosti korišćenih algoritama, već iz pravilnog funkcionisanja svih međusobno povezanih procesa koji čine životni ciklus bezbedne komunikacije. Savremeni koncept zaštite zasnovan na procesnom pristupu dodatno proširuje ulogu ESP protokola uključivanjem sistema za kontinuirani monitoring, kao što su SIEM, EDR, NDR i SOAR platforme. Analizom VPN logova, NetFlow/IPFIX zapisa, telemetrije mrežnih uređaja i događaja sa krajnjih sistema moguće je pratiti funkcionisanje ESP komunikacije u realnom vremenu, identifikovati odstupanja od uobičajenih obrazaca ponašanja i pravovremeno reagovati na potencijalne incidente. Na taj način zaštita digitalnog poverenja postaje dinamičan proces koji objedinjuje kriptografske mehanizme, operativni nadzor, upravljanje rizicima i kontinuirano unapređenje bezbednosnih kontrola. Može se zaključiti da Encapsulating Security Payload predstavlja centralni operativni mehanizam IPsec arhitekture, jer omogućava praktičnu realizaciju bezbednosnih ciljeva definisanih tokom procesa razmene kriptografskih ključeva. Integracijom mehanizama za zaštitu tajnosti, integriteta, autentifikacije porekla podataka i zaštite od replay napada, uz podršku savremenih algoritama i kontinuiranog procesa monitoringa i upravljanja bezbednošću, ESP predstavlja ključni element izgradnje i očuvanja digitalnog poverenja u savremenim IP komunikacionim sistemima. Njegov značaj prevazilazi ulogu pojedinačnog protokola, jer predstavlja operativnu osnovu na kojoj se zasniva bezbedna realizacija VPN komunikacije i ukupna bezbednosna otpornost IKE/IPsec okruženja.

Tabela 5. AH vs ESP – bezbednosne karakteristike

Karakteristika	AH (Authentication Header)	ESP (Encapsulating Security Payload)
Autentifikacija izvora	Da	Da
Integritet podataka	Da	Da (opciono u starijim verzijama, standardno u savremenim AEAD implementacijama)
Tajnost (šifrovanje)	Ne	Da
Zaštita od replay napada	Da	Da
Zaštita IP zaglavlja	Delimično (nepromenljivi delovi)	Ne
Kompatibilnost sa NAT	Ograničena	Visoka uz NAT-T
Transport Mode	Podrжан	Podrжан
Tunnel Mode	Podrжан	Podrжан
Tipična savremena primena	Retko	Dominantan IPsec mehanizam
Status u praksi	Ograničena upotreba	Preporučena upotreba

Napomena: AH obezbeđuje autentifikaciju i integritet, dok ESP obezbeđuje i tajnost podataka, zbog čega predstavlja dominantan mehanizam u savremenim IPsec implementacijama.

Izvor: Autor, na osnovu sinteze relevantnih RFC dokumenata (RFC 4301, RFC 4302, RFC 4303, RFC 3947)
Podaci u tabeli 5 ukazuju komparativnu analizu dva osnovna IPsec mehanizma zaštite: Authentication Header (AH) i Encapsulating Security Payload (ESP) ukazujući na njihovu

funkcionalnu komplementarnost u okviru bezbednosne arhitekture IPsec-a. Oba protokola obezbeđuju autentifikaciju izvora podataka i zaštitu od *replay* napada, dok se ključna razlika ogleda u obimu pružene zaštite: AH pruža zaštitu integriteta i za nepromenljive delove IP zaglavlja, dok ESP ovu funkcionalnost ne obuhvata, ali zato jedini od ova dva mehanizma obezbeđuje tajnost podataka putem enkripcije. Ova razlika direktno određuje njihovu praktičnu primenljivost — dok AH pruža širu proveru integriteta na nivou paketa, izostanak enkripcije čini ga nedovoljnim za scenarije koji zahtevaju poverljivost komunikacije.

Sa aspekta savremene primene, tabela jasno ukazuje na dominaciju ESP mehanizma u odnosu na AH, što je posledica nekoliko međusobno povezanih faktora. Pre svega, ESP poseduje znatno bolju kompatibilnost sa NAT uređajima kroz NAT-Traversal (NAT-T) ekstenziju, dok je AH u ovom pogledu ograničen usled zaštite čitavog IP zaglavlja koje NAT proces neizbežno modifikuje. Dodatno, savremene AEAD (Authenticated Encryption with Associated Data) implementacije ESP-a standardno objedinjuju proveru integriteta i enkripciju u jednoj kriptografskoj operaciji, čime se eliminiše potreba za paralelnom primenom AH mehanizma. Iz ovih razloga, u savremenim IPsec implementacijama AH se koristi retko i u ograničenom obimu, dok ESP predstavlja preporučeni i dominantan mehanizam zaštite mrežnog saobraćaja.

Tabela 6. Transport Mode vs Tunnel Mode

Karakteristika	Transport Mode	Tunnel Mode
Nivo zaštite	Štiti korisničke podatke (payload)	Štiti kompletan originalni IP paket
Originalno IP zaglavlje	Ostaje vidljivo	Nalazi se unutar šifrovanog tunela
Novo IP zaglavlje	Ne dodaje se	Dodaje se novo spoljašnje IP zaglavlje
Šifrovani sadržaj	Payload	Celokupan originalni IP paket
Tipična primena	Host–Host komunikacija	Gateway–Gateway ili Remote Access VPN
Kompatibilnost sa VPN	Ograničena	Dominantan način rada
Komunikacioni overhead	Manji	Veći zbog dodatnog IP zaglavlja
Performanse	Veća efikasnost	Nešto veći režijski troškovi
Sakrivanje interne mreže	Ne	Da
Tipične implementacije	Zaštita krajnjih sistema	Site-to-Site VPN i udaljeni pristup

Napomena: Transport Mode je pogodan za direktnu zaštitu komunikacije između krajnjih sistema, dok je Tunnel Mode standardni izbor za VPN implementacije jer omogućava zaštitu celokupnog IP paketa i prikrivanje interne adresne strukture.

Izvor: Autor, na osnovu sinteze relevantnih RFC dokumenata (RFC 4301, RFC 4302, RFC 4303)

Prikazani podaci u tabeli 6 predstavljaju komparativnu analizu dva osnovna moda rada IPsec protokola: *Transport Mode* i *Tunnel Mode* koji se međusobno razlikuju prema obimu IP paketa koji podležu kriptografskoj zaštiti. *Transport Mode* štiti isključivo korisničke podatke (*payload*) originalnog paketa, dok originalno IP zaglavlje ostaje vidljivo i nezaštićeno, što ovaj mod čini pogodnim za direktnu komunikaciju između krajnjih sistema (*host-to-host*) gde nema potrebe za prikrivanjem mrežne topologije. *Tunnel Mode*, nasuprot tome, enkapsulira celokupan originalni IP paket — uključujući izvorno zaglavlje — unutar novog, spoljašnjeg IP zaglavlja, čime se čitav originalni paket nalazi unutar kriptografski zaštićenog tunela. Sa aspekta praktične primene, tabela ukazuje da *Tunnel Mode* predstavlja dominantan način rada u savremenim VPN implementacijama, budući da omogućava zaštitu komunikacije između mrežnih gateway uređaja

(*Gateway-to-Gateway*) i podršku za udaljeni pristup (Remote Access VPN), uz dodatnu prednost sakrivanja interne adresne strukture mreže od spoljnog posmatrača. Ova funkcionalnost dolazi uz izvestan kompromis u pogledu performansi — dodavanje novog IP zaglavlja povećava komunikacioni overhead u odnosu na Transport Mode, koji, usled manjeg režijskog opterećenja, ostaje efikasniji izbor u scenarijima zaštite krajnjih sistema gde enkapsulacija celokupnog paketa nije neophodna [2], [31], [51].

3.8.1. Teorijsko-kriptografska osnova encapsulating security payload mehanizma

Osnovni cilj savremene mrežne bezbednosti nije samo uspostavljanje poverenja između komunikacionih učesnika, već i obezbeđivanje da podaci koji se razmenjuju tokom komunikacije ostanu tajni, da strane u komunikaciji mogu verifikovati autentičnost i da su podaci zaštićeni od neovlašćenih izmena u procesu prenosa. U okviru IPsec arhitekture upravo ovu funkciju ostvaruje *Encapsulating Security Payload* (ESP), koji predstavlja osnovni mehanizam za zaštitu korisničkog mrežnog saobraćaja [59; RFC 4303].

Sa kriptografskog aspekta, ESP omogućava primenu simetričnih algoritama za šifrovanje podataka, mehanizama za proveru integriteta i autentifikaciju, kao i zaštitu od napada ponovnim emitovanjem paketa. Savremene implementacije ESP najčešće koriste algoritme kao što su AES-CBC, AES-GCM i ChaCha20-Poly1305, pri čemu posebno mesto zauzimaju *Authenticated Encryption with Associated Data* (AEAD) algoritmi koji objedinjeno ostvaruju poverljivost i integritet podataka. Time ESP predstavlja praktičnu primenu kriptografskih principa analiziranih u prethodnim poglavljima [59; RFC 4303], [81; SP 800-38D], [78; FIPS 197].

Posmatrano kroz procesni model razvijen u okviru ove magistarske teze, *Encapsulating Security Payload* predstavlja završnu operativnu fazu procesa uspostavljanja digitalnog poverenja. Sve prethodne faze procesa – definisanje bezbednosnih politika, pregovaranje *Internet Key Exchange* protokola, uspostavljanje *Security Association* i upravljanje njenim parametrima – stvaraju predušlove za pravilno funkcionisanje ESP mehanizma [2].

Tek nakon uspešno uspostavljene *Security Association* moguće je primeniti odgovarajuće kriptografske algoritme na korisnički mrežni saobraćaj. Parametri definisani tokom procesa pregovaranja određuju algoritme šifrovanja, dužinu ključeva, način zaštite integriteta i ostale bezbednosne karakteristike komunikacije. Zbog toga ESP ne predstavlja samostalan bezbednosni mehanizam, već završnu realizaciju procesa digitalnog poverenja koji je prethodno uspostavljen u okviru IPsec arhitekture [59; RFC 4303].

3.8.2. Esp kao operacionalizacija digitalnog poverenja

Jedan od osnovnih doprinosa procesnog modela razvijenog u ovom istraživanju jeste posmatranje *Encapsulating Security Payload* mehanizma kao procesa kojim digitalno poverenje dobija svoju praktičnu vrednost. Digitalno poverenje uspostavljeno između učesnika u komunikaciji ne ostvaruje tajnost komunikacije ukoliko se ne primeni na zaštitu mrežnog saobraćaja. Upravo tu funkciju ostvaruje ESP i obezbeđuje da su podaci kriptografski zaštićeni [34]. Svaki IP paket koji prolazi kroz ESP obrađuje se primenom bezbednosnih parametara definisanih u odgovarajućoj *Security Association*. Na taj način svaki pojedinačni paket predstavlja praktičnu manifestaciju prethodno uspostavljenog poverenja između komunikacionih učesnika. ESP predstavlja mehanizam kojim se rezultati procesa pregovaranja *Internet Key Exchange* protokola neposredno primenjuju na kriptografsku zaštitu podataka koji se prenose putem informaciono-komunikacioni sistema [19].

3.8.3. Implementaciono-bezbednosna dimenzija

Efikasnost *Encapsulating Security Payload* mehanizma u velikoj meri zavisi od kvaliteta njegove implementacije, pravilnog izbora algoritama i odgovarajuće konfiguracije sistema. Istorijska analiza razvoja IPsec implementacija pokazuje da bezbednosni incidenti retko proizlaze iz matematičkih slabosti savremenih algoritama, dok su znatno češće posledica implementacionih grešaka, neadekvatne konfiguracije ili nepravilnog upravljanja kriptografskim parametrima [25].

Posebno značajni bezbednosni izazovi odnose se na pravilno upravljanje inicijalizacionim vrednostima, *nonce* parametrima kod AEAD algoritama, životnim ciklusom sesijskih ključeva i periodičnom obnovom *Security Association*. Primena pravila najbolje prakse u zaštiti informaciono-komunikacionih sistema i implementacija ovih mehanizama može značajno umanjiti bezbednosne karakteristike sistema zaštite čak i kada su korišćeni algoritmi matematički otporni na kriptanalizu u određenom vremenskom periodu (*kvantni računari mogu dešifrovati u znatno kraćem vremenskom periodu, vreme potrebno za dešifrovanje zavisi od primenjenog kriptografskog algoritma*) [92; BSI TR-02102-1], [93; BSI TR-02102-3].

3.8.4. Savremeni izazovi primene esp mehanizma

Razvoj *cloud* infrastrukture, virtualizovanih mrežnih funkcija, softverski definisanih mreža (SDN) i velikih VPN sistema postavlja nove zahteve pred *Encapsulating Security Payload* mehanizam. Savremene implementacije moraju obezbediti visok nivo bezbednosti uz minimalno povećanje latencije i racionalno korišćenje računarskih resursa. Istovremeno, ubrzani razvoj postkvantne kriptografije nameće potrebu za prilagođavanjem kriptografskih algoritama koji će u budućnosti biti korišćeni u okviru IPsec arhitekture [91; NIST IR 8547].

Pored tehnoloških izazova, poseban značaj imaju implementacione ranjivosti evidentirane u različitim IPsec rešenjima. One potvrđuju da bezbednost ESP mehanizma ne zavisi isključivo od izbora algoritama, već i od kvaliteta njihove implementacije, pravilnog upravljanja *Security Association* parametrima i kontinuiranog održavanja stanja bezbednosti sistema u kontekstu izloženosti riziku i aktivnostima aktera koji imaju kapacitete da dovedu sistem u nebezbedno stanje. Zbog toga se analiza bezbednosti ESP ne može ograničiti na kriptografsku dimenziju, već mora obuhvatiti čitav proces upravljanja digitalnim poverenjem [7].

U većini stručnih radova *Encapsulating Security Payload* opisuje se prvenstveno kao mehanizam za ostvarivanje tajnosti mrežnog saobraćaja. Iako je takav pristup tehnički opravdan, on ne prikazuje njegov stvarni značaj u ukupnoj IPsec arhitekturi. Procesni model razvijen u ovom radu omogućava šire metodološko tumačenje. ESP predstavlja završnu operativnu fazu procesa uspostavljanja digitalnog poverenja u kojoj rezultati bezbednosnih politika, pregovaranja *Internet Key Exchange* protokola, *Security Association* mehanizama i upravljanja njihovim parametrima postaju konkretna zaštita mrežnog saobraćaja. Time ESP dobija ulogu centralnog operativnog mehanizma kojim se ostvaruju ciljevi celokupne IPsec arhitekture [59; RFC 4303].

Encapsulating Security Payload predstavlja centralni operativni mehanizam IPsec arhitekture kojim se digitalno poverenje uspostavlja tokom procesa *Internet Key Exchange* pregovaranja pretvara u bezbednosni mehanizam i zaštitu mrežnog saobraćaja. Njegova funkcija prevazilazi primenu algoritama za šifrovanje, budući da objedinjuje tajnost, integritet, autentifikaciju i zaštitu od ponovnog emitovanja paketa u jedinstven proces zaštite komunikacije. Posmatran kroz metodološki okvir ovog istraživanja, ESP predstavlja završnu fazu operacionalizacije digitalnog poverenja i potvrđuje da se bezbednost IPsec arhitekture može pravilno razumeti jedino kao rezultat koordinisanog delovanja svih prethodno analiziranih komponenti i procesa [31].

4. Bezbednosne karakteristike internet key exchange version 1 (ikev1) protokola kroz procesnu analizu faza, modova i mehanizama upravljanja bezbednosnim asocijacijama

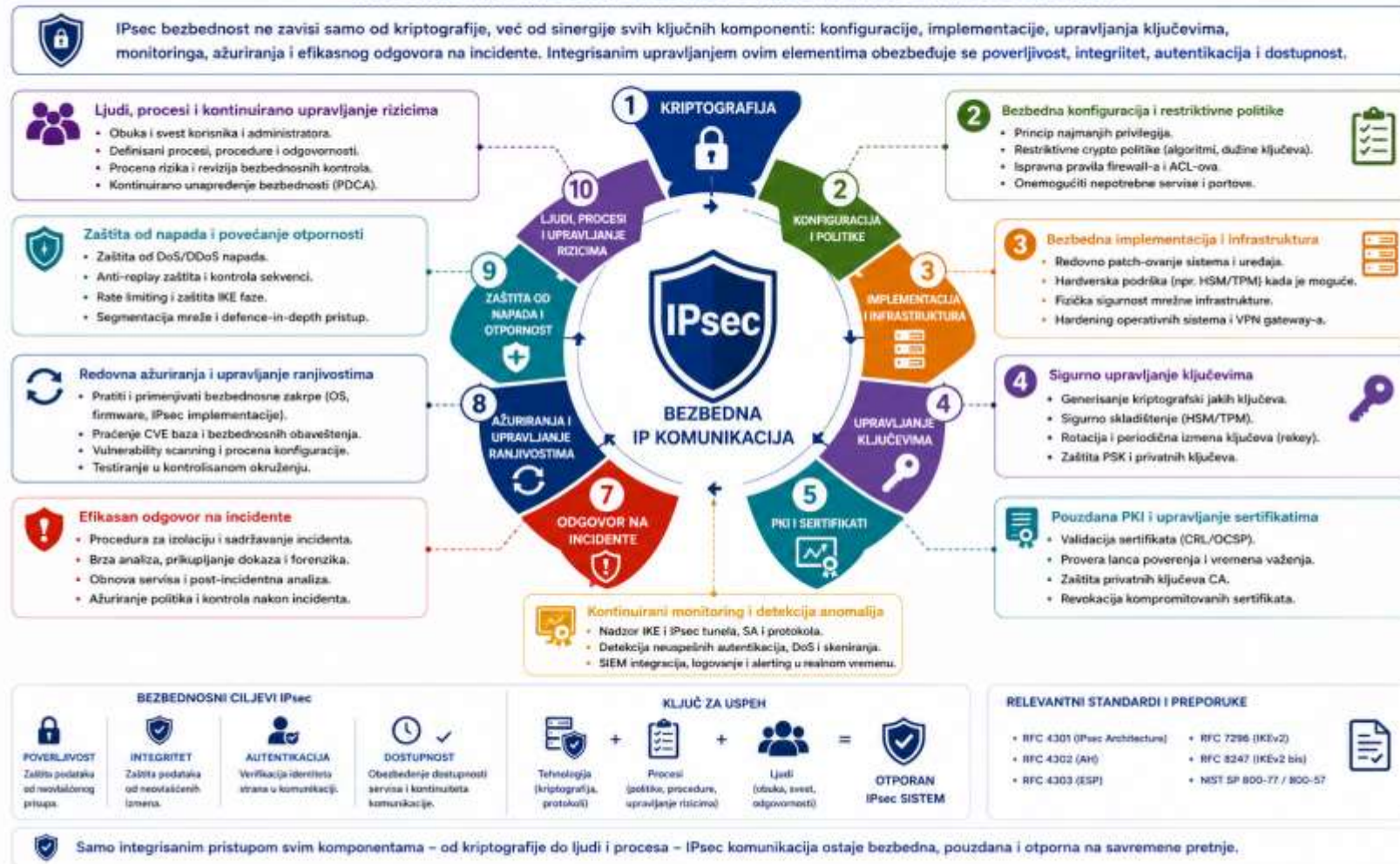
Internet Key Exchange Version 1 (IKEv1) predstavlja prvi standardizovani protokol namenjen automatizovanom uspostavljanju bezbednosnih asocijacija (*Security Associations – SA*) i razmeni kriptografskog materijala u okviru IPsec arhitekture. Osnovna funkcija IKEv1 nije neposredna zaštita korisničkih podataka, već uspostavljanje bezbednosnog okruženja u kome će *Encapsulating Security Payload (ESP)* i *Authentication Header (AH)* moći da obezbede kriptografski zaštićenu (obezbeđenje tajnosti podataka) i autentifikovanu komunikaciju. Upravo zbog toga IKEv1 predstavlja kontrolni mehanizam IPsec arhitekture, dok operativnu zaštitu saobraćaja realizuju odgovarajući IPsec protokoli. Sa metodološkog aspekta, IKEv1 se ne može adekvatno analizirati isključivo kroz opis pojedinačnih poruka ili kriptografskih algoritama. Njegovo funkcionisanje zasniva se na jasno definisanom procesu u kome svaka faza izvršava određenu bezbednosnu funkciju, pri čemu rezultati prethodne faze predstavljaju ulazne parametre narednog koraka. Zbog toga procesni pristup omogućava znatno potpunije razumevanje načina na koji se uspostavlja digitalno poverenje između komunikacionih učesnika, kao i identifikaciju tačaka u kojima mogu nastati bezbednosne ranjivosti [2],[31].

Za razliku od klasičnog pristupa analizi protokola, procesna analiza polazi od pretpostavke da bezbednost predstavlja dinamičan sled međusobno povezanih procesa koji zajedno omogućavaju uspostavljanje, održavanje i bezbedno ukidanje komunikacionih odnosa. U tom smislu, IKEv1 može se posmatrati kao životni ciklus upravljanja bezbednosnim asocijacijama, koji obuhvata inicijalno pregovaranje parametara, autentifikaciju komunikacionih partnera, generisanje zajedničkog kriptografskog materijala, uspostavljanje IPsec SA, periodično obnavljanje kriptografskih ključeva itd. Poseban značaj procesnog pristupa ogleda se u činjenici da omogućava istovremenu analizu tehničkih, organizacionih i operativnih aspekata zaštite. Bezbednost IKEv1 ne zavisi isključivo od matematičke otpornosti primenjenih algoritama, već i od pravilnog izbora konfiguracionih parametara, kvaliteta implementacije, upravljanja sertifikatima, bezbednog generisanja slučajnih brojeva, pravilnog rukovanja kriptografskim ključevima (primena HSM) i kontinuiranog monitoringa rada sistema. Posmatrano iz ove perspektive, svaki element procesa može predstavljati potencijalni izvor kompromitacije ukoliko nije pravilno implementiran ili nadziran [38].

Bezbednosna otpornost/rezistentnost/rezilijentnost IPsec sistema počiva na usaglašenoj primeni kriptografskih, tehničkih, organizacionih i proceduralnih mera, definisanih politikom bezbednosti i relevantnim standardima (RFC 4301, RFC 4303, RFC 7296 i dr.). U nastavku je predstavljen integrisani model koji ove mere sistematizuje kroz deset međusobno povezanih domena IP komunikacije i bezbednosnih mehanizama zaštite informaciono-komunikacionog sistema.

BEZBEDNOSNE KARAKTERISTIKE IPsec

INTEGRISANI MODEL BEZBEDNOSNE OTPORNOSTI IPsec SISTEMA



Slika 5. Integrisani prikaz komponenti bezbedne IP komunikacije u okviru IPsec protokola, od kriptografske zaštite do upravljanja rizikom i odgovora na incidente

Grafički prikaz ukazuje na to da se bezbednosna otpornost IPsec sistema ostvaruje kroz deset međusobno povezanih domena — od kriptografske zaštite, preko bezbedne konfiguracije, implementacije i upravljanja ključevima, do kontinuiranog monitoringa, odgovora na incidente i upravljanja rizikom. Svaki od navedenih domena doprinosi ostvarenju četiri osnovna bezbednosna cilja IPsec komunikacije — poverljivosti, integriteta, autentičnosti i dostupnosti — čime se potvrđuje da tehnologija, procesi i ljudski faktor predstavljaju neodvojive komponente otpornog sistema.

Procesna analiza takođe omogućava jasnu identifikaciju uzročno-posledičnih veza između pojedinih faza protokola. Greške nastale tokom inicijalnog pregovaranja algoritama mogu imati neposredan uticaj na nivo zaštite koji će biti ostvaren tokom prenosa podataka. Slično tome, kompromitacija autentifikacionog mehanizma može dovesti do uspostavljanja bezbednosnih asocijacija sa neovlašćenim učesnikom, bez obzira na kriptografsku otpornost algoritama koji će kasnije biti korišćeni za zaštitu komunikacije. Upravo zbog toga analiza procesa omogućava identifikaciju kritičnih tačaka koje imaju najveći uticaj na ukupnu bezbednosnu otpornost IPsec okruženja. U okviru IKEv1 protokola posebno se izdvajaju dve osnovne faze. Prva faza (Phase 1) namenjena je uspostavljanju IKE Security Association, odnosno izgradnji bezbednog komunikacionog kanala između učesnika pregovaranja. Tokom ove faze pregovaraju se kriptografski algoritmi, razmenjuju Diffie–Hellman javne vrednosti, generiše zajednička tajna i sprovodi međusobna autentifikacija komunikacionih partnera. Nakon uspešno završene prve faze uspostavlja se poverljiv i autentifikovan kanal preko koga se odvija druga faza (Phase 2), čiji je osnovni cilj uspostavljanje jedne ili više IPsec *Security Association* koje će koristiti ESP ili AH protokol za zaštitu korisničkog saobraćaja [2],[10],[31], [51].

Jedna od karakteristika IKEv1 protokola jeste postojanje različitih modova rada prve faze. *Main Mode* prioritet daje zaštiti identiteta komunikacionih učesnika i postiže viši nivo bezbednosti kroz razmenu šest poruka. Nasuprot tome, *Aggressive Mode* koristi svega tri poruke, čime smanjuje komunikaciono opterećenje i vreme uspostavljanja veze, ali istovremeno izlaže identitete učesnika većem riziku i povećava mogućnost izvođenja offline dictionary napada kada se koristi autentifikacija unapred podeljenim ključem (Pre-Shared Key – PSK). Ova razlika jasno pokazuje da izbor moda rada predstavlja kompromis između performansi i nivoa bezbednosti, što predstavlja jedan od osnovnih predmeta procesne analize.

Pored modova rada, procesni pristup obuhvata i analizu mehanizama upravljanja bezbednosnim asocijacijama. Security Association ne predstavlja samo skup kriptografskih parametara, već dinamički bezbednosni objekat čiji životni ciklus obuhvata kreiranje, održavanje, obnovu i bezbedno uklanjanje. Tokom rada sistema može postojati veliki broj aktivnih bezbednosnih asocijacija, pri čemu svaka od njih poseduje sopstvene identifikatore, algoritme, ključeve i vremenska ograničenja važenja. Upravljanje ovim objektima predstavlja jedan od najvažnijih procesa unutar IKEv1 protokola, jer direktno utiče na kontinuitet rada VPN infrastrukture i otpornost komunikacionog sistema na različite vrste napada [2].

Sa aspekta savremenih bezbednosnih zahteva, analiza IKEv1 dobija dodatni značaj zbog činjenice da je ovaj protokol tokom godina postao predmet brojnih kryptoanalitičkih i implementacionih istraživanja. Identifikovane su slabosti koje se odnose na pojedine autentifikacione mehanizme, izbor Diffie–Hellman grupa, zaštitu identiteta u Aggressive Mode-u, mogućnost izvođenja DoS napada, kao i različite konfiguracione propuste. Međutim, procesni pristup omogućava da se ove ranjivosti ne posmatraju kao izolovani tehnički

problemi, već kao posledica međusobnog delovanja različitih faza životnog ciklusa bezbednosnih asocijacija. Time se omogućava preciznija identifikacija kritičnih tačaka sistema i definisanje odgovarajućih bezbednosnih kontrola [2].

Može se zaključiti da procesna analiza predstavlja metodološki najpogodniji okvir za proučavanje bezbednosnih karakteristika IKEv1 protokola. Umesto parcijalnog sagledavanja pojedinačnih algoritama ili poruka, ovaj pristup omogućava razumevanje međusobnih zavisnosti između faza pregovaranja, autentifikacionih mehanizama, upravljanja bezbednosnim asocijacijama i operativnog funkcionisanja IPsec arhitekture. Takav način analize stvara čvrstu osnovu za detaljno razmatranje pojedinačnih modova rada, bezbednosnih mehanizama i ranjivosti koje će biti predmet narednih potpoglavlja, kao i za njihovu kritičku komparaciju sa unapređenjima uvedenim u IKEv2 protokolu [10].

4.1. Bezbednosne karakteristike faze 1 ikev1 protokola – uspostavljanje ike security association

Tokom razvoja Internet Key Exchange Version 1 (IKEv1) protokola primenjen je pristup da se proces uspostavljanja bezbedne komunikacije podeli u jasno definisane funkcionalne celine[53; RFC 2409];[54; RFC 4306], pri čemu svaka od celina rešava određenu grupu bezbednosnih problema. Takav pristup nije rezultat isključivo organizacionih razloga, već je uslovljen činjenicom da bezbedna razmena kriptografskih ključeva zahteva prethodno uspostavljanje međusobnog poverenja između komunikacionih entiteta. Upravo iz tog razloga Faza 1 IKEv1 protokola predstavlja jednu od najvažnijih komponenti bezbednosne arhitekture IKEv1 protokola, budući da se u okviru nje uspostavlja inicijalni bezbednosni odnos koji predstavlja osnov za sve kasnije procese zaštite mrežnog IP saobraćaja [31].

Sa naučno-istraživačkog aspekta, osnovna funkcija Faze 1 nije razmena korisničkih podataka niti neposredno uspostavljanje IPsec zaštite. Njena primarna uloga jeste formiranje *IKE Security Association* (IKE SA), odnosno uspostavljanje kriptografski zaštićenog komunikacionog kanala između strana koje iniciraju *IKE Security Association* (IKE SA). Tek nakon uspešno uspostavljenog IKE SA moguće je bezbedno pregovarati o parametrima koji će biti korišćeni za zaštitu podataka u okviru druge faze protokola. Na taj način arhitektura IKEv1 uvodi princip višeslojne zaštite, prema kojem se bezbednosni mehanizmi aktiviraju sukcesivno, pri čemu svaki naredni nivo zaštite zavisi od uspešno uspostavljenog prethodnog nivoa [2],[42].

Jedna od najznačajnijih bezbednosnih karakteristika Faze 1 ogleda se u činjenici da komunikacioni entiteti pre razmene osetljivih bezbednosnih informacija međusobno pregovaraju o kriptografskim algoritmima, parametrima autentifikacije, *Diffie–Hellman* grupama i drugim elementima koji određuju nivo bezbednosti buduće komunikacije. Ovakav pristup omogućava da se na osnovu bezbednosnih politika i prema definisanim mogućnostima oba učesnika komunikacije, uz istovremeno očuvanje interoperabilnosti između različitih implementacija IPsec sistema. Time se postiže ravnoteža između visokog nivoa bezbednosti i praktične primenljivosti protokola u heterogenim informaciono-komunikacionim okruženjima [43].

Analizirajući arhitekturu Faze 1 može se uočiti da bezbednost ne zavisi od samo jednog mehanizma zaštite, već od koordinisanog delovanja više međusobno povezanih bezbednosnih mehanizama i procesa. Pregovaranje bezbednosnih parametara, razmena *Diffie–Hellman* vrednosti, generisanje zajedničke tajne, autentifikacija komunikacionih entiteta i

uspostavljanje *IKE Security Association* predstavljaju logički povezane korake čija međusobna zavisnost značajno povećava otpornost sistema na različite kategorije napada na informaciono-komunikacioni sistem. Kompromitacija bilo kog od ovih procesa može ugroziti celokupnu bezbednost informaciono-komunikacionog sistema, što potvrđuje da se bezbednost IKEv1 mora posmatrati kao rezultat integrisanog funkcionisanja celokupne bezbednosne arhitekture. Važno je naglasiti da upravo kompleksnost Faze 1 predstavlja jedan od razloga zbog kojih je IKEv1 tokom višegodišnje primene pokazao određena ograničenja [2].

Naučno posmatrano, Faza 1 predstavlja operativnu realizaciju svih arhitektonskih principa analiziranih u prethodnom poglavlju. Integracijom organizacionih mehanizama ISAKMP okvira, kriptografskih principa Oakley okvira i adaptivnih karakteristika SKEME okvira uspostavlja se *IKE Security Association* kao prvi formalni izraz digitalnog poverenja između entiteta koji komuniciraju putem kriptografski zaštićenog komunikacionog kanala. Upravo će detaljna analiza pojedinačnih režima rada Faze 1 i njihovih bezbednosnih karakteristika i međusobnih razlika omogućiti potpunije razumevanje načina na koji IKEv1 ostvaruje zaštitu procesa razmene kriptografskih ključeva i predstavlja osnov za uspostavljanje bezbedne IPsec komunikacije [2], [77; SP 800-77 Rev. 1.].

Rezultati sprovedene analize pokazuju da se bezbednosne karakteristike Faze 1 ne mogu razumeti bez detaljnog razmatranja njenih operativnih režima rada. Iz tog razloga u nastavku rada posebno će biti analizirani *Main Mode* i *Aggressive Mode*, kao dva različita pristupa uspostavljanju *IKE Security Association*, sa posebnim osvrtom na njihove bezbednosne karakteristike, prednosti i ograničenja [53. RFC 2409]; [54; RFC 4306]; [77. SP 800-77 Rev. 1.]

4.2. Main mode – detaljna analiza bezbednosnih karakteristika

Main Mode predstavlja osnovni i bezbednosno najznačajniji režim rada prve faze *Internet Key Exchange Version 1* (IKEv1) protokola. Njegova primarna funkcija nije samo razmena kontrolnih poruka između komunikacionih entiteta, već uspostavljanje *IKE Security Association* (IKE SA) kao osnova za sve kasnije procese zaštite IPsec komunikacije.

Sa naučno-istraživačkog aspekta, *Main Mode* predstavlja formalizovani proces uspostavljanja digitalnog poverenja između komunikacionih strana, pri čemu se kroz sukcesivno definisane korake ostvaruju pregovaranje bezbednosnih parametara, razmena kriptografskog materijala, autentifikacija identiteta i formiranje zajedničkog bezbednosnog konteksta [2].

Jedna od najvažnijih karakteristika *Main Mode* režima jeste njegova višefazna struktura zasnovana na razmeni šest poruka između komunikacionih entiteta. Ovakva organizacija nije rezultat nepotrebne složenosti protokola, već predstavlja posledicu nastojanja projekatanta da svaka kritična bezbednosna funkcija bude realizovana u zasebnom, jasno definisanom procesu. Na taj način pregovaranje kriptografskih algoritama odvaja se od razmene *Diffie–Hellman* parametara, dok se autentifikacija učesnika komunikacije realizuje tek nakon što je uspostavljen odgovarajući nivo kriptografske zaštite. Ovakva sekvencijalna organizacija procesa značajno smanjuje mogućnost kompromitacije osetljivih bezbednosnih informacija tokom inicijalnog uspostavljanja komunikacije [31].

Proces započinje pregovaranjem bezbednosnih politika, pri čemu komunikacione strane razmenjuju informacije o podržanim algoritmima za enkripciju tj. zaštitu tajnosti, zaštitu integriteta, autentifikaciju i razmenu kriptografskih ključeva. Ovaj korak ima izuzetno veliki bezbednosni značaj, jer omogućava da obe strane usaglase skup kriptografskih mehanizama koji će biti korišćeni tokom uspostavljanja i održavanja komunikacije. Standardizovano pregovaranje parametara doprinosi interoperabilnosti različitih implementacija IKE protokola,

ali istovremeno zahteva pažljiv izbor bezbednosnih algoritama kako bi se izbegla upotreba zastarelih ili kriptografski oslabljenih rešenja [2].

Nakon uspešno usaglašenih bezbednosnih politika sledi razmena *Diffie–Hellman* parametara i generisanje zajedničke tajne. Upravo u ovom delu procesa ostvaruje se jedna od najvažnijih bezbednosnih karakteristika *Main Mode* režima rada IKE protokola, jer komunikacione strane uspostavljaju zajednički kriptografski materijal bez direktnog prenosa preko komunikacione mreže. Time se ostvaruje visok nivo otpornosti na prisluškivanje komunikacije, dok primena efemernih *Diffie–Hellman* vrednosti omogućava ostvarivanje principa *Perfect Forward Secrecy*, čime kompromitacija ključeva ne dovodi do kompromitacije prethodno uspostavljenih komunikacionih sesija. Poseban bezbednosni značaj *Main Mode* režima ogleda se u zaštiti identiteta komunikacionih entiteta [42].

Autentifikacija komunikacionih entiteta predstavlja završni korak procesa uspostavljanja IKE *Security Association*. U zavisnosti od konfiguracije sistema, autentifikacija može biti zasnovana na unapred deljenim ključevima (*Pre-Shared Key*), digitalnim sertifikatima ili digitalnim potpisima. Bez obzira na izabrani metod, osnovni cilj ostaje isti – kriptografski potvrditi identitet komunikacionih strana i sprečiti uspostavljanje poverenja sa neautorizovanim entitetima. Na taj način *Main Mode* objedinjuje kriptografsku razmenu ključeva i pouzdanu autentifikaciju u jedinstven proces uspostavljanja digitalnog poverenja. Koordinisano delovanje pregovaranja bezbednosnih politika, *Diffie–Hellman* razmene, zaštite identiteta, autentifikacije i uspostavljanja IKE *Security Association* omogućava ostvarivanje visokog nivoa otpornosti na različite kategorije napada.

Na primeru primene *Main Mode* potvrđujemo jednu od osnovnih teza ovog istraživanja da bezbednost ne predstavlja osobinu jednog algoritma ili jednog protokola, već rezultat pažljivo projektovane arhitekture u kojoj više međusobno povezanih bezbednosnih mehanizama funkcioniše kao jedinstven sistem zaštite informaciono-komunikacionog sistema [2].

Međutim, ovakav visok nivo bezbednosti ostvaren je uz cenu povećane složenosti procesa pregovaranja. Razmena šest poruka, veliki broj podržanih algoritama i različite mogućnosti konfiguracije povećavaju složenost sistema, složenost administracije sistema i zahtevaju pravilnu implementaciju svih komponenti IKEv1 arhitekture. Upravo zbog toga bezbednost *Main Mode* režima ne zavisi isključivo od njegove teorijske arhitekture, već i od kvaliteta implementacije, pravilne konfiguracije uređaja, izbora savremenih kriptografskih algoritama i efikasnog upravljanja životnim ciklusom formiranja *Security Association*. Ova činjenica potvrđuje da se bezbednosne karakteristike *Main Mode* režima mogu u potpunosti razumeti samo kroz integrisanu analizu kriptografskih, protokolarnih, implementacionih i operativnih aspekata njegovog funkcionisanja [51].

4.3. Aggressive mode – detaljna analiza bezbednosnih karakteristika

Aggressive Mode predstavlja alternativni režim rada prve faze *Internet Key Exchange Version 1* (IKEv1) protokola, razvijen sa ciljem ubrzavanja procesa uspostavljanja IKE *Security Association* između komunikacionih entiteta. Za razliku od *Main Mode* režima, koji razmenjuje šest poruka i postepeno ostvaruje pregovaranje bezbednosnih parametara, *Aggressive Mode* isti proces realizuje razmenom tri poruke. Sa operativnog aspekta, ovakav pristup omogućava brže uspostavljanje bezbedne komunikacije i smanjuje vreme potrebno za inicijalno pregovaranje, što može predstavljati značajnu prednost u okruženjima u kojima su brzina uspostavljanja veze, ograničeni mrežni resursi ili dinamične komunikacione sesije od posebnog značaja [2].

Jedna od osnovnih razlika između *Aggressive Mode* i *Main Mode* režima ogleda se u načinu razmene identiteta komunikacionih strana. Dok *Main Mode* identitet učesnika razmenjuje tek nakon uspostavljanja odgovarajuće kriptografske zaštite, *Aggressive Mode* prenosi identifikacione informacije u ranoj fazi pregovaranja. Posledica ovakvog projektantskog rešenja jeste da identitet komunikacionih entiteta može biti izložen posmatraču komunikacije pre nego što bude uspostavljen puni nivo zaštite. Sa aspekta zaštite privatnosti i anonimnosti komunikacionih strana, ovo predstavlja jedno od najznačajnijih bezbednosnih ograničenja *Aggressive Mode* režima [31].

Poseban bezbednosni izazov javlja se u slučajevima kada se autentifikacija zasniva na unapred dodeljenim kriptografskim ključevima (*Pre-Shared Key* – PSK). U takvim konfiguracijama informacije razmenjene tokom procesa pregovaranja mogu omogućiti napadaču prikupljanje materijala pogodnog za sprovođenje *offline dictionary* napada. Za razliku od napada koji zahtevaju kontinuiranu komunikaciju sa ciljnim sistemom, *offline dictionary* napadi omogućavaju da se prikupljeni podaci analiziraju van mreže korišćenjem velikog broja pretpostavljenih lozinki ili unapred pripremljenih rečnika. Ukoliko unapred dodeljeni ključ nije dovoljno složen ili je rezultat neadekvatne bezbednosne politike organizacije, povećava se verovatnoća njegove kompromitacije, čime može biti ugrožena celokupna bezbednost uspostavljenog komunikacionog odnosa [2].

Međutim, važno je naglasiti da uzrok navedenog bezbednosnog rizika nije isključivo sam *Aggressive Mode* protokola. Efikasnost ovakvih napada u velikoj meri zavisi od kvaliteta autentifikacionih kredencijala, izbora metoda autentifikacije, snage unapred dodeljenih ključeva i pravilne konfiguracije informaciono-komunikacionog sistema. Organizacije koje koriste kompleksne kriptografske tajne, sertifikate i PKI infrastrukturu i savremene bezbednosne politike mogu značajno umanjiti praktični rizik od uspešne realizacije ovakvih vektora napada. Ova činjenica potvrđuje jednu od centralnih teza istraživanja u okviru ove magistraske teze da bezbednost ne zavisi isključivo od arhitekture protokola, već podjednako od implementacije, konfiguracije i operativnog upravljanja informaciono-komunikacionim sistemom i monitoringom procesa koji se izvršavaju u realnom vremenu [46].

Sa aspekta bezbednosnog inženjerstva, *Aggressive Mode* predstavlja primer kompromisa između performansi i zaštite. Smanjenje broja razmenjenih poruka doprinosi povećanju efikasnosti procesa pregovaranja i smanjenju latencije uspostavljanja veze, ali istovremeno povećava izloženost pojedinih bezbednosno osetljivih informacija tokom inicijalne faze komunikacije. Time se potvrđuje da pojednostavljenje protokolarnih procedura ne mora uvek rezultirati povećanjem ukupnog nivoa bezbednosti, već može dovesti do povećanja površine izložene vektorima napada (*podložne napadu*) koja je meta napadača (eng: *attack surface*) ukoliko nisu primenjene odgovarajuće kompenzacije mere zaštite [38],[42].

Analiza višegodišnje primene IKEv1 pokazala je da je upravo *Aggressive Mode* bio predmet brojnih bezbednosnih istraživanja, akademskih analiza i praktičnih procena rizika. Identifikovane slabosti nisu dovele u pitanje osnovne kriptografske principe na kojima počiva IKEv1, već su ukazale na potrebu pojednostavljenja protokolarnе arhitekture, unapređenja zaštite identiteta i smanjenja mogućnosti pogrešne konfiguracije sistema. Upravo su ova iskustva predstavljala jedan od značajnih podsticaja za razvoj *Internet Key Exchange Version 2* (IKEv2), u kojem su brojna projektantska rešenja redefinisana sa ciljem povećanja bezbednosti, interoperabilnosti i povećanja otpornosti na savremene vektore napada na informaciono-komunikacione sisteme [2], [31].

Naučno posmatrano, *Aggressive Mode* potvrđuje da projektovanje bezbednosnih protokola predstavlja proces balansiranja između različitih bezbednosnih i operativnih zahteva. Njegova analiza pokazuje da povećanje efikasnosti može biti ostvareno samo uz pažljivu procenu bezbednosnih posledica svake projektantske odluke. Iz tog razloga *Aggressive Mode* ne predstavlja neuspeh IKEv1 arhitekture, već vredan izvor iskustava koji je omogućio identifikaciju ograničenja prve generacije *Internet Key Exchange* protokola i postavio osnov za razvoj bezbednosno unapređene arhitekture IKEv2 [2].

Analiza bezbednosnih karakteristika *Aggressive Mode*-a pokazuje da njegove identifikovane ranjivosti ne predstavljaju isključivo ograničenja jednog autentifikacionog mehanizma, već odražavaju razvojni stepen tadašnje generacije protokola za automatizovanu razmenu kriptografskih ključeva. Prioritet koji je tokom projektovanja dat smanjenju broja komunikacionih poruka i ubrzanju procesa uspostavljanja bezbednosne asocijacije imao je neposredan uticaj na nivo zaštite identiteta komunikacionih učesnika i otpornost sistema na određene klase napada. Time je potvrđena jedna od osnovnih karakteristika bezbednosnog inženjerstva – unapređenje performansi veoma često zahteva kompromis u pogledu pojedinih bezbednosnih svojstava. Međutim, upravo kroz praktičnu primenu *Aggressive Mode*-a postalo je moguće identifikovati njegove operativne i bezbednosne nedostatke u realnim mrežnim okruženjima. Analize sprovedene tokom višegodišnje primene IKEv1 pokazale su da zaštita identiteta učesnika, otpornost na offline dictionary napade, jednostavnost implementacije i mogućnost efikasnijeg upravljanja bezbednosnim asocijacijama predstavljaju oblasti koje zahtevaju sistemski unapređenja. Ova saznanja nisu predstavljala argument za odbacivanje koncepta *Internet Key Exchange* protokola, već su postala osnov za njegovo metodološko i arhitektonsko unapređenje [2], [31].

Posmatrano kroz procesni pristup, *Aggressive Mode* predstavlja značajnu fazu evolucije bezbednosnih protokola. Njegove identifikovane slabosti omogućile su precizno definisanje zahteva koje nova generacija protokola mora da ispuni kako bi obezbedila viši nivo bezbednosne otpornosti. Upravo na osnovu ovih iskustava razvijen je IKEv2, u kome su unapređeni proces pregovaranja, zaštita identiteta učesnika, upravljanje bezbednosnim asocijacijama, mehanizmi otpornosti na DoS napade, podrška za NAT Traversal, efikasnije upravljanje životnim ciklusom *Security Association* objekata i pojednostavljena implementacija protokola. Sa naučno-istraživačkog aspekta, razvoj IKEv2 ne može se posmatrati kao diskontinuitet u odnosu na IKEv1, već kao rezultat procesa institucionalnog i tehničkog učenja zasnovanog na iskustvima stečenim tokom implementacije prve generacije protokola.

Iz perspektive procesnog modela razvijenog u ovom radu, može se zaključiti da bezbednost nije rezultat jednokratnog projektovanja protokola, već kontinuiranog procesa analize, evaluacije, identifikacije ograničenja, implementacije unapređenja i ponovne validacije bezbednosnih mehanizama. Upravo zbog toga razvoj *Internet Key Exchange* protokola predstavlja ilustrativan primer kako se kroz sistematsku analizu ranjivosti ostvaruje kontinuirano povećanje bezbednosne otpornosti komunikacionih sistema. Iz tog razloga, *Aggressive Mode* ne predstavlja neuspeh arhitekture IKEv1, već dragocen izvor empirijskih saznanja koji je omogućio identifikaciju ograničenja prve generacije *Internet Key Exchange* protokola i postavio naučne, metodološke i tehničke osnove za razvoj bezbednosno unapređene arhitekture IKEv2. Upravo sposobnost da se identifikovane slabosti transformišu u unapređene bezbednosne mehanizme predstavlja jedno od temeljnih obeležja evolucije savremenih kriptografskih protokola i potvrđuje da se bezbednosna otpornost ostvaruje kroz

kontinuirani proces učenja, prilagođavanja i unapređenja, a ne kroz statički skup tehnologija.

Tabela 7. Komparativna analiza IKEv1 i IKEv2

Karakteristika	IKEv1	IKEv2
Godina standardizacije	1998 (RFC 2409)	2005 / 2014 (RFC 4306, RFC 7296)
Status	Historic (RFC 9395)	Preporučeni standard
Broj poruka za inicijalnu razmenu	6 (Main Mode) ili 3 (Aggressive Mode)	4
Faze razmene	Phase 1 i Phase 2	IKE_SA_INIT i IKE_AUTH
Zaštita identiteta	Main Mode: da; Aggressive Mode: ne	Da (u svim konfiguracijama)
Autentifikacija	PSK, digitalni sertifikati, RSA	PSK, digitalni sertifikati, EAP
Perfect Forward Secrecy	Podržano	Podržano
NAT Traversal	Proširenje (dodatna specifikacija)	Integrisana podrška
MOBIKE	Nije podržan	Podržan
Otpornost na DoS napade	Ograničena	Cookie mehanizam
Složenost implementacije	Veća kompleksnost implementacije u produkcionom okruženju	Manja i efikasnija
Preporučena upotreba	Legacy sistemi (još uvek se koriste na hardveru koji ne podržava IKEv2 protokol)	Savremene implementacije

Izvor: Autor, na osnovu sinteze relevantnih RFC dokumenata (RFC 2409, RFC 4306, RFC 7296, RFC 9395)

Podaci prikazani u tabeli 7 sumiraju ključne arhitekturne i proceduralne razlike između IKEv1 i IKEv2 protokola, ukazujući na fundamentalnu evoluciju u pristupu uspostavljanju bezbednih asocijacija. Dok IKEv1 karakteriše dvofazna struktura razmene (Phase 1 i Phase 2) sa mogućnošću izbora između Main Mode i Aggressive Mode, IKEv2 uvodi pojednostavljenu i objedinjenu proceduru kroz (IKE_SA_INIT i IKE_AUTH) razmene, čime se broj neophodnih poruka za inicijalno uspostavljanje asocijacije redukuje sa šest (u Main Mode konfiguraciji) na svega četiri. Ova strukturna konsolidacija direktno se odražava na smanjenu kompleksnost implementacije i veću efikasnost protokola, što je i formalno potvrđeno statusom IKEv1 kao „Historic” protokola prema RFC 9395, u odnosu na IKEv2 koji predstavlja preporučeni savremeni standard.

Sa bezbednosnog stanovišta, tabela ukazuje na značajna unapređenja koja IKEv2 unosi u odnosu na prethodnika, posebno u pogledu otpornosti na DoS napade kroz implementaciju cookie mehanizma, koji u IKEv1 nije bio standardizovan na jednak način. Dodatno, IKEv2 obezbeđuje doslednu zaštitu identiteta učesnika u svim konfiguracijama, za razliku od IKEv1 gde je ova zaštita uslovljena izborom moda razmene (Aggressive Mode ne pruža zaštitu

identiteta). Uvođenje integrisane podrške za NAT Traversal i MOBIKE ekstenziju u IKEv2 dodatno proširuje funkcionalni obim protokola, omogućavajući stabilnije funkcionisanje u mobilnim i NAT okruženjima, dok mehanizam Perfect Forward Secrecy ostaje zajednička karakteristika oba protokola kao jedan od temeljnih bezbednosnih zahteva IKE arhitekture.

4.4. Komparativna analiza main mode i aggressive mode

Komparativna analiza *Main Mode* i *Aggressive Mode* režima predstavlja jedan od ključnih elemenata za razumevanje bezbednosne arhitekture *Internet Key Exchange Version 1* (IKEv1) protokola. Iako oba režima rada protokola imaju isti osnovni cilj – uspostavljanje *IKE Security Association* (IKE SA) između komunikacionih entiteta – projektovana su prema različitim bezbednosnim i operativnim prioritetima. Upravo zbog toga njihovo poređenje ne treba posmatrati kao analizu dva različita protokola, već kao analizu dva različita pristupa rešavanju istog bezbednosnog problema, pri čemu svaki od njih predstavlja kompromis između nivoa zaštite, efikasnosti komunikacije i složenosti implementacije [2].

Sa aspekta arhitekture informaciono-komunikacionog sistema, *Main Mode* zasniva se na principu postepenog uspostavljanja digitalnog poverenja. Razmena šest poruka omogućava da se svaka kritična bezbednosna funkcija – pregovaranje bezbednosnih politika, razmena *Diffie-Hellman* parametara, zaštita identiteta i autentifikacija – realizuje u zasebnoj fazi procesa. Ovakav pristup omogućava da se identitet komunikacionih strana razmenjuje tek nakon uspostavljanja odgovarajućeg nivoa kriptografske zaštite, čime se značajno povećava zaštita privatnosti i smanjuje mogućnost prikupljanja podataka od strane potencijalnog napadača [2], [77; SP 800-77 Rev. 1.].

Nasuprot tome, *Aggressive Mode* projektovan je sa ciljem smanjenja broja razmenjenih poruka i ubrzavanja procesa uspostavljanja komunikacije. Ovakva optimizacija omogućava efikasnije uspostavljanje *IKE Security Association*, ali istovremeno zahteva da se pojedine bezbednosne funkcije izvršavaju ranije tokom procesa pregovaranja. Posledica takvog projektantskog pristupa jeste da identitet komunikacionih entiteta može biti izložen pre nego što bude uspostavljen neophodan stepen kriptografske zaštite da bi informaciono-komunikacioni sistem bio su stanju bezbednosti. Time se povećava mogućnost prikupljanja informacija koje mogu biti iskorišćene tokom pripreme budućih napada ili prilikom sprovođenja *offline dictionary* napada u konfiguracijama koje koriste autentifikaciju zasnovanu na unapred dodeljenim ključevima [2].

Naučno posmatrano, osnovna razlika između ova dva režima ne ogleda se u njihovoj funkcionalnosti, već u različitom pristupu upravljanju bezbednosnim rizikom. *Main Mode* daje prioritet zaštiti identiteta, otpornosti na napade i očuvanju poverljivosti bezbednosno osetljivih informacija, prihvatajući veću složenost procesa pregovaranja kao cenu višeg nivoa bezbednosti. *Aggressive Mode*, sa druge strane, daje prioritet brzini uspostavljanja komunikacije i operativnoj efikasnosti, prihvatajući povećanu izloženost pojedinih bezbednosnih informacija kao projektantski kompromis. Ovakva razlika potvrđuje da bezbednost informaciono-komunikacionih sistema ne predstavlja apsolutnu kategoriju, već rezultat kontinuiranog balansiranja između različitih funkcionalnih i operativnih zahteva [31].

Posebno značajna razlika između analiziranih režima rada odnosi se na zaštitu identiteta komunikacionih strana. U savremenim informaciono-komunikacionim sistemima zaštita identiteta predstavlja važnu komponentu ukupne bezbednosti, budući da identifikacija učesnika komunikacije može predstavljati početni korak u planiranju ciljanih napada, prikupljanju obaveštajnih podataka ili profilisanju mrežne infrastrukture. Iz tog razloga *Main*

Mode ostvaruje viši nivo zaštite privatnosti u odnosu na *Aggressive Mode*, što predstavlja jednu od njegovih najznačajnijih bezbednosnih prednosti [30].

Komparativna analiza pokazuje da *Main Mode* i *Aggressive Mode* predstavljaju dva različita projektantska pristupa ostvarivanju istog bezbednosnog cilja – uspostavljanju *IKE Security Association*. *Main Mode* ostvaruje viši nivo zaštite identiteta i veću otpornost na pojedine kategorije napada, dok *Aggressive Mode* omogućava veću operativnu efikasnost kroz smanjenje broja razmenjenih poruka i vremena potrebnog za uspostavljanje komunikacije. Iskustva stečena višegodišnjom primenom oba režima pokazala su da povećanje fleksibilnosti i performansi može dovesti do povećanja površine (eng: *attack surface*) raspoložive napadaču za vektor napada usmeren ka informaciono-komunikacionom sistemu. Ukoliko nije primenjen monitoring procesa u realnom vremenu u sistemu sa odgovarajućim mehanizmima zaštite (u praksi se primenjuje automatizovana analiza *log* datoteka i neophodna je uključenost *IT security* personala). Upravo su ove projektantske pouke predstavljale jedan od ključnih razloga za redefinisane procesa uspostavljanja bezbedne komunikacije u *Internet Key Exchange Version 2* (IKEv2), čija arhitektura nastoji da objedini visok nivo bezbednosti, pojednostavljenu implementaciju i unapređenu interoperabilnost, uz istovremeno smanjenje mogućnosti konfiguracionih i implementacionih grešaka [2].

4.5. Bezbednosne karakteristike faze 2 ikev1 protokola quick mode i uspostavljanje ipsec security association

Quick Mode predstavlja drugu fazu *Internet Key Exchange Version 1* (IKEv1) protokola i ima ključnu ulogu u operacionalizaciji bezbednosnih mehanizama uspostavljenih tokom prve faze pregovaranja. Dok je osnovni cilj Faze 1 bio uspostavljanje *IKE Security Association* (IKE SA) i izgradnja kriptografski zasnovanog digitalnog poverenja između komunikacionih entiteta, *Quick Mode* koristi već uspostavljeni zaštićeni upravljački kanal za pregovaranje parametara neophodnih za zaštitu korisničkog IP saobraćaja. Sa naučno-istraživačkog aspekta, Faza 2 predstavlja prelazak sa uspostavljanja poverenja na njegovu operativnu primenu, čime IKEv1 ostvaruje osnovnu svrhu svog postojanja – omogućavanje bezbednog funkcionisanja IPsec arhitekture [2].

Povezanost između Faze 1 i Faze 2 predstavlja jednu od najvažnijih bezbednosnih karakteristika IKEv1 protokola. *Quick Mode* ne može funkcionisati nezavisno od prethodno uspostavljenog *IKE Security Association*, budući da se svi pregovori u drugoj fazi odvijaju kroz već autentifikovan i kriptografski zaštićen komunikacioni kanal.

Ovakvo projektantsko rešenje značajno smanjuje mogućnost kompromitacije procesa pregovaranja, jer se bezbednosno osetljive informacije razmenjuju tek nakon što su komunikacioni entiteti uspešno izvršili međusobnu autentifikaciju i uspostavili zajedničku kriptografsku osnovu. Time se potvrđuje princip višeslojne zaštite, prema kojem svaki naredni bezbednosni mehanizam zavisi od uspešno realizovanog prethodnog koraka [52; RFC 2408], [53; RFC 2409].

Osnovni rezultat *Quick Mode* pregovaranja jeste uspostavljanje *IPsec Security Association* (IPsec SA), koja predstavlja operativni bezbednosni kontekst za zaštitu korisničkog mrežnog saobraćaja. Za razliku od *IKE Security Association*, čija je funkcija zaštita upravljačkih poruka i procesa pregovaranja, *IPsec Security Association* definiše konkretne parametre koji će biti primenjeni prilikom zaštite IP paketa. U okviru IPsec SA određuju se algoritmi za enkripciju, algoritmi za zaštitu integriteta, bezbednosni identifikatori (SPI), trajanje bezbednosne asocijacije, kao i drugi parametri koji neposredno određuju način funkcionisanja *Authentication Header* (AH) i *Encapsulating Security Payload* (ESP) protokola [2].

Jedna od najvažnijih funkcija *Quick Mode* procesa jeste pregovaranje bezbednosnih parametara koji će biti korišćeni za zaštitu korisničkog saobraćaja. Poseban značaj *Quick Mode* procesa ogleda se u generisanju i izvođenju sesijskog kriptografskog materijala (KEYMAT). Za razliku od zajedničke tajne uspostavljene tokom Faze 1, KEYMAT predstavlja skup kriptografskih ključeva izvedenih za potrebe konkretne IPsec *Security Association*. Ovi ključevi koriste se za zaštitu korisničkog saobraćaja primenom AH i ESP protokola i predstavljaju neposrednu osnovu za ostvarivanje poverljivosti, integriteta i autentifikacije IP paketa. Izvođenje KEYMAT vrednosti iz prethodno uspostavljenog kriptografskog materijala omogućava da različite bezbednosne asocijacije koriste međusobno nezavisne sesijske ključeve, čime se povećava ukupna otpornost sistema na kompromitaciju pojedinačnih komunikacionih sesija [53; RFC 2409].

Dodatni nivo bezbednosti može biti ostvaren opcionom primenom *Perfect Forward Secrecy* (PFS) tokom *Quick Mode* procesa. U tom slučaju generiše se novi *Diffie–Hellman* materijal za potrebe uspostavljanja IPsec *Security Association*, čime kompromitacija jednog skupa ključeva ne dovodi do kompromitacije drugih komunikacionih sesija. Primena PFS povećava složenost procesa pregovaranja, ali značajno unapređuje dugoročnu otpornost sistema na postkompromitacione scenarije. Iz tog razloga odluka o primeni PFS predstavlja primer balansiranja između bezbednosnih zahteva i raspoloživih računarskih resursa, pri čemu organizacije sa visokim zahtevima za zaštitu poverljivih podataka često daju prednost povećanom nivou bezbednosti u odnosu na performanse [25].

Važan aspekt *Quick Mode* procesa odnosi se na upravljanje životnim ciklusom IPsec *Security Association*. Bezbednosna asocijacija nije trajna kategorija, već poseduje unapred definisano vreme trajanja ili količinu prenosa podataka nakon koje je neophodno izvršiti obnovu IPsec *Security Association*.. Ovakav pristup smanjuje rizik dugotrajne upotrebe istog kriptografskog materijala i omogućava periodičnu obnovu bezbednosnih parametara. Upravljanje životnim ciklusom *Security Association* predstavlja važan element ukupne bezbednosne arhitekture, jer omogućava očuvanje kontinuiteta zaštite uz istovremeno ograničavanje posledica eventualne kompromitacije pojedinačnih sesijskih ključeva [2].

Naučno posmatrano, *Quick Mode* potvrđuje jednu od osnovnih teza ovog istraživanja da bezbednost informaciono-komunikacionog sistema predstavlja kontinuirani proces u kojem se digitalno poverenje uspostavljeno tokom inicijalnog pregovaranja transformiše u praktičnu zaštitu korisničkog saobraćaja. Istovremeno, analiza ovog mehanizma pokazuje da efikasnost IPsec arhitekture ne zavisi isključivo od kvaliteta pojedinačnih algoritama, već od njihove pravilne integracije sa protokolima za upravljanje ključevima, odgovarajućeg upravljanja životnim ciklusom *Security Association* struktura i dosledne primene bezbednosnih politika. Upravo ovakav integrisani pristup predstavlja osnov dugoročne otpornosti savremenih informaciono-komunikacionih sistema na kompleksne bezbednosne pretnje [10].

Prikazani model ističe da SAD funkcioniše kao izvršni sloj IPsec arhitekture koji se logički razlikuje od SPD-a: dok SPD određuje šta i kako treba zaštititi na osnovu bezbednosne politike, SAD čuva konkretne operative parametre (SPI, algoritme, ključeve, lifetime, sekvencne brojeve) neophodne za stvarnu primenu zaštite nad paketima. Ova podela odgovornosti, prikazana kroz odnos SPD–SAD–IPsec modul, obezbeđuje skalabilnost i efikasnu pretragu u realnom vremenu čak i pri velikom broju istovremenih SA zapisa, dok mehanizmi sinhronizacije preklapajućih (overlapping) SA tokom rekeying procesa garantuju kontinuitet zaštićene komunikacije bez prekida saobraćaja. Ove karakteristike SAD-a direktno

utiču na otpornost IPsec infrastrukture na napade tipa key exhaustion i replay, što je relevantno za dalju analizu bezbednosnih izazova IKE protokola u kontekstu IRNL i IRNL-PQC modela razvijenih u ovom radu. (Prilog “B”) u radu.

4.6. Metode autentifikacije u ikev1 protokolu i njihov bezbednosni značaj

Autentifikacija predstavlja jednu od fundamentalnih bezbednosnih funkcija savremenih informaciono-komunikacionih sistema i jedan od osnovnih preduslova za uspostavljanje digitalnog poverenja između komunikacionih entiteta. U kontekstu *Internet Key Exchange Version 1* (IKEv1) protokola, njen značaj prevazilazi klasičnu proveru identiteta korisnika ili uređaja, budući da predstavlja završnu fazu procesa tokom kojeg se potvrđuje da je entitet sa kojim se ostvaruje komunikacija zaista entitet za koji se predstavlja. Tek nakon uspešno sprovedene autentifikacije može se smatrati da su ispunjeni uslovi za bezbedno uspostavljanje *IKE Security Association* (IKE SA), a samim tim i za dalje pregovaranje IPsec *Security Association* (IPsec SA) koja će štititi korisnički mrežni saobraćaj [53; RFC 2409].

Sa naučno-istraživačkog aspekta, neophodno je razlikovati pojmove identifikacije, autentifikacije i autorizacije, budući da se u stručnoj literaturi oni često pogrešno poistovećuju. Identifikacija predstavlja proces u kojem komunikacioni entitet saopštava svoj identitet drugoj strani, dok autentifikacija podrazumeva kriptografski zasnovanu proveru da je taj identitet autentičan i da zaista pripada subjektu koji ga predstavlja. Autorizacija predstavlja naredni korak u kojem se, nakon uspešno potvrđenog identiteta, određuju prava pristupa resursima informaciono-komunikacionog sistema. U arhitekturi IKEv1 upravo autentifikacija predstavlja kritičnu tačku prelaska sa deklarisanog na dokazani identitet, čime se uspostavlja osnova za izgradnju međusobnog poverenja između komunikacionih strana [53; RFC 2409].

Poseban značaj autentifikacije proizlazi iz činjenice da bezbedna razmena kriptografskih ključeva sama po sebi nije dovoljna za ostvarivanje bezbedne komunikacije. *Diffie–Hellman* algoritam omogućava dvema stranama da uspostave zajedničku tajnu preko nesigurne mreže, ali ne pruža garantovanje identiteta komunikacionih strana. Ukoliko proces autentifikacije izostane ili bude neadekvatno implementiran, napadač može pokušati da se predstavi kao legitimni učesnik komunikacije i time ugrozi bezbednost celokupnog procesa pregovaranja. Iz tog razloga autentifikacija predstavlja mehanizam kojim se matematička sigurnost razmene ključeva dopunjuje proverom identiteta, čime se uspostavlja potpuni model digitalnog poverenja [44].

U okviru IKEv1 protokola autentifikacija nije izolovana funkcija, već sastavni deo integrisane bezbednosne arhitekture. Njena uspešnost neposredno zavisi od kvaliteta prethodno sprovedenog pregovaranja bezbednosnih parametara, pravilne implementacije *Diffie–Hellman* razmene, pouzdanog generisanja kriptografskog materijala i pravilnog upravljanja *Security Association* strukturama. Na taj način autentifikacija predstavlja završni korak u procesu uspostavljanja poverenja, ali istovremeno i početnu tačku od koje zavisi bezbednost svih narednih operacija koje će biti realizovane unutar IPsec okruženja [10],[2].

Analizirajući bezbednosnu arhitekturu IKEv1 može se uočiti da različiti modeli autentifikacije ne pružaju isti nivo zaštite niti su podjednako pogodni za sva operativna okruženja iz razloga što svako operativno okruženje ima svoje specifičnosti i izloženo je različitim vrstama napada. Upotreba unapred dodeljenih ključeva (*Pre-Shared Key* – PSK), digitalnih sertifikata ili digitalnih potpisa predstavlja različite pristupe rešavanju istog bezbednosnog problema – dokazivanju identiteta komunikacionih entiteta. Svaki od ovih modela poseduje specifične prednosti, ograničenja i bezbednosne implikacije koje se moraju analizirati u kontekstu

konkretnih organizacionih, tehničkih i operativnih zahteva. Izbor odgovarajuće metode autentifikacije zbog toga predstavlja stratešku bezbednosnu odluku koja neposredno utiče na nivo otpornosti celokupnog informaciono-komunikacionog sistema [4].

Sa aspekta savremenog bezbednosnog inženjerstva, autentifikacija predstavlja mnogo više od tehničkog postupka potvrde identiteta. Ona je centralni mehanizam kojim se uspostavlja odnos poverenja između komunikacionih strana i kojim se sprečava da kriptografski zaštićeni komunikacioni kanal bude uspostavljen sa neautorizovanim ili zlonamernim entitetima. Upravo zbog toga kvalitet implementiranog autentifikacionog mehanizma neposredno određuje ukupni nivo bezbednosti IKEv1 protokola, bez obzira na snagu primenjenih algoritama za enkripciju ili razmenu ključeva [53; RFC 2409].

Naučno posmatrano, analiza metoda autentifikacije potvrđuje jednu od osnovnih teza ovog istraživanja da digitalno poverenje ne predstavlja isključivu posledicu primene snažnih kriptografskih algoritama. Ono nastaje tek integracijom pouzdane razmene kriptografskih ključeva, verifikacije identiteta, pravilnog upravljanja bezbednosnim asocijacijama i dosledne primene bezbednosnih politika. Iz tog razloga autentifikacija predstavlja ključnu vezu između kriptografske sigurnosti i operativne bezbednosti informaciono-komunikacionog sistema, čime postaje jedan od najznačajnijih elemenata ukupne bezbednosne arhitekture Internet Key Exchange Version 1 protokola [31].

– ***Pre-Shared Key (PSK)*** – bezbednosna analiza i kritička evaluacija

Pre-Shared Key (PSK) predstavlja jedan od najstarijih i najčešće primenjivanih metoda autentifikacije u *Internet Key Exchange Version 1 (IKEv1)* protokolu. Njegov osnovni princip zasniva se na činjenici da komunikacioni entiteti pre uspostavljanja VPN komunikacije poseduju unapred dogovorenu zajedničku tajnu koja se koristi za dokazivanje identiteta tokom procesa autentifikacije. Za razliku od modela zasnovanih na infrastrukturi javnih ključeva, PSK ne zahteva postojanje sertifikacionih autoriteta niti složene mehanizme upravljanja digitalnim sertifikatima, zbog čega predstavlja jednostavno i praktično rešenje za manja informaciono-komunikaciona okruženja [53; RFC 2409].

Sa arhitektonskog aspekta, PSK nije mehanizam za razmenu kriptografskih ključeva, već metod potvrde identiteta komunikacionih strana nakon što je tokom Diffie–Hellman procesa uspostavljen zajednički kriptografski materijal. Njegova funkcija jeste dokazivanje da obe strane raspolazu istom unapred definisanom tajnom, čime se potvrđuje njihov identitet i omogućava bezbedno uspostavljanje *IKE Security Association*. Na taj način PSK predstavlja završni korak procesa uspostavljanja digitalnog poverenja između komunikacionih entiteta, pri čemu kvalitet tog poverenja neposredno zavisi od kvaliteta unapred definisane zajedničke tajne [31].

Međutim, upravo jednostavnost rešenja u ovom slučaju predstavlja i jedno od osnovnih ograničenja PSK autentifikacije. Bezbednost PSK autentifikacije u potpunosti zavisi od kvaliteta unapred definisane zajedničke tajne. Ukoliko korisnici primenjuju kratke, predvidive ili lozinke koje se lako pamte, povećava se mogućnost njihove kompromitacije različitim tehnikama pogađanja ili iscrpnog pretraživanja prostora mogućih vrednosti. U takvim okolnostima matematička otpornost kriptografskih algoritama više nije odlučujući faktor bezbednosti, već ljudski faktor i kvalitet bezbednosne politike upravljanja autentifikacionim podacima [42].

– Digitalni sertifikati i infrastruktura javnih ključeva (PKI) – bezbednosna analiza i kritička evaluacija

Digitalni sertifikati i infrastruktura javnih ključeva (*Public Key Infrastructure* – PKI) predstavljaju jedan od najznačajnijih modela autentifikacije u *Internet Key Exchange Version 1* (IKEv1) protokolu. Za razliku od autentifikacije zasnovane na unapred deljenim tajnama, koja poverenje gradi na zajedničkom poznavanju istog autentifikacionog podatka, PKI uvodi model u kojem se identitet komunikacionog entiteta potvrđuje primenom kriptografije javnog ključa i digitalno potpisanih sertifikata. Na taj način digitalno poverenje više ne zavisi od čuvanja zajedničke tajne između svih učesnika komunikacije, već od pouzdanosti infrastrukture koja izdaje, potvrđuje i održava digitalne identitete.

Osnovu ovog modela čine digitalni sertifikati, najčešće u skladu sa standardom X.509, koji predstavljaju elektronske dokumente kojima se potvrđuje veza između identiteta subjekta i njegovog javnog kriptografskog ključa. Sertifikat sadrži podatke o vlasniku, javni ključ, period važenja, identitet izdavaoca i digitalni potpis sertifikacionog autoriteta (CA). Uloga digitalnog potpisa jeste da omogući svakom učesniku komunikacije proveru autentičnosti sertifikata i utvrđivanje da njegov sadržaj nije menjan nakon izdavanja. Time sertifikat postaje kriptografski dokaz identiteta koji može biti verifikovan bez potrebe za prethodno uspostavljenom zajedničkom tajnom između komunikacionih strana [46].

Centralnu ulogu u PKI arhitekturi ima sertifikacioni autoritet (*Certification Authority* – CA), koji predstavlja instituciju od poverenja odgovornu za izdavanje, potpisivanje i upravljanje digitalnim sertifikatima. Bezbednost celokupnog modela zasniva se na pretpostavci da komunikacioni entiteti imaju poverenje u sertifikacioni autoritet i njegov javni ključ. Drugim rečima, poverenje se ne uspostavlja direktno između svih korisnika sistema, već se prenosi preko pouzdanog posrednika koji potvrđuje identitet svakog učesnika komunikacije. Ovakav model omogućava značajno veću skalabilnost (veći broj korisnika) u odnosu na autentifikaciju zasnovanu na unapred deljenim ključevima, jer se broj potrebnih zajedničkih tajni ne povećava proporcionalno broju komunikacionih entiteta [46].

Poseban bezbednosni značaj PKI infrastrukture ogleda se u mogućnosti provere statusa sertifikata tokom njegovog životnog ciklusa. Digitalni sertifikat može biti opozvan pre isteka perioda važenja ukoliko dođe do kompromitacije privatnog ključa, promene identiteta vlasnika ili drugih bezbednosno relevantnih okolnosti (prekid radnog odnosa i sl.). Zbog toga savremena infrastruktura javnih ključeva predviđa mehanizme za proveru opozvanih sertifikata, čime se sprečava da kompromitovani ili nevažeći identiteti ostanu prihvaćeni u procesu autentifikacije. Ovakav pristup značajno unapređuje upravljanje digitalnim poverenjem, jer omogućava da se status identiteta dinamički prilagođava stvarnim bezbednosnim okolnostima [9].

Sa aspekta bezbednosne arhitekture IKEv1 protokola, primena digitalnih sertifikata značajno povećava otpornost procesa autentifikacije na vektore napada. Za razliku od modela zasnovanih na zajedničkim tajnama, kompromitacija jednog privatnog ključa ne zahteva promenu autentifikacionih podataka svih ostalih učesnika sistema. Istovremeno, mogućnost izdavanja jedinstvenog sertifikata svakom komunikacionom entitetu omogućava preciznije upravljanje identitetima, jednostavnije sprovođenje bezbednosnih politika (autorizacija pristupa određenim bazama podataka koje su po klasifikaciji od vitalnog značaja za nacionalnu bezbednost) i efikasnije upravljanje distribuiranim informaciono-komunikacionim sistemima [38],[42].

Međutim, primena PKI infrastrukture uvodi i nove organizacione i bezbednosne izazove. Bezbednost sistema više ne zavisi isključivo od kvaliteta kriptografskih algoritama, već i od pravilnog funkcionisanja sertifikacionih autoriteta, zaštite njihovih privatnih ključeva, tačnosti procesa izdavanja sertifikata i bezbednog upravljanja čitavim životnim ciklusom digitalnih identiteta. Kompromitacija sertifikacionog autoriteta može imati dalekosežne posledice, jer može dovesti u pitanje poverenje u veliki broj sertifikata i komunikacionih odnosa koji su zasnovani na toj infrastrukturi. Iz tog razloga zaštita PKI sistema predstavlja jedan od najznačajnijih organizacionih izazova savremenog bezbednosnog inženjerstva [46]. Naučno posmatrano, infrastruktura javnih ključeva predstavlja prelazak sa lokalnog modela poverenja zasnovanog na zajedničkim tajnama na institucionalni model digitalnog poverenja zasnovan na kriptografski proverljivim identitetima. Ovakav pristup omogućava veću skalabilnost, efikasnije upravljanje velikim brojem komunikacionih entiteta i viši nivo interoperabilnosti između različitih informaciono-komunikacionih sistema. Istovremeno, analiza pokazuje da bezbednost PKI modela nije određena isključivo kvalitetom kriptografije javnog ključa, već podjednako zavisi od pouzdanosti sertifikacionih autoriteta, pravilnog upravljanja životnim ciklusom sertifikata, bezbedne implementacije i dosledne primene organizacionih procedura. Time se potvrđuje osnovna teza ovog istraživanja da digitalno poverenje predstavlja rezultat integrisanog delovanja tehničkih, organizacionih i institucionalnih mehanizama zaštite, a ne isključivo primene pojedinačnih kriptografskih algoritama [33],[46],[71; RFC 4945.].

4.7. Kriptografski algoritmi u ikev1 protokolu i njihov bezbednosni značaj

Kriptografski algoritmi predstavljaju osnovu bezbednosne arhitekture *Internet Key Exchange Version 1* (IKEv1) protokola, budući da omogućavaju ostvarivanje osnovnih bezbednosnih ciljeva koji obuhvataju poverljivost, integritet i autentifikaciju komunikacije. Međutim, njihova uloga u okviru IKEv1 ne može se posmatrati izolovano od celokupne protokolarne arhitekture. Za razliku od teorijskih aspekata kriptografije, koji su detaljno analizirani u prethodnim poglavljima ove magistarske teze, u okviru IKEv1 algoritmi predstavljaju funkcionalne komponente integrisanog sistema za uspostavljanje i održavanje digitalnog poverenja između komunikacionih entiteta. Njihova bezbednosna vrednost proizlazi iz međusobne koordinacije tokom procesa pregovaranja, razmene ključeva i zaštite korisničkog IP saobraćaja [2].

Za ostvarivanje tajnosti podataka IKEv1 podržava primenu različitih simetričnih algoritama za šifrovanje, među kojima su istorijski značaj imali *Data Encryption Standard* (DES), *Triple Data Encryption Standard* (3DES) i *Advanced Encryption Standard* (AES). Tokom razvoja protokola izbor algoritma predstavljao je važan element pregovaranja bezbednosnih politika između komunikacionih entiteta, pri čemu su obe strane morale postići saglasnost o algoritmu koji će biti korišćen za zaštitu komunikacije. Ovakav model pregovaranja omogućio je interoperabilnost između različitih implementacija IKEv1, ali je istovremeno zahtevao pažljivo upravljanje podržanim skupom algoritama kako bi se izbegla primena kriptografski zastarelih rešenja [31], [47].

Sa savremenog bezbednosnog aspekta, istorijski razvoj ovih algoritama jasno pokazuje evoluciju zahteva za zaštitom digitalnih komunikacija. DES, koji je predstavljao važan standard u ranim fazama razvoja simetrične kriptografije, danas se smatra nedovoljno otpornim na kriptanalizu zbog ograničene dužine ključa i značajnog napretka računarskih kapaciteta. Triple DES predstavljao je prelazno rešenje koje je produžilo upotrebljivost DES arhitekture povećanjem efektivne bezbednosti, ali uz cenu smanjene efikasnosti.

Nasuprot tome, AES je postao dominantni standard zahvaljujući visokom nivou bezbednosti,

efikasnoj implementaciji i širokoj podršci u savremenim hardverskim i softverskim platformama.

Analiza IKEv1 pokazuje da izbor algoritma za šifrovanje nije statična odluka, već proces koji mora pratiti razvoj kriptografskih saznanja, preporuka standardizacionih tela i procenu aktuelnih bezbednosnih rizika [2].

Pored zaštite poverljivosti, IKEv1 zahteva pouzdane mehanizme za očuvanje integriteta razmenjenih poruka. U tu svrhu koriste se kriptografske hash funkcije, među kojima su tokom razvoja protokola dominantnu ulogu imali MD5 i SHA-1. Njihova osnovna funkcija u okviru IKEv1 nije enkripcija podataka, već generisanje jedinstvenih kontrolnih vrednosti koje omogućavaju otkrivanje svake neovlašćene izmene sadržaja poruka tokom procesa pregovaranja. Time hash funkcije predstavljaju važan element zaštite upravljačke komunikacije i doprinose očuvanju integriteta procesa uspostavljanja bezbednosnih asocijacija [34].

Poseban značaj u bezbednosnoj arhitekturi IKEv1 ima primena HMAC (*Hash-based Message Authentication Code*) mehanizma, koji kombinuje hash funkcije sa tajnim ključem radi ostvarivanja istovremene zaštite integriteta i potvrde autentičnosti poruka. Primenom HMAC-a komunikacioni entitet može proveriti da sadržaj poruke nije izmenjen tokom prenosa i da poruka potiče od legitimnog učesnika komunikacije koji raspolaže odgovarajućim kriptografskim materijalom. Time HMAC predstavlja važnu vezu između mehanizama zaštite integriteta i procesa autentifikacije, čime dodatno doprinosi uspostavljanju digitalnog poverenja unutar IKEv1 protokola.

Analiza savremenih bezbednosnih preporuka pokazuje da izbor kriptografskih algoritama predstavlja dinamičan proces koji mora pratiti razvoj novih kriptanalitičkih saznanja i tehničko-tehnoloških mogućnosti. Algoritmi poput DES-a i hash funkcije MD5 danas više ne zadovoljavaju savremene zahteve visokog nivoa bezbednosti, dok se i za SHA-1 preporučuje zamena savremenijim hash funkcijama u novim implementacijama. Ova činjenica potvrđuje da dugoročna bezbednost IKEv1 ne zavisi isključivo od projektantskih rešenja definisanih u trenutku nastanka protokola, već i od kontinuiranog usklađivanja implementacija sa razvojem kriptografskih standarda i preporuka [2] [5].

Naučno posmatrano, analiza kriptografskih algoritama u okviru IKEv1 potvrđuje da bezbednost protokola nije rezultat primene jednog algoritma za šifrovanje ili jedne hash funkcije. Iz tog razloga izbor odgovarajućih algoritama mora biti posmatran kao sastavni deo procesa upravljanja bezbednosnim rizikom, pri čemu pravilna konfiguracija, redovno usklađivanje sa savremenim standardima i dosledna primena bezbednosnih politika imaju podjednako veliki značaj kao i sama matematička otpornost na kriptanalizu u slučaju primenjenih kriptografskih algoritama. IKEv1 protokol zasniva svoju bezbednosnu arhitekturu na mehanizmima za bezbednu razmenu kriptografskih ključeva i derivaciju kriptografskog materijala koji će biti korišćen tokom zaštite korisničkog IP saobraćaja. Ovi mehanizmi predstavljaju jednu od ključnih funkcionalnih komponenti IKEv1, budući da omogućavaju komunikacionim entitetima da preko nebezbedne mrežne infrastrukture (*Internet*) uspostave zajedničku kriptografsku osnovu bez potrebe za prethodnim prenosom tajnih ključeva. Na taj način razmena ključeva postaje osnov celokupnog procesa uspostavljanja digitalnog poverenja.

Centralnu ulogu u ovom procesu ima *Diffie–Hellman* algoritam za razmenu ključeva. Njegova osnovna funkcija u okviru IKEv1 nije samo generisanje zajedničke tajne, već stvaranje

kriptografske osnove na kojoj će biti izvedeni svi naredni sesijski ključevi potrebni za funkcionisanje protokola. Bezbednosni značaj *Diffie–Hellman* mehanizma proizlazi iz činjenice da zajednička tajna nikada nije direktno preneti kroz komunikacionu mrežu, čime se značajno umanjuje mogućnost njenog presretanja tokom procesa pregovaranja. Istovremeno, izbor odgovarajuće *Diffie–Hellman* grupe predstavlja važan element bezbednosne politike, budući da veličina i karakteristike grupe neposredno utiču na nivo otpornosti sistema prema savremenim kriptanalitičkim metodama [2],[53. RFC 2409]; [54; RFC 4306].

Međutim, zajednička tajna dobijena primenom *Diffie–Hellman* algoritma ne koristi se neposredno za zaštitu korisničkog saobraćaja. IKEv1 primenjuje mehanizam derivacije ključeva kojim se iz zajedničkog kriptografskog materijala izvodi više međusobno različitih ključeva namenjenih različitim bezbednosnim funkcijama. Ovakav pristup omogućava funkcionalnu podelu kriptografskog materijala i sprečava da kompromitacija jednog ključa automatski dovede do kompromitacije svih ostalih bezbednosnih funkcija sistema. Time se ostvaruje princip kriptografske segmentacije, koji predstavlja važan element savremenog bezbednosnog inženjerstva u domenu informacione bezbednosti.

Posebnu ulogu u procesu derivacije ključeva imaju pseudo-slučajne funkcije (*Pseudo-Random Function* – PRF). Njihova primena omogućava determinističko izvođenje novih kriptografskih vrednosti iz zajedničke tajne, *nonce* vrednosti i drugih parametara razmenjenih tokom procesa pregovaranja. Na ovaj način generiše se kriptografski materijal koji je potreban za zaštitu upravljačkih poruka i korisničkog IP saobraćaja. Kvalitet primenjene pseudo-slučajne funkcije neposredno utiče na kvalitet izvedenih ključeva, zbog čega izbor odgovarajuće PRF funkcije predstavlja važan deo ukupne bezbednosne konfiguracije IKEv1 implementacije [31].

Rezultat procesa derivacije predstavlja skup sesijskih ključeva poznat pod nazivom KEYMAT. Ovaj kriptografski materijal koristi se za uspostavljanje IPsec *Security Association* i predstavlja neposrednu osnovu za *funkcionisanje Authentication Header (AH)* i *Encapsulating Security Payload (ESP)* protokola. Primenom različitih ključeva za različite bezbednosne funkcije postiže se viši nivo izolacije između pojedinačnih komponenti sistema, čime se smanjuje mogućnost širenja posledica eventualne kompromitacije jednog dela kriptografske arhitekture na celokupni informaciono-komunikacioni sistem[58; RFC 4302], [59; RFC 4303].

Dodatni nivo zaštite može biti ostvaren primenom *Perfect Forward Secrecy (PFS)*, koji predstavlja jedan od najznačajnijih bezbednosnih mehanizama u okviru IKEv1. Njegova suština ogleda se u generisanju novog *Diffie–Hellman* kriptografskog materijala prilikom uspostavljanja novih IPsec *Security Association*, čime se obezbeđuje da kompromitacija jednog skupa ključeva ne dovede do kompromitacije prethodnih ili budućih komunikacionih sesija. Ovakav pristup značajno povećava dugoročnu otpornost sistema na postkompromitacione scenarije i predstavlja važan element zaštite komunikacija koje zahtevaju visok nivo poverljivosti [53; RFC 2409].

Analiza bezbednosnih karakteristika ovih mehanizama pokazuje da njihova efikasnost ne zavisi isključivo od matematičke otpornosti pojedinačnih algoritama, već i od pravilnog izbora *Diffie–Hellman* grupa, kvaliteta izvora entropije, bezbednog generisanja *nonce* vrednosti, pouzdane implementacije PRF funkcija i pravilnog upravljanja životnim ciklusom izvedenih ključeva. Svaka slabost u bilo kojoj od navedenih komponenti može negativno uticati na kvalitet izvedenog kriptografskog materijala i umanjiti ukupni nivo bezbednosti

IKEv1 protokola [42], [44],[50].

Naučno posmatrano, algoritmi za razmenu ključeva i derivaciju kriptografskog materijala predstavljaju funkcionalni most između matematičkih principa kriptografije i njihove praktične primene u bezbednosnoj arhitekturi IKEv1. Njihova međusobna integracija omogućava da zajednička tajna dobijena tokom procesa pregovaranja bude transformisana u skup namenski izvedenih sesijskih ključeva koji obezbeđuju zaštitu upravljačke komunikacije i korisničkog IP saobraćaja. Time se potvrđuje osnovna teza ovog istraživanja da digitalno poverenje nije rezultat jednog algoritma ili jednog bezbednosnog mehanizma, već koordinisanog delovanja razmene ključeva, derivacije kriptografskog materijala, autentifikacije i upravljanja bezbednosnim asocijacijama u okviru jedinstvene bezbednosne arhitekture IKEv1 protokola [2].

Komparativna analiza kriptografskih algoritama primenjenih u *Internet Key Exchange Version 1* (IKEv1) protokolu pokazuje da bezbednosna arhitektura ovog protokola nije zasnovana na dominaciji jednog algoritma ili jedne kriptografske tehnike, već na koordinisanoj primeni više međusobno povezanih mehanizama koji sinergijski realizuju bezbednosne ciljeve. Simetrični algoritmi obezbeđuju poverljivost podataka, hash funkcije i HMAC štite integritet i autentičnost poruka, Diffie–Hellman omogućava bezbednu razmenu zajedničke tajne, dok PRF i KEYMAT transformišu zajednički kriptografski materijal u namenske sesijske ključeve potrebne za funkcionisanje IKEv1 i IPsec arhitekture. Posmatrani pojedinačno, ovi algoritmi rešavaju različite bezbednosne probleme, ali tek njihovom međusobnom integracijom ostvaruje se funkcionalno i pouzdano digitalno poverenje.

Sa aspekta zaštite poverljivosti može se uočiti evolucija od istorijski značajnih algoritama, poput *DES* i *Triple DES*, ka savremenim algoritmima kao što je *AES*. Ovaj razvoj pokazuje da izbor algoritma nije trajna projektantska odluka, već proces koji mora pratiti napredak kriptografskih istraživanja, povećanje računarskih kapaciteta i nove bezbednosne preporuke. Sličan primer potreba za unapređenjem može se uočiti i kod hash funkcija, gde su MD5 i SHA-1 tokom vremena ustupili mesto savremenijim rešenjima zbog identifikovanih slabosti i povećanih zahteva za zaštitu integriteta podataka. Time se potvrđuje da dugoročna bezbednost IKEv1 ne zavisi isključivo od originalne specifikacije protokola, već i od sposobnosti implementacija da prate razvoj kriptografskih standarda i detektovanih ranjivosti informaciono-komunikacionih tehnologija [2],[78; FIPS 197].

Analiza mehanizama za razmenu ključeva pokazuje da Diffie–Hellman algoritam predstavlja osnovu uspostavljanja zajedničke kriptografske tajne, ali da njegova bezbednosna vrednost zavisi od pravilnog izbora grupa, kvaliteta generisanih slučajnih vrednosti i bezbedne implementacije. Dodatno, primena *Perfect Forward Secrecy* unapređuje otpornost sistema ograničavanjem posledica eventualne kompromitacije pojedinačnih sesijskih ključeva. Time se pokazuje da bezbednost razmene ključeva nije određena isključivo matematičkom složenošću algoritma, već i načinom njegove praktične primene u okviru protokola.

Posebno je značajno istaći da nijedan od analiziranih algoritama ne funkcioniše kao samostalni bezbednosni mehanizam. Simetrični algoritmi ne mogu ostvariti svoju funkciju bez pouzdano izvedenih ključeva. Ključevi izvedeni primenom PRF i KEYMAT nemaju praktičnu vrednost bez uspešno realizovane *Diffie–Hellman* razmene i odgovarajuće autentifikacije komunikacionih entiteta. Istovremeno, integritet upravljačkih poruka predstavlja preduslov za pouzdano pregovaranje bezbednosnih parametara. Ovakva međuzavisnost potvrđuje da IKEv1 predstavlja integrisanu kriptografsku arhitekturu u kojoj

svaki mehanizam ostvaruje svoju funkciju kao deo šireg bezbednosnog procesa [31],[34].

Sa stanovišta upravljanja bezbednosnim rizicima, analiza pokazuje da izbor kriptografskih algoritama predstavlja samo jedan segment ukupne bezbednosne strategije. Podjednako važni faktori obuhvataju kvalitet implementacije, pravilnu konfiguraciju uređaja, ažurno održavanje softvera, izbor odgovarajućih bezbednosnih politika i pravilno upravljanje životnim ciklusom Security Association struktura i kriptografskih ključeva. Čak i primena kriptografski snažnih algoritama ne može obezbediti odgovarajući nivo zaštite ukoliko postoje implementacione greške, neadekvatna konfiguracija ili propusti u upravljanju ključevima.

Ovakav zaključak potvrđuje savremeni koncept „defense in depth“, prema kojem se bezbednost ostvaruje kroz međusobno dopunjavanje više zaštitnih slojeva. Upravo ovakav integrisani pristup omogućava uspostavljanje, održavanje i kontinuirano unapređenje digitalnog poverenja, koje predstavlja osnov bezbedne komunikacije u IPsec okruženju [77; SP 800-77 Rev. 1.];[92. BSI TR-02102-1].

4.8. Životni ciklus security association i upravljanje bezbednosnim asocijacijama

Security Association (SA) predstavlja osnovni operativni mehanizam IPsec arhitekture putem kojeg se definišu i održavaju bezbednosni parametri neophodni za zaštitu komunikacije između mrežnih entiteta. U okviru *Internet Key Exchange Version 1* (IKEv1) protokola upravljanje bezbednosnim asocijacijama predstavlja kontinuirani proces koji obuhvata njihovo uspostavljanje, održavanje, ažuriranje i bezbedno ukidanje. Na taj način *Security Association* ne predstavlja statičku konfiguraciju, već dinamički bezbednosni kontekst koji se prilagođava promenama u tehničko-tehnološkom okruženju i zahtevima bezbednosne politike [53; RFC 2409].

Bezbednosna arhitektura IKEv1 zasniva se na jasno definisanoj podeli između IKE *Security Association* (IKE SA) i *IPsec Security Association* (IPsec SA). IKE SA uspostavlja se tokom prve faze pregovaranja i obezbeđuje zaštićen upravljački kanal kojim se razmenjuju poruke potrebne za dalje pregovaranje bezbednosnih parametara.

Nakon uspešno završene autentifikacije i uspostavljanja digitalnog poverenja, kroz *Quick Mode* formiraju se IPsec *Security Association* strukture koje neposredno određuju način zaštite korisničkog IP saobraćaja primenom *Authentication Header* (AH) i/ili *Encapsulating Security Payload* (ESP) protokola. Ovakva funkcionalna podela omogućava razdvajanje upravljačke i operativne ravni komunikacije, čime se povećava preglednost i bezbednost celokupne arhitekture [2],[58; RFC 4302]; [59; RFC 4303].

Životni ciklus *Security Association* započinje pregovaranjem bezbednosnih politika između komunikacionih strana. Tokom ovog procesa usaglašavaju se kriptografski algoritmi, metode autentifikacije, parametri razmene ključeva, trajanje bezbednosne asocijacije i drugi elementi koji određuju način zaštite komunikacije. Tek nakon uspešno završenog pregovaranja i potvrde međusobne kompatibilnosti bezbednosnih parametara može biti uspostavljena odgovarajuća *Security Association*. Time se obezbeđuje da obe strane primenjuju identične bezbednosne mehanizme i da komunikacija bude ostvarena u skladu sa unapred definisanim bezbednosnim pravilima tj na osnovu politika bezbednosti [31],[71; RFC 4945].

Jedna od osnovnih karakteristika *Security Association* jeste njena vremenska ograničenost. Svaka bezbednosna asocijacija poseduje unapred definisan životni vek koji može biti određen vremenskim intervalom, količinom prenetih podataka ili kombinacijom oba kriterijuma. Nakon isteka definisanih parametara neophodno je izvršiti obnovu ili zamenu postojeće

Security Association novom SA. Ovakav pristup ograničava period korišćenja istog kriptografskog materijala i smanjuje mogućnost uspešne kriptanalize ili zloupotrebe kompromitovanih ključeva. Upravljanje životnim ciklusom *Security Association* zbog toga predstavlja važnu komponentu strategije dugoročne zaštite informaciono-komunikacionog sistema [2],[31].

Efikasno upravljanje bezbednosnim asocijacijama podrazumeva i pravilno održavanje stanja SA tokom čitavog perioda važenja SA. To uključuje praćenje vremena trajanja, kontrolu statusa aktivnih bezbednosnih asocijacija, bezbedno uklanjanje zastarelih ili kompromitovanih SA i usklađivanje njihovog rada sa važećim bezbednosnim politikama organizacije.

Poseban značaj ima sinhronizacija između komunikacionih strana, jer neusaglašeno stanje *Security Association* može dovesti do prekida komunikacije, neuspešne autentifikacije ili do odbacivanja legitimnog saobraćaja. Sa aspekta bezbednosnog inženjerstva, upravljanje *Security Association* strukturama predstavlja spoj kriptografskih, implementacionih i organizacionih aktivnosti. Kvalitet algoritama, pravilna derivacija ključeva i pouzdana autentifikacija predstavljaju neophodne preduslove za uspostavljanje bezbednosne asocijacije, ali njena dugoročna efikasnost zavisi od pravilnog upravljanja životnim ciklusom, redovnog obnavljanja bezbednosnih parametara, adekvatnog nadzora i dosledne primene bezbednosnih procedura zasnovanih na politici bezbednosti. Time se potvrđuje da bezbednost IKEv1 ne proizlazi isključivo iz početnog procesa pregovaranja, već iz kontinuiranog upravljanja bezbednosnim odnosima koji se održavaju tokom čitavog trajanja komunikacije [31],[53; RFC 2409].

Analiza životnog ciklusa *Security Association* pokazuje da bezbednosna asocijacija predstavlja dinamički element bezbednosne arhitekture IKEv1, čija vrednost nije ograničena na trenutak njenog uspostavljanja. Naprotiv, njena bezbednosna funkcija ostvaruje se kroz kontinuirano upravljanje, periodično obnavljanje i usklađivanje sa promenama bezbednosnih zahteva i operativnog okruženja. Time se potvrđuje osnovna teza ovog istraživanja da digitalno poverenje nije jednokratni rezultat procesa autentifikacije ili razmene ključeva, već kontinuirani proces koji zahteva sistematsko upravljanje bezbednosnim asocijacijama tokom celokupnog životnog ciklusa procesa komunikacije. Upravo takav pristup predstavlja jedan od ključnih preduslova za očuvanje dugoročne otpornosti IPsec infrastrukture i bezbednosti savremenih informaciono-komunikacionih sistema [53; RFC 2409].

4.9. Rekeying mehanizmi i kontinuitet bezbednosti

Jedna od najznačajnijih karakteristika *Internet Key Exchange Version 1* (IKEv1) protokola jeste sposobnost periodične obnove kriptografskog materijala tokom trajanja bezbedne komunikacije. Ovaj proces, poznat kao *rekeying*, predstavlja osnovni mehanizam kojim se obezbeđuje kontinuitet zaštite i ograničava vreme upotrebe istih kriptografskih ključeva. Njegova osnovna svrha nije samo zamena postojećih ključeva novim, već očuvanje dugoročne otpornosti bezbednosne arhitekture kroz kontinuirano prilagođavanje bezbednosnih parametara tokom životnog ciklusa komunikacije [2],[31].

U okviru IKEv1 protokola *rekeying* je neposredno povezan sa životnim ciklusom IKE *Security Association* (IKE SA) i IPsec *Security Association* (IPsec SA). Kako svaka bezbednosna asocijacija poseduje unapred definisan period važenja ili ograničenje u količini prenetih podataka, neophodno je pre isteka tih parametara uspostaviti novu bezbednosnu asocijaciju i nove sesijske ključeve. Na taj način komunikacija može biti nastavljena bez prekida, uz istovremeno unapređenje nivoa kriptografske zaštite. Rekeying zbog toga predstavlja sastavni deo procesa upravljanja bezbednosnim asocijacijama, a ne dodatnu ili

opcionu funkcionalnost protokola [2], [44].

Sa aspekta bezbednosnog inženjerstva, periodična obnova ključeva predstavlja važnu meru za smanjenje posledica eventualne kompromitacije kriptografskog materijala. Dugotrajna upotreba istih ključeva povećava mogućnost uspešne kriptanalize, naročito u okruženjima sa velikim obimom saobraćaja ili dugotrajnim VPN sesijama. *Rekeying* ograničava količinu podataka zaštićenih istim ključem i smanjuje vremenski period u kojem kompromitovani ključ može biti zloupotrebljen. Time se umanjuju potencijalne posledice bezbednosnog incidenta i povećava otpornost informaciono-komunikacionog sistema na dugotrajne napade.

Poseban značaj *rekeying* mehanizma dolazi do izražaja u kombinaciji sa primenom *Perfect Forward Secrecy* (PFS). Kada se prilikom obnove bezbednosnih asocijacija generiše novi *Diffie-Hellman* kriptografski materijal, svaki novi skup sesijskih ključeva postaje nezavisan od prethodnih. Na taj način kompromitacija jednog ključa ne omogućava kompromitaciju prethodnih niti budućih komunikacionih sesija. Ovakav pristup predstavlja jedan od najvažnijih mehanizama očuvanja dugoročne tajnosti podataka i značajno povećava otpornost sistema na postkompromitacione scenarije [31].

Efikasna primena *rekeying* procesa zahteva preciznu koordinaciju između komunikacionih strana. Novoformirana *Security Association* mora biti uspostavljena pre isteka postojeće kako bi se obezbedio kontinuitet komunikacije bez gubitka paketa ili prekida VPN tunela. Istovremeno, neophodno je obezbediti pravilno uklanjanje zastarelih bezbednosnih asocijacija kako bi se sprečilo paralelno korišćenje više nevažećih ili kompromitovanih bezbednosnih konteksta. Ovakvo upravljanje zahteva pouzdanu implementaciju protokola, sinhronizaciju uređaja i doslednu primenu definisanih bezbednosnih politika [2],[51].

Sa organizacionog aspekta, politika *rekeying*-a predstavlja važan deo strategije upravljanja informacionom bezbednošću. Period obnavljanja ključeva mora biti usklađen sa procenom rizika, značajem podataka koji se štite, raspoloživim računarskim resursima i operativnim zahtevima organizacije. Dugi vremenski periodi između obnova kriptografskih ključeva mogu povećati izloženost sistema kriptanalitičkim napadima, dok previše česta obnova može dovesti do nepotrebnog opterećenja mrežnih uređaja i smanjenja performansi. Zbog toga pravilno definisanje politike *rekeying*-a predstavlja primer balansiranja između bezbednosti i operativne efikasnosti [43].

Analiza implementacija u praksi pokazuje da kvalitet *rekeying* mehanizma ne zavisi isključivo od specifikacije protokola, već i od kvaliteta implementacije, pravilne konfiguracije uređaja i sposobnosti sistema da pouzdano upravlja velikim brojem aktivnih bezbednosnih asocijacija. Implementacione greške, neusklađeni vremenski parametri ili nepravilno upravljanje životnim ciklusom ključeva mogu umanjiti bezbednosne prednosti koje *rekeying* mehanizam pruža. Ova činjenica dodatno potvrđuje da bezbednost IKEv1 proizlazi iz usklađenog delovanja protokolarnih, implementacionih i organizacionih elemenata [31].

Analiza *rekeying* mehanizama potvrđuje da dugoročna bezbednost *Internet Key Exchange Version 1* protokola ne zavisi isključivo od uspešnog uspostavljanja početne bezbednosne asocijacije, već od sposobnosti sistema da kontinuirano obnavlja kriptografski materijal i prilagođava bezbednosne parametre tokom čitavog životnog ciklusa komunikacije. *Rekeying* predstavlja mehanizam kojim se održava kontinuitet digitalnog poverenja, ograničavaju posledice eventualne kompromitacije i unapređuje otpornost sistema na savremene bezbednosne pretnje. Time se potvrđuje osnovna hipoteza ovog istraživanja da bezbednost

informaciono-komunikacionih sistema predstavlja kontinuirani proces upravljanja rizikom, u kojem periodična obnova ključeva predstavlja jedan od ključnih mehanizama očuvanja poverljivosti, integriteta i dugoročne pouzdanosti bezbedne komunikacije [2].

4.10. Savremene napredne persistentne pretnje (advanced persistent threat – apt) u slučaju ikev1

Savremene napredne persistentne pretnje (*Advanced Persistent Threat* – APT) razlikuju se od tradicionalnih oblika računarskih napada po tome što njihov osnovni cilj nije trenutno narušavanje dostupnosti informaciono-komunikacionog sistema, već dugotrajno, prikriveno i sistematsko ostvarivanje pristupa zaštićenim resursima uz minimizaciju verovatnoće otkrivanja. Posmatrano iz perspektive APT aktera, *Internet Key Exchange Version 1* (IKEv1) protokol ne predstavlja primarni cilj napada, već jednu od komponenti šire mrežne infrastrukture čija analiza može doprineti identifikaciji potencijalnih slabosti, određivanju napadne površine i planiranju narednih faza kompromitacije. Takav pristup potvrđuje da bezbednost IKEv1 nije moguće posmatrati izolovano od celokupnog operativnog okruženja u kojem se protokol implementira [31],[38],[50].

Prva faza APT operacija najčešće obuhvata pasivno i aktivno prikupljanje informacija (*reconnaissance*), pri čemu napadač nastoji da identifikuje javno dostupne VPN *gateway* uređaje, njihove mrežne adrese, otvorene servise, podržane verzije protokola i karakteristične implementacione osobine. Analizom odgovora VPN uređaja moguće je izvršiti tzv. *fingerprinting* implementacije, odnosno utvrditi proizvođača, verziju operativnog sistema ili softverske platforme, kao i prisustvo poznatih ranjivosti. U ovoj fazi cilj nije kompromitacija sistema, već izgradnja preciznog modela ciljne infrastrukture koji će omogućiti izbor najefikasnijeg vektora napada [10],[11].

Nakon identifikacije VPN infrastrukture sledi faza detaljne enumeracije bezbednosnih karakteristika. Napadač analizira podržane *Diffie–Hellman* grupe, analizira kriptografske algoritme za šifrovanje, hash funkcije, metode autentifikacije i druge parametre koji se mogu zaključiti iz procesa pregovaranja. Ovakva analiza omogućava procenu nivoa kriptografske otpornosti ciljnog sistema, ali i identifikaciju zastarelih ili nebezbednih konfiguracija koje mogu predstavljati osnovu za dalje napade ili biti deo kompleksnih vektora napada na informaciono-komunikacioni sistem. Poseban značaj imaju implementacije koje i dalje podržavaju zastarele algoritme ili slabije *Diffie–Hellman* grupe, jer njihovo prisustvo može ukazivati na nedovoljno održavanu infrastrukturu i povećanu verovatnoću postojanja drugih bezbednosnih propusta.[2]

U okruženjima u kojima se autentifikacija zasniva na unapred deljenim ključevima (*Pre-Shared Key* – PSK), APT akteri mogu pokušati da iskoriste karakteristike *Aggressive Mode* režima za prikupljanje materijala pogodnog za sprovođenje offline dictionary napada. Važno je naglasiti da uspešnost ovakvog napada ne proizlazi iz fundamentalne kriptografske slabosti *Diffie–Hellman* algoritma, već iz kombinacije projektantskih karakteristika *Aggressive Mode* režima i nedovoljno složenih unapred deljenih tajni [2],[19].

Međutim, savremeni APT akteri retko se zaustavljaju na pokušaju direktne kompromitacije IKEv1 protokola. Njihov operativni cilj mnogo češće podrazumeva iskorišćavanje implementacionih ranjivosti VPN uređaja, operativnih sistema ili pomoćnih servisa koji realizuju IKE/IPsec funkcionalnost. U tom kontekstu IKEv1 predstavlja ulaznu tačku za širu kompromitaciju sistema, pri čemu se nakon početnog pristupa sprovede faze eskalacije privilegija, lateralnog kretanja kroz mrežu, uspostavljanja mehanizama trajnog pristupa (*persistence*) i prikrivanja aktivnosti radi dugotrajnog ostanka unutar kompromitovanog

okruženja. Iz tog razloga procena bezbednosti IKEv1 mora obuhvatiti ne samo analizu samog protokola, već i procenu otpornosti implementacije, konfiguracije i operativnog okruženja u kojem se protokol izvršava [10],[18].

Tabela 8. Mehanizmi zaobilaženja kriptografske zaštite

Mehanizam	Osnovna karakteristika	Uticaj na IPsec/IKE okruženje	Detekcija i zaštitne kontrole
Kompromitacija krajnje tačke (endpoint)	Pristup podacima pre šifrovanja ili nakon dešifrovanja na legitimnom uređaju.	Može ugroziti poverljivost podataka bez narušavanja kriptografskih algoritama.	EDR/XDR, upravljanje zakrpama, hardening sistema, analiza telemetrije.
Krađa akreditiva	Neovlašćeno korišćenje legitimnih identiteta ili autentifikacionih podataka.	Može omogućiti neovlašćeno uspostavljanje VPN sesija.	Višefaktorska autentifikacija, nadzor prijava, revizija logova.
Nepravilna konfiguracija	Slabe ili zastarele konfiguracije protokola i algoritama.	Smanjuje ukupni nivo bezbednosti implementacije.	Redovne bezbednosne provere, usklađenost sa RFC i internim politikama.
Kompromitacija privilegovanih komponenti	Narušavanje integriteta komponenti sa visokim privilegijama.	Može uticati na rad bezbednosnih servisa i VPN procesa.	Kontrola integriteta, zaštita kernela, nadzor privilegovanih događaja.
Socijalni inženjering	Navođenje korisnika na otkrivanje poverljivih informacija ili izvršavanje neželjenih radnji.	Može dovesti do kompromitacije naloga ili uređaja koji koriste IPsec/IKE.	Obuka korisnika, zaštita elektronske pošte, procedure verifikacije.
Nedovoljno ažuriran softver	Prisustvo poznatih ranjivosti u operativnom sistemu ili aplikacijama.	Povećava rizik kompromitacije uređaja na kojima rade IPsec/IKE komponente.	Program upravljanja zakrpama, skeniranje ranjivosti, kontinuirani monitoring.

Napomena: Tabela prikazuje reprezentativne mehanizme kojima može biti ugrožena bezbednost sistema bez direktnog narušavanja kriptografskih algoritama. Naglasak je na zaštiti implementacije, krajnjih tačaka i operativnog okruženja kroz preventivne i detektivne kontrole.

Izvor: Autor, na osnovu sinteze opšteprihvaćenih okvira za upravljanje bezbednosnim rizikom (NIST SP 800-53 Rev. 5, MITRE ATT&CK) i dokumentovanih obrazaca savremenih napada na IPsec/IKE infrastrukturu

U tabeli 8 prikazano je šest tipičnih vektora napada na informaciono-komunikacione sisteme putem kojih otpornost/rezistentnost/rezilijentnost IPsec/IKE infrastrukture može biti dovedena u pitanje, a da pritom sami kriptografski algoritmi ne budu meta napadača. Ovi mehanizmi, počev od kompromitacije krajnje tačke i krađe akreditiva (primer je: password), preko nepravilne konfiguracije i kompromitacije privilegovanih komponenti, do socijalnog inženjeringa i neažuriranog softvera, dele zajednički metodološki imenitelj: svi zaobilaze kriptografsku zaštitu kroz kompromitaciju okruženja, identiteta ili procesa koji okružuju kriptografski mehanizam, umesto da pokušavaju njegovo direktno kriptanalitičko narušavanje.

Podaci u tabeli time potvrđuje centralnu tezu ovog istraživanja, prema kojoj savremeni napadači sve ređe usmeravaju napore na razbijanje algoritama, a sve češće na pronalaženje najslabije karike u širem lancu poverenja informaciono-komunikacionog sistema. Sa aspekta odbrambenog pristupa, tabela ukazuje da svaki mehanizam zahteva specifičnu, prilagođenu kontrolu i primenu tehničkih rešenja poput EDR/XDR i upravljanja sa *security update* efikasno adresiraju kompromitaciju krajnje tačke i neažuriran softver, dok organizacione mere poput višefaktorske autentifikacije i obuke korisnika ciljano odgovaraju na prevenciju i sprečavanje krađe akreditiva i socijalni inženjering. Značajno je uočiti da nepravilna konfiguracija, iako naizgled najjednostavniji mehanizam za otklanjanje, zahteva kontinuiranu usklađenost sa RFC preporukama i internim bezbednosnim politikama, što je proces, a ne jednokratna aktivnost. Ova diferencijacija potvrđuje da efikasna zaštita IPsec/IKE infrastrukture ne može se osloniti na jedinstven, univerzalan zaštitni mehanizam, već zahteva slojevit, međusobno komplementaran skup tehničkih i organizacionih kontrola prilagođenih prirodi svakog pojedinačnog rizika.

Sa stanovišta bezbednosnog inženjerstva, od posebnog značaja jeste činjenica da APT akteri nastoje da minimizuju broj aktivnosti koje mogu izazvati alarmne mehanizme sistema za detekciju napada. Zbog toga se aktivnosti poput *fingerprinting*-a, enumeracije i analize toka i procesa pregovaranja često izvode sporim intenzitetom i u vremenskim intervalima koji otežavaju njihovo uočavanje primenom tradicionalnih IDS/IPS rešenja. Ovakav pristup potvrđuje potrebu za primenu procesnog pristupa, od izuzetne važnosti je potreba za integracijom mrežnog monitoringa, analize log datoteka, SIEM platformi, NDR/XDR sistema i obaveštajnih podataka o pretnjama (*Threat Intelligence*), kako bi se na osnovu korelacije većeg broja naizgled bezazlenih događaja blagovremeno identifikovalo prisustvo naprednih persistentnih pretnji.

Rezultati sprovedene analize potvrđuju da APT akteri *Internet Key Exchange Version 1* ne posmatraju kao izolovani kriptografski protokol, već kao sastavni deo kompleksne bezbednosne arhitekture informaciono-komunikacionog sistema. Njihova pažnja usmerena je na identifikaciju najslabije karike u sistemu zaštite, koja može biti posledica zastarele konfiguracije, implementacione ranjivosti, slabih autentifikacionih podataka ili nedovoljnog operativnog nadzora. Zbog toga se naučno utemeljena procena bezbednosti IKEv1 ne može ograničiti isključivo na analizu kriptografskih algoritama i protokolarnih mehanizama, već mora obuhvatiti celokupan životni ciklus sistema, uključujući implementaciju, konfiguraciju, kontinuirani monitoring, odgovor na incidente i proces stalnog unapređenja bezbednosne arhitekture. Upravo ovakav integrisani pristup predstavlja jedan od ključnih preduslova za povećanje otpornosti savremenih informaciono-komunikacionih sistema na sofisticirane višefazne APT kampanje [2].

4.11. Savremeni značaj analize ikev1 protokola u uslovima postepene migracije ka ikev2

Internet Key Exchange Version 1 (IKEv1) predstavlja jedan od najznačajnijih protokola u istorijskom razvoju bezbedne razmene kriptografskih ključeva putem otvorenih komunikacionih mreža. Njegova arhitektura postavila je temelje savremenog upravljanja bezbednosnim asocijacijama u okviru IPsec okruženja i omogućila široku primenu virtuelnih privatnih mreža u državnim institucijama, finansijskim organizacijama, telekomunikacionim sistemima i kritičnoj informacionoj infrastrukturi. Međutim, razvoj novih bezbednosnih zahteva, identifikacija određenih arhitektonskih ograničenja i iskustva stečena tokom dugogodišnje operativne primene doveli su do razvoja *Internet Key Exchange Version 2* (IKEv2), koji predstavlja evolutivno unapređenje prethodne generacije protokola [53; RFC

2409]. Značajnu prekretnicu predstavlja objavljivanje RFC 9395, kojim su osnovni standardi za IKEv1 prebačeni u status *Historic*, uz preporuku da se nove implementacije zasnivaju na IKEv2.

Ova odluka standardizacionog tela ne predstavlja tvrdnju da je svaki postojeći IKEv1 sistem automatski nebezbedan niti da je njegova operativna primena trenutno prestala. Naprotiv, njome se potvrđuje da je razvoj protokola završen i da se buduća unapređenja bezbednosti usmeravaju ka IKEv2 i njegovim naslednicima. Iz metodološke perspektive, status *Historic* označava promenu pravca razvoja standarda, ali ne i nestanak postojećih implementacija iz realnih informaciono-komunikacionih sistema [31],[71; RFC 4945].

Analiza savremene mrežne infrastrukture pokazuje da je veliki broj organizacija i dalje u fazi postepene migracije sa IKEv1 na IKEv2. Razlozi za ovakvo stanje nisu prvenstveno tehničke prirode, već proizlaze iz složenosti velikih informacionih sistema, visokih troškova modernizacije, potrebe za očuvanjem interoperabilnosti i zahteva za neprekidnim radom kritičnih servisa. U državnim organima, finansijskim institucijama, energetskim kompanijama i drugim organizacijama koje upravljaju kompleksnim distribuiranim mrežama često postoji veliki broj VPN tunela uspostavljenih tokom prethodnih godina. Njihova istovremena zamena mogla bi izazvati prekide rada, narušavanje interoperabilnosti i povećanje operativnog rizika, zbog čega se migracija najčešće realizuje postepeno i planski [55; RFC 7296],[56; RFC 9395].

Poseban značaj imaju industrijski informaciono-komunikacioni sistemi (ICS/SCADA), u kojima se mrežna oprema često koristi tokom veoma dugog vremenskog perioda. Za razliku od kancelarijskih informacionih sistema, kod industrijskih postrojenja prioritet predstavljaju raspoloživost i kontinuitet rada. Zbog toga VPN uređaji koji koriste IKEv1 mogu ostati u funkciji godinama nakon završetka razvoja samog protokola, sve dok ispunjavaju operativne zahteve i ne postoji mogućnost njihove bezbedne zamene bez prekida proizvodnog procesa. Ovakve implementacije predstavljaju tipičan primer nasleđenih (*legacy*) sistema, čija se bezbednost mora procenjivati u skladu sa njihovim stvarnim operativnim okruženjem [31]. Slična situacija može se uočiti kod međusobno povezanih organizacija koje održavaju dugogodišnje site-to-site IPsec VPN veze. Interoperabilnost između različitih proizvođača mrežne opreme, kompatibilnost sa starijim verzijama firmvera i potreba za održavanjem postojećih komunikacionih kanala često uslovljavaju nastavak korišćenja IKEv1 tokom prelaznog perioda. Pored toga, pojedini sistemi za udaljeni pristup (*Remote Access VPN*) i dalje koriste starije klijentske platforme ili uređaje koji ne podržavaju sve funkcionalnosti IKEv2, što dodatno produžava operativni životni ciklus prve generacije Internet Key Exchange protokola [2].

Sa aspekta upravljanja životnim ciklusom informaciono-komunikacionih sistema, posebno je značajna činjenica da se u praksi još uvek mogu pronaći uređaji kojima je istekao period proizvođačke podrške (*End-of-Life*), ali koji iz ekonomskih, organizacionih ili operativnih razloga nastavljaju da budu deo aktivne mrežne infrastrukture. Takvi sistemi predstavljaju povećan bezbednosni rizik, ne zato što koriste IKEv1 kao takav, već zato što često ne dobijaju bezbednosna ažuriranja, podršku proizvođača i zaštitu od novootkrivenih implementacionih ranjivosti. Upravo zbog toga analiza njihovih bezbednosnih karakteristika zadržava visok praktični značaj za organizacije koje upravljaju kritičnom infrastrukturom [56; RFC 9395]. Posmatrano iz perspektive savremenih naprednih persistentnih pretnji (*Advanced Persistent Threat* – APT), prisustvo IKEv1 u mrežnoj infrastrukturi ne predstavlja automatski cilj napada zbog same verzije protokola. Naprotiv, ono može predstavljati indikator postojanja

nasleđene infrastrukture u kojoj postoji veća verovatnoća zastarelih konfiguracija, neadekvatno održavanih VPN uređaja, slabijih kriptografskih politika bezbednosti ili postojanje hardverskih uređaja kojima je istekla proizvođačka podrška. Drugim rečima, APT akteri ne posmatraju IKEv1 izolovano, već kao jedan od elemenata ukupnog “bezbednosnog profila organizacije”. Zbog toga analiza načina na koji napadači vrše identifikaciju, profilisanje i procenu ovakvih sistema predstavlja važan deo savremenog bezbednosnog inženjerstva i doprinosi boljem razumevanju operativnih rizika u prelaznom periodu između dve generacije protokola [2],[74; RFC 9370].

Rezultati sprovedene analize potvrđuju da naučno istraživanje IKEv1 nije usmereno na razvoj novih implementacija ovog protokola niti na preporuku njegove buduće primene. Naprotiv, njegov cilj jeste razumevanje bezbednosnih karakteristika sistema koji su i dalje prisutni u značajnom broju realnih informaciono-komunikacionih okruženja i koji će, usled postepene migracije, još određeni vremenski period predstavljati sastavni deo kritične mrežne infrastrukture. Upravo zbog toga analiza APT scenarija, implementacionih ranjivosti i operativnih bezbednosnih rizika ne predstavlja proučavanje zastarele tehnologije radi istorijskog pregleda, već naučno utemeljenu procenu rizika koja omogućava bezbednije upravljanje nasleđenim sistemima tokom njihove tranzicije ka savremenijim arhitekturama zasnovanim na IKEv2. Time se potvrđuje da predmet ovog istraživanja nije isključivo sam protokol, već i proces upravljanja bezbednošću informaciono-komunikacionih sistema u uslovima tehnološke tranzicije, što predstavlja jednu od ključnih tema savremenog bezbednosnog inženjerstva [2],[31],[38].

5. Razvoj ikev2 protokola kroz procesnu analizu arhitekture, bezbednosnih mehanizama i evolucije u odnosu na ikev1 protokol

Analiza sprovedena u prethodnom poglavlju pokazala je da bezbednosna arhitektura Internet Key Exchange Version 1 (IKEv1) protokola, uprkos svom istorijskom značaju u razvoju savremene primenjene kriptografije, poseduje niz strukturnih ograničenja koja proizlaze iz same arhitektonske kompleksnosti protokola. Činjenica da je Faza 1 protokola dozvoljavala izbor između dva suštinski različita režima razmene (*Main Mode* i *Aggressive Mode*), da su primenjivane metode autentifikacije međusobno odstupale po ostvarenom nivou bezbednosne otpornosti, te da protokol nije predviđao ujednačen, standardizovan pristup zaštiti od napada uskraćivanjem usluge, ukazivala je ne toliko na pojedinačne bezbednosne propuste koliko na posledicu šireg projektantskog pristupa u kojem je fleksibilnost protokola ostvarena po ceni njegove predvidivosti i implementacione jednostavnosti. Upravo su ova ograničenja, sistematizovana kroz procesnu analizu sprovedenu u prethodnom poglavlju, predstavljala polaznu osnovu za razvoj nove generacije protokola.

Internet Key Exchange Version 2 (IKEv2) protokol, definisan izvorno kroz RFC 4306, a potom ažuriran i objedinjen kroz RFC 7296 kao trenutno važeću specifikaciju, ne predstavlja jednostavnu tehničku dogradnju prethodne verzije, već rezultat sistemskog preispitivanja arhitektonskih principa na kojima počiva bezbedna razmena kriptografskih ključeva. Umesto umnožavanja funkcionalnih varijanti, projektanti IKEv2 protokola opredelili su se za racionalizaciju protokolarne logike kroz uvođenje jedinstvenog, standardizovanog toka razmene poruka (IKE_SA_INIT i IKE_AUTH), čime je broj mogućih stanja protokola sveden na minimum neophodan za ostvarivanje osnovnih bezbednosnih ciljeva. Ovakav pristup neposredno se nadovezuje na centralnu metodološku tezu ovog istraživanja, prema kojoj bezbednost informaciono-komunikacionog sistema ne proizlazi isključivo iz snage primenjenih kriptografskih algoritama, već iz kvaliteta i predvidivosti procesa kojim se ti algoritmi integrišu u širu bezbednosnu arhitekturu.

Ovo poglavlje sprovodi sveobuhvatnu procesnu analizu IKEv2 protokola, dosledno prateći metodološki okvir uspostavljen u prethodnim poglavljima ove magistarske teze. Analiza započinje razmatranjem istorijskih okolnosti i konkretnih projektantskih unapređenja koja su dovela do standardizacije IKEv2 protokola (odeljak 5.1), nakon čega sledi detaljna analiza njegove arhitekture i funkcionalnog modela, sa posebnim osvrtom na hijerarhijski odnos IKE_SA i CHILD_SA bezbednosnih asocijacija (odeljak 5.2). Naredni odeljci obrađuju proces uspostavljanja IKE_SA kao osnove digitalnog poverenja (odeljak 5.3), mehanizme upravljanja CHILD_SA asocijacijama i životni ciklus kriptografskih ključeva, uključujući rekeying procese (odeljak 5.4), kao i integrisanu arhitekturu bezbednosnih mehanizama koji obuhvataju autentifikaciju, tajnost i integritet komunikacije (odeljak 5.5).

Poseban deo analize posvećen je naprednim funkcionalnostima IKEv2 protokola, uključujući podršku za mobilnost i interoperabilnost u savremenim, heterogenim mrežnim okruženjima (odeljak 5.6), kao i sistematskoj analizi bezbednosnih ranjivosti protokola, sprovedenoj kroz teorijski model klasifikacije i pregled dokumentovanih implementacionih propusta (odeljak 5.7). Poglavlje se zaokružuje komparativnom analizom bezbednosne arhitekture, upravljanja ključevima i operativnih karakteristika IKEv1 i IKEv2 protokola (odeljak 5.8), kritičkom evaluacijom IKEv2 protokola u kontekstu savremenih VPN sistema (odeljak 5.9), te naučno-istraživačkom sintezom nalaza koja predstavlja osnovu za dalju analizu sprovedenu u narednim poglavljima ove teze (odeljak 5.10).

Na ovaj način, procesna analiza IKEv2 protokola sprovedena u ovom poglavlju ne predstavlja izolovano razmatranje jedne nove verzije protokola, već direktan nastavak i produbljivanje analitičkog okvira uspostavljenog kroz analizu IKEv1 protokola, čime se omogućava sistematsko, uzročno-posledično sagledavanje evolucije bezbednosnih karakteristika Internet Key Exchange protokola u celini.

5.1. Evolucija bezbednosne arhitekture: istorijski razvoj, razlozi za nastanak i standardizacija internet key exchange (ikev2) protokola

Razvoj savremenih bezbednosnih protokola predstavlja kontinuirani evolutivni proces u kojem se arhitektura informaciono-komunikacionih sistema prilagođava novim operativnim zahtevima, tehnološkim promenama i identifikovanim bezbednosnim izazovima (*lawful hacking, kompleksni vektori napada itd*). IKEv2 predstavlja evoluciju bezbednosne arhitekture zasnovanu na principima pojednostavljenja IKEv1 protokola, standardizacije (u kontekstu hardverskih komponenti sistema i konkretnih implementacija IPSec/IKE mehanizama zaštite), interoperabilnosti i povećanja bezbednosti informaciono-komunikacionih sistema [2].

Upravo zbog toga razvoj IKEv2 predstavlja idealan primer procesa evolucije savremenih bezbednosnih standarda, u kojoj se unapređenje bezbednosti postiže optimizacijom arhitekture protokola. Takav pristup zasniva se na pretpostavci da ukupna otpornost informaciono-komunikacionog sistema zavisi od međusobnog delovanja više komplementarnih komponenti: kvaliteta protokolarnog dizajna, standardizacije i detaljnog dokumentovanja implementacije, pravilnog upravljanja bezbednosnim asocijacijama, pouzdane razmene kriptografskih ključeva, interoperabilnosti između različitih proizvođača mrežne opreme i efikasnog upravljanja životnim ciklusom bezbednosnih mehanizama. Drugim rečima, bezbednost se više ne posmatra kao statička osobina pojedinačnog algoritma, već kao dinamičko svojstvo celokupne arhitekture sistema [31],[38].

Istorijski posmatrano, razvoj IKEv1 predstavljao je izuzetno značajan korak u standardizaciji bezbedne razmene kriptografskih ključeva u okviru IPsec arhitekture. Integracijom koncepata razvijenih kroz ISAKMP, Oakley i SKEME uspostavljen je jedinstveni okvir koji je omogućio automatizovanu autentifikaciju komunikacionih entiteta, bezbednu razmenu Diffie–Hellman parametara, uspostavljanje *Security Association* (SA) struktura i generisanje zajedničkog kriptografskog materijala potrebnog za zaštitu komunikacije preko nepouzdanih mreža. U trenutku svog nastanka IKEv1 predstavljao je jedno od najznačajnijih dostignuća u oblasti mrežne bezbednosti, jer je omogućio praktičnu implementaciju IPsec VPN sistema u različitim informaciono-komunikacionim okruženjima i postavio osnovu za široku primenu virtualnih privatnih mreža u državnim institucijama, vojnim sistemima Ministarstva odbrane, infrastrukturi specijalne namene Ministarstva unutrašnjih poslova, finansijskom sektoru, telekomunikacionim operatorima i velikim korporativnim mrežama [52; RFC 2408].

Međutim, upravo široka primena IKEv1 omogućila je prikupljanje dragocenih empirijskih saznanja o njegovom ponašanju u realnim operativnim uslovima. Za razliku od teorijskih analiza koje uglavnom razmatraju matematičku sigurnost korišćenih algoritama, praktična implementacija pokazala je da ukupna pouzdanost bezbednosnog sistema zavisi od znatno većeg broja međusobno povezanih faktora. Uočeno je da složenost protokolarnog logike povećava mogućnost implementacionih grešaka, veliki broj opcionih funkcionalnosti otežava interoperabilnost između različitih implementacija, dok različita tumačenja standarda mogu dovesti do nepredvidivog ponašanja komunikacionih entiteta tokom procesa uspostavljanja bezbednosne asocijacije. Time je potvrđeno da povećanje funkcionalnosti bez odgovarajuće

standardizacije može istovremeno povećati i ukupnu površinu napada (*attack surface*), čime se smanjuje ukupna otpornost informaciono-komunikacionog sistema na kompleksne vektore napada [16].

5.1.1. Kritička analiza evolucije bezbednosne arhitekture: projektna unapređenja implementirana u ikev2 protokolu

Razvoj i implementacija *Internet Key Exchange Version 2* (IKEv2) protokola predstavlja jedan od najznačajnijih primera evolucije bezbednosne arhitekture u oblasti zaštite informaciono-komunikacionih sistema. Za razliku od pristupa koji razvoj nove generacije protokola posmatra prvenstveno kroz prizmu uvođenja novih funkcionalnosti ili unapređenja pojedinačnih kriptografskih mehanizama, naučno-istraživačka analiza u okviru ove magistarske teze pokazuje da je osnovni cilj razvoja IKEv2 bio sistemsko unapređenje celokupne protokolarne arhitekture zasnovane na analizi ranjivosti IKEv1 protokola [2],[92; BSI TR-02102-1],[93; BSI TR-02102-3].

Polazeći od iskustava stečenih tokom višegodišnje eksploatacije IKEv1, projektanti IKEv2 usvojili su drugačiju razvojnu filozofiju u odnosu na prethodnu generaciju protokola. Umesto proširivanja postojećih funkcionalnosti i povećavanja složenosti IKE protokola, razvoj je usmeren ka racionalizaciji arhitekture, smanjenju broja međusobno zavisnih procedura i preciznijoj standardizaciji u procesu uspostavljanja kriptografski zaštićene komunikacije. Ovakav pristup predstavlja primenu jednog od osnovnih principa bezbednog projektovanja informacionih sistema, prema kojem se informaciona bezbednost sistema povećava smanjenjem njene kompleksnosti, odnosno eliminacijom nepotrebnih funkcionalnih i logičkih elemenata koji mogu predstavljati potencijalne izvore implementacionih grešaka ili bezbednosnih ranjivosti [64; RFC 8221],[65; RFC 8247].

Prvo značajno projektno unapređenje implementirano u IKEv2 odnosi se na racionalizaciju logike protokola. U IKEv1 arhitekturi istovremeno su postojali *Main Mode*, *Aggressive Mode* i *Quick Mode*, pri čemu je svaki režim posedovao sopstveni sled razmene poruka, specifične bezbednosne karakteristike i različite operative zahteve. Iako je ovakav koncept omogućavao određeni stepen fleksibilnosti, istovremeno je povećavao složenost implementacije, otežavao formalnu analizu protokola i stvarao dodatni prostor za različita tumačenja standarda. Iz perspektive bezbednosnog inženjerstva, postojanje većeg broja alternativnih procedura povećava broj mogućih stanja kroz koja protokol prolazi, čime raste i verovatnoća pojave implementacionih grešaka koje mogu negativno uticati na bezbednost sistema. Projektanti IKEv2 upravo su zbog toga napustili koncept višestrukih režima rada i usvojili jedinstveni model razmene poruka, čime je značajno pojednostavljena protokolarna arhitektura i smanjena ukupna površina napada (*attack surface*) [30].

Posmatrano iz naučno-istraživačke perspektive, navedena projektna odluka ima znatno širi značaj od smanjenja broja poruka ili pojednostavljenja implementacije. Njena osnovna vrednost ogleda se u činjenici da smanjenje protokolarne složenosti neposredno doprinosi povećanju pouzdanosti implementacija, olakšava formalnu verifikaciju bezbednosnih svojstava protokola i povećava mogućnost interoperabilnosti između različitih proizvođača mrežne opreme. Time je potvrđena uzročno-posledična veza između racionalizacije arhitekture i povećanja ukupne bezbednosti informaciono-komunikacionog sistema, što predstavlja jednu od centralnih ideja projektovanja i razvoja IKEv2 protokola [2].

Drugo projektno unapređenje odnosilo se na unapređenje modela upravljanja bezbednosnim asocijacijama. Analiza IKEv1 pokazala je da administrativna složenost procesa uspostavljanja, održavanja i obnove *Security Association* struktura predstavlja značajan operativni izazov, naročito u velikim distribuiranim informacionim sistemima. Zbog toga je razvoj IKEv2 bio usmeren ka uspostavljanju arhitekture koja omogućava jasnije razdvajanje upravljačkih funkcija, efikasnije upravljanje životnim ciklusom bezbednosnih asocijacija i jednostavnije održavanje većeg broja simultanih VPN sesija [2], [64; RFC 8221].

Treće unapređenje odnosilo se na povećanje interoperabilnosti između implementacija različitih proizvođača. Iskustva stečena kroz primenu IKEv1 pokazala su da heterogena mrežna okruženja predstavljaju jedan od najvećih izazova za uspešno funkcionisanje bezbednosnih protokola. Različita tumačenja opcionihi delova standarda često su dovodila do problema kompatibilnosti između uređaja različitih proizvođača, povećavajući složenost implementacije i troškove administracije. Projektanti IKEv2 odgovorili su na ovaj izazov preciznijim definisanjem protokolarnih procedura i smanjenjem prostora za proizvoljna implementaciona odstupanja [23].

Sa aspekta informacione bezbednosnog ovakva projektna odluka ima višestruki značaj. Pojednostavljenjem upravljanja *Security Association* strukturama smanjuje se mogućnost nastanka administrativnih grešaka koje mogu dovesti do pogrešne konfiguracije kriptografskih parametara ili nepravilnog upravljanja životnim ciklusom sesija. Na taj način bezbednost više nije rezultat isključivo kvaliteta pojedinačnih algoritama, već rezultat efikasnog upravljanja celokupnim životnim ciklusom bezbednosnih mehanizama [30], [31].

Naučno istraživačka analiza u okviru ove magistarske teze potvrđuje da razvoj IKEv2 nije predstavljao linearan proces dodavanja novih funkcionalnosti postojećem protokolu. Naprotiv, reč je o sistematski planiranoj transformaciji arhitekture zasnovanoj na rezultatima empirijskih istraživanja, iskustvima stečenim kroz praktičnu primenu i kontinuiranom procesu standardizacije međunarodnih bezbednosnih mehanizama u oblasti informacione bezbednosti. Upravo zbog toga IKEv2 predstavlja primer kako se savremeni bezbednosni protokoli razvijaju kroz proces institucionalnog i tehničkog učenja, u kojem svako identifikovano ograničenje prethodne generacije postaje polazna osnova za projektovanje otpornijih, interoperabilnijih i operativno efikasnijih arhitektonskih rešenja [2]. Posebnu pažnju potrebno je posvetiti činjenici da su savremene metode kompromitacije informaciono-komunikacionih sistema u velikoj meri usmerene na zaobilazanje kriptografskih mehanizama (*Lawful Hacking*), a ne na direktno kriptanalitički aspekt (*brute force* napade na kriptografski zaštićene poruke/dokumente i sl.). Primena *lawful hacking* metoda, eksploatacija ranjivosti operativnih sistema, kompromitacija aplikativnog softvera, napadi na *endpoint* uređaje, kao i iskorišćavanje implementacionih propusta potvrđuju da napadači u praksi često ostvaruju pristup informacijama pre uspostavljanja kriptografske zaštite ili nakon njihove dekripcije na krajnjem komunikacionom uređaju. Posmatrano iz ove perspektive, razvoj IKEv2 predstavlja neophodan, ali ne i dovoljan uslov za postizanje visokog nivoa bezbednosti. Efikasna zaštita zahteva integraciju protokolarnih mehanizama sa bezbednim operativnim sistemima, pouzdanim upravljanjem identitetima, kontinuiranim upravljanjem ranjivostima, digitalnom forenzikom, bezbednosnim monitoringom (u realnom vremenu povezanim sa *incident response* timovima) i institucionalnim procedurama upravljanja rizikom [5],[7],[10],[11].

Naučno-istraživačka analiza potvrđuje da u kontekstu metodološkog aspekta, razvoj IKEv2 protokola predstavlja kontinuirani proces učenja u kojem se rezultati praktične primene, analiza bezbednosnih incidenata, standardizacija i tehnološke inovacije međusobno dopunjuju

i uslovljavaju razvoj kvalitativno boljih rešenja u domenu informacione bezbednosti. Svako novo projektno unapređenje predstavlja odgovor na prethodno identifikovana ograničenja, dok istovremeno postavlja osnovu za budući razvoj i prilagođavanje novim bezbednosnim izazovima. Takav evolutivni model razvoja predstavlja jedno od osnovnih obeležja savremene sajber bezbednosti i potvrđuje da bezbednost nije statično stanje, već dinamičan proces kontinuiranog unapređenja arhitekture, implementacije i operativne primene bezbednosnih mehanizama [15].

5.2. Arhitektura i funkcionalni model ikev2

Savremeni bezbednosni protokoli predstavljaju znatno više od skupa procedura za razmenu kriptografskih ključeva ili autentifikaciju komunikacionih učesnika. Posmatrano sa aspekta bezbednosnog inženjerstva, arhitektura protokola predstavlja skup projektnih odluka kojima se definiše organizacija sistema, raspodela funkcionalnih odgovornosti i način međusobne koordinacije svih komponenti sistema. Kvalitet arhitekture neposredno utiče na otpornost sistema prema bezbednosnim pretnjama, složenost implementacije, mogućnost formalne verifikacije stanja bezbednosti, interoperabilnost između različitih implementacija i efikasnost upravljanja životnim ciklusom bezbednosnih mehanizama. Iz tog razloga arhitektonsko projektovanje predstavlja jednu od najznačajnijih faza razvoja savremenih bezbednosnih protokola, jer upravo u toj fazi nastaju odluke koje dugoročno određuju nivo njihove pouzdanosti i sposobnosti prilagođavanja novim tehnološkim i operativnim zahtevima. Naučno-istraživačka analiza razvoja IKEv2 pokazuje da je njegova arhitektura projektovana polazeći od iskustava stečenih tokom eksploatacije IKEv1, pri čemu je osnovni cilj bio uspostavljanje jednostavnijeg, preglednijeg i otpornijeg modela upravljanja bezbednim komunikacionim sesijama. Umesto pristupa karakterističnog za prethodnu generaciju protokola, u kojem je povećana funkcionalna složenost predstavljala izvor brojnih implementacionih i operativnih izazova, IKEv2 uvodi arhitekturu zasnovanu na jasnoj hijerarhijskoj organizaciji bezbednosnih funkcija. Takva organizacija omogućava preciznije razdvajanje odgovornosti pojedinačnih komponenti, racionalnije upravljanje kriptografskim materijalom i veću predvidivost ponašanja protokola u različitim mrežnim okruženjima.

Jedna od osnovnih karakteristika arhitekture IKEv2 jeste razdvajanje upravljačke i ravni podataka u procesu komunikacije (*control plane* i *data plane*). Upravljačka ravan odgovorna je za autentifikaciju komunikacionih učesnika, uspostavljanje međusobnog poverenja, pregovaranje kriptografskih algoritama, razmenu kriptografskog materijala i upravljanje životnim ciklusom bezbednosnih asocijacija. Nasuprot tome, podatkovna ravan zadužena je za zaštitu korisničkog saobraćaja primenom mehanizama definisanih u okviru IPsec arhitekture. Ovakvo razdvajanje predstavlja jednu od ključnih projektnih odluka implementiranih u IKEv2, jer omogućava da se upravljanje bezbednosnim procesima odvija nezavisno od prenosa korisničkih podataka, čime se povećava fleksibilnost, pojednostavljuje administracija i unapređuje ukupna otpornost sistema [2].

Sa aspekta bezbednosne arhitekture, razdvajanje upravljačke i ravni podataka ima višestruki značaj. Pre svega, omogućava jasnu funkcionalnu podelu odgovornosti između procesa koji upravljaju bezbednosnim parametrima i procesa koji koriste već uspostavljene kriptografske ključeve za zaštitu komunikacije. Takav pristup smanjuje međusobnu zavisnost pojedinačnih komponenti sistema i doprinosi smanjenju ukupne složenosti protokolarne logike. Istovremeno, svaka promena u okviru upravljačke ravni može biti realizovana bez neposrednog uticaja na prenos korisničkih podataka, čime se povećava stabilnost komunikacije i olakšava upravljanje bezbednosnim sesijama u složenim informaciono-komunikacionim sistemima [2],[10].

Projektovanje ovakve arhitekture nije rezultat isključivo tehničke optimizacije, već predstavlja odgovor na fundamentalni izazov savremenih VPN sistema: kako istovremeno obezbediti visok nivo bezbednosti, efikasno upravljanje velikim brojem komunikacionih sesija i dovoljnu fleksibilnost za funkcionisanje u heterogenim mrežnim okruženjima. Upravo zbog toga IKEv2 uvodi hijerarhijski organizovan model upravljanja bezbednosnim mehanizmima u kojem se upravljačke funkcije izdvajaju u zaseban logički sloj. Time se postiže veća preglednost arhitekture, olakšava razvoj interoperabilnih implementacija i stvara pouzdana osnova za dalji razvoj novih funkcionalnosti bez narušavanja osnovne bezbednosne logike protokola.

Posmatrano iz metodološke perspektive, ovakva organizacija potvrđuje jednu od centralnih hipoteza ove magistarske teze: bezbednost savremenih VPN sistema proizlazi iz kvaliteta projektovanja njihove arhitekture jednako koliko i iz snage primenjenih kriptografskih algoritama. Kriptografski algoritmi predstavljaju neophodan element zaštite, ali tek njihova pravilna organizacija u okviru jasno definisane bezbednosne arhitekture omogućava ostvarivanje visokog nivoa poverljivosti, integriteta, autentifikacije i operativne otpornosti komunikacionog sistema. U tom smislu arhitektura IKEv2 predstavlja primer kako se principi bezbednog projektovanja mogu transformisati u praktično primenljiv međunarodni standard sposoban da odgovori na zahteve savremenih informaciono-komunikacionih sistema [2],[10].

Jedna od najznačajnijih odluka u kontekstu implementacija u IKEv2 protokolu jeste uvođenje posebne upravljačke bezbednosne asocijacije, označene kao *IKE Security Association* (IKE_SA). Posmatrano sa stanovišta savremenog bezbednosnog inženjerstva, ova projektna odluka predstavlja mnogo više od tehničkog mehanizma za razmenu kriptografskih ključeva. Naprotiv, IKE_SA predstavlja centralni upravljački element kompletne bezbednosne arhitekture IKEv2, čija je osnovna funkcija uspostavljanje digitalnog poverenja između komunikacionih entiteta, upravljanje bezbednosnim parametrima i koordinacija svih narednih bezbednosnih procesa koji se odvijaju tokom životnog ciklusa komunikacione sesije [2], [39], [51].

Za razliku od pojednostavljenog shvatanja prema kojem se IKE_SA posmatra isključivo kao kanal za razmenu ključeva, naučno-istraživačka analiza pokazuje da njegova stvarna uloga obuhvata znatno širi skup funkcionalnih odgovornosti. Nakon uspešne autentifikacije komunikacionih učesnika, upravo putem IKE_SA realizuju se pregovaranje kriptografskih algoritama, uspostavljanje zajedničkog kriptografskog konteksta, zaštita upravljačkih poruka, kreiranje novih CHILD_SA struktura, obnova postojećih bezbednosnih asocijacija (*rekeying*), razmena informacija neophodnih za održavanje sesije, kao i kontrolisano uklanjanje bezbednosnih asocijacija po završetku komunikacije. Time IKE_SA postaje centralna upravljačka komponenta kroz koju se koordinira celokupni životni ciklus bezbedne komunikacije. [55; RFC 7296.], [63; RFC 8031], [65; RFC 8247],[71; RFC 4945.].

Posmatrano iz arhitektonske perspektive, izdvajanje upravljačkih funkcija u okviru posebne bezbednosne asocijacije predstavlja primenu principa funkcionalne modularnosti. U savremenom projektovanju složenih informaciono-komunikacionih sistema modularnost predstavlja jedan od osnovnih principa kojim se postižu preglednost arhitekture, lakše održavanje, jednostavnija nadogradnja i povećana otpornost sistema na greške. Primenom istog principa u IKEv2 protokolu postignuto je jasno razdvajanje procesa koji upravljaju bezbednošću od procesa koji obezbeđuju zaštitu korisničkog saobraćaja.

Na taj način upravljačka logika postaje nezavisna od konkretnih tokova podataka, čime se povećava fleksibilnost sistema i pojednostavljuje upravljanje velikim brojem istovremenih komunikacionih sesija [2].

Ovakva organizacija ima neposredne bezbednosne implikacije. Razdvajanjem upravljačke i podatkovne ravni smanjuje se mogućnost da promena jednog dela sistema izazove neželjene posledice u drugom delu arhitekture. U slučaju potrebe za promenom kriptografskih parametara ili obnovom ključeva, nije neophodno ponovo uspostavljati celokupnu komunikaciju, već se odgovarajuće izmene realizuju kroz već uspostavljeni upravljački kanal. Time se smanjuje operativna složenost, povećava kontinuitet rada sistema i umanjuje mogućnost nastanka bezbednosnih propusta tokom procesa rekonfiguracije komunikacione sesije. Kompromitacija endpoint uređaja, eksploatacija implementacionih ranjivosti, kompromitacija identiteta korisnika ili zloupotreba privilegovanih naloga mogu omogućiti zaobilazanje kriptografske zaštite bez narušavanja same arhitekture protokola. Ova činjenica potvrđuje da ni najkvalitetnije projektovana bezbednosna arhitektura ne može biti posmatrana izolovano od šireg koncepta višeslojne zaštite (*defence in depth*), koji podrazumeva integraciju protokolarnih, sistemskih, organizacionih i operativnih mera bezbednosti [10]. Osnovna prednost ogleda se u jasnom razdvajanju upravljačkih i podatkovnih funkcija, racionalizaciji protokolarne logike i unapređenju upravljanja životnim ciklusom bezbednosnih asocijacija, čime se istovremeno povećavaju bezbednost, interoperabilnost, skalabilnost i operativna otpornost informaciono-komunikacionog sistema.

Jedna od najvažnijih karakteristika funkcionalnog modela IKEv2 jeste jasno razdvajanje između IKE Security Association (IKE_SA) i CHILD Security Association (CHILD_SA). Ovakva organizacija predstavlja jednu od ključnih arhitektonskih inovacija u odnosu na prethodnu generaciju Internet Key Exchange protokola, budući da uvodi hijerarhijski model upravljanja bezbednosnim sesijama u kojem se upravljačke funkcije i zaštita korisničkog saobraćaja realizuju kroz dve međusobno povezane, ali funkcionalno različite bezbednosne asocijacije. Time se postiže viši stepen modularnosti, efikasnije upravljanje životnim ciklusom komunikacionih sesija i veća otpornost sistema na operativne promene tokom trajanja komunikacije [77; SP 800-77 Rev. 1.],[87; FIPS 140-3], [88; FIPS 203], [89; FIPS 204.].

U okviru ovakvog modela, IKE_SA predstavlja trajni upravljački kontekst između komunikacionih učesnika. Njegova osnovna funkcija nije prenos korisničkih podataka, već uspostavljanje i održavanje bezbednosnog odnosa poverenja između strana koje učestvuju u komunikaciji. Kroz IKE_SA realizuju se međusobna autentifikacija, pregovaranje kriptografskih algoritama, razmena i obnova kriptografskog materijala, zaštita upravljačkih poruka, kao i koordinacija svih procesa koji se odnose na upravljanje bezbednosnim asocijacijama. Na taj način IKE_SA predstavlja centralni kontrolni mehanizam koji omogućava da se sve bezbednosne odluke donose u okviru jedinstvenog i kriptografski zaštićenog upravljačkog kanala [2]. Nasuprot tome, CHILD_SA predstavlja bezbednosnu asocijaciju namenjenu zaštiti stvarnog korisničkog saobraćaja. Svaka CHILD_SA koristi bezbednosne parametre dogovorene kroz IKE_SA, ali funkcioniše kao zasebna logička celina odgovorna za zaštitu IPsec komunikacije primenom odgovarajućih ESP mehanizama. Ovakvo razdvajanje omogućava da se više različitih CHILD_SA uspostavi i održava u okviru jedne IKE_SA, čime se ostvaruje značajno povećanje fleksibilnosti i skalabilnosti sistema. U praktičnim implementacijama to omogućava zaštitu različitih tokova saobraćaja ili različitih bezbednosnih politika bez potrebe za ponovnim uspostavljanjem kompletne upravljačke sesije [10].

Sa stanovišta arhitektonskog projektovanja, ovakav hijerarhijski odnos između IKE_SA i CHILD_SA predstavlja primenu principa razdvajanja odgovornosti (*separation of concerns*), jednog od osnovnih načela savremenog softverskog i bezbednosnog inženjerstva. Umesto objedinjavanja svih funkcija u okviru jedinstvenog komunikacionog procesa, upravljački i podatkovni aspekt komunikacije organizovani su kao međusobno povezane, ali jasno diferencirane funkcionalne celine. Time se smanjuje međusobna zavisnost komponenti, pojednostavljuje održavanje sistema i omogućava efikasnije upravljanje promenama koje nastaju tokom životnog ciklusa komunikacije [77; SP 800-77 Rev. 1],[78; FIPS 197],[79; FIPS 180-4].

Jedna od najvažnijih posledica ovakvog funkcionalnog modela jeste mogućnost nezavisnog upravljanja životnim ciklusom bezbednosnih asocijacija. Tokom trajanja komunikacije može biti potrebno obnoviti kriptografske ključeve, promeniti bezbednosne algoritme, kreirati novu CHILD_SA ili ukloniti postojeću bezbednosnu asocijaciju usled promene bezbednosne politike ili završetka određenog toka komunikacije. Zahvaljujući postojanju centralnog upravljačkog konteksta, sve navedene aktivnosti mogu se realizovati bez prekida osnovne upravljačke sesije, čime se obezbeđuje kontinuitet rada sistema i smanjuje operativna složenost upravljanja komunikacijom [31].

Jedna od osnovnih prednosti funkcionalnog modela IKEv2 ogleda se u tome što bezbednosne asocijacije nisu posmatrane kao statični elementi komunikacije, već kao dinamičke strukture čiji se životni ciklus kontinuirano prilagođava operativnim zahtevima informaciono-komunikacionog sistema. Takav pristup predstavlja značajnu promenu u odnosu na tradicionalne modele u kojima je uspostavljanje bezbedne komunikacije često predstavljalo jednokratni proces nakon kojeg su bezbednosni parametri ostajali nepromenjeni do završetka sesije. U IKEv2 arhitekturi bezbednosne asocijacije prolaze kroz jasno definisane faze kreiranja, održavanja, modifikacije, obnove i kontrolisanog uklanjanja, čime se ostvaruje visok stepen fleksibilnosti i dugoročne otpornosti komunikacionog sistema.

Životni ciklus započinje uspostavljanjem IKE_SA, čime se formira inicijalni odnos poverenja između komunikacionih entiteta. Tokom ove faze izvršava se međusobna autentifikacija, pregovaranje kriptografskih algoritama, razmena Diffie–Hellman parametara i generisanje zajedničkog kriptografskog materijala koji predstavlja osnov za sve naredne bezbednosne procese. Tek nakon uspešnog završetka ove faze moguće je uspostaviti jednu ili više CHILD_SA struktura namenjenih zaštiti korisničkog saobraćaja. Ovakav redosled nije slučajni, već predstavlja direktnu posledicu arhitektonskog principa prema kojem se poverenje između komunikacionih učesnika mora uspostaviti pre nego što se omogući prenos zaštićenih podataka. [31],[54; RFC 4306.].

Nakon uspostavljanja komunikacije funkcionalni model IKEv2 omogućava kontinuirano upravljanje postojećim bezbednosnim asocicijama bez potrebe za prekidanjem aktivne VPN sesije. Tokom eksploatacije sistema može doći do potrebe za promenom kriptografskih algoritama, obnovom ključeva, uspostavljanjem dodatnih CHILD_SA za nove tokove saobraćaja ili uklanjanjem postojećih asocijacija koje više nisu potrebne. Zahvaljujući postojanju centralnog upravljačkog konteksta, sve navedene aktivnosti realizuju se kroz već uspostavljenu IKE_SA, čime se izbegava ponovno pokretanje celokupnog procesa autentifikacije i razmene kriptografskog materijala. Time se postiže značajno smanjenje operativnog opterećenja i povećava kontinuitet komunikacije [2].

Poseban značaj u okviru životnog ciklusa bezbednosnih asocijacija ima mehanizam *rekeying*. Dugotrajna upotreba istog kriptografskog ključa povećava rizik od njegove kompromitacije i može negativno uticati na ukupnu kriptografsku otpornost sistema. Iz tog razloga IKEv2 omogućava periodičnu obnovu kriptografskog materijala pre isteka bezbednosnog veka postojećih ključeva. Proces obnove realizuje se kontrolisano, uz očuvanje kontinuiteta komunikacije i bez prekida aktivnih aplikativnih sesija. Na taj način funkcionalni model IKEv2 objedinjuje dva zahteva koja su često međusobno suprotstavljena: visok nivo bezbednosti i visok nivo dostupnosti komunikacionih servisa [2].

Sa aspekta upravljanja rizikom, ovakav pristup ima izuzetno veliki značaj. Periodična zamena ključeva smanjuje količinu podataka zaštićenih istim kriptografskim materijalom, ograničava potencijalne posledice eventualne kompromitacije i doprinosi očuvanju dugoročne poverljivosti komunikacije. Istovremeno, mogućnost nezavisne obnove CHILD_SA bez ponovnog uspostavljanja IKE_SA omogućava racionalnije korišćenje mrežnih i procesorskih resursa, što je naročito značajno u velikim distribuiranim VPN okruženjima sa hiljadama aktivnih komunikacionih sesija [51].

Naučno-istraživačka analiza pokazuje da ovakav funkcionalni model predstavlja primenu principa adaptivnog upravljanja bezbednošću. Umesto statičkog modela zaštite, u kojem se bezbednosni parametri određuju samo na početku komunikacije, IKEv2 uvodi koncept kontinuiranog upravljanja bezbednosnim stanjem sistema. Time se omogućava da bezbednosna arhitektura dinamički odgovara na promene u komunikacionom okruženju, promene bezbednosnih politika i potrebe za periodičnim unapređenjem kriptografske zaštite, bez narušavanja kontinuiteta rada informaciono-komunikacionog sistema. Još jedna važna karakteristika funkcionalnog modela jeste kontrolisano uklanjanje bezbednosnih asocijacija po završetku komunikacije. Pravilno gašenje IKE_SA i svih pripadajućih CHILD_SA struktura predstavlja važan element bezbednosnog životnog ciklusa, jer sprečava zadržavanje nepotrebnog kriptografskog materijala u memoriji sistema i smanjuje mogućnost njegove kasnije zloupotrebe. Time se potvrđuje da upravljanje bezbednošću obuhvata ne samo uspostavljanje i održavanje komunikacije, već i njeno bezbedno okončanje u skladu sa principima savremenog bezbednosnog inženjerstva. Sprovedena analiza funkcionalnog modela IKEv2 potvrđuje da njegova osnovna vrednost ne proizlazi iz postojanja pojedinačnih bezbednosnih mehanizama, već iz načina na koji su oni organizovani u jedinstvenu arhitektonsku celinu. IKE_SA i CHILD_SA ne predstavljaju dva nezavisna elementa protokola, već međusobno povezan sistem u kojem svaka komponenta izvršava jasno definisanu funkciju u okviru ukupnog procesa uspostavljanja, održavanja i zaštite komunikacije. Takva organizacija omogućava da se proces autentifikacije, upravljanje kriptografskim materijalom i zaštita korisničkog saobraćaja odvijaju koordinisano, uz očuvanje funkcionalne modularnosti i visokog nivoa operativne fleksibilnosti [2].

Primena ovog principa u IKEv2 omogućila je da se upravljačke funkcije izdvoje od procesa zaštite korisničkog mrežnog saobraćaja, čime je povećana preglednost arhitekture, pojednostavljena implementacija i smanjena mogućnost neželjenih međusobnih uticaja između različitih bezbednosnih procesa. Posmatrano iz perspektive dugoročnog razvoja bezbednosnih protokola, upravo ovakav pristup predstavlja jedno od osnovnih obeležja savremenog arhitektonskog projektovanja [55; RFC 7296].

Operativne prednosti ovakve organizacije posebno dolaze do izražaja u informaciono-komunikacionim sistemima u kojima istovremeno postoji veliki broj aktivnih VPN komunikacionih sesija. Mogućnost uspostavljanja više CHILD_SA unutar jedne IKE_SA

omogućava racionalnije korišćenje računarskih i mrežnih resursa, efikasnije sprovođenje različitih bezbednosnih politika i jednostavnije upravljanje komunikacionim tokovima različitih nivoa bezbednosti i pristupa klasifikacija tajnosti podataka. Time se postiže visok stepen skalabilnosti bez povećanja administrativne složenosti, što predstavlja jedan od osnovnih zahteva savremenih korporativnih, državnih i kritičnih informaciono-komunikacionih sistema. Obnova kriptografskih ključeva, uspostavljanje novih CHILD_SA ili uklanjanje postojećih bezbednosnih asocijacija mogu se realizovati bez prekida osnovnog upravljačkog odnosa između komunikacionih učesnika. Takav pristup omogućava kontinuitet rada informaciono-komunikacionog sistema, smanjuje vreme potrebno za sprovođenje bezbednosnih procedura i povećava dostupnost komunikacionih servisa. U savremenim okruženjima, u kojima se zahteva neprekidna dostupnost kritičnih informacionih servisa, ovakva sposobnost adaptivnog upravljanja komunikacionim sesijama predstavlja jednu od najvažnijih operativnih prednosti IKEv2 arhitekture [55; RFC 7296], [71; RFC 4945].

5.3. Uspostavljanje ike_sa: proces razmene poruka i uspostavljanje digitalnog poverenja

Uspostavljanje bezbedne komunikacije između dva entiteta koji prethodno nisu uspostavili međusobni odnos poverenja predstavlja jedan od osnovnih izazova savremene primenjene kriptografije i mrežne bezbednosti. Za razliku od komunikacije u zatvorenim sistemima, u kojima se može pretpostaviti postojanje unapred definisanog odnosa poverenja između učesnika, komunikacija preko javnih IP mreža odvija se u okruženju koje se smatra inherentno nepouzdanim. U takvim uslovima nije dovoljno samo zaštititi sadržaj komunikacije primenom snažnih kriptografskih algoritama. Pre bilo kakve razmene poverljivih podataka neophodno je uspostaviti pouzdan mehanizam kojim će komunikacioni entiteti izgraditi zajednički kriptografski kontekst, potvrditi međusobni identitet i usaglasiti bezbednosne parametre koji će predstavljati osnov za dalju zaštićenu komunikaciju. Upravo zbog toga proces uspostavljanja **IKE Security Association (IKE_SA)** predstavlja centralni element bezbednosne arhitekture IKEv2 protokola.

Posmatrano iz perspektive bezbednosnog inženjerstva, uspostavljanje IKE_SA ne predstavlja samo razmenu nekoliko protokolarnih poruka između dva uređaja. Reč je o sistematski projektovanom procesu postepenog smanjivanja neizvesnosti između komunikacionih učesnika, pri čemu svaka faza razmene ima jasno definisanu bezbednosnu funkciju. Tokom ovog procesa učesnici najpre usaglašavaju kriptografske algoritme, zatim uspostavljaju zajednički kriptografski materijal primenom *Diffie-Hellman* razmene, nakon čega potvrđuju međusobni identitet i tek na kraju omogućavaju zaštitu korisničkog saobraćaja. Ovakav sled aktivnosti nije rezultat proizvoljnog projektovanja, već predstavlja posledicu jasno definisanih principa savremene kriptografske arhitekture, prema kojima se poverenje između učesnika mora graditi postepeno, kroz niz međusobno zavisnih bezbednosnih koraka [12],[74; RFC 9370].

Jedna od najvažnijih projektnih odluka implementiranih u IKEv2 jeste razdvajanje procesa uspostavljanja zajedničkog kriptografskog konteksta od procesa potvrđivanja identiteta komunikacionih učesnika. Iz bezbednosne perspektive, ovakav pristup ima izuzetno veliki značaj. Pre nego što bude moguće bezbedno razmeniti autentifikacione informacije, neophodno je uspostaviti zajednički skup kriptografskih parametara koji će omogućiti zaštitu tih informacija od prisluškivanja, modifikacije ili drugih oblika kompromitacije. Drugim rečima, autentifikacija nije početna faza procesa uspostavljanja komunikacije, već njegov logički nastavak, koji se može bezbedno realizovati tek nakon što je uspostavljen odgovarajući kriptografski okvir [71; RFC 4945],[77. SP 800-77 Rev. 1.], [87. FIPS 140-3].

Prva faza procesa uspostavljanja IKE_SA, realizovana kroz IKE_SA_INIT razmenu poruka, upravo zbog toga ima zadatak da uspostavi zajedničku kriptografsku osnovu buduće komunikacije. Tokom ove faze komunikacioni entiteti pregovaraju o izboru kriptografskih algoritama, razmenjuju Diffie–Hellman javne vrednosti i nonce parametre, na osnovu kojih se generiše zajednički kriptografski materijal. Posebno je značajno naglasiti da u ovoj fazi identitet komunikacionih učesnika još uvek nije potvrđen. Projektanti IKEv2 namerno su razdvojili uspostavljanje kriptografskog konteksta od autentifikacije, čime je omogućeno da se podaci koji potvrđuju identitet razmenjuju tek nakon što je uspostavljen zaštićeni komunikacioni kanal. Takva projektna odluka predstavlja jedan od najvažnijih razloga zbog kojih IKEv2 ostvaruje viši nivo bezbednosti u odnosu na prethodnu generaciju *Internet Key Exchange* protokola [70; RFC 7427.], [71; RFC 4945.], [74; RFC 9370].

Sa aspekta projektovanja bezbednosnih protokola, izbor kriptografskih algoritama predstavlja prvi korak u procesu izgradnje digitalnog poverenja. Komunikacioni entiteti moraju postići saglasnost o algoritmima za razmenu ključeva, zaštitu integriteta, šifrovanje i generisanje pseudo-slučajnih vrednosti, pri čemu se bira skup algoritama koji podržavaju obe strane komunikacije. Ovakav postupak omogućava interoperabilnost između različitih implementacija IKEv2 i obezbeđuje da se dalji bezbednosni procesi odvijaju na zajednički prihvaćenim kriptografskim osnovama. Time pregovaranje algoritama dobija znatno širi značaj od tehničke konfiguracije protokola, jer predstavlja prvi korak u uspostavljanju zajedničkog bezbednosnog okruženja između komunikacionih učesnika [2],[31].

Posebnu ulogu u ovoj fazi imaju *Diffie–Hellman* javne vrednosti i **nonce** parametri. Njihova zajednička funkcija nije samo generisanje zajedničkog kriptografskog materijala, već i obezbeđivanje kriptografske svežine (*freshness*) svake nove komunikacione sesije. Uvođenjem novih *Diffie–Hellman* vrednosti i jedinstvenih nonce parametara za svaku sesiju sprečava se ponovno korišćenje prethodno generisanog kriptografskog materijala i značajno smanjuje mogućnost uspešne realizacije napada zasnovanih na reprodukciji ranije presretnutih komunikacionih poruka (*replay attacks*). Time se potvrđuje da projektovanje procesa uspostavljanja IKE_SA nije usmereno samo na generisanje zajedničkog ključa, već i na očuvanje dugoročne kriptografske otpornosti sistema kroz obezbeđivanje jedinstvenosti svake komunikacione sesije [2].

Jedna od najznačajnijih karakteristika procesa IKE_SA_INIT ogleda se u činjenici da je njegov redosled kriptografskih operacija pažljivo projektovan kako bi se svaka naredna faza zasnivala na rezultatima prethodne. Posmatrano sa aspekta bezbednosnog inženjerstva, ovakav pristup predstavlja primenu principa postepenog uspostavljanja digitalnog poverenja, prema kojem nijedna bezbednosna funkcija ne može biti izvršena pre nego što budu ispunjeni svi neophodni kriptografski preduslovi za njeno bezbedno sprovođenje. Upravo zbog toga IKEv2 ne započinje komunikaciju autentifikacijom učesnika, već uspostavljanjem zajedničkog kriptografskog konteksta koji će omogućiti da autentifikacioni podaci budu razmenjeni kroz zaštićen komunikacioni kanal [2],[10], [31].

Prvi korak u okviru IKE_SA_INIT razmene predstavlja pregovaranje kriptografskih algoritama. Na prvi pogled, ovaj postupak može delovati kao administrativna ili konfiguraciona faza komunikacije. Međutim, detaljna naučno-istraživačka analiza pokazuje da njegovo bezbednosno značenje prevazilazi izbor konkretnih algoritama. Pregovaranjem kriptografskih parametara komunikacioni entiteti uspostavljaju zajednički skup bezbednosnih pravila kojima će biti određeni svi naredni kriptografski procesi. Drugim rečima, pre nego što bude moguće govoriti o zaštiti komunikacije, obe strane moraju postići saglasnost o načinu na

koji će ta zaštita biti realizovana. Time pregovaranje algoritama predstavlja prvi korak u izgradnji zajedničkog bezbednosnog okruženja između komunikacionih učesnika [2].

Neposredno nakon usaglašavanja kriptografskih parametara sledi razmena **Diffie–Hellman** javnih vrednosti. Posmatrano iz perspektive teorijske kriptografije, osnovna svrha ovog procesa jeste omogućavanje generisanja zajedničke tajne vrednosti bez njenog direktnog prenosa preko komunikacionog kanala. Međutim, sa stanovišta bezbednosne arhitekture IKEv2 značaj Diffie–Hellman razmene znatno je širi. Ova faza predstavlja trenutak u kojem dva prethodno nepovezana komunikaciona entiteta prvi put uspostavljaju zajednički kriptografski kontekst koji će predstavljati osnov za sve naredne bezbednosne operacije. Time Diffie–Hellman razmena postaje centralni mehanizam transformacije međusobnog nepoverenja u početni odnos kriptografskog poverenja, pri čemu nijedan učesnik ne otkriva svoju privatnu vrednost, a zajednički kriptografski materijal nastaje kao rezultat matematički definisanog procesa saradnje obe strane [10].

Posebno značajnu ulogu u okviru IKE_SA_INIT imaju *nonce* vrednosti. Njihova funkcija nije ograničena na povećanje entropije prilikom generisanja kriptografskog materijala, već predstavlja jedan od osnovnih mehanizama zaštite od ponovne upotrebe prethodno razmenjenih komunikacionih poruka. Uvođenjem jedinstvenih slučajnih vrednosti za svaku novu komunikacionu sesiju obezbeđuje se da svako uspostavljanje IKE_SA predstavlja kriptografski jedinstven događaj, nezavisan od svih prethodnih sesija. Time se značajno povećava otpornost sistema na **replay** napade i druge oblike pokušaja ponovnog korišćenja prethodno presretnutih komunikacionih podataka [2].

Naučno-istraživačka analiza pokazuje da se puna vrednost *Diffie–Hellman* razmene i *nonce* parametara ne može razumeti ukoliko se posmatraju izolovano. Njihov bezbednosni doprinos proizlazi upravo iz međusobne povezanosti. Dok *Diffie–Hellman* omogućava generisanje zajedničke tajne vrednosti, *nonce* parametri obezbeđuju jedinstvenost svake komunikacione sesije i sprečavaju ponovno korišćenje prethodno generisanog kriptografskog materijala. Tek njihovom zajedničkom primenom nastaje kriptografska osnova koja omogućava bezbedno izvođenje sesijskih ključeva i nastavak procesa uspostavljanja digitalnog poverenja [65; RFC 8247].

Jedna od najznačajnijih projektnih odluka implementiranih u IKEv2 odnosi se na činjenicu da tokom IKE_SA_INIT faze identitet komunikacionih učesnika još uvek nije potvrđen. Ovakav pristup predstavlja svesno projektno opredeljenje čiji je cilj da se autentifikacione informacije nikada ne razmenjuju pre uspostavljanja odgovarajuće kriptografske zaštite. Time se značajno smanjuje mogućnost kompromitacije identiteta komunikacionih učesnika tokom inicijalne faze uspostavljanja komunikacije i potvrđuje osnovni princip savremenog bezbednosnog projektovanja prema kojem se zaštita identiteta mora zasnivati na prethodno uspostavljenom kriptografskom poverenju [71; RFC 4945].

Kritička naučno-istraživačka analiza pokazuje da proces IKE_SA_INIT predstavlja znatno više od inicijalne razmene protokolarnih poruka između komunikacionih entiteta. Njegova suštinska funkcija ogleda se u postepenom uspostavljanju kriptografske osnove na kojoj će biti izgrađeno digitalno poverenje između učesnika komunikacije. Projektanti IKEv2 protokola napustili su pristup u kojem se autentifikacija posmatra kao početna faza komunikacije i usvojili arhitektonski model prema kojem se identitet potvrđuje tek nakon što je uspostavljen zajednički kriptografski kontekst. Takva projektna odluka predstavlja jednu od najznačajnijih bezbednosnih inovacija IKEv2, jer omogućava da se autentifikacioni podaci

razmenjuju kroz već zaštićen komunikacioni kanal, čime se značajno smanjuje mogućnost njihove kompromitacije tokom inicijalne faze komunikacije [54; RFC 4306].

Sa aspekta bezbednosnog inženjerstva, posebno je značajno uočiti da svaka faza IKE_SA_INIT razmene predstavlja neophodan preduslov za uspešno izvršavanje naredne faze procesa. Pregovaranje kriptografskih algoritama definiše zajednički skup bezbednosnih pravila, Diffie–Hellman razmena omogućava generisanje zajedničke tajne vrednosti bez njenog direktnog prenosa preko mreže, dok nonce parametri obezbeđuju kriptografsku svežinu svake komunikacione sesije i povećavaju otpornost na replay napade. Nijedna od ovih funkcija pojedinačno nije dovoljna za uspostavljanje bezbedne komunikacije, ali njihova međusobna povezanost omogućava formiranje pouzdanog kriptografskog okruženja koje predstavlja osnov za sve naredne bezbednosne operacije. Time se potvrđuje da bezbednost IKEv2 ne proizlazi iz pojedinačnih mehanizama, već iz njihove pažljivo projektovane međusobne koordinacije [2].

Operativni značaj ovakvog pristupa posebno dolazi do izražaja u savremenim informaciono-komunikacionim sistemima koji funkcionišu u uslovima visoke heterogenosti, distribuirane infrastrukture i velikog broja istovremenih VPN komunikacionih sesija. Standardizovan proces uspostavljanja zajedničkog kriptografskog konteksta omogućava interoperabilnost između implementacija različitih proizvođača mrežne opreme, pojednostavljuje administraciju i povećava predvidivost ponašanja protokola u složenim mrežnim okruženjima. Istovremeno, jasno definisan sled kriptografskih operacija olakšava formalnu verifikaciju implementacija, smanjuje mogućnost konfiguracionih odstupanja i doprinosi ukupnoj pouzdanosti bezbednosne arhitekture IKEv2 [51].

Međutim, kritička analiza pokazuje da ni pravilno projektovan proces IKE_SA_INIT ne može samostalno obezbediti potpunu bezbednost komunikacije. Njegova efikasnost zavisi od kvaliteta implementacije protokola, pouzdanosti generatora slučajnih brojeva, pravilnog izbora i konfiguracije kriptografskih algoritama, kao i od bezbednosti krajnjih uređaja na kojima se komunikacija uspostavlja. Kompromitacija implementacije, eksploatacija ranjivosti operativnog sistema, neadekvatno upravljanje kriptografskim ključevima ili kompromitacija endpoint uređaja mogu ugroziti bezbednost komunikacije bez narušavanja same logike IKE_SA_INIT procesa. Ovakva činjenica potvrđuje da kriptografski protokol predstavlja samo jednu komponentu šireg sistema sajber bezbednosti, čija efikasnost zavisi od koordinisanog delovanja tehničkih, organizacionih i operativnih mera zaštite [38].

Savremeni bezbednosni izazovi dodatno potvrđuju značaj ovakvog višeslojnog pristupa. Napredne pretnje, uključujući eksploataciju implementacionih ranjivosti, kompromitaciju identiteta, napade usmerene na krajnje uređaje i lawful hacking metode zasnovane na kompromitaciji endpoint sistema, pokazuju da napadači često nastoje da zaobiđu kriptografske mehanizme umesto da ih direktno naruše. Iz tog razloga uspešna implementacija IKE_SA_INIT predstavlja neophodan, ali ne i dovoljan uslov ukupne bezbednosti VPN komunikacije. Njegova puna vrednost ostvaruje se tek kada je integrisan sa pouzdanim upravljanjem identitetima, bezbednom konfiguracijom sistema, kontinuiranim upravljanjem ranjivostima i višeslojnom zaštitom informaciono-komunikacione infrastrukture [2].

5.4. Child_sa mehanizam i upravljanje ključevima

5.4.1. Arhitektura child_sa mehanizma, životni ciklus i upravljanje kriptografskim ključevima

Nakon uspešno uspostavljene IKE Security Association (IKE_SA), koja predstavlja bezbednosni i upravljački kanal između komunikacionih učesnika, Internet Key Exchange Version 2 (IKEv2) protokol prelazi u narednu fazu svog funkcionisanja – uspostavljanje CHILD Security Association (CHILD_SA). Za razliku od IKE_SA, čija je osnovna funkcija autentifikacija komunikacionih strana, pregovaranje bezbednosnih parametara i zaštita upravljačkih poruka IKE protokola, CHILD_SA predstavlja operativni bezbednosni mehanizam čija je primarna namena zaštita stvarnog korisničkog saobraćaja koji se prenosi putem IPsec protokola. Time se ostvaruje jasno funkcionalno razdvajanje između upravljačke ravni (control plane) i ravni prenosa podataka (data plane), čime IKEv2 ostvaruje visok stepen modularnosti, fleksibilnosti i bezbednosti [10].

Sa arhitektonskog aspekta, CHILD_SA predstavlja skup bezbednosnih parametara koji definišu način na koji će se korisnički IP paketi štititi primenom odgovarajućih IPsec mehanizama, prvenstveno korišćenjem *Encapsulating Security Payload (ESP)* protokola. Svaki CHILD_SA sadrži precizno definisane kriptografske algoritme, odgovarajuće ključeve za šifrovanje i proveru integriteta, identifikatore *Security Parameter Index (SPI)*, definiše parametre važenja CHILD_SA, kao i ostale bezbednosne attribute neophodne za pouzdanu zaštitu komunikacije. Na taj način CHILD_SA ne predstavlja samo skup tehničkih konfiguracionih vrednosti, već dinamički bezbednosni kontekst koji određuje komponente i način zaštite podataka tokom trajanja komunikacione sesije [31].

Jedna od najznačajnijih karakteristika IKEv2 arhitekture jeste mogućnost da jedna uspostavljena IKE_SA istovremeno upravlja sa više nezavisnih CHILD_SA instanci. Ovakav koncept omogućava uspostavljanje više paralelnih bezbednosnih kanala između istih komunikacionih učesnika, pri čemu svaki CHILD_SA može koristiti različite kriptografske algoritme, različite bezbednosne politike ili štititi različite tokove saobraćaja (*i predstavlja prednost u razmeni podataka koji prema klasifikaciji imaju različite stepene tajnosti*). Posmatrano sa aspekta upravljanja informaciono-komunikacionim sistemima, ovakva arhitektura značajno povećava fleksibilnost implementacije, omogućava precizniju segmentaciju mrežnog saobraćaja i olakšava primenu različitih bezbednosnih politika u okviru jedne VPN infrastrukture [51].

Posebnu vrednost ovakvog arhitektonskog rešenja predstavlja razdvajanje životnog ciklusa IKE_SA i CHILD_SA asocijacija. Dok IKE_SA ostaje aktivna kao centralni upravljački kanal odgovoran za održavanje bezbednosnog odnosa između komunikacionih strana, pojedinačne CHILD_SA asocijacije mogu se nezavisno uspostavljati, obnavljati (*rekeying*), menjati ili uklanjati bez potrebe za ponovnim sprovođenjem ponovne autentifikacije korisnika koji su uspostavili kriptografski zaštićeni kanal komunikacije. Ovakav pristup značajno smanjuje količinu razmenjenih podataka, povećava raspoloživost sistema i omogućava kontinuirano održavanje bezbedne komunikacije čak i tokom periodične zamene kriptografskih ključeva ili promene bezbednosnih politika [2].

Upravljanje kriptografskim ključevima predstavlja jednu od najvažnijih funkcija CHILD_SA mehanizma. Bezbednost celokupnog IPsec sistema ne zavisi isključivo od izbora snažnih kriptografskih algoritama, već u značajnoj meri od načina generisanja, distribucije, korišćenja, obnavljanja i bezbednog uništavanja kriptografskog materijala tokom čitavog životnog ciklusa komunikacione sesije. Upravo zbog toga IKEv2 implementira strogo definisan model

upravljanja ključevima koji omogućava da svaki novoformirani CHILD_SA koristi jedinstveni skup sesijskih ključeva izvedenih iz prethodno uspostavljenog zajedničkog kriptografskog materijala, čime se obezbeđuje visok stepen kriptografske nezavisnosti između pojedinačnih bezbednosnih asocijacija. Kvalitetno generisani i pravilno distribuirani ključevi predstavljaju osnov za pouzdanu primenu kriptografskih algoritama; pravilna primena algoritama omogućava očuvanje poverljivosti, integriteta i autentičnosti prenetih podataka; očuvanje ovih bezbednosnih svojstava doprinosi otpornosti komunikacionog kanala na različite oblike kriptanalitičkih i implementacionih napada; dok dugoročna otpornost sistema direktno zavisi od mogućnosti periodičnog obnavljanja kriptografskog materijala bez narušavanja kontinuiteta komunikacije [77; SP 800-77 Rev. 1.].

5.4.2. Rekeying, create_child_sa mehanizam i bezbednosni značaj upravljanja životnim ciklusom kriptografskih ključeva

Jedna od najznačajnijih bezbednosnih karakteristika Internet Key Exchange Version 2 (IKEv2) protokola ogleda se u sposobnosti kontinuiranog upravljanja životnim ciklusom bezbednosnih asocijacija i pripadajućeg kriptografskog materijala bez prekidanja zaštićene komunikacije. Za razliku od pristupa u kojem bi isti kriptografski ključevi bili korišćeni tokom celokupnog trajanja VPN sesije, IKEv2 implementira mehanizme periodične obnove (**rekeying**) kojima se obezbeđuje da svaka faza komunikacije koristi novi skup sesijskih kriptografskih ključeva. Time se značajno smanjuje količina podataka zaštićenih jednim ključem, ograničavaju potencijalne posledice kompromitacije kriptografskog ključa i povećava ukupna kriptografska otpornost informaciono-komunikacionog sistema [2].

Centralni mehanizam kojim se ostvaruje ovakav model upravljanja predstavlja CREATE_CHILD_SA razmena. Njena osnovna funkcija nije ograničena isključivo na uspostavljanje nove CHILD_SA asocijacije, već obuhvata i obnovu postojećih CHILD_SA, kao i obnovu same IKE_SA kada to zahtevaju bezbednosna politika, vremenski parametri ili operativni uslovi rada sistema. Ovakvo objedinjavanje više funkcionalnosti u jedinstveni mehanizam predstavlja jedno od značajnih arhitektonskih unapređenja IKEv2 protokola, jer pojednostavljuje implementaciju, smanjuje signalizacioni saobraćaj i povećava efikasnost upravljanja bezbednosnim sesijama [51].

Poseban bezbednosni značaj CREATE_CHILD_SA mehanizma proizlazi iz činjenice da se tokom procesa obnove generiše novi kriptografski materijal (KEYMAT) koji se koristi za zaštitu narednog perioda komunikacije. Novi ključevi nisu prost nastavak prethodno korišćenih vrednosti, već predstavljaju rezultat pažljivo definisanog procesa derivacije zasnovanog na zajedničkim tajnama, svežim nonce vrednostima i odgovarajućim pseudonasumičnim funkcijama (PRF). Time se postiže visok stepen kriptografske nezavisnosti između uzastopnih generacija sesijskih ključeva, čime se sprečava da kompromitacija jednog skupa ključeva automatski ugrozi bezbednost budućih komunikacionih sesija [2].

Jedan od osnovnih principa na kojima počiva ovakav model jeste primena koncepta **Perfect Forward Secrecy (PFS)**. Njegova suština ogleda se u tome da kompromitacija dugoročnih autentifikacionih ključeva ili jednog sesijskog ključa ne omogućava retroaktivnu dekriptaciju prethodno zabeleženog komunikacionog saobraćaja. U slučaju kada se tokom procesa CREATE_CHILD_SA sprovodi nova razmena kriptografskog materijala korišćenjem dodatnog mehanizma razmene ključeva, svaka nova CHILD_SA dobija sopstvenu kriptografsku osnovu nezavisnu od prethodnih sesija. Posledica ovakvog pristupa jeste značajno povećanje otpornosti sistema na dugotrajno presretanje komunikacija, kasniju

kompromitaciju identiteta učesnika i različite oblike odloženih kriptanalitičkih napada [2].

Sa aspekta upravljanja rizicima, periodična zamena ključeva predstavlja jednu od najefikasnijih preventivnih mera za ograničavanje posledica eventualne kompromitacije kriptografskog materijala. Produžena upotreba istih sesijskih ključeva povećava količinu raspoloživog šifrovanog materijala koji potencijalni napadač može analizirati, produžava vremenski interval u kojem kompromitovani ključ ostaje operativno upotrebljiv i povećava verovatnoću uspeha različitih kriptanalitičkih ili implementacionih napada. Nasuprot tome, pravilno definisane politike rekeying-a periodično prekidaju kontinuitet korišćenja postojećeg ključa, ograničavaju njegov operativni životni vek i značajno umanjuju potencijalni obim posledica uspešne kompromitacije [73; RFC 9242.].

Efikasnost ovakvog modela ne zavisi isključivo od kriptografskih algoritama, već i od pravilnog upravljanja celokupnim životnim ciklusom bezbednosnih asocijacija. Svaka CHILD_SA prolazi kroz jasno definisane faze uspostavljanja, aktivne upotrebe, periodične obnove i bezbednog uklanjanja iz sistema. Tokom svake od ovih faza neophodno je obezbediti konzistentnost kriptografskih parametara, sinhronizaciju između komunikacionih učesnika i pouzdano uklanjanje zastarelog kriptografskog materijala iz memorije uređaja. Neadekvatno upravljanje bilo kojom od navedenih faza može dovesti do degradacije bezbednosti, čak i kada se koriste savremeni i kriptografski snažni algoritmi [2].

Posebnu pažnju zaslužuje činjenica da bezbednost upravljanja ključevima predstavlja rezultat međusobnog delovanja više različitih komponenti bezbednosne arhitekture. Kvalitet generatora slučajnih brojeva neposredno utiče na entropiju generisanih nonce vrednosti; kvalitet nonce vrednosti utiče na nepredvidivost izvedenog KEYMAT materijala; kvalitet izvedenih ključeva određuje efikasnost primenjenih algoritama za zaštitu poverljivosti i integriteta; dok pravilno definisane politike rekeying-a određuju koliko dugo će svaki pojedinačni ključ ostati operativno aktivan. Na taj način nastaje kontinuirani uzročno-posledični lanac u kojem kvalitet svake pojedinačne faze neposredno utiče na ukupni nivo bezbednosti celokupnog VPN sistema [85; SP 800-57 Part 1 Rev. 5.].

Sa metodološkog aspekta, analiza CHILD_SA mehanizma potvrđuje da upravljanje ključevima predstavlja proces, a ne jednokratni događaj tokom uspostavljanja komunikacije. Bezbednost IKEv2 ne proizlazi samo iz inicijalne razmene ključeva, već iz sposobnosti protokola da tokom čitavog trajanja komunikacione sesije kontinuirano održava visok nivo kriptografske zaštite kroz kontrolisanu obnovu bezbednosnih asocijacija i kriptografskog materijala. Time se ostvaruje dinamički model bezbednosti koji omogućava da VPN infrastruktura ostane otporna na promene bezbednosnog okruženja, dugotrajne komunikacione sesije i evoluciju savremenih tehnika napada [10].

Završna naučno-istraživačka sinteza ovog podpoglavlja potvrđuje da CHILD_SA mehanizam predstavlja jednu od ključnih arhitektonskih prednosti IKEv2 protokola. Njegov značaj prevazilazi tehničku funkciju uspostavljanja bezbednosnih asocijacija, jer omogućava sistematsko upravljanje životnim ciklusom kriptografskih ključeva, implementaciju principa Perfect Forward Secrecy, kontrolisanu obnovu sesijskih parametara i očuvanje kontinuiteta zaštićene komunikacije bez ponovne autentifikacije učesnika. Uzročno-posledično posmatrano, pravilno upravljanje životnim ciklusom ključeva povećava kriptografsku otpornost sistema; povećana otpornost umanjuje posledice eventualne kompromitacije pojedinačnih ključeva; ograničavanje posledica kompromitacije povećava ukupnu pouzdanost VPN infrastrukture; dok pouzdana VPN infrastruktura predstavlja osnov za bezbednu

razmenu podataka u savremenim informaciono-komunikacionim sistemima. Upravo zbog toga upravljanje ključevima u IKEv2 treba posmatrati kao jedan od fundamentalnih procesa očuvanja dugoročne bezbednosti digitalnih komunikacija, a ne isključivo kao tehnički mehanizam za generisanje i zamenu kriptografskog materijala [2], [51].

5.5. Bezbednosni mehanizmi ikev2

5.5.1. Integrisana arhitektura autentifikacije, tajnosti i integriteta u ikev2 protokolu

Bezbednosna arhitektura Internet Key Exchange Version 2 (IKEv2) protokola zasnovana je na principu višeslojne zaštite, pri čemu se osnovna bezbednosna svojstva – autentifikacija, poverljivost i integritet ne ostvaruju kao nezavisni mehanizmi, već kao međusobno povezane komponente jedinstvenog sistema zaštite. Za razliku od pristupa u kojem bi pojedinačne bezbednosne funkcije bile implementirane izolovano, IKEv2 integriše kriptografske algoritme, procedure autentifikacije, mehanizme razmene ključeva i zaštite komunikacionih poruka u koherentnu bezbednosnu arhitekturu čiji je cilj očuvanje sigurnosti komunikacije tokom čitavog životnog ciklusa VPN sesije. Upravo ovakva integracija predstavlja jednu od osnovnih projektantskih prednosti IKEv2 u odnosu na ranije generacije protokola.

Prvi i osnovni element ove arhitekture jeste autentifikacija komunikacionih učesnika, čiji je cilj potvrđivanje identiteta obe strane pre uspostavljanja zaštićenog komunikacionog kanala. U zavisnosti od zahteva konkretnog informaciono-komunikacionog sistema, IKEv2 podržava više modela autentifikacije, uključujući korišćenje unapred podeljenih ključeva (*Pre-Shared Key* – PSK), digitalnih sertifikata zasnovanih na infrastrukturi javnih ključeva (*Public Key Infrastructure* – PKI) i *Extensible Authentication Protocol* (EAP) metoda koje omogućavaju integraciju sa savremenim sistemima upravljanja identitetima. Ovakva fleksibilnost omogućava primenu IKEv2 u različitim operativnim okruženjima – od manjih poslovnih mreža do složenih informacionih sistema velikih organizacija i kritične infrastrukture [31], [87; FIPS 140-3].

Međutim, autentifikacija sama po sebi nije dovoljna za obezbeđivanje bezbednosti komunikacije. Njena osnovna funkcija jeste uspostavljanje poverenja između komunikacionih učesnika, koje zatim predstavlja osnov za bezbedno generisanje i korišćenje zajedničkog kriptografskog materijala. Ukoliko identitet učesnika nije pouzdano potvrđen, celokupan proces razmene ključeva postaje podložan napadima lažnog predstavljanja (*impersonation*) i posredničkim napadima (*Man-in-the-Middle* – MITM). Iz tog razloga autentifikacija predstavlja početnu kariku uzročno-posledičnog lanca na kojem počiva kompletna bezbednosna arhitektura IKEv2.

Nakon uspešno završene autentifikacije, centralnu ulogu preuzima mehanizam obezbeđivanja tajnosti komunikacije primenom savremenih algoritama za simetrično šifrovanje. IKEv2 podržava više standardizovanih algoritama, među kojima posebno mesto zauzimaju Advanced Encryption Standard (AES) u različitim režimima rada, uključujući AES-CBC i AES-GCM, dok savremene implementacije podržavaju i algoritam **ChaCha20-Poly1305**, naročito u okruženjima gde je potrebno postići visok nivo performansi uz ograničene hardverske resurse. Izbor odgovarajućeg algoritma vrši se tokom procesa pregovaranja bezbednosnih parametara, čime se omogućava prilagođavanje nivoa zaštite konkretnim bezbednosnim zahtevima i performansama sistema.

Poverljivost komunikacije predstavlja jedno od osnovnih bezbednosnih svojstava IKEv2, jer

sprečava neovlašćena lica da pristupe sadržaju prenetih podataka čak i u slučaju njihovog presretanja na komunikacionom kanalu. Međutim, efikasnost šifrovanja neposredno zavisi od kvaliteta upravljanja kriptografskim ključevima, što potvrđuje da poverljivost nije rezultat isključivo primene snažnog algoritma, već zajedničkog delovanja autentifikacije, razmene ključeva, pravilne derivacije KEYMAT materijala i bezbednog upravljanja životnim ciklusom sesijskih ključeva analiziranih u prethodnom podpoglavlju.

Treći osnovni stub bezbednosne arhitekture IKEv2 predstavlja zaštita integriteta komunikacije. Za razliku od poverljivosti, čiji je cilj sprečavanje otkrivanja sadržaja poruka, mehanizmi integriteta omogućavaju otkrivanje svake neovlašćene izmene podataka tokom njihovog prenosa. U tu svrhu IKEv2 koristi odgovarajuće kriptografske funkcije za proveru autentičnosti poruka, uključujući algoritme zasnovane na *Hash-based Message Authentication Code* (HMAC) konstrukciji, kao i integrisane autentifikovane režime šifrovanja poput AES-GCM, koji istovremeno obezbeđuju i poverljivost i integritet prenetih podataka. Time se postiže visok stepen zaštite od pokušaja modifikacije sadržaja komunikacije, ubacivanja lažnih poruka ili narušavanja konzistentnosti bezbednosnog dijaloga između komunikacionih učesnika [80; FIPS 198-1.], [81; SP 800-38D].

Poseban značaj mehanizama integriteta ogleda se u njihovoj ulozi u sprečavanju aktivnih napada na komunikacioni kanal. Napadač koji nije u mogućnosti da proizvede ispravne autentifikacione vrednosti ne može neprimećeno izmeniti sadržaj IKE ili IPsec poruka, niti može uspešno kreirati nove validne poruke koje bi bile prihvaćene od strane legitimnih učesnika komunikacije. Time zaštita integriteta neposredno doprinosi očuvanju autentičnosti komunikacionog procesa i predstavlja neophodnu dopunu mehanizmima zaštite tajnosti komunikacije [2].

Analiza međusobnih odnosa između autentifikacije, poverljivosti i integriteta pokazuje da nijedno od navedenih bezbednosnih svojstava ne može samostalno obezbediti odgovarajući nivo zaštite informaciono-komunikacionog sistema. Pouzdana autentifikacija predstavlja osnov za bezbednu razmenu ključeva; kvalitetno upravljanje ključevima omogućava efikasnu primenu algoritama za šifrovanje; pravilno sprovedeno šifrovanje obezbeđuje poverljivost komunikacije; dok zaštita integriteta garantuje da sadržaj poruka neće biti neprimećeno izmenjen tokom prenosa. Izostanak bilo koje od navedenih komponenti narušava bezbednost celokupnog sistema, što potvrđuje da IKEv2 svoju otpornost ne zasniva na pojedinačnim mehanizmima, već na njihovom koordinisanom i međusobno zavisnom delovanju [31].

Savremeni informaciono-komunikacioni sistemi izloženi su širokom spektru pretnji koje prevazilaze pokušaje kompromitacije poverljivosti ili autentifikacije komunikacije. Napadači često nastoje da naruše raspoloživost servisa, izazovu prekid komunikacije ili zloupotrebe mrežnu infrastrukturu radi onemogućavanja legitimnog uspostavljanja bezbednosnih sesija. Iz tog razloga *Internet Key Exchange Version 2* (IKEv2) ne ograničava svoju bezbednosnu arhitekturu na primenu kriptografskih algoritama, već implementira dodatne zaštitne mehanizme kojima se povećava otpornost protokola na različite operative i mrežne napade [55; RFC 7296].

Jedan od osnovnih mehanizama predstavlja zaštita od replay napada, čiji je cilj sprečavanje ponovne upotrebe prethodno presretnutih legitimnih poruka. U odsustvu ovakve zaštite, napadač bi mogao da reprodukuje ranije zabeležene komunikacione poruke kako bi pokušao da izazove neželjene promene stanja komunikacione sesije ili da simulira legitimnu aktivnost učesnika. IKEv2 ovaj rizik umanjuje korišćenjem jedinstvenih identifikatora poruka (*Message*

ID), strogo definisanog redosleda razmene poruka i mehanizama za proveru njihove konzistentnosti. Time se obezbeđuje da svaka poruka bude obrađena isključivo u odgovarajućem kontekstu i samo jednom, čime se čuva integritet protokolskog dijaloga [2].

Posebnu pažnju IKEv2 posvećuje zaštiti od napada uskraćivanja usluge (*Denial-of-Service – DoS*), koji predstavljaju jednu od najčešćih pretnji dostupnosti VPN infrastrukture. Tokom procesa uspostavljanja bezbednosnih asocijacija server mora izdvojiti procesorske, memorijske i mrežne resurse radi obrade zahteva klijenta. Napadač može pokušati da zloupotrebi ovu činjenicu slanjem velikog broja lažnih zahteva sa ciljem iscrpljivanja raspoloživih resursa sistema. Radi ublažavanja ovakvog rizika, IKEv2 implementira **Cookie** mehanizam kojim server može zahtevati dokaz da klijent zaista poseduje mogućnost prijema odgovora na navedenoj mrežnoj adresi pre nego što alokira značajnije resurse za nastavak pregovora. Na taj način veliki broj lažnih zahteva može biti odbačen u ranoj fazi komunikacije, čime se značajno povećava otpornost sistema na pokušaje iscrpljivanja resursa [2].

Važan element operativne otpornosti predstavlja i *Network Address Translation Traversal* (NAT-T) mehanizam. U savremenim mrežnim okruženjima veliki broj korisnika pristupa Internetu preko uređaja koji primenjuju prevođenje mrežnih adresa (NAT), što može izazvati probleme pri korišćenju IPsec protokola. IKEv2 prepoznaje prisustvo NAT uređaja tokom procesa uspostavljanja komunikacije i po potrebi automatski prelazi na prenos IPsec saobraćaja putem UDP enkapsulacije. Ovakav pristup omogućava očuvanje funkcionalnosti VPN komunikacije bez narušavanja bezbednosnih svojstava protokola, čime se značajno povećava njegova interoperabilnost i primenljivost u različitim mrežnim topologijama [2], [66; RFC 3947],[87; FIPS 140-3.].

Dugotrajna pouzdanost komunikacije dodatno se unapređuje primenom mehanizama za proveru dostupnosti udaljenog učesnika, poznatih kao liveness detection i *Dead Peer Detection* (DPD). Njihova osnovna funkcija jeste pravovremeno utvrđivanje da li udaljena komunikaciona strana i dalje aktivno učestvuje u komunikaciji. U slučaju prekida mrežne veze, gašenja uređaja ili drugih operativnih problema, IKEv2 može identifikovati neaktivnu sesiju i blagovremeno osloboditi zauzete resurse ili pokrenuti postupak ponovnog uspostavljanja komunikacije. Time se povećava raspoloživost sistema i smanjuje mogućnost nastanka nekonzistentnih bezbednosnih stanja [2].

Analizirani mehanizmi imaju zajedničku karakteristiku: svaki od njih rešava specifičan bezbednosni problem, ali nijedan pojedinačno ne može obezbediti potpunu zaštitu informaciono-komunikacionog sistema. Zaštita od replay napada sprečava zloupotrebu prethodno presretnutih poruka; Cookie mehanizam povećava otpornost na DoS napade; NAT-T omogućava bezbednu komunikaciju kroz heterogene mrežne infrastrukture; dok DPD doprinosi očuvanju raspoloživosti i stabilnosti VPN sesije. Njihova puna vrednost ostvaruje se tek kroz međusobnu integraciju sa autentifikacijom, razmenom ključeva, šifrovanjem i zaštitom integriteta, koji su analizirani u prethodnom delu ovog podpoglavlja [66. RFC 3947], [67. RFC 3948].

Sa metodološkog aspekta može se uočiti da bezbednosna arhitektura IKEv2 predstavlja tipičan primer primene principa višeslojne odbrane (*defense-in-depth*). Svaki pojedinačni zaštitni mehanizam projektovan je da umanjí određenu kategoriju rizika, dok koordinisano delovanje svih mehanizama omogućava postizanje znatno višeg nivoa bezbednosti informaciono-komunikacionog sistema nego što bi bilo moguće pojedinačnom primenom

mera zaštite. Ovakav pristup smanjuje verovatnoću uspeha kompleksnih vektora napada i omogućava stanje bezbednosti čak i u situacijama kada jedan zaštitni sloj bude delimično narušen.

Završna naučno-istraživačka sinteza potvrđuje da bezbednost IKEv2 predstavlja rezultat integrisane arhitekture u kojoj autentifikacija uspostavlja poverenje između učesnika; razmena i upravljanje ključevima omogućavaju bezbedno formiranje kriptografskog materijala; mehanizmi poverljivosti i integriteta štite sadržaj komunikacije; zaštita od replay i DoS napada čuva pouzdanost procesa pregovaranja i uspostavljanja kriptografski zaštićene sesije; NAT-T obezbeđuje funkcionalnost u heterogenim mrežnim okruženjima; dok DPD doprinosi kontinuitetu i raspoloživosti komunikacije. Uzročno-posledično posmatrano, međusobna povezanost ovih mehanizama formira jedinstven sistem zaštite u kojem svaki bezbednosni sloj dopunjuje i jača ostale slojeve zaštite. Upravo ovakav sistemski pristup predstavlja jednu od najznačajnijih arhitektonskih prednosti IKEv2 i potvrđuje njegovu sposobnost da odgovori na zahteve savremenih VPN implementacija u pogledu poverljivosti, integriteta, autentičnosti, raspoloživosti i dugoročne otpornosti komunikacionih sistema [2], [31], [66. RFC 3947]; [67. RFC 3948].

5.6. Napredne funkcionalnosti ikev2

5.6.1. Mobilnost, interoperabilnost i adaptivnost ikev2 u savremenim mrežnim okruženjima

Razvoj savremenih informaciono-komunikacionih sistema karakteriše kontinuirano povećanje mobilnosti korisnika, heterogenost mrežnih infrastruktura i potreba za neprekidnom dostupnošću bezbednih komunikacionih servisa. Tradicionalni modeli uspostavljanja VPN komunikacije bili su prvenstveno projektovani za relativno stabilna mrežna okruženja u kojima su komunikacioni učesnici tokom čitave sesije koristili nepromenljive mrežne adrese i jedinstvenu pristupnu infrastrukturu. Međutim, intenzivan razvoj mobilnih uređaja, bežičnih mreža, cloud infrastrukture i distribuiranih informacionih sistema nametnuo je potrebu za protokolima koji mogu očuvati kontinuitet bezbedne komunikacije uprkos dinamičkim promenama mrežnog okruženja. Upravo u tom kontekstu Internet Key Exchange Version 2 (IKEv2) uvodi skup naprednih funkcionalnosti koje značajno proširuju njegove operativne mogućnosti u odnosu na prethodne generacije protokola [10].

Jedna od najznačajnijih inovacija predstavlja podrška za Mobility and Multihoming Protocol (MOBIKE). Ovaj mehanizam omogućava da već uspostavljena IKE_SA i pripadajuće CHILD_SA asocijacije ostanu aktivne čak i kada komunikacioni učesnik promeni svoju IP adresu ili pređe sa jedne pristupne mreže na drugu. U praktičnim uslovima to znači da korisnik može nesmetano preći sa poslovne Ethernet mreže na bežičnu Wi-Fi infrastrukturu ili mobilnu mrežu bez potrebe za ponovnim uspostavljanjem VPN sesije. Time se eliminišu prekidi komunikacije, smanjuje signalizaciono opterećenje i povećava raspoloživost bezbednih servisa [68; RFC 4555.], [70; RFC 7427], [75; RFC 9867].

Sa arhitektonskog aspekta, MOBIKE razdvaja logički identitet bezbednosne asocijacije od trenutne mrežne lokacije komunikacionog učesnika. Bezbednosni odnos uspostavljen između dve strane ostaje nepromenjen, dok se mrežni parametri prilagođavaju novim uslovima komunikacije. Ovakav pristup predstavlja značajan iskorak u odnosu na tradicionalne modele u kojima je promena IP adrese često zahtevala ponovno sprovođenje procesa autentifikacije i pregovaranja svih bezbednosnih parametara. Rezultat je efikasnije korišćenje mrežnih resursa, kraće vreme oporavka komunikacije i veći kvalitet korisničkog iskustva [68; RFC 4555].

Pored mobilnosti, značajnu ulogu ima i podrška za multihoming, odnosno mogućnost korišćenja više mrežnih interfejsa ili više komunikacionih putanja između istih učesnika. U savremenim informacionim sistemima uređaji često raspolažu istovremeno aktivnim Ethernet, Wi-Fi i mobilnim interfejsima, dok serverska infrastruktura koristi višestruke mrežne veze radi povećanja raspoloživosti i otpornosti na otkaze. IKEv2 omogućava efikasno upravljanje ovakvim okruženjima bez narušavanja bezbednosti uspostavljenih VPN sesija. Time protokol doprinosi izgradnji robusnijih komunikacionih sistema koji mogu nastaviti rad čak i u slučaju parcijalnog otkaza pojedinih mrežnih komponenti [76; RFC 6071].

Napredne funkcionalnosti IKEv2 posebno dolaze do izražaja u okruženjima koja karakterišu česte promene mrežnih uslova, poput mobilnih poslovnih aplikacija, sistema za daljinski rad, industrijskih informaciono-komunikacionih sistema i infrastrukture kritičnih službi. U ovakvim sistemima kontinuitet komunikacije ima neposredan uticaj na raspoloživost usluga, operativnu efikasnost i ukupni nivo bezbednosti. Mogućnost prilagođavanja promenama mrežnog okruženja bez prekidanja bezbednosnih asocijacija značajno smanjuje operativne rizike i povećava otpornost sistema na spoljne poremećaje [77. SP 800-77 Rev. 1.].

Sa metodološkog aspekta može se uočiti jasna uzročno-posledična veza između adaptivnosti protokola i njegove ukupne bezbednosne vrednosti. Veća sposobnost prilagođavanja promenama mrežnog okruženja omogućava očuvanje kontinuiteta komunikacije; kontinuitet komunikacije smanjuje potrebu za čestim ponovnim uspostavljanjem bezbednosnih sesija; rede ponovno pregovaranje parametara umanjuje izloženost određenim operativnim rizicima; dok stabilnije i pouzdanije komunikacione sesije povećavaju ukupnu otpornost informaciono-komunikacionog sistema. Time adaptivnost IKEv2 postaje sastavni deo njegove bezbednosne arhitekture, a ne samo dodatna funkcionalnost namenjena unapređenju performansi [2].

Posmatrano u celini, napredne funkcionalnosti IKEv2 potvrđuju da je protokol projektovan imajući u vidu zahteve savremenih mrežnih okruženja u kojima mobilnost, interoperabilnost i raspoloživost predstavljaju jednako važne ciljeve kao i poverljivost, integritet i autentifikacija. Integracijom mehanizama za mobilnost i multihoming IKEv2 uspešno povezuje visoke bezbednosne standarde sa operativnom fleksibilnošću, čime omogućava pouzdanu zaštitu komunikacija u dinamičnim i distribuiranim informaciono-komunikacionim sistemima [55; RFC 7296.].

5.6.2. Interoperabilnost, proširivost i evolutivna arhitektura ikev2 protokola

Jedna od najznačajnijih projektovanih karakteristika *Internet Key Exchange Version 2* (IKEv2) protokola ogleda se u njegovoj sposobnosti da se prilagođava promenama tehnološkog okruženja bez narušavanja osnovne bezbednosne arhitekture. Savremeni informaciono-komunikacioni sistemi karakterišu kontinuirani razvoj kriptografskih algoritama, pojava novih mrežnih tehnologija, promena bezbednosnih zahteva i rastuća potreba za interoperabilnošću između različitih proizvođača mrežne opreme i softverskih platformi. U takvim uslovima dugoročna vrednost jednog bezbednosnog protokola ne zavisi isključivo od njegove trenutne kriptografske snage, već od sposobnosti da prihvati nove tehnologije i standarde bez potrebe za potpunim redizajnom protokola [10].

Projektovanjem modularne arhitekture IKEv2 omogućeno je da se pojedine funkcionalne celine razvijaju nezavisno od osnovne logike protokola. Pregovaranje kriptografskih algoritama, metode autentifikacije, parametri razmene ključeva i bezbednosne politike nisu statički definisani, već predstavljaju promenljive elemente koji se usaglašavaju tokom procesa

uspostavljanja bezbednosne asocijacije. Ovakav pristup omogućava relativno jednostavno uvođenje novih algoritama i kriptografskih mehanizama kada postojeći postanu zastareli ili kada tehnološki razvoj nametne potrebu za njihovom zamenom. Time se značajno produžava operativni životni vek protokola i smanjuje potreba za razvojem potpuno novih rešenja pri svakoj značajnijoj promeni kriptografskog okruženja [2].

Posebnu vrednost predstavlja visok nivo interoperabilnosti između implementacija različitih proizvođača. Zahvaljujući precizno definisanim standardima za razmenu poruka, pregovaranje bezbednosnih parametara i upravljanje *Security Association* mehanizmima, uređaji različitih proizvođača mogu uspešno uspostaviti zajedničke VPN sesije uz očuvanje visokog nivoa bezbednosti. Ovakva interoperabilnost ima veliki praktični značaj za organizacije koje raspolazu heterogenom mrežnom infrastrukturom, jer omogućava postepenu modernizaciju sistema bez potrebe za istovremenom zamenom kompletne opreme [51].

Napredne mogućnosti interoperabilnosti posebno dolaze do izražaja u distribuiranim informaciono-komunikacionim sistemima, cloud okruženjima i hibridnim mrežnim arhitekturama. Savremene organizacije često koriste kombinaciju lokalnih data centara, javnih cloud servisa, mobilnih korisnika i udaljenih poslovnih lokacija. U takvim uslovima IKEv2 omogućava uspostavljanje bezbednih komunikacionih kanala između različitih mrežnih segmenata uz zadržavanje jedinstvene bezbednosne politike i centralizovanog upravljanja bezbednosnim parametrima. Time protokol postaje važna komponenta izgradnje fleksibilnih i skalabilnih VPN infrastruktura koje mogu odgovoriti na zahteve digitalne transformacije [30], [51].

Jedna od projektantskih prednosti IKEv2 jeste i podrška za različite modele autentifikacije i upravljanja identitetima. Integracija sa *Extensible Authentication Protocol* (EAP) metodama omogućava povezivanje VPN infrastrukture sa savremenim sistemima za upravljanje identitetima, višefaktorskom autentifikacijom i centralizovanim servisima za kontrolu pristupa. Na taj način IKEv2 prevazilazi ulogu protokola za razmenu kriptografskih ključeva i postaje deo šire arhitekture upravljanja digitalnim identitetima i pristupnim privilegijama [55; RFC 7296.], [74; RFC 9370].

Sa bezbednosnog aspekta posebno je značajna sposobnost protokola da prihvati nove kriptografske algoritme i mehanizme razmene ključeva bez narušavanja osnovne arhitekture. Razvoj kvantnog računarstva i postkvantne kriptografije predstavlja jedan od najvećih izazova za savremene bezbednosne protokole. Modularna struktura IKEv2 omogućava postepenu integraciju novih algoritama za razmenu ključeva i zaštitu komunikacije, čime se stvaraju preduslovi za razvoj hibridnih modela koji kombinuju tradicionalne i postkvantne kriptografske mehanizme. Time se potvrđuje da je dugoročna otpornost protokola uslovljena njegovom sposobnošću evolucije, a ne isključivo trenutnim izborom algoritama [75; RFC 9867], [88; FIPS 203.], [91; NIST IR 8547], [93; BSI TR-02102-3]. Međutim, analiza naprednih funkcionalnosti pokazuje da interoperabilnost i proširivost istovremeno predstavljaju i određeni bezbednosni izazov. Veći broj podržanih algoritama, metoda autentifikacije i opcionih funkcionalnosti povećava složenost implementacije, što može dovesti do konfiguracionih grešaka, različitih interpretacija standarda ili pojave implementacionih ranjivosti. Iz tog razloga dugoročna bezbednost IKEv2 ne zavisi samo od kvaliteta projektantske arhitekture, već i od pravilne implementacije standarda, redovnog ažuriranja softvera, bezbedne konfiguracije uređaja i dosledne primene preporučenih bezbednosnih politika [2].

Sa metodološkog aspekta može se uočiti jasna uzročno-posledična povezanost između modularnosti, interoperabilnosti i dugoročne bezbednosti protokola. Modularna arhitektura omogućava jednostavnije uvođenje novih tehnologija; mogućnost uvođenja novih tehnologija povećava interoperabilnost i prilagodljivost različitim mrežnim okruženjima; povećana prilagodljivost produžava operativni životni vek protokola; dok dugoročna održivost omogućava kontinuirano očuvanje visokog nivoa bezbednosti uprkos razvoju novih tehnoloških i kriptografskih izazova. Time IKEv2 potvrđuje da savremeni bezbednosni protokol mora biti projektovan ne samo za rešavanje aktuelnih bezbednosnih problema, već i za uspešno prilagođavanje budućim promenama u informaciono-komunikacionom okruženju [10].

Završna naučno-istraživačka sinteza podpoglavlja potvrđuje da napredne funkcionalnosti IKEv2 predstavljaju mnogo više od skupa dodatnih mogućnosti namenjenih unapređenju performansi ili povećanju kompatibilnosti različitih mrežnih uređaja. Njihov suštinski značaj ogleda se u sposobnosti protokola da objedini mobilnost, interoperabilnost, modularnost, proširivost i prilagodljivost u jedinstvenu evolutivnu bezbednosnu arhitekturu. Uzročno-posledično posmatrano, modularna projektantska struktura omogućava prihvatanje novih tehnologija; prihvatanje novih tehnologija povećava otpornost na buduće bezbednosne izazove; povećana otpornost produžava upotrebnu vrednost protokola; dok dugoročna održivost omogućava da IKEv2 ostane relevantan i bezbedan uprkos kontinuiranim promenama tehnološkog i bezbednosnog okruženja. Upravo zbog toga napredne funkcionalnosti IKEv2 predstavljaju jedan od najvažnijih razloga njegove široke primene u savremenim VPN sistemima i potvrđuju da je njegova arhitektura projektovana sa jasnom orijentacijom ka dugoročnoj evoluciji i održivosti [93; BSI TR-02102-3].

5.7. Bezbednosne ranjivosti ikev2

5.7.1. Teorijski model bezbednosnih ranjivosti ikev2 protokola

Analiza bezbednosnih karakteristika savremenih kriptografskih protokola ne može biti ograničena isključivo na razmatranje njihove projektantske arhitekture i izbora kriptografskih algoritama. Iako Internet Key Exchange Version 2 (IKEv2) predstavlja jedan od najsigurnijih standardizovanih protokola za uspostavljanje i upravljanje IPsec bezbednosnim asocijacijama, njegova stvarna bezbednost u praktičnim implementacijama zavisi od znatno šireg skupa tehničkih, organizacionih i operativnih činilaca. Zbog toga je neophodno razlikovati teorijsku bezbednost protokola od bezbednosti njegove implementacije u konkretnom informaciono-komunikacionom sistemu. Ovakvo razlikovanje predstavlja osnov za razumevanje prirode savremenih bezbednosnih ranjivosti i omogućava objektivnu procenu stvarnog nivoa zaštite VPN infrastrukture [51].

U naučnoj i stručnoj literaturi pojam bezbednosne ranjivosti označava slabost ili nedostatak u projektovanju, implementaciji, konfiguraciji ili upravljanju informacionim sistemom koji može biti iskorišćen radi narušavanja poverljivosti, integriteta, raspoloživosti ili autentičnosti podataka i komunikacionih procesa. Posmatrano u kontekstu IKEv2 protokola, ranjivost ne predstavlja nužno grešku u samoj specifikaciji standarda, već može nastati kao posledica nepravilne implementacije standardizovanih funkcionalnosti, neadekvatne konfiguracije bezbednosnih parametara, nepravilnog upravljanja kriptografskim ključevima ili kompromitacije okruženja u kojem se protokol izvršava. Time se potvrđuje da je bezbednost rezultat zajedničkog delovanja više međusobno povezanih komponenti, a ne isključivo kvaliteta jednog protokola ili algoritma [31].

Sa metodološkog aspekta, bezbednosne ranjivosti IKEv2 mogu se klasifikovati u četiri

osnovne kategorije. Prvu grupu čine projektantske ranjivosti, koje bi nastale ukoliko bi sam standard sadržao logičke ili kriptografske nedostatke koji omogućavaju sistematsko narušavanje njegovih bezbednosnih svojstava. Međutim, dosadašnja naučna istraživanja i višegodišnja praktična primena ukazuju da je osnovna arhitektura IKEv2 projektovana uz visok stepen kriptografske i bezbednosne konzistentnosti, zbog čega se najveći broj savremenih bezbednosnih incidenata ne može pripisati samom dizajnu protokola [10].

Drugu kategoriju predstavljaju implementacione ranjivosti, koje nastaju tokom razvoja softverskih ili hardverskih implementacija IKEv2 protokola. Greške u obradi ulaznih podataka, upravljanju memorijom, proveru granica bafera, validaciji poruka ili obradi izuzetaka mogu dovesti do ozbiljnih posledica, uključujući uskraćivanje usluge (Denial-of-Service), curenje osetljivih podataka ili čak izvršavanje proizvoljnog programskog koda. Upravo iz ove kategorije potiče najveći broj ranjivosti evidentiranih u bazama *Common Vulnerabilities and Exposures (CVE)*, što potvrđuje da kvalitet implementacije predstavlja jedan od ključnih činilaca ukupne bezbednosti VPN sistema [87. FIPS 140-3].

Treću grupu čine konfiguracione ranjivosti, koje nastaju usled neadekvatnog izbora bezbednosnih parametara ili odstupanja od preporučenih bezbednosnih politika. Upotreba slabih ili zastarelih Diffie–Hellman grupa, nedovoljno složenih unapred podeljenih ključeva (PSK), zastarelih algoritama za šifrovanje ili neadekvatno definisanih politika upravljanja ključevima može značajno umanjiti bezbednost sistema uprkos pravilno implementovanom protokolu. Na taj način konfiguracija postaje jednako važan element bezbednosne arhitekture kao i sam kriptografski dizajn.

Četvrtu kategoriju predstavljaju operativne ranjivosti, koje proizlaze iz načina upravljanja i eksploatacije informaciono-komunikacionog sistema. Neredovno ažuriranje softvera, izostanak bezbednosnih zakrpa, neadekvatan nadzor nad radom VPN infrastrukture, kompromitacija krajnjih uređaja, nepravilno upravljanje privilegijama administratora ili nedovoljna zaštita pristupnih kredencijala mogu omogućiti napadaču kompromitaciju sistema bez potrebe za narušavanjem same kriptografske zaštite IKEv2 protokola. Ovakvi scenariji jasno potvrđuju da se bezbednost VPN sistema ne može posmatrati izolovano od ukupnog operativnog okruženja u kojem funkcioniše [2], [27].

Analiza međusobnih odnosa navedenih kategorija pokazuje da snažna kriptografija sama po sebi nije dovoljna da garantuje visok nivo bezbednosti. Čak i kada protokol koristi savremene algoritme za razmenu ključeva, šifrovanje i proveru integriteta, bezbednost može biti ozbiljno ugrožena ukoliko implementacija sadrži programske greške, konfiguracija odstupa od preporučenih bezbednosnih smernica ili operativni procesi ne obezbeđuju adekvatnu zaštitu sistema. Time se potvrđuje da kriptografska snaga predstavlja neophodan, ali ne i dovoljan uslov za očuvanje bezbednosti savremenih VPN infrastruktura. Sa metodološkog stanovišta može se formulisati jasan uzročno-posledični model bezbednosti IKEv2. Projektantska arhitektura određuje teorijski nivo otpornosti protokola; kvalitet implementacije određuje koliko će projektovana bezbednosna svojstva biti verno ostvarena u praksi; konfiguracija definiše nivo zaštite u konkretnom operativnom okruženju; dok način upravljanja sistemom određuje njegovu dugoročnu otpornost na promene bezbednosnog okruženja i nove tehnike napada. Slabost u bilo kojoj od ovih komponenti može narušiti ukupnu bezbednost sistema, bez obzira na kvalitet svih preostalih elemenata. Zbog toga se bezbednost IKEv2 mora posmatrati kao **svojstvo** koje proizlazi iz međusobnog delovanja projektantskih, implementacionih, konfiguracionih i operativnih komponenti bezbednosne arhitekture [38].

Završna naučno-istraživačka sinteza potvrđuje da analiza bezbednosnih ranjivosti IKEv2 zahteva višeslojni metodološki pristup koji prevazilazi tradicionalno razmatranje kriptografskih algoritama. Projektantska arhitektura predstavlja osnov bezbednosti, ali njena stvarna vrednost zavisi od kvaliteta implementacije, pravilne konfiguracije i odgovornog operativnog upravljanja sistemom. Uzročno-posledično posmatrano, bezbedna arhitektura omogućava pouzdanu implementaciju; kvalitetna implementacija omogućava pravilnu konfiguraciju; pravilna konfiguracija povećava operativnu otpornost; dok kontinuirano upravljanje ranjivostima omogućava očuvanje bezbednosti tokom čitavog životnog ciklusa VPN sistema. Upravo zbog toga bezbednost IKEv2 ne treba posmatrati kao statičko svojstvo protokola, već kao dinamički proces u kojem su kriptografija, implementacija, konfiguracija i operativno upravljanje podjednako važni činioci ukupne bezbednosti informaciono-komunikacionog sistema [51].

Tabela 9. Lawful Hacking tehnike kao vektor na IPsec/IKE

Kategorija	Opšti opis	Potencijalni uticaj na IPsec/IKE okruženje	Preporučene zaštitne mere
Kompromitacija krajnje tačke	Pristup podacima na ovlašćenom uređaju u skladu sa odgovarajućim pravnim ovlašćenjima.	Može omogućiti pristup podacima pre šifrovanja ili nakon dešifrovanja na krajnjoj tački.	Hardening sistema, EDR/XDR, upravljanje zakrpama, zaštita identiteta.
Forenzičko prikupljanje podataka	Prikupljanje digitalnih dokaza sa sistema u cilju forenzičke analize.	Omogućava rekonstrukciju događaja i analizu bez menjanja kriptografskih protokola.	Integritet logova, kontrola pristupa i bezbedno čuvanje dokaza.
Analiza mrežne telemetrije	Analiza metapodataka i bezbednosnih incidenata u mreži.	Pomaže u otkrivanju anomalija tokom uspostavljanja i korišćenja VPN komunikacije.	SIEM, NDR, korelacija događaja i kontinuirani monitoring.
Analiza memorije	Ispitivanje sadržaja radne memorije na ovlašćen način.	Može doprineti razumevanju stanja procesa i bezbednosnog incidenta.	Zaštita memorije, kontrola privilegija i forenzičke procedure.
Analiza sistemskih logova	Pregled evidencija operativnog sistema i VPN servisa.	Olakšava identifikaciju neuspelih autentifikacija, promena konfiguracije i drugih bezbednosnih događaja.	Centralizovano prikupljanje logova, revizija i zaštita integriteta.

Napomena: Tabela prikazuje kategorije aktivnosti koje se mogu koristiti u zakonito sprovedenim digitalnim istragama i njihov odnos prema IPsec/IKE okruženju. Naglasak je na razumevanju bezbednosnog konteksta, zaštitnim merama i očuvanju integriteta sistema.

Izvor: Autor, na osnovu sinteze opšteprihvaćenih standarda digitalne forenzike (NIST SP 800-86 – Guide to Integrating Forensic Techniques into Incident Response) i uporednopravne analize okvira za zakonito sprovedene digitalne istrage.

Tabela 9 sistematizuje pet kategorija aktivnosti koje se, u okviru zakonom propisanih ovlašćenja i sudskih odluka, mogu primeniti u digitalnim istragama koje uključuju IPsec/IKE zaštićenu komunikaciju, od kompromitacije krajnje tačke i forenzičkog prikupljanja podataka, preko analize mrežne telemetrije i memorije, do analize sistemskih logova. Zajednička karakteristika svih navedenih kategorija jeste da nijedna ne podrazumeva kriptanalitičko narušavanje IKE/IPsec algoritama, već se zasniva na pristupu podacima na uređaju (po odluci suda), pre šifrovanja ili nakon dešifrovanja, odnosno na analizi metapodataka i evidencija koje prate proces uspostavljanja i održavanja kriptografski zaštićene komunikacije. Ova distinkcija je od suštinskog metodološkog značaja, budući da razgraničava zakonito sprovedene istražne aktivnosti od kriptanalitičkih napada koji predstavljaju predmet analize u prethodnim poglavljima ove teze.

Sa aspekta bezbednosne arhitekture, tabela ukazuje da svaka kategorija zahteva specifičan skup zaštitnih mera koje istovremeno služe dvostrukoj svrsi — sprečavanju zloupotrebe od strane neovlašćenih aktera i očuvanju integriteta prikupljenih podataka u slučaju zakonito sprovedene istrage. Mere poput integriteta logova, bezbednog čuvanja dokaza i kontrole pristupa, navedene u koloni preporučenih zaštitnih mera, ukazuju da isti tehnički mehanizmi (SIEM, NDR, forenzičke procedure) služe i kao odbrambena kontrola protiv neovlašćene kompromitacije i kao garancija verodostojnosti podataka prikupljenih u ovlašćenom kontekstu. Ova dvostruka funkcija potvrđuje da granica između legitimne digitalne forenzike i neovlašćenog napada nije određena primenjenom tehnikom kao takvom, već isključivo pravnim okvirom, ovlašćenjima i procedurama pod kojima se ta tehnika sprovodi.

5.7.2. Implementacione ranjivosti, cve analiza i bezbednosni izazovi praktičnih implementacija ikev2

Iako je projektantska arhitektura Internet Key Exchange Version 2 (IKEv2) protokola zasnovana na savremenim kriptografskim principima i predstavlja značajno unapređenje u odnosu na prethodne generacije protokola za razmenu ključeva, iskustva iz praktične primene pokazuju da najveći broj ozbiljnih bezbednosnih incidenata nije posledica nedostataka u samoj specifikaciji standarda, već grešaka nastalih tokom implementacije. Ovakva zapažanja potvrđuju osnovnu tezu da teorijska bezbednost protokola ne garantuje automatski bezbednost konkretnih VPN sistema. Step en ostvarene bezbednosti informaciono-komunikacione infrastrukture zavisi od kvaliteta implementacije, pravilnog upravljanja memorijom, bezbedne obrade ulaznih podataka, odgovarajuće konfiguracije i blagovremenog otklanjanja identifikovanih ranjivosti.

Posebno značajan izvor saznanja o implementacionim slabostima predstavljaju javno dostupne baze **Common Vulnerabilities and Exposures (CVE)**, koje dokumentuju bezbednosne nedostatke otkrivene u implementacijama različitih proizvođača mrežne opreme i VPN softvera. Analiza ovih ranjivosti pokazuje da se najveći broj problema odnosi na nepravilnu obradu ulaznih poruka, greške u upravljanju memorijom, nedovoljnu validaciju protokolskih parametara i neadekvatnu obradu izuzetaka tokom procesa uspostavljanja ili održavanja Security Association mehanizama. Ovakve ranjivosti potvrđuju da bezbednost IKEv2 u praksi zavisi podjednako od kvaliteta programskog koda kao i od kvaliteta same kriptografske arhitekture.

Jedan od karakterističnih primera predstavljaju ranjivosti evidentirane u implementacijama mrežne opreme različitih proizvođača, uključujući i pojedine implementacije kompanije **Cisco Systems**, kod kojih su identifikovane greške koje su omogućavale uskraćivanje usluge (*Denial-of-Service*), narušavanje stabilnosti procesa ili druge oblike kompromitacije

dostupnosti VPN servisa. Ovakvi slučajevi ne ukazuju na slabost IKEv2 standarda kao takvog, već na činjenicu da složenost implementacije bezbednosnih protokola povećava verovatnoću pojave programskih grešaka koje mogu biti iskorišćene od strane napadača. Time se potvrđuje da bezbednost protokola predstavlja zajednički rezultat projektantskih i implementacionih odluka [42].

Posebnu grupu implementacionih ranjivosti čine greške u upravljanju memorijom, među kojima se izdvajaju buffer overflow, integer overflow i različiti oblici memory corruption. Buffer overflow nastaje kada implementacija dozvoli upis podataka izvan predviđenih granica memorijskog prostora, čime se mogu narušiti integritet procesa ili omogućiti izvršavanje proizvoljnog programskog koda. Integer overflow nastaje usled nepravilne obrade numeričkih vrednosti tokom računanja veličina memorijskih struktura ili protokolskih parametara, dok memory corruption predstavlja širu kategoriju grešaka koje dovode do narušavanja konzistentnosti memorijskog prostora procesa. Zajednička karakteristika ovih ranjivosti jeste činjenica da nastaju u implementacionom sloju, dok kriptografski algoritmi i projektantska logika protokola ostaju nepromenjeni [49].

Pored grešaka u upravljanju memorijom, značajan bezbednosni izazov predstavljaju i problemi povezani sa nepravilnim upravljanjem **nonce** vrednostima i autentifikovanim režimima šifrovanja, posebno prilikom korišćenja algoritma AES-GCM. Bezbednost ovog režima rada zasniva se na pretpostavci da se ista kombinacija ključa i nonce vrednosti neće ponoviti. Ukoliko usled implementacione greške ili nepravilnog upravljanja kriptografskim materijalom dođe do ponovne upotrebe (**nonce reuse**), mogu nastati ozbiljne posledice po poverljivost i integritet komunikacije. Ovakvi primeri jasno potvrđuju da ni primena savremenih autentifikovanih algoritama za šifrovanje ne može obezbediti visok nivo zaštite ukoliko implementacija ne poštuje njihove osnovne bezbednosne pretpostavke [61; RFC 4106.], [78; FIPS 197.], [81; SP 800-38D.].

Analiza bezbednosnih izazova obuhvata i mogućnost **downgrade** napada, čiji je cilj navođenje komunikacionih učesnika da koriste slabije ili zastarele kriptografske algoritme od onih koje bi inače podržavali. Savremene implementacije IKEv2 predviđaju mehanizme kojima se ovakav rizik značajno umanjuje kroz zaštitu procesa pregovaranja bezbednosnih parametara i proveru integriteta razmenjenih poruka. Međutim, neadekvatna konfiguracija ili podrška za zastarele algoritme može povećati izloženost ovakvim scenarijima, zbog čega pravilna konfiguracija ostaje važan element ukupne bezbednosti sistema [64; RFC 8221.].

Poseban bezbednosni rizik predstavlja kompromitacija unapred podeljenih ključeva (*Pre-Shared Key* – PSK). Iako PSK predstavlja efikasan model autentifikacije u manjim i kontrolisanim okruženjima, njegova bezbednost neposredno zavisi od kvaliteta generisanog ključa, načina njegove distribucije, čuvanja i periodične zamene. Slabi ili ponovo korišćeni PSK, kao i neadekvatne procedure upravljanja kredencijalima, mogu značajno povećati rizik od kompromitacije procesa autentifikacije. Ovakvi problemi ne proizlaze iz nedostataka IKEv2 arhitekture, već iz organizacionih i operativnih slabosti u upravljanju bezbednosnim politikama [31].

Sa metodološkog aspekta može se uočiti jasan uzročno-posledični obrazac koji povezuje implementaciju i bezbednost. Projektantska arhitektura definiše teorijske bezbednosne granice protokola; implementacija određuje da li će te granice biti dosledno ostvarene; konfiguracija određuje nivo zaštite u konkretnom okruženju; dok blagovremeno otkrivanje i otklanjanje ranjivosti kroz upravljanje bezbednosnim *update*-ima (*patch management*) određuje

dugoročnu otpornost sistema. Svaka greška u ovom lancu povećava verovatnoću uspešne eksploatacije bez obzira na kriptografsku snagu korišćenih algoritama.

5.7.3. Integrirani model upravljanja bezbednosnim komponentama ikev2: endpoint bezbednost, višeslojna zaštita i perspektive razvoja

Rezultati prethodne analize pokazuju da se bezbednost Internet Key Exchange Version 2 (IKEv2) protokola ne može procenjivati isključivo kroz prizmu njegove projektantske arhitekture ili kriptografske snage algoritama koje koristi. Savremeno bezbednosno okruženje karakterišu sofisticirani napadi koji u velikom broju slučajeva zaobilaze samu kriptografsku zaštitu i usmeravaju se na kompromitaciju komponenti koje okružuju protokol. Iz tog razloga analiza bezbednosnih ranjivosti mora obuhvatiti čitav bezbednosni ekosistem u kojem IKEv2 funkcioniše, uključujući krajnje uređaje, operativne sisteme, VPN gateway infrastrukturu, softverski lanac snabdevanja i procese upravljanja životnim ciklusom bezbednosnih komponenti [2].

Jedan od najznačajnijih savremenih izazova predstavlja kompromitacija krajnjih uređaja (*endpoint compromise*). Čak i kada su razmena ključeva, autentifikacija i zaštita komunikacije realizovani u skladu sa najvišim kriptografskim standardima, kompromitovan krajnji uređaj može omogućiti napadaču pristup podacima pre njihovog šifrovanja ili neposredno nakon dešifrovanja. Time se potvrđuje da kriptografija štiti komunikacioni kanal, ali ne može zaštititi podatke u trenutku njihove obrade na kompromitovanom uređaju. Ovakva činjenica predstavlja jednu od osnovnih granica svih savremenih kriptografskih protokola i potvrđuje potrebu za integriranjem zaštite komunikacije sa zaštitom krajnjih sistema [40],[48].

Posebno mesto u savremenim bezbednosnim analizama zauzimaju metode poznate kao lawful hacking, koje nadležni državni organi mogu primenjivati u skladu sa važećim zakonodavstvom i sudskim odlukama u okviru krivičnih istraga. Njihova osnovna karakteristika jeste da ne pokušavaju da kompromituju kriptografske algoritme IKEv2 ili IPsec protokola, već ciljaju operativni sistem, aplikacije ili druge komponente krajnjeg uređaja. Ukoliko se ostvari kontrola nad uređajem, moguće je pristupiti komunikacionim podacima pre procesa šifrovanja ili nakon njihove dešifrovanja, čime se kriptografska zaštita praktično zaobilazi bez potrebe za njenim kryptoanalitičkim narušavanjem. Ovakav pristup jasno potvrđuje da granica bezbednosti savremenih VPN sistema nije određena isključivo kvalitetom kriptografskih algoritama, već ukupnim nivoom zaštite informaciono-komunikacionog okruženja [2].

– Dodatni izazov savremenog digitalnog okruženja predstavlja *supply chain* rizik

Savremene VPN implementacije oslanjaju se na veliki broj softverskih biblioteka, razvojnih alata, operativnih sistema i hardverskih komponenti koje potiču od različitih proizvođača. Kompromitacija bilo koje od tih komponenti može ugroziti bezbednost sistema čak i kada je sama implementacija IKEv2 u potpunosti usklađena sa standardima. Zbog toga bezbednost više nije moguće posmatrati isključivo kroz analizu jednog protokola, već kao rezultat poverenja u čitav lanac razvoja, distribucije i održavanja softverskih i hardverskih komponenti. Upravljanje ovakvim rizicima zahteva kontinuiranu primenu **patch management** procesa i dosledno sprovođenje principa **secure configuration**. Pravovremena instalacija bezbednosnih *update*-a omogućava otklanjanje poznatih implementacionih ranjivosti pre njihove eksploatacije, dok pravilna konfiguracija uređaja obezbeđuje korišćenje preporučenih kriptografskih algoritama, odgovarajućih *Diffie-Hellman* grupa, bezbednih politika

upravljanja ključevima i odgovarajućih mehanizama autentifikacije. Time upravljanje konfiguracijom prerasta iz administrativne aktivnosti u jedan od ključnih bezbednosnih procesa koji neposredno utiče na otpornost VPN infrastrukture [31],[62; RFC 5903].

Analiza savremenih bezbednosnih modela pokazuje da se zaštita IKEv2 protokola mora zasnivati na principu višeslojne odbrane (*defense-in-depth*). Ovaj koncept podrazumeva istovremenu primenu više međusobno nezavisnih zaštitnih mehanizama na različitim nivoima sistema – od fizičke i mrežne zaštite, preko zaštite operativnog sistema, aplikacija i krajnjih uređaja, do kriptografskih protokola, sistema za detekciju napada i kontinuiranog bezbednosnog monitoringa. Prednost ovakvog pristupa ogleda se u činjenici da kompromitacija jednog zaštitnog sloja ne dovodi automatski do kompromitacije celokupnog informaciono-komunikacionog sistema [38].

Sa razvojem distribuiranih informacionih sistema sve veći značaj dobija i koncept Zero Trust bezbednosne arhitekture. Za razliku od tradicionalnog modela zasnovanog na pretpostavci da su korisnici i uređaji unutar mreže pouzdani, *Zero Trust* polazi od principa da nijedan korisnik, uređaj ili komunikaciona sesija ne treba unapred da bude smatrana pouzdanom. U kontekstu IKEv2 to podrazumeva kontinuiranu proveru identiteta, strogu kontrolu privilegija, segmentaciju mreže i stalno praćenje bezbednosnog stanja uređaja koji učestvuju u VPN komunikaciji. Time se dodatno umanjuju posledice eventualne kompromitacije pojedinačnih komponenti sistema [51].

Posmatrano dugoročno, jedan od najznačajnijih strateških izazova predstavlja razvoj postkvantne kriptografije. Iako savremeni IKEv2 protokol pruža visok nivo zaštite u odnosu na trenutno poznate kriptoanalitičke metode, očekivani razvoj kvantnog računarstva zahteva postepenu integraciju novih algoritama otpornih na kvantne napade. Modularna arhitektura IKEv2 omogućava relativno jednostavno uvođenje novih mehanizama razmene ključeva i hibridnih kriptografskih modela, čime se stvaraju pretpostavke za očuvanje dugoročne bezbednosti protokola i nakon pojave praktično primenljivih kvantnih računara [2].

Sa metodološkog aspekta, sprovedena analiza omogućava formulisanje integrisanog modela upravljanja bezbednosnim ranjivostima IKEv2. Projektantska arhitektura određuje teorijsku otpornost protokola; kvalitet implementacije određuje njegovu praktičnu bezbednost; pravilna konfiguracija obezbeđuje odgovarajući nivo zaštite u operativnom okruženju; bezbednost krajnjih uređaja i VPN gateway infrastrukture sprečava zaobilaženje kriptografske zaštite; upravljanje zakrpama i supply chain rizicima održava bezbednost tokom životnog ciklusa sistema; dok višeslojna zaštita i *Zero Trust* koncept omogućavaju adaptivnu otpornost na savremene i buduće oblike napada. Ovakav model pokazuje da nijedna pojedinačna mera nije dovoljna sama za sebe, već da bezbednost nastaje kao rezultat njihove međusobne koordinacije [51].

5.8. Komparativna analiza bezbednosne arhitekture, upravljanja ključevima i operativnih karakteristika ikev1 i ikev2

Komparativna analiza Internet Key Exchange Version 1 (IKEv1) i Internet Key Exchange Version 2 (IKEv2) protokola pokazuje da razlike između ove dve generacije ne predstavljaju samo evoluciju pojedinačnih funkcionalnosti, već odražavaju promenu projektantske filozofije razvoja bezbednosnih protokola. Dok je IKEv1 razvijan u periodu kada su osnovni izazovi bili uspostavljanje bezbedne razmene ključeva i zaštita komunikacionog kanala između relativno statičnih mrežnih čvorova, IKEv2 je projektovan imajući u vidu zahteve savremenih informaciono-komunikacionih sistema koje karakterišu mobilnost korisnika,

distribuirane arhitekture, heterogene mrežne infrastrukture i potreba za dugoročnom održivošću bezbednosnih mehanizama. Posmatrano sa metodološkog aspekta, razvoj IKEv2 predstavlja odgovor na praktična iskustva stečena višegodišnjom primenom IKEv1 i težnju ka stvaranju jednostavnijeg, pouzdanijeg i otpornijeg bezbednosnog protokola [2].

Jedna od najuočljivijih razlika između dva protokola odnosi se na bezbednosnu arhitekturu. IKEv1 koristi složeniji model zasnovan na fazama i različitim režimima rada, što povećava broj mogućih scenarija uspostavljanja komunikacije i zahteva veću pažnju prilikom implementacije i konfiguracije. Veći broj opcija pruža određenu fleksibilnost, ali istovremeno povećava rizik od nekonzistentnih implementacija i konfiguracionih odstupanja. IKEv2 napušta ovakav pristup i uvodi jedinstven, jasno definisan tok razmene poruka koji smanjuje kompleksnost bez narušavanja funkcionalnosti. Time se postiže bolja preglednost protokola, jednostavnija implementacija i manja verovatnoća nastanka bezbednosnih grešaka.

Komparativna analiza upravljanja *Security Association* mehanizmima dodatno potvrđuje ovu projektantsku evoluciju. U IKEv1 uspostavljanje i održavanje bezbednosnih asocijacija zahteva veći broj odvojenih procedura i signalizacionih razmena. Nasuprot tome, IKEv2 uvodi koncept CHILD_SA, kojim se upravljanje životnim ciklusom bezbednosnih asocijacija integriše u jedinstven model. Time se pojednostavljuje proces obnove sesijskih ključeva, povećava efikasnost komunikacije i smanjuje operativno opterećenje mrežne infrastrukture. Posebna prednost ovakvog pristupa ogleda se u mogućnosti periodičnog **rekeying** procesa bez prekidanja aktivne VPN sesije, čime se istovremeno unapređuju bezbednost i raspoloživost sistema [77; SP 800-77 Rev. 1.].

Značajna razlika između dva protokola postoji i u oblasti upravljanja kriptografskim ključevima. IKEv2 sistematski unapređuje mehanizme generisanja, distribucije i obnove sesijskih ključeva kroz preciznije definisan proces derivacije KEYMAT materijala i jednostavniju primenu principa *Perfect Forward Secrecy* (PFS). Posledica ovakvog pristupa jeste smanjenje rizika da kompromitacija jednog sesijskog ključa ugrozi prethodno ostvarene komunikacije. U poređenju sa IKEv1, gde je upravljanje ključevima bilo funkcionalno, ali složenije za administraciju i implementaciju, IKEv2 postiže viši nivo bezbednosti uz istovremeno smanjenje operativne kompleksnosti [2].

Komparativna analiza bezbednosnih mehanizama pokazuje da IKEv2 uvodi unapređenja koja prevazilaze pojedinačne algoritamske izmene. Podrška za efikasnije algoritme autentifikacije i šifrovanja, unapređena zaštita od **replay** napada, integrisaniji mehanizmi očuvanja integriteta komunikacije i bolja otpornost na određene vrste aktivnih mrežnih napada doprinose formiranju robusnije bezbednosne arhitekture. Međutim, najznačajnije unapređenje ne ogleda se u izboru pojedinačnih algoritama, već u njihovoj međusobnoj koordinaciji i jasnije definisanim procedurama upravljanja bezbednosnim sesijama [38],[51].

Pored bezbednosnih karakteristika, IKEv2 ostvaruje značajna unapređenja u oblasti operativne efikasnosti. Podrška za MOBIKE omogućava očuvanje aktivne VPN komunikacije tokom promene IP adrese ili pristupne mreže, čime se postiže visok nivo mobilnosti korisnika bez potrebe za ponovnim uspostavljanjem kompletne bezbednosne sesije. U vreme razvoja IKEv1 ovakav zahtev nije imao isti značaj, dok savremena mobilna i cloud okruženja čine ovu funkcionalnost jednom od ključnih prednosti IKEv2. Time se jasno pokazuje da je novi protokol projektovan u skladu sa promenjenim zahtevima informaciono-komunikacionih sistema [68;RFC 4555], [76; RFC 6071.].

Sa aspekta interoperabilnosti, IKEv2 takođe ostvaruje značajan napredak. Jednostavnija projektantska arhitektura, standardizovaniji tokovi komunikacije i modularna organizacija funkcionalnosti omogućavaju lakšu interoperabilnost između implementacija različitih proizvođača. Time se smanjuje verovatnoća problema tokom uspostavljanja VPN sesija u heterogenim mrežnim okruženjima, što predstavlja važan faktor za velike organizacije koje koriste opremu i softver različitih proizvođača.

Analiza skalabilnosti pokazuje da IKEv2 efikasnije odgovara zahtevima savremenih informaciono-komunikacionih sistema sa velikim brojem korisnika i velikim brojem istovremenih VPN sesija. Pojednostavljene procedure upravljanja *Security Association* mehanizmima, efikasnije upravljanje životnim ciklusom ključeva i smanjenje signalizacionog opterećenja omogućavaju bolje iskorišćenje mrežnih i procesorskih resursa. Time se povećava mogućnost primene IKEv2 u velikim distribuiranim sistemima, cloud okruženjima i infrastrukturna kritičnih informacionih servisa [2].

Sa metodološkog aspekta može se uočiti jasna uzročno-posledična veza između projektantskih odluka i ostvarenih bezbednosnih svojstava. Pojednostavljena arhitektura IKEv2 smanjuje mogućnost implementacionih grešaka; unapređeno upravljanje ključevima povećava dugoročnu kriptografsku otpornost; efikasnije upravljanje *Security Association* mehanizmima povećava raspoloživost komunikacije; dok napredne funkcionalnosti mobilnosti i interoperabilnosti omogućavaju uspešnu primenu protokola u savremenim distribuiranim mrežnim okruženjima. Ovakav razvoj potvrđuje da evolucija IKEv2 nije bila usmerena isključivo ka povećanju kriptografske snage, već ka unapređenju ukupne bezbednosne i operativne arhitekture VPN sistema [51].

Sa aspekta otpornosti na savremene pretnje, IKEv2 ostvaruje značajna unapređenja zahvaljujući unapređenom modelu upravljanja ključevima, jednostavnijoj primeni principa ***Perfect Forward Secrecy***, efikasnijem procesu obnove bezbednosnih asocijacija i boljoj podršci za savremene kriptografske algoritme. Međutim, analiza bezbednosnih ranjivosti sprovedena u prethodnom podpoglavlju pokazala je da savremeni napadači sve češće usmeravaju aktivnosti ka kompromitaciji krajnjih uređaja, operativnih sistema, VPN gateway infrastrukture ili softverskog lanca snabdevanja, umesto ka direktnom narušavanju samog protokola. Time se potvrđuje da se bezbednosna paradigma pomera sa pitanja „koliko je snažan algoritam“ ka pitanju „koliko je na vektore napada otporan celokupan informaciono-komunikacioni sistem“.

Posebnu pažnju zaslužuje analiza dugoročne održivosti oba protokola. Projektantska modularnost IKEv2 omogućava lakšu integraciju novih algoritama za razmenu ključeva, autentifikaciju i zaštitu komunikacije. Ovakva karakteristika ima poseban značaj u kontekstu razvoja postkvantne kriptografije, jer omogućava postepenu integraciju novih kriptografskih mehanizama bez potrebe za potpunim redizajnom protokola. Nasuprot tome, arhitektura IKEv1 znatno je manje pogodna za ovakav evolutivni razvoj, što dodatno potvrđuje stratešku prednost IKEv2 u dugoročnoj perspektivi [76; RFC 6071].

Komparativna analiza takođe pokazuje da IKEv2 uspešno odgovara na zahteve savremenih mrežnih okruženja u kojima interoperabilnost, mobilnost, raspoloživost i automatizovano upravljanje bezbednosnim sesijama predstavljaju podjednako važne ciljeve kao i tradicionalna kriptografska zaštita. Integracija podrške za MOBIKE, unapređeno upravljanje CHILD_SA mehanizmima, efikasniji model pregovaranja bezbednosnih parametara i bolja podrška za

različite modele autentifikacije potvrđuju da je IKEv2 projektovan imajući u vidu celokupan životni ciklus bezbedne komunikacije, a ne samo proces inicijalne razmene ključeva [68; RFC 4555].

Međutim, objektivna naučna analiza zahteva i ukazivanje na činjenicu da IKEv2 nije univerzalno rešenje za sve bezbednosne izazove. Njegova uspešna primena i dalje zavisi od pravilnog izbora kriptografskih algoritama, bezbedne implementacije, redovnog ažuriranja softvera, pravilnog upravljanja ključevima, zaštite krajnjih uređaja i kontinuiranog bezbednosnog monitoringa. Stoga se može zaključiti da IKEv2 značajno unapređuje bezbednosnu arhitekturu u odnosu na IKEv1, ali ne menja osnovni princip da je bezbednost rezultat koordinisanog delovanja tehničkih, organizacionih i operativnih mera zaštite [91; NIST IR 8547.].

Sa metodološkog aspekta može se identifikovati jasan obrazac evolucije bezbednosnih protokola. Iskustva stečena primenom IKEv1 omogućila su identifikaciju arhitektonskih i operativnih ograničenja; identifikovana ograničenja usmerila su razvoj IKEv2; unapređena arhitektura povećala je bezbednost, interoperabilnost i operativnu efikasnost; dok iskustva stečena primenom IKEv2 danas predstavljaju osnov za razvoj budućih generacija protokola i integraciju postkvantnih kriptografskih rešenja. Ovakav razvoj potvrđuje da bezbednosni protokoli predstavljaju evolutivne sisteme koji se kontinuirano prilagođavaju promenama tehnološkog i bezbednosnog okruženja [31].

5.9. Kritička evaluacija ikev2 u savremenim vpn sistemima

Razvoj Internet Key Exchange Version 2 (IKEv2) protokola predstavlja jednu od najznačajnijih evolutivnih etapa u oblasti bezbedne razmene kriptografskih ključeva i upravljanja IPsec VPN komunikacijom. Rezultati prethodnih analiza pokazali su da IKEv2 uvodi značajna unapređenja u odnosu na svog prethodnika kroz pojednostavljenu arhitekturu, unapređeno upravljanje bezbednosnim asocijacijama, efikasniji model upravljanja kriptografskim ključevima, veću interoperabilnost i bolju prilagođenost savremenim mrežnim okruženjima. Međutim, objektivna naučno-istraživačka evaluacija zahteva da se, pored njegovih nespornih prednosti, razmotre i ograničenja, izazovi implementacije i perspektive budućeg razvoja. Tek takav uravnotežen pristup omogućava formulisanje stručne ocene stvarnog mesta IKEv2 u savremenim bezbednosnim arhitekturama [2],[10].

Jedna od najvećih vrednosti IKEv2 ogleda se u činjenici da njegova projektantska arhitektura uspešno povezuje bezbednost, operativnu efikasnost i dugoročnu održivost. Za razliku od brojnih bezbednosnih protokola koji su tokom vremena postajali sve složeniji, IKEv2 je pojednostavio tokove komunikacije, smanjio broj procedura neophodnih za uspostavljanje i održavanje bezbednosnih sesija i istovremeno unapredio njihovu kriptografsku otpornost. Takav pristup potvrđuje da povećanje bezbednosti ne mora biti praćeno povećanjem projektantske kompleksnosti, već da pažljivo osmišljena arhitektura može istovremeno unaprediti i bezbednost i operativnu pouzdanost sistema.

Posebnu vrednost predstavlja način na koji IKEv2 integriše različite bezbednosne mehanizme u jedinstvenu arhitekturu. Upravljanje **IKE_SA** i **CHILD_SA** mehanizmima, podrška za periodičnu obnovu ključeva, primena principa **Perfect Forward Secrecy (PFS)**, zaštita od replay napada, podrška za mobilnost putem **MOBIKE** funkcionalnosti i modularna organizacija protokola čine međusobno povezane elemente jedinstvenog sistema zaštite. Upravo ovakva integracija predstavlja jednu od najznačajnijih projektantskih prednosti IKEv2, jer omogućava da pojedinačni mehanizmi međusobno dopunjuju svoju zaštitnu

funkciju umesto da funkcionišu kao izolovane bezbednosne komponente [68; RFC 4555].

Međutim, rezultati sprovedene analize bezbednosnih ranjivosti jasno pokazuju da ni ovako unapređena arhitektura ne može garantovati apsolutnu bezbednost. Najveći broj savremenih bezbednosnih incidenata povezanih sa IKEv2 proizlazi iz implementacionih grešaka, konfiguracionih propusta ili kompromitacije okruženja u kojem se protokol izvršava. Time se potvrđuje da bezbednost savremenih VPN sistema nije određena isključivo kvalitetom protokola, već kvalitetom celokupnog procesa njegovog razvoja, implementacije, konfiguracije, održavanja i operativnog upravljanja. Ovakav zaključak predstavlja jednu od ključnih naučnih poruka ovog rada [78. FIPS 197.], [87. FIPS 140-3].

Poseban izazov predstavlja činjenica da se savremene pretnje sve manje usmeravaju na pokušaje direktnog narušavanja kriptografskih algoritama, a sve više na kompromitaciju krajnjih uređaja, operativnih sistema, VPN gateway infrastrukture, identiteta korisnika i softverskog lanca snabdevanja. Ovakva promena bezbednosne paradigme zahteva da se IKEv2 posmatra kao deo šire bezbednosne arhitekture, a ne kao samostalno rešenje koje može nezavisno obezbediti poverljivost i integritet komunikacije. U tom kontekstu, koncepti višeslojne zaštite (*defense-in-depth*), kontinuiranog upravljanja ranjivostima, bezbednog razvoja softvera i **Zero Trust** arhitekture postaju neophodni komplementarni elementi uspešne primene IKEv2 [2].

Kritička evaluacija pokazuje i da IKEv2 poseduje značajan potencijal za dugoročnu primenu zahvaljujući svojoj modularnoj arhitekturi. Mogućnost integracije novih kriptografskih algoritama, različitih metoda autentifikacije i budućih postkvantnih mehanizama razmene ključeva omogućava da protokol ostane relevantan i u uslovima ubrzanog tehnološkog razvoja. Upravo ova sposobnost evolucije predstavlja jednu od njegovih najvažnijih strateških prednosti u odnosu na brojne druge bezbednosne protokole čija je arhitektura znatno manje prilagodljiva [89. FIPS 204],[93; BSI TR-02102-3].

Sa metodološkog aspekta može se zaključiti da IKEv2 predstavlja primer uspešne evolucije bezbednosnog protokola zasnovane na kontinuiranom učenju iz prethodnih iskustava. Ograničenja uočena tokom višegodišnje primene IKEv1 predstavljala su osnov za razvoj jednostavnije i efikasnije arhitekture IKEv2. Kasnija iskustva stečena kroz implementaciju IKEv2 omogućila su identifikaciju novih implementacionih i operativnih izazova, koji danas predstavljaju osnov za razvoj postkvantnih i adaptivnih bezbednosnih rešenja. Time se potvrđuje da razvoj bezbednosnih protokola predstavlja kontinuirani proces učenja, prilagođavanja i unapređivanja, a ne niz izolovanih tehnoloških inovacija.

Kritička evaluacija IKEv2 potvrđuje da savremeni bezbednosni protokoli više ne mogu biti vrednovani isključivo prema snazi kriptografskih algoritama koje koriste. Njihova stvarna vrednost određena je sposobnošću da integrišu bezbednosnu arhitekturu, efikasno upravljanje ključevima, otpornost na implementacione i operativne ranjivosti, interoperabilnost, prilagodljivost novim tehnologijama i dugoročnu održivost. Uzročno-posledično posmatrano, kvalitet projektantske arhitekture omogućava visok teorijski nivo zaštite; kvalitet implementacije omogućava ostvarivanje projektovanih bezbednosnih svojstava; pravilna konfiguracija smanjuje operativni rizik; kontinuirano upravljanje ranjivostima održava otpornost sistema; dok sposobnost evolucije omogućava da protokol ostane bezbedan i relevantan uprkos promenama tehnološkog i bezbednosnog okruženja. Upravo zbog toga IKEv2 predstavlja ne samo uspešnu evoluciju IKEv1, već i referentni model za projektovanje budućih generacija protokola za bezbednu razmenu kriptografskih ključeva i zaštitu digitalnih

komunikacija [2].

5.10. Naučno-istraživačka sinteza i perspektive daljeg razvoja

Sprovedena analiza bezbednosnih mehanizama pokazala je da IKEv2 ostvaruje poverljivost, integritet, autentifikaciju i raspoloživost komunikacije primenom međusobno povezanih zaštitnih slojeva. Autentifikacija uspostavlja poverenje između komunikacionih učesnika; razmena ključeva omogućava generisanje zajedničkog kriptografskog materijala; mehanizmi šifrovanja štite sadržaj komunikacije; zaštita integriteta sprečava neovlašćenu izmenu poruka; dok mehanizmi zaštite od replay i DoS napada doprinose očuvanju pouzdanosti komunikacionog procesa. Na osnovu toga može se zaključiti da bezbednosna svojstva IKEv2 predstavljaju rezultat koordinisanog delovanja svih navedenih mehanizama, a ne posledicu primene jednog algoritma ili jedne procedure.

Dalja analiza pokazala je da bezbednost IKEv2 proizlazi iz međuzavisnog i koordiniranog delovanja više funkcionalnih mera zaštite informaciono-komunikacionih sistema koje zajedno čine integrisanu bezbednosnu arhitekturu. Uspostavljanje **IKE_SA** predstavlja osnov za uspostavljanje međusobnog poverenja između komunikacionih učesnika, dok **CHILD_SA** omogućava efikasno upravljanje zaštićenim komunikacionim kanalima tokom čitavog životnog ciklusa kriptografski zaštićene sesije. Upravljanje bezbednosnim asocijacijama nije ograničeno na inicijalnu razmenu ključeva, već obuhvata njihovu periodičnu obnovu, kontrolisanu zamenu i bezbedno uklanjanje a samim tim se ostvaruje visok nivo kontinuiteta zaštite komunikacije.

Analiza naprednih funkcionalnosti dodatno potvrđuje da je IKEv2 projektovan imajući u vidu zahteve savremenih informaciono-komunikacionih sistema. Integracija podrške za mobilnost putem **MOBIKE** mehanizma, unapređena interoperabilnost između implementacija različitih proizvođača i modularna organizacija protokola omogućavaju njegovu uspešnu primenu u distribuiranim mrežnim okruženjima, cloud infrastrukturna i sistemima sa velikim brojem mobilnih korisnika. Time je potvrđeno da projektantska vrednost IKEv2 nije ograničena na kriptografsku zaštitu komunikacije, već obuhvata i sposobnost prilagođavanja promenljivim operativnim uslovima.

Savremeni informaciono-komunikacioni sistemi nalaze se u periodu intenzivne tehnološke transformacije koju karakterišu razvoj distribuiranih cloud platformi, virtualizacija mrežnih funkcija, masovna primena mobilnih komunikacija, IoT, industrijskih komunikacionih sistema i sve veća automatizacija procesa upravljanja informacionom bezbednošću (*usled velike količine log podataka i neophodnosti višekriterijumske analize i korelacije iz više izvora podataka*). U takvom okruženju uloga protokola za razmenu kriptografskih ključeva značajno prevazilazi prvobitnu funkciju uspostavljanja bezbednog komunikacionog kanala. IKEv2 se sve više posmatra kao sastavni deo šire bezbednosne arhitekture čija je osnovna uloga uspostavljanje, održavanje i prilagođavanje bezbednosnog stanja komunikacionih sistema tokom čitavog njihovog životnog ciklusa.

Dalji razvoj informacionih sistema podrazumeva sve intenzivniju primenu **cloud-native arhitektura, softverski definisanih mreža (SDN) i virtualizacije mrežnih funkcija (NFV)**. Ove tehnologije omogućavaju visok stepen fleksibilnosti i automatizacije, ali istovremeno povećavaju složenost bezbednosnog okruženja.

U takvim uslovima protokoli poput IKEv2 moraju zadržati interoperabilnost i mogućnost efikasne integracije sa platformama za SDN i orkestriranje, sistemima za upravljanje mrežnim politikama i automatizovanim mehanizmima za raspodelu bezbednosnih resursa. Time se potvrđuje da budući razvoj nije usmeren samo ka unapređenju kriptografskih algoritama, već i

ka njihovom uspešnom uklapanju u kompleksne digitalne sisteme [31],[51].

Sa metodološkog aspekta i rezultati naučno-istraživačkog rada projektantska arhitektura određuje teorijske granice bezbednosti; kvalitet implementacije omogućava ostvarivanje projektovanih svojstava; pravilna konfiguracija obezbeđuje otpornost u konkretnom operativnom okruženju; upravljanje ključevima održava kontinuitet kriptografske zaštite; zaštita krajnjih uređaja i mrežne infrastrukture sprečava zaobilaženje bezbednosnih mehanizama; kontinuirano upravljanje ranjivostima omogućava očuvanje otpornosti tokom životnog ciklusa sistema; dok sposobnost prilagođavanja novim tehnologijama i pretnjama obezbeđuje dugoročnu održivost bezbednosne arhitekture.

Rezultati sprovedene naučno-istraživačke analize potvrđuju da *Internet Key Exchange Version 2* predstavlja kvalitativni iskorak u razvoju protokola za bezbednu razmenu kriptografskih ključeva i upravljanje IPsec VPN komunikacijama. Evolucija od IKEv1 ka IKEv2 nije bila usmerena samo na unapređenje pojedinačnih funkcionalnosti, već na izgradnju bezbednosne arhitekture koju karakteriše integrisanost, modularnost, adaptabilnost i kapacitet da odgovori zahtevima zaštite savremenih informaciono-komunikacionih sistema.

6. Savremeni bezbednosni izazovi ike protokola

6.1. Analiza bezbednosnih karakteristika i ranjivosti ike implementacija

Bezbednosna analiza kriptografskog protokola, koliko god teorijski rigorozna bila, ostaje nepotpuna ukoliko se ograniči isključivo na formalna svojstva same specifikacije. Protokol poput IKE (*Internet Key Exchange*), čija arhitektura i kriptografske osnove su detaljno analizirane u prethodnim delovima ovog magistarskog rada, u praktičnoj primeni postoje kao konkretan softverski artefakt implementiran u milionima linija programskog koda, ugrađen u mrežnu opremu različitih proizvođača, konfigurisan od strane administratora sa različitim nivoom stručnosti i iskustva, i izložen kontinuiranim vektorima napada od strane napadača sa različitim motivima (*modus operandi*) i resursima. Razumevanje ove kategorije ranjivosti zahteva metodološki pristup koji se razlikuje od formalne analize protokola – pristup zasnovan na sistematskom pregledu dokumentovanih bezbednosnih incidenata, njihovoj klasifikaciji prema uzročnim mehanizmima, i identifikaciji ponavljajućih obrazaca koji ukazuju na sistemske, a ne izolovane slabosti [2],[3],[11].

Cilj ovog magistarskog rada jeste upravo takva sistematska analiza. Rad polazi od pretpostavke da pojedinačni CVE (*Common Vulnerabilities and Exposures*) zapis, posmatran izolovano, pruža ograničen uvid u bezbednosno stanje IKE sistema u celini, dok sistematski analizirani vektori napada (primenom procesnog pristupa je dobijaju kvalitativno značajnije informacije) jer metodološki utemeljena analiza većeg broja takvih zapisa uz klasifikaciju CVE zapisa, poređenje i sintezu – omogućava identifikaciju dubljih, strukturnih obrazaca koji prevazilaze pojedinačne implementacione podatke koji mogu dovesti informaciono-komunikacioni sistem u nebezbedno stanje. Takav pristup ima i praktičnu vrednost izvan akademskog konteksta: administratori mreža, projektanti bezbednosnih sistema, i akteri zaduženi za procenu bezbednosnog rizika kritične infrastrukture mogu na osnovu ovako izvršene analize dobiti neophodne informacije značajne za procenu bezbednosti konkretnih IKE implementacija koje nisu nužno bile predmet javno dokumentovanog CVE zapisa, ali dele strukturne karakteristike sa implementacijama koje su detaljno analizirane u CVE bazi podataka [44].

Predmet ovog poglavlja obuhvata nekoliko međusobno povezanih, ali analitički razdvojivih tematskih celina. Prva celina posvećena je sistematskoj analizi poznatih CVE ranjivosti u kontekstu IPsec, IKEv1 i IKEv2 protokola, uključujući metodološki okvir za njihovu klasifikaciju, identifikaciju uzročno-posledičnih veza između implementacionih propusta i njihovih bezbednosnih posledica, i komparativnu sintezu koja omogućava dobijanje generalizovanih zaključaka o obrascima nastanka bezbednosnih propusta. Druga celina usmerena je na jedan specifičan, ali kritično značajan element bezbednosne konfiguracije IKE sistema – izbor Diffie-Hellman grupa – sa analizom istorijskog razvoja, matematičkih osnova, i, što je od posebnog praktičnog značaja, kriterijuma na osnovu kojih se u savremenim implementacijama vrši (ili treba da se vrši) izbor konkretne grupe. Treća celina obuhvata tri tematski različita, ali bezbednosno srodna pitanja savremene primene IKE protokola: problem ponovne upotrebe nonce vrednosti u kontekstu AES-GCM šifarskog algoritma, rizike koji proizilaze iz implementacionih i konfiguracionih grešaka tokom validacije digitalnih sertifikata, i izazove koje razvoj kvantnih računara postavlja pred dugoročnu bezbednost IKE ekosistema, uključujući pregled post-quantum kriptografskih mehanizama koji su usvojeni ili se razmatraju za usvajanje u okviru protokola [31],[47],[50].

Metodološki, rad kombinuje nekoliko komplementarnih pristupa. Za analizu CVE ranjivosti koristi se metod sistematski sprovedene analize javno dostupnih baza podataka o ranjivostima (pre svega NVD – *National Vulnerability Database*, i pratećih izvora poput bezbednosnih savetovanja proizvođača opreme), praćen kvalitativnom klasifikacijom prema uzročnom mehanizmu (*na primer, greška u upravljanju memorijom, greška u kriptografskoj implementaciji, greška u logici validacije*), i kvantitativnom analizom distribucije ranjivosti prema kategorijama i vremenskom periodu nastanka. Za analizu *Diffie-Hellman* grupa i post-kvantne kriptografije koristi se komparativni metod, zasnovan na sistematizaciji tehničkih i bezbednosnih karakteristika kroz strukturirane tabele koje omogućavaju direktno poređenje alternativnih rešenja prema više relevantnih kriterijuma istovremeno – pristup koji, za razliku od čisto deskriptivnog izlaganja, ima veći metodološki i praktični doprinos, budući da čitaocu pruža instrument za donošenje informisane odluke, a ne samo skup izolovanih činjenica [2],[31].

Vredno je već na ovom mestu naglasiti distinkciju koja će biti dosledno primenjivana kroz čitav rad: distinkciju između ranjivosti protokola (slabosti u samoj kriptografskoj ili arhitekturnoj specifikaciji IKE/IKEv2, kakve su, na primer, bile predmet analize IKEv1 *Aggressive Mode*-a u ranijim delovima ovog istraživanja) i ranjivosti implementacije (slabosti/ranjivosti nastalih u konkretnom softverskom ili konfiguracionom aspektu IKE protokola). Ova distinkcija nije isključivo akademska: ima direktne praktične implikacije po strategiju otklanjanja ranjivosti tj. ranjivost protokola zahteva izmenu same specifikacije (proces koji uključuje IETF standardizacioni proces i, po pravilu, traje godinama), dok ranjivost implementacije, u principu, može biti otklonjena znatno brže, kroz bezbednosni *update* konkretnog softvera, bez potrebe za izmenom protokola kao takvog. Međutim, kako će pokazati analiza sprovedena u narednim odeljcima ovog rada, granica između ove dve kategorije u praksi nije uvek oštra – pojedine implementacione ranjivosti proizilaze iz nejasnoća ili opcionalnosti u samoj specifikaciji protokola, koje različiti proizvođači tumače i implementiraju na različite, ponekad bezbednosno neujednačene načine, čime implementaciona ranjivost postaje posredna posledica nedovoljno precizne specifikacije protokola [2].

Značaj ove teme dodatno je pojačan činjenicom da se IKE/IPsec infrastruktura koristi za zaštitu komunikacija širokog spektra aktera – od komercijalnih organizacija koje štite poslovne podatke, preko državnih institucija koje štite komunikacije od nacionalnog značaja, do kritične infrastrukture čija kompromitacija može imati posledice koje znatno prevazilaze gubitak tajnosti podataka. U tom kontekstu, sistematsko razumevanje obrazaca nastanka bezbednosnih propusta u IKE implementacijama predstavlja i predmet od direktnog značaja za oblast nacionalne bezbednosti i rad bezbednosnih agencija i obaveštajnih službi, budući da isti obrasci implementacionih slabosti koji omogućavaju eksploataciju od strane kriminalnih aktera mogu biti, i prema javno dostupnim analizama često i jesu, predmet ciljanog iskorišćavanja od strane državno sponzorisanih aktera u kontekstu kompjuterske špijunaže i ofanzivnih sajber operacija [24],[44].

Preostali deo rada organizovan je prateći redosled tematskih celina najavljen u ovom uvodu. Naredni odeljak uvodi sistematski pregled poznatih CVE ranjivosti u kontekstu IPsec, IKEv1 i IKEv2 protokola.

6.2. Analiza poznatih cve ranjivosti u kontekstu ipsec, ikev1 i ikev2

Sistematski pregled javno dokumentovanih CVE zapisa vezanih za IPsec, IKEv1 i IKEv2 implementacije, sproveden za potrebe ovog rada, obuhvata period od kasnih 1990-ih godina do sredine 2026. godine, i uključuje zapise koji se odnose na tri kategorije softvera: otvorene implementacije (*strongSwan*, njegov prethodnik *FreeS/WAN* i srodni *Openswan/Libreswan projekti*), komercijalnu mrežnu opremu (pre svega Cisco ASA i srodne platforme), i operativne sisteme sa ugrađenom IKE/IPsec podrškom (*Windows Server* i *klijentske verzije operativnog sistema*). Ova tri izvora nisu odabrana proizvoljno – ona predstavljaju tri strukturno različita konteksta implementacije istog protokola, sa različitim modelima razvoja (*zajednica otvorenog koda naspram zatvorenog komercijalnog razvoja*), različitim ciklusima bezbednosnih *update-a*, i, kako će analiza pokazati, delimično različitim specifičnostima ranjivosti.

U kategoriji otvorenih implementacija, *strongSwan* projekat, kao najrasprostranjenija otvorena IKEv2 implementacija i direktan naslednik ranijih *FreeS/WAN* i *Openswan* projekata, poseduje najopsežniju javno dokumentovanu istoriju CVE zapisa, delom usled transparentnosti sopstvenog procesa objavljivanja bezbednosnih saopštenja, a delom usled širine funkcionalnog obima (*podrška za brojne autentifikacione metode, EAP varijante, kriptografske pluginove*) koja uvodi veći broj potencijalnih ranjivosti. Analiza dokumentovanih *strongSwan* CVE zapisa ukazuje na nekoliko ponavljajućih kategorija: (1) greške u validaciji dolaznih poruka koje dovode do *NULL pointer dereference* ili sličnih uslova prekida rada (CVE-2014-2338 – DoS putem IKEv1 fragmentacionog paketa; CVE-2016-10396 – DoS putem *ID_DER_ASN1_DN* identifikatora sa nedovoljnom proverom dužine); (2) greške u implementaciji kriptografskih primitiva unutar pojedinačnih plugin-ova (CVE-2018-16151 i CVE-2018-16152 – RSA implementacija u *gmp plugin-u* ne odbacuje višak podataka tokom PKCS#1 v1.5 verifikacije potpisa, što omogućava falsifikovanje potpisa pri korišćenju digitalnih sertifikata koji ne zadovoljavaju bezbednosne standarde); i (3) logičke greške u autentifikacionom toku koje omogućavaju zaobilazanje autentifikacije (CVE-2015-8023 – nedovoljna verifikacija lokalnog stanja u *EAP-MSCHAPv2* implementaciji omogućava klijentu da dovede server kompromitovano stanje bezbednosti tako što napadač prouzrokuje pogrešno zaključivanje uspešne autentifikacije; CVE-2021-45079 – IKEv2 klijent koji izostavi AUTH payload u početnom zahtevu može, u određenim EAP konfiguracijama, dovesti server u stanje koje ugrožava redosled koraka u procesu autentifikacije).

Posebno je indikativan slučaj CVE-2025-62291, dokumentovan u *strongSwan* bezbednosnom saopštenju iz oktobra 2025. godine, koji ilustruje kako i dalje, gotovo dve decenije nakon standardizacije IKEv2 protokola, implementacije ostaju izložene klasičnoj kategoriji grešaka u proveru dužine podataka: *eap-mschapv2* plugin, prilikom obrade poruke o neuspehu autentifikacije, proverava dužinu čitavog paketa umesto dužine samo njegovog sadržaja (payload-a), što u određenim graničnim slučajevima dužine paketa (između 6 i 8 bajtova) dovodi do toga da rezultat oduzimanja dužine zaglavlja postane negativan, sa posledničnim rizikom prekoračenja bafera. Ovaj primer, iako ograničenog dometa (*zahteva zlonamerni server ili posrednika sa pristupom RADIUS lozinci*), zasluhuje pažnju kao ilustracija da implementacione greške vezane za rukovanje dužinom podataka kategorija koja je, kako će biti pokazano u narednom odeljku ovog rada, dominantan uzročni mehanizam kroz čitavu istoriju IKE implementacija – nastavljaju da se javljaju i u zreloj, dugogodišnjoj i intenzivno testiranoj kodnoj bazi kakva je *strong Swan* [2],[31],[51].

U kategoriji komercijalne mrežne opreme, reprezentativan primer predstavlja CVE-2018-0101, objavljen januara 2018. godine, odnosi se na Cisco ASA (*Adaptive Security Appliance*) i *Firepower Threat Defense* platforme. Od izuzetne važnosti je precizno navesti prirodu ove ranjivosti: osnovni uzrok jeste greška tipa „double free“ (dvostruko oslobađanje istog regiona memorije) u XML parseru koji Cisco ASA koristi u okviru *webvpn* (SSL VPN) funkcionalnosti. Iako osnovni uzrok nije direktno vezan za IKE protokol, Cisco je u naknadnoj analizi utvrdio da uređaji kod kojih je funkcionalnost IKEv2 Remote Access VPN aktivirana (*konkretno, kombinacija komandi crypto ikev2 enable i anyconnect enable*) takođe postaju izloženi ranjivosti, usled deljenog koda između SSL VPN i IKEv2 funkcionalnosti na istoj platformi. Ovaj slučaj predstavlja važnu metodološku pouku za CVE analizu IKE sistema: bezbednosna izloženost IKE funkcionalnosti konkretnog uređaja ne zavisi isključivo od ranjivosti u kodu koji direktno implementira IKE protokol, već i od ranjivosti u susednim, funkcionalno povezanim komponentama istog uređaja koje dele infrastrukturne resurse (*u ovom slučaju, mehanizme za obradu XML/autentifikacionih podataka*) [2],[31],[51].

U kategoriji operativnih sistema, dva Windows CVE zapisa zaslužuju posebnu pažnju kao ilustracija dugoročne perzistentnosti kategorije implementacionih ranjivosti u memorijskom upravljanju. CVE-2022-34721, objavljen 2022. godine, predstavlja ranjivost u Windows IKE Extension (IKEEXT) servisu, uzrokovanu greškom u proveru dužine dolaznih podataka prilikom obrade IKEv1 poruka, koja dovodi do vektora napada koji cilja memorijske kapacitete informaciono-komunikacionog sistema. Značajno je da je ova ranjivost formalno ograničena na IKEv1 obradu, ali, budući da svi Windows serveri po podrazumevanoj konfiguraciji prihvataju i IKEv1 i IKEv2 pakete na istom mrežnom portu, praktična izloženost ranjivosti obuhvatala je i sisteme kod kojih je IKEv2 bio jedini namerno konfigurisani protokol – još jedna potvrda metodološke pouke iz prethodnog pasusa, ovoga puta u kontekstu koegzistencije dva protokola unutar iste implementacije, a ne dve funkcionalno odvojene komponente [2],[43].

Znatno ozbiljniji i vremenski bliži primer predstavlja CVE-2026-33824, objavljen u okviru Microsoft-ovog aprilskog ciklusa bezbednosnih ažuriranja 2026. godine, sa CVSS 3.1 osnovnom ocenom 9,8 (kritično). Ranjivost je uzrokovana greškom tipa „double free“ u Windows IKE Extension biblioteci (*ikeext.dll*), do koje dolazi tokom procesa ponovnog sastavljanja fragmentisanih IKEv2 IKE_AUTH poruka – funkcionalnosti čiji je bezbednosni značaj već razmatran u ranijim delovima ovog istraživanja u kontekstu robusnosti protokola prema mrežnim uslovima koji zahtevaju fragmentaciju poruka. Prema javno dostupnoj tehničkoj analizi objavljenoj kroz *Zero Day Initiative*, greška nastaje okviru *Main Mode Security Association* strukture, pri čemu naredna obrada fragmentisane IKE_AUTH poruke kopira taj pokazivač na neadekvatan način i dovodi informaciono-komunikacioni sistem u nebezbedno stanje. Ranjivost ne zahteva autentifikaciju niti interakciju korisnika, dostupna je putem standardnih IKE mrežnih portova (UDP 500 i 4500), i targetira OS Windows (*u više verzija*), uključujući server verzije od Windows Server 2016 OS-a do Windows Server 2025 [47], [49].

Sa metodološke tačke gledišta, CVE-2026-33824 zaslužuje da bude istaknut kao poseban predmet dalje analize u ovom radu iz nekoliko razloga. Prvo, radi se o ranjivosti otkrivenoj u periodu neposredno pre završetka pisanja magistarskog rada, što je čini reprezentativnim primerom za naslov naučno-istraživačkog rada, bezbednosni izazovi IKE protokola u doslovnom smislu. Drugo, uzročni mehanizam tj. greška u upravljanju memorijom tokom

obrade fragmentacije IKE poruka – direktno je povezan sa specifičnom funkcionalnom komponentom protokola (*IKE fragmentacija, definisana u RFC 7383*) čiji je bezbednosni značaj razmatran u okviru prethodnih poglavlja magistarskog rada, čime se potvrđuje da funkcionalnosti uvedene radi poboljšanja robusnosti protokola prema nepovoljnim mrežnim uslovima (*IP fragmentacije IKE poruka*) same po sebi mogu postati izvor nove implementacione površine napada. Treće, visoka CVSS ocena (9,8) i odsustvo zahteva za autentifikacijom ili interakcijom korisnika čine ovaj slučaj instruktivnim za dalju kvalitativnu klasifikaciju prema kriterijumu ozbiljnosti posledica ove klase vektora napada. Iz navedenih razloga, ovaj rad neće detaljno reprodukovati specifične tehničke korake eksploatacije ove ranjivosti, budući da takav nivo detalja nadilazi svrhu akademske bezbednosne analize i mogao bi predstavljati neopravdan operativni rizik (u kontekstu ofanzivne bezbednosti); umesto toga, analiza se ograničava na uzročni mehanizam, klasu ranjivosti, i bezbednosne implikacije, u meri dovoljnoj za svrhu ovog istraživanja [2],[31].

6.3. Naučno-istraživačka klasifikacija cve ranjivosti ike implementacija i analiza uzročno-posledičnih veza

Preliminarni obrasci identifikovani u prethodnom odeljku zahtevaju formalizaciju kroz eksplicitan klasifikacioni okvir, kako bi se pojedinačni CVE zapisi mogli sistematski porediti, a ne samo deskriptivno nabrajati. Za potrebe ovog rada, predlaže se trodimenzionalni klasifikacioni model, koji ćemo u daljem tekstu označavati skraćenicom IKE-VCM (*IKE Vulnerability Classification Model*), zasnovan na tri međusobno nezavisne analitičke ose: (I) uzročni mehanizam ranjivosti, (II) funkcionalna komponenta protokola u kojoj se ranjivost manifestuje, i (III) neposredna bezbednosna posledica eksploatacije. Nezavisnost ovih triju osa je namerna dizajnerska odluka: isti uzročni mehanizam (*na primer, greška u proveru dužine podataka*) može se manifestovati u različitim funkcionalnim komponentama (*fragmentacija poruka, EAP autentifikacija, validacija sertifikata*) i proizvesti različite posledice (*DoS, RCE, zaoblazanje procesa autentifikacije*) [26],[42],[44].

Prva osa – uzročni mehanizam – obuhvata pet kategorija, izvedenih induktivno iz pregleda sprovedenog u prethodnom odeljku ovog rada, ali usklađenih i sa opštije prihvaćenim taksonomijama softverskih ranjivosti (poput CWE – *Common Weakness Enumeration* klasifikacije koju održava MITRE korporacija). Kategorija U1 obuhvata greške upravljanja memorijom (*buffer overflow, double-free, use-after-free, NULL pointer dereference*) – kategoriju kojoj pripadaju, prema analizi iz prethodnog odeljka, CVE-2026-33824, CVE-2018-0101, i više strongSwan zapisa vezanih za obradu ID *payload*-a. Kategorija U2 obuhvata greške validacije ulaznih podataka koje ne rezultuju direktno memorijskom korupcijom, već logičkim propustom u proveru dužine, formata ili granica dozvoljenih vrednosti – kojoj pripada, između ostalog, CVE-2025-62291. Kategorija U3 obuhvata greške u implementaciji kriptografskih primitiva – nepravilnu primenu inače ispravno specificiranog kriptografskog algoritma – kojoj pripadaju CVE-2018-16151 i CVE-2018-16152. Kategorija U4 obuhvata logičke greške u protokolarnom toku odnosno automatu stanja (*state machine*) – propuste u redosledu ili uslovima prelaska između stanja protokola – kojoj pripadaju CVE-2015-8023 i CVE-2021-45079. Kategorija U5, konačno, obuhvata konfiguracione i podrazumevane vrednosti koje, iako ne predstavljaju grešku u kodu u strogom smislu, proizvode bezbednosno neadekvatno ponašanje sistema u podrazumevanoj instalaciji – kategorija koja će biti posebno relevantna u odeljku ovog rada posvećenom validaciji digitalnih sertifikata [2],[31].

Druga osa – funkcionalna komponenta – oslanja se direktno na arhitekturnu analizu IKEv2 protokola sprovedenu u ranijim delovima ovog istraživanja, i razlikuje sledeće komponente:

K1 – osnovna IKE_SA_INIT/IKE_AUTH razmena; K2 – mehanizam fragmentacije poruka (RFC 7383); K3 – EAP autentifikacioni sloj i njegove varijante (EAP-MSCHAPv2, EAP-TLS i srodne); K4 – validacija i obrada digitalnih sertifikata i asocirane kriptografske verifikacije potpisa; K5 – CREATE_CHILD_SA razmena i mehanizmi rekeying-a; i K6 – periferne, funkcionalno pomoćne komponente koje dele infrastrukturu sa IKE obradom, ali nisu direktno deo protokola u užem smislu (kao u slučaju CVE-2018-0101, gde je osnovni uzrok lociran u XML parseru webvpn funkcionalnosti, deljenom sa IKEv2 kodnom bazom na istoj platformi) [31].

Treća osa – bezbednosna posledica – razlikuje četiri kategorije: P1 – uskraćivanje usluge (DoS), obično posledica kategorije U1 ili U2 ranjivosti koje dovode do prekida rada IKE demona ili servisa; P2 – zaobilaženje autentifikacije odnosno impersonacija, po pravilu posledica U3 ili U4 kategorije ranjivosti; P3 – izvršavanje proizvoljnog koda (RCE), najozbiljnija posledica, po pravilu vezana za U1 kategoriju kada greška u upravljanju memorijom omogućava napadaču kontrolu nad tokom izvršavanja programa, a ne samo prekid rada; i P4 – neovlašćeno otkrivanje informacija, ređe zastupljena posledica u analiziranom uzorku, ali od značaja u kontekstu ranjivosti vezanih za kriptografsku implementaciju [38],[44],[46].

Primenom ovog trodimenzionalnog modela na CVE zapise razmotrene u prethodnom odeljku ovog rada, dobija se sledeća klasifikaciona mapa: CVE-2026-33824 klasifikuje se kao (U1, K2, P3) – greška upravljanja memorijom u komponenti fragmentacije, sa posledicom izvršavanja proizvoljnog koda; CVE-2018-0101 klasifikuje se kao (U1, K6, P3) – greška upravljanja memorijom u perifernoj komponenti, sa istom, najozbiljnijom posledicom; CVE-2022-34721 klasifikuje se kao (U2, K1, P1) – greška validacije dužine u osnovnoj IKE_SA_INIT/IKE_AUTH obradi (u kontekstu IKEv1), sa posledicom uskraćivanja usluge; CVE-2018-16151/16152 klasifikuju se kao (U3, K4, P2) – greška kriptografske implementacije u komponenti validacije sertifikata/potpisa, sa posledicom omogućavanja impersonacije; i CVE-2015-8023/CVE-2021-45079 klasifikuju se kao (U4, K3, P2) – logička greška u automatu stanja EAP komponente, sa istom posledicom zaobilaženja autentifikacije. Ova klasifikaciona mapa, iako zasnovana na ograničenom uzorku od šest reprezentativnih zapisa, već ukazuje na uočljivu pravilnost: kombinacija (U1, *, P3) – greška upravljanja memorijom koja rezultuje mogućnošću izvršavanja proizvoljnog koda, nezavisno od funkcionalne komponente u kojoj se javlja – predstavlja najozbiljniju i istovremeno najčešće dokumentovanu kombinaciju u analiziranom uzorku, dok se kombinacija (U4, K3, P2) – logička greška u EAP automatu stanja koja omogućava zaobilaženje autentifikacije – ponavlja kao specifičan obrazac vezan isključivo za komponentu autentifikacije, što je u skladu sa očekivanjem da funkcionalno kompleksnije komponente protokola (poput EAP integracije, koja uvodi sopstveni, ugnježdjeni automat stanja unutar šireg IKEv2 protokola) nose veći rizik od logičkih grešaka u odnosu na jednostavniji, uniformniji tok osnovne IKE_SA_INIT/IKE_AUTH razmene analiziran u ranijim delovima ovog istraživanja [2],[10],[51].

Pored same klasifikacije, od jednake je važnosti eksplicitna analiza uzročno-posledičnih veza – odnosno mehanizma kroz koji se latentna slabost u kodu transformiše u iskoristivu bezbednosnu ranjivost sa konkretnom operativnom posledicom. Za potrebe ovog magistarskog naučno-istraživačkog rada, predlaže se uzročno-posledični lanac (*specificiran u pet tačaka*), primenljiv na svaku analiziranu ranjivost nezavisno od njene klasifikacije prema IKE-VCN modelu: (1) izvor slabosti – nejasnoća, opcionalnost, ili nedovoljna preciznost u protokolarnoj specifikaciji, ili, alternativno, greška nastala u fazi implementacije bez oslonca

u nejasnoći same specifikacije; (2) implementaciona odluka – konkretan način na koji je programer preveo specifikaciju (*ili sopstvenu pretpostavku o njoj*) u izvorni kod, pri čemu ova odluka uvodi latentnu slabost koja u normalnim uslovima rada ostaje neispoljena; (3) specifični uslovi koji dovode do kompromitacije bezbednosti – specifična ulazna vrednost, sekvenca poruka, ili mrežno stanje koje aktivira latentnu slabost, po pravilu zahtevajući da napadač konstruiše neuobičajen, van granica normalne specifikacije smešten ulazni parametar (*primeri su : malformed payload, neuobičajena kombinacija dužine polja, neočekivan redosled poruka*); (4) neposredna manifestacija – tehnički efekat manifestacije slabosti/ranjivosti, kao što je *memory corruption vulnerability*, pogrešno izračunata kriptografska vrednost, ili pogrešna procena stanja automata; i (5) bezbednosna posledica – krajnji, operativno relevantan ishod (DoS, RCE, zaobilaženje procesa autentifikacije, otkrivanje informacija), koji određuje ozbiljnost ranjivosti sa stanovišta upravljanja rizikom [38],[44].

Primena ovog kauzalnog lanca na slučaj CVE-2026-33824 ilustruje njegovu analitičku vrednost: izvor slabosti (1) leži u kompleksnosti upravljanja vlasništvom nad *heap*-alociranim strukturama podataka kada se podaci iz jedne faze protokola (obrada Security Realm Vendor ID payload-a tokom IKE_SA_INIT razmene) prenose i koriste u kasnijoj fazi (obrada ponovno sastavljene IKE_AUTH poruke) – kompleksnost koja proističe iz činjenice da IKEv2 arhitektura, opisana u ranijim delovima ovog istraživanja, dozvoljava da se podaci iz ranije faze prenose u kontekst kasnije faze, što implementacija mora ispravno da odrazi u upravljanju životnim vekom odgovarajućih memorijskih struktura. Implementaciona odluka (2) sastojala se u načinu na koji je Windows IKE implementacija strukturirala vlasništvo nad pokazivačem na strukturu unutar šire *Main Mode Security Association* strukture. Uslov aktiviranja stanja nebezbednosti informaciono-komunikacionog sistema (3) predstavlja specifičnu sekvencu paketa – IKE_SA_INIT zahtev sa Microsoft Security Realm Vendor ID payload-om, praćen fragmentisanim IKE_AUTH zahtevom – koja dovodi do toga da se isti memorijski resurs oslobodi dva puta. Neposredna manifestacija (4) jeste memorijska ranjivost (*memory corruption vulnerability*) usled dvostrukog oslobađanja (*double-free*), a bezbednosna posledica (5), s obzirom na prirodu *memory corruption vulnerability* u kontekstu privilegovanog sistemskog servisa, jeste mogućnost izvršavanja proizvoljnog koda sa višim privilegijama u targetiranom informaciono-komunikacionom sistemu, bez potrebe za autentifikacijom ili interakcijom korisnika, što ovu ranjivost svrstava u najozbiljniju kategoriju posledica (P3) u okviru IKE-VCN modela[44],[47].

Slična primena kauzalnog lanca na slučaj CVE-2015-8023/CVE-2021-45079 (EAP logičke greške) pokazuje suštinski drugačiji obrazac: izvor slabosti (1) ovde nije memorijska kompleksnost, već protokolarna kompleksnost automata stanja – EAP razmena, kao opcionalna nadogradnja osnovne IKE_AUTH razmene, uvodi sopstvenu sekvencu poruka (*EAP-Request, EAP-Response, EAP-Success/Failure*) koja mora biti pravilno usklađena sa spoljašnjim IKE_AUTH tokom, i upravo ta dodatna slojevitost automata stanja predstavlja uslov za nastanak logičkih propusta. Implementaciona odluka (2) i ispunjen uslov kompromitacije bezbednosti IKT sistema (3) u ovim slučajevima svode se na nedovoljnu proveru da li je server (ili klijent) zaista prošao kroz sve očekivane korake EAP automata pre nego što prihvati konačan ishod autentifikacije – propust koji napadač aktivira jednostavnim slanjem poruke van očekivanog konteksta. Neposredna manifestacija (4) jeste pogrešno stanje autentifikacionog automata (*sistem veruje da je autentifikacija uspešno okončana iako suštinski kriptografski dokaz nije pružen*), a bezbednosna posledica (5) jeste zaobilaženje autentifikacije (P2) – kategorijalno različita, ali ne nužno manje ozbiljna posledica u odnosu na RCE, budući da direktno ugrožava osnovnu funkciju IKE protokola kao mehanizma za uzajamnu autentifikaciju strana u komunikaciji, analiziranu u ranijim delovima ovog

istraživanja.

Poređenje ova dva primera kauzalnog lanca ukazuje na širi metodološki zaključak od značaja za ostatak ovog rada: kompleksnost, bilo memorijska (*upravljanje životnim vekom struktura podataka kroz više faza protokola*) bilo protokolarna (*ugnježdeni automati stanja unutar šireg IKE toka*) – predstavlja zajednički imenitelj kroz obe kategorije uzročnog mehanizma, uprkos tome što se manifestuje kroz kvalitativno različite tehničke mehanizme i proizvodi kvalitativno različite bezbednosne posledice. Ovaj nalaz dobijen na osnovu naučno-istraživačke analize, koji će biti dalje razrađen kroz metodološki okvir predstavljen u narednom odeljku ovog rada, sugerise da funkcionalna proširenja IKE protokola koja uvode dodatnu kompleksnost, bilo na nivou memorijskog upravljanja bilo na nivou protokolarne logike, sistematski nose veći bezbednosni rizik od osnovnog, arhitekturno pojednostavljenog toka IKE_SA_INIT/IKE_AUTH razmene, čije je pojednostavljenje u odnosu na IKEv1 bilo predmet detaljne analize u ranijim delovima ovog magistarskog rada. Primena procesnog pristupa i detaljna (fokusirana) naučno-istraživačka analiza formiraju analitičku osnovu za metodološki okvir izbora reprezentativnih CVE ranjivosti koji je predmet ovog rada.

6.4. Metodološki okvir za izbor reprezentativnih cve ranjivosti i analiza obrazaca nastanka bezbednosnih propusta

Javne baze podataka o ranjivostima, poput NVD (*National Vulnerability Database*) koju održava NIST, sadrže, u trenutku pisanja ovog rada, više stotina zapisa direktno ili posredno vezanih za IPsec, IKEv1 i IKEv2 implementacije, akumuliranih tokom perioda dužeg od dve i po decenije. Metodološki je izuzetno važno i sa aspekta ovog magistarskog rada je neophodno eksplicitno definisati kriterijume prema kojima je iz tog šireg skupa izabran ograničen broj reprezentativnih zapisa razmotrenih u prethodnim odeljcima ovog rada – kriterijume koji obezbeđuju da odabrani uzorak, uprkos svojoj ograničenoj veličini, adekvatno reprezentuje širinu obrazaca nastanka ranjivosti prisutnih u širem skupu [2],[31].

Za potrebe ovog rada, primenjena su četiri eksplicitna kriterijuma selekcije, primenjena konjunktivno (zapis je uključen u analizu ukoliko zadovoljava dovoljan broj kriterijuma da bude reprezentativan za bar jednu kategoriju u okviru IKE-VCM modela predstavljenog u prethodnom odeljku ovog rada). Prvi kriterijum jeste kriterijum kategorijalne pokrivenosti – zahtev da odabrani uzorak, uzet u celini, pokriva sve kategorije prve analitičke ose IKE-VCM modela (U1 do U5), kako bi se izbegla sistemska pristrasnost analize ka jednoj, eventualno lakše dokumentovanoj kategoriji uzročnog mehanizma. Ovaj kriterijum je bio odlučujući, na primer, za uključivanje CVE-2018-16151/16152 (kategorija U3 – greška u kontekstu kriptografske implementacije), budući da je ova kategorija, za razliku od kategorija U1 i U2, u širem skupu CVE zapisa zastupljena u manjem broju, ali predstavlja analitički posebno značajnu kategoriju s obzirom na direktnu vezu sa kriptografskim mehanizmima analiziranim u ranijim delovima ovog istraživanja u okviru magistarskog rada [42].

Drugi kriterijum jeste kriterijum vremenske raspoređenosti – zahtev da odabrani uzorak obuhvata zapise raspoređene kroz čitav period primene protokola, a ne isključivo najnovije ili isključivo najstarije zapise. Ovaj kriterijum ima dvostruko obrazloženje: sa jedne strane, uključivanje starijih zapisa (poput CVE-2018-0101 iz 2018. godine ili CVE-2015-8023 iz 2015. godine) omogućava analizu perzistentnosti obrazaca ranjivosti kroz vreme, dok, sa druge strane, uključivanje najnovijih zapisa (poput CVE-2025-62291 iz 2025. godine i CVE-2026-33824 iz 2026. godine) obezbeđuje da rad, u skladu sa svojim naslovom, adekvatno

reprezentuje savremeno, a ne isključivo istorijsko stanje analize bezbednosnih karakteristika IKE protokola [34],[42].

Treći kriterijum jeste kriterijum raznovrsnosti implementacione osnove – zahtev da odabrani uzorak obuhvata zapise iz različitih kategorija softvera (*open source implementacije, komercijalna oprema, operativni sistemi*), budući da, kako je dokazano različite implementacione osnove mogu ispoljavati različite obrasce ranjivosti usled razlika u modelu razvoja, procesu bezbednosne revizije, i ciklusu objavljivanja *software security update*-a. Zanimarivanje ovog kriterijuma i oslanjanje isključivo na jednu implementacionu osnovu (na primer, isključivo na strongSwan, usled njegove transparentne i opsežne javne dokumentacije) rizikovalo bi da zaključci izvedeni iz analize budu artefakt specifičnosti te specifične implementacije, a ne generalizovan nalaz o IKE sistemu u celini i bezbednosnim karakteristikama [2],[51].

Četvrti kriterijum jeste kriterijum ozbiljnosti i dokumentovanosti posledica – zahtev da odabrani zapis poseduje dovoljno detaljnu javno dostupnu tehničku dokumentaciju (*bilo kroz zvanično bezbednosno saopštenje proizvođača, bilo kroz nezavisnu tehničku analizu objavljenu od strane priznatih bezbednosnih istraživačkih tela poput Zero Day Initiative ili akademskih izvora*) da omogući sprovođenje kauzalne analize opisane u prethodnom odeljku ovog rada. Zapisi sa nedovoljno detaljnom javnom dokumentacijom, uprkos tome što bi mogli biti relevantni za neku od kategorija IKE-VCM modela, isključeni su iz detaljne analize upravo usled nedovoljne mogućnosti verifikacije uzrocnog mehanizma – metodološka odluka koja daje prednost analitičkoj pouzdanosti nad brojčanom obimnošću uzorka. Primena ova četiri kriterijuma na širi skup dostupnih CVE zapisa rezultovala je uzorkom od šest reprezentativnih zapisa analiziranih u ovom radu, koji zajedno pokrivaju sve kategorije prve analitičke ose IKE-VCM modela, obuhvataju period od 2015. do 2026. godine, uključuju sve tri kategorije implementacione osnove, i poseduju dovoljno detaljnu javnu dokumentaciju za sprovođenje kauzalne analize. Vredno je napomenuti da ovaj uzorak ne predstavlja iscrpan popis svih relevantnih CVE zapisa, već namerno ograničen, kriterijumski utemeljen izbor osmišljen da maksimizuje analitički doprinos magistarskog rada – pristup koji je u skladu sa opštom metodološkom praksom kvalitativne naučno-istraživačke analize slučaja (*case study analysis*) u društvenim i tehničkim naukama, gde se dubina analize ograničenog broja pažljivo odabranih slučajeva pretpostavlja površnoj analizi znatno šireg, ali analitički manje eksploatisanog uzorka [38],[39].

Na osnovu primene IKE-VCM modela i kauzalne analize sprovedene u prethodnim odeljcima ovog rada, moguće je formulisati nekoliko generalizovanih obrazaca nastanka bezbednosnih propusta u IKE implementacijama, koji prevazilaze pojedinačne analizirane slučajeve. Prvi obrazac, koji ćemo označiti kao obrazac granularnog upravljanja stanjem kroz više faza protokola, odnosi se na sistemsku tendenciju da ranjivosti nastaju na tačkama u kojima implementacija mora da prenese ili poveže podatke ili stanje između dve strukturno različite faze IKE razmene – kao što je slučaj sa CVE-2026-33824, gde podaci iz IKE_SA_INIT faze bivaju nepravilno upravljani u kontekstu kasnije IKE_AUTH faze. Ovaj obrazac sugerise da tačke prelaska između arhitekturnih faza protokola, uprkos pojednostavljenju arhitekture IKEv2 u odnosu na IKEv1 analiziranom u ranijim delovima ovog istraživanja, ostaju implementaciono osetljive tačke, budući da čak i pojednostavljena, uniformna arhitektura zahteva pažljivo upravljanje memorijskim resursima čiji vek trajanja premašuje granice pojedinačne razmene poruka.

Drugi obrazac, koji ćemo označiti kao obrazac ugnježđenih protokolarnih ekstenzija, odnosi se na sistemsku tendenciju da funkcionalne ekstenzije IKE protokola koje uvode skup ranjivosti u procesu autentifikacije šireg IKE konteksta – poput EAP autentifikacionog sloja analiziranog u kontekstu CVE-2015-8023 i CVE-2021-45079 – nose neproporcionalno visok rizik logičkih ranjivosti u odnosu na osnovni, uniforman tok protokola. Ovaj obrazac ima direktnu vezu sa arhitekturnom analizom sprovedenom u ranijim delovima ovog istraživanja: dok je osnovna IKE_SA_INIT/IKE_AUTH arhitektura projektovana da minimizuje broj mogućih stanja i prelaza, opcione ekstenzije poput EAP-a, po prirodi stvari, uvode dodatnu slojevitost koja delimično poništava tu arhitekturnu prednost u domenu koji ekstenzija pokriva [38],[49].

Treći obrazac, koji ćemo označiti kao obrazac deljene implementacione infrastrukture, odnosi se na tendenciju da ranjivosti nastale u funkcionalno susednim, ali protokolarno odvojenim komponentama iste platforme (kao u slučaju CVE-2018-0101, gde je osnovni uzrok lociran u XML parseru webvpn funkcionalnosti) mogu proizvesti bezbednosnu izloženost IKE funkcionalnosti usled deljenja koda ili infrastrukturnih resursa na nivou konkretne implementacije, nezavisno od bezbednosnog stanja koda koji direktno implementira IKE protokol. Ovaj obrazac ukazuje na ograničenje analize koja bi se fokusirala isključivo na kod koji direktno implementira IKE protokol, zanemarujući širi kontekst platforme u kojoj je taj kod ugrađen [41],[42]. Ova tri generalizovana obrasca, izvedena iz ograničenog ali pažljivo odabranog uzorka reprezentativnih CVE ranjivosti, formiraju analitičku osnovu za komparativnu sintezu koja je predmet narednog, petog odeljka ovog rada, u kojem će biti sistematizovane šire implikacije ovih obrazaca za procenu i unapređenje bezbednosti IKE implementacija u praksi.

6.5. Komparativna analiza reprezentativnih cve ranjivosti, metodološka sinteza i implikacije za bezbednost ike implementacija

Ovaj odeljak zaokružuje tematsku celinu ovog rada sintetizujući nalaze iz prethodnih poglavlja u koherentan skup implikacija za teoriju i praksu bezbednosti IKE implementacija. Umesto ponovnog nabiranja pojedinačnih CVE zapisa, analiza se ovde pomera na viši nivo apstrakcije – poređenje reprezentativnih slučajeva duž nekoliko dimenzija koje prevazilaze pojedinačnu klasifikaciju u okviru IKE-VCM modela, sa ciljem dobijanja zaključaka primenjivih na procenu bezbednosnog rizika IKE infrastrukture.

Prva komparativna dimenzija odnosi se na vremensku dinamiku ozbiljnosti ranjivosti. Poređenje CVE zapisa razmotrenih u radu prema hronološkom redosledu ne ukazuje na jednoznačan trend opadanja ozbiljnosti ranjivosti tokom vremena, uprkos očekivanju da bi ključne karakteristike kodne baze (vreme korišćenja i analiza programskog koda, naročito u slučaju kodnih baza za specijalne sisteme kao što su vojska i policija i kritičnu infrastrukturu) i napredak alata za bezbednosno testiranje trebalo da vode ka postepenom smanjenju ozbiljnosti novootkrivenih propusta. Naprotiv, najozbiljniji analizirani slučaj prema kriterijumu neposredne posledice (CVE-2026-33824, sa CVSS ocenom 9,8 i mogućnošću izvršavanja proizvoljnog koda bez autentifikacije) predstavlja i vremenski najnoviji zapis u analiziranom uzorku. Ovaj nalaz ne treba tumačiti kao dokaz da se bezbednost IKE implementacija generalno pogoršava tokom vremena, već kao potvrdu da karakteristike(*zrelost i dugogodišnja primena u produkcionom okruženju*) kodne baze same po sebi ne predstavljaju garanciju odsustva ozbiljnih ranjivosti, posebno u delovima koda (poput mehanizma fragmentacije analiziranog u kontekstu CVE-2026-33824) koji, iako dugo

prisutni u specifikaciji protokola, ne moraju biti podjednako intenzivno testirani kao osnovni, najčešće korišćeni tok protokola [34],[38].

Druga komparativna dimenzija odnosi se na razlike u obrascima ranjivosti između tri kategorije implementacione osnove analizirane u okviru ovog rada. Otvorene implementacije (*strongSwan*) pokazuju najveću raznovrsnost kategorija uzročnog mehanizma u analiziranom uzorku – zastupljene su kategorije U1 (memorijske greške), U2 (validacija) i U4 (logičke greške automata stanja) – što je delom posledica šireg funkcionalnog obima ovih implementacija (*podrška za brojne autentifikacione metode i kriptografske pluginove*), a delom i posledica transparentnosti procesa objavljivanja bezbednosnih saopštenja, koja omogućava detaljniju javnu dokumentaciju uzročnog mehanizma nego što je to po pravilu slučaj kod komercijalne opreme zatvorenog koda. Komercijalna oprema i operativni sistemi, sa druge strane, u analiziranom uzorku pokazuju koncentraciju na kategoriju U1 (memorijske greške) sa posledicom P3 (izvršavanje koda) – obrazac koji je delimično posledica same prirode analiziranog uzorka (kriterijum ozbiljnosti iz odeljka 4 ovog rada favorizuje uključivanje najozbiljnijih, javno dobro dokumentovanih zapisa, a memorijske ranjivosti sa RCE posledicom po pravilu privlače veću pažnju bezbednosne zajednice i, posledično, detaljniju javnu analizu), ali je delimično i odraz stvarne razlike u modelu razvoja – zatvoren proces razvoja komercijalne opreme i operativnih sistema ograničava mogućnost nezavisne, spoljašnje bezbednosne revizije koda u istoj meri u kojoj je to slučaj kod otvorenih implementacija, što potencijalno odlaže otkrivanje suptilnijih logičkih ranjivosti (kategorija U4) u korist kasnijeg otkrivanja putem eksploatacije u realnim uslovima ili putem namenskog, resursno zahtevnog istraživanja bezbednosnih timova poput onih koji su identifikovali CVE-2026-33824.

Treća komparativna dimenzija manifestuje se na odnos između arhitekturne pozicije ranjivosti (*u smislu funkcionalne komponente prema drugoj osi IKE-VCM modela*) i njene otkrivenosti odnosno vremena koje je proteklo od standardizacije relevantne funkcionalnosti do otkrivanja ranjivosti. Važno je uočiti da je RFC 7383, kojim je standardizovan mehanizam fragmentacije IKE poruka čija je implementacija bila uzrok CVE-2026-33824, objavljen još 2014. godine – što znači da je proteklo više od jedne decenije između standardizacije funkcionalnosti i otkrivanja ove konkretne implementacione ranjivosti u Windows operativnom sistemu. Ovaj vremenski razmak sugerise da funkcionalnosti koje se aktiviraju samo u specifičnim, ređe primenjivanim mrežnim uslovima (*fragmentacija se aktivira prvenstveno kada veličina IKE poruke premašuje MTU vrednost mrežne putanje, što nije uvek slučaj u standardnim mrežnim konfiguracijama*) mogu ostati nedovoljno testirane znatno duže nego funkcionalnosti koje se aktiviraju u svakoj, pa i najosnovnijoj instanci protokola, nalaz koji ima direktnu praktičnu implikaciju za prioritizaciju bezbednosnog testiranja IKE implementacija: komponente aktivirane u ređim, ali specifikacijom predviđenim mrežnim uslovima zaslužuju najmanje jednaku, ako ne i veću pažnju bezbednosnih revizora u odnosu na najčešće korišćeni osnovni tok protokola, upravo usled manje verovatnoće da će biti otkrivene kroz uobičajenu operativnu upotrebu [35],[38],[41],[42].

Iz ove tri komparativne dimenzije proizilazi nekoliko praktičnih implikacija od značaja za administratore IKE infrastrukture, projektante bezbednosnih sistema, i stručnjake zadužene za procenu bezbednosnog rizika, uključujući i kontekst nacionalne bezbednosti i rada bezbednosnih agencija najavljen u uvodnom odeljku ovog rada. Prva implikacija odnosi se na neophodnost kontinuiranog praćenja bezbednosnih saopštenja (*security advisories*) svih komponenti IKE infrastrukture – ne samo softvera koji direktno implementira IKE protokol, već i funkcionalno povezanih komponenti (kako je pokazano u analizi CVE-2018-0101),

imajući u vidu da obrazac deljene implementacione infrastrukture, identifikovana tokom naučno-istraživačke analize i procesa pisanja ovog magistarskog rada, ukazuje da bezbednosna izloženost IKE funkcionalnosti nije uvek u potpunosti predvidljiva isključivo iz analize koda koji direktno implementira protocol [35],[38].

Druga implikacija odnosi se na prioritizaciju testiranja ređe aktiviranih funkcionalnosti protokola – uključujući fragmentaciju, ređe korišćene kombinacije autentifikacionih metoda, i granične slučajeve u pregovaranju kriptografskih parametara, u okviru internih programa bezbednosnog testiranja (penetraciono testiranje i sl.) organizacija koje upravljaju kritičnom IKE infrastrukturom, budući da obrazac granularnog upravljanja stanjem kroz više faza protokola, identifikovan u okviru ovog rada, sugerise da upravo ovakve, ređe aktivirane komponente nose neproporcionalno visok rizik neotkrivenih implementacionih propusta u odnosu na najčešće korišćeni osnovni tok protokola [24],[35].

Treća implikacija, od posebnog značaja za kontekst nacionalne bezbednosti, odnosi se na vremenski okvir između objavljivanja bezbednosnog saopštenja i primene odgovarajućeg *update*-a na kritičnoj infrastrukturi. Kao što je najavljeno u uvodnom odeljku ovog rada, isti obrasci implementacionih slabosti koji omogućavaju eksploataciju od strane oportunističkih kriminalnih aktera predstavljaju i predmet ciljanog iskorišćavanja od strane sofisticiranih, državno sponzorisanih aktera, čiji vremenski horizont planiranja i resursi za samostalno otkrivanje ranjivosti (uključujući i mogućnost otkrivanja i eksploatacije ranjivosti pre njihovog javnog objavljivanja – tzv. *zero-day* eksploatacija) mogu znatno prevazilaziti one dostupne oportunističkim akterima. U tom kontekstu, generalizovani obrasci nastanka bezbednosnih propusta identifikovani u ovom radu – posebno obrazac ugnježenih protokolarnih ekstenzija i obrazac granularnog upravljanja stanjem kroz više faza protokola – pružaju analitički okvir koristan ne samo za reaktivnu procenu već objavljenih ranjivosti, već i za proaktivnu procenu rizika komponenti IKE infrastrukture koje dele strukturne karakteristike sa analiziranim slučajevima, a još nisu bile predmet javno dokumentovane ranjivosti [3],[6],[11].

6.6. Rop i byovd tehnika eksploatacije sa ipsec/ikev1/ikev2

ROP i BYOVD tehnika eksploatacije sa IPsec/IKEv1/IKEv2 infrastrukturom, sprovedena kroz sistematsku primenu procesnog pristupa — istog metodološkog okvira primenjenog kroz naučno istraživačku anлізу u magistarskom radu posvećenom bezbednosnim karakteristikama IKE protokola i fokus na sloj koji u ovoj magistarskoj tezi nije bio centralni predmet analize: interakciju između kriptografske bezbednosti (*uključujući njenu postkvantnu dimenziju*) i memorijsko-izvršne bezbednosti mrežnih uređaja koji IKE/IPsec protokole implementiraju u produkcionom okruženju informaciono-komunikacionih sistema. Magistarski rad analizira ROP i BYOVD vektore napada kao specifičnu klasu pretnji po bezbednost čije razumevanje zahteva uvid u arhitekturu IKE/IPsec protokola jer upravo ta arhitektura (*obim i struktura paketa, format payload-a, način parsiranja pregovaranih transformacija*) određuje gde i kako se memorijske ranjivosti u konkretnim implementacijama manifestuju [24],[30].

6.6.1. Predmet, ciljevi i metodologija istraživanja rop/byovd rizika

Na osnovu definisanog predmeta, formulisani su sledeći istraživački ciljevi:

- Sistematizovati dokumentovane slučajeve ROP eksploatacije IKE/IPsec implementacija (Windows IKE Extension, FortiOS SSL-VPN/IPsec, WatchGuard Fireware IKEv2) kroz jedinstvenu analitičku tabelu, sa naznakom tehničkog mehanizma svake ranjivosti.
- Sistematizovati dokumentovane BYOVD napade koji targetiraju VPN/IPsec gateway

infrastrukturu, sa fokusom na konkretne hardverske uređaje i drajvere koji su tom prilikom zloupotrebljeni.

- Proceniti, kroz procesni i višekriterijumski analitički pristup, da li i u kojoj meri postkvantna kriptografska zaštita (RFC 9370, ML-KEM) utiče — pozitivno, negativno, ili neutralno — na rizik od ROP/BYOVD kompromitacije.
- Formulirati prošireni analitički model koji integriše nalaze u jedinstven okvir primenjiv na buduću procenu bezbednosti kriptografskih mrežnih uređaja u periodu tranzicije ka postkvantnoj kriptografiji.
- ROP i BYOVD tehnike eksploatacije deluju na sloju koji je arhitekturno nezavisan od kriptografskog algoritma i karakteristika kriptografskog ključa, usled čega snaga primenjenog algoritma za razmenu ključeva (klasičnog ili postkvantnog) ne utiče na verovatnoću uspešne memorijske ili kernel-nivo kompromitacije uređaja.
- Postkvantna migracija IKEv2 infrastrukture (RFC 9370/ML-KEM) ne samo da ne smanjuje rizik od ROP/BYOVD kompromitacije, već ga u pojedinim implementacijama može u određenoj meri povećati usled proširene ranjivosti na nivou programskog koda — dodatnih payload tipova, IKE_FOLLOWUP_KEY razmena i mehanizama fragmentacije neophodnih za podršku obimnom PQC ključnom materijalu.
- Kombinacija ROP kompromitacije (kao mehanizma inicijalnog pristupa) i BYOVD tehnike (*kao mehanizma lateralnog kretanja (APT akteri) prikrivanja infiltracije u produkciono okruženje informaciono-komunikacionog sistema i onemogućavanja detekcije*) predstavlja koherentan, empirijski dokumentovan lanac napada primenjiv na savremenu VPN/IPsec infrastrukturu, nezavisno od generacije IKE protokola (IKEv1 ili IKEv2) koja se u konkretnom sistemu koristi.
- Postojeći modeli procene bezbednosnog rizika koji se oslanjaju isključivo na kriptografske metrike (dužina ključa, otpornost na kvantne algoritme) sistematski potcenjuju stvarni bezbednosni rizik uređaja, usled čega je neophodna višekriterijumska nadogradnja koja eksplicitno uključuje dimenziju memorijsko-izvršne ranjivosti.

Procesni pristup u kontekstu ROP i BYOVD tehnika eksploatacije i analitički okvir razvijen i dosledno primenjivan kroz celokupnu tezu posvećenu bezbednosnim karakteristikama IKE protokola koji bezbednosni fenomen ne posmatra kao statičko svojstvo protokola ili hardverskog uređaja, već kao dinamički proces koji se odvija kroz vremenski uređene faze:

- inicijalni pristup, eksploataciju,
- eskalaciju privilegija,
- lateralno kretanje i
- konačno, ostvarenje cilja napadača.

(eksfiltracija podataka, onemogućavanje rada informaciono-komunikacionog sistema, ili uspostavljanje trajnog pristupa u cilju subverzivne aktivnosti i prikupljanja obaveštajnih podataka).

ROP eksploatacija i BYOVD tehnika se u ovom radu eksplicitno pozicioniraju u okviru te procesne sekvence. ROP kao mehanizam inicijalnog pristupa (*remote code execution na internet-facing IKE/IPsec uređaju*), a BYOVD kao mehanizam koji sledi nakon ostvarenog pristupa, radi eskalacije privilegija i onemogućavanja bezbednosnog softvera da obavlja svoju funkciju (da informaciono-komunikacioni sistem bude u stanju bezbednosti).

Pored procesnog pristupa, rad primenjuje višekriterijumsku analizu (*multi-criteria decision analysis, MCDA*) prilikom ocene stepena rizika koji različite kombinacije ROP/BYOVD tehnika i kriptografskih konfiguracija (*klasične kriptografije u poređenju performansi sa*

postkvantnim kriptografskim algoritmima) predstavljaju za konkretan uređaj. Ovaj deo metodologije nadovezuje se na Indeks Rizika od Napredne Lateralne kompromitacije (IRNL), originalni model razvijen u okviru teze, koji će u ovom radu biti eksplicitno proširen dodatnom dimenzijom: sposobnošću tehnike da zaobiđe ili učini irelevantnom postkvantnu kriptografsku zaštitu uspostavljene veze. Fokus je stavljen na one arhitekturne elemente — format paketa, faze pregovaranja, obradu payload-a — koji direktno determinišu površinu napada eksploatabilnu ROP i BYOVD tehnikama.

6.7. Ipvsec arhitektura: ah, esp i security association u kontekstu rop i byovd tehnika eksploatacije

IPsec (*Internet Protocol Security*) predstavlja skup protokola koji obezbeđuju tajnost, integritet i autentičnost IP saobraćaja kroz dva osnovna protokola za zaštitu podataka — *Authentication Header* (AH) i *Encapsulating Security Payload* (ESP) — koji funkcionišu nad prethodno uspostavljenom *Security Association* (SA). SA predstavlja logičku vezu koja definiše kriptografske parametre korišćene za zaštitu saobraćaja između dva entiteta, a njeno uspostavljanje je upravo funkcija IKE protokola. Iz perspektive ovog magistarskog rada, ključno je da se SA uspostavljanje odvija kroz obradu strukturiranih binarnih payload-a od strane IKE procesa koji, kao i svaki drugi softver koji parsira eksterno kontrolisan binarni ulaz, predstavlja potencijalnu metu memorijske eksploatacije [2].

IKEv1, definisan kroz RFC 2409 i dopunjen brojnim RFC dokumentima, uspostavlja SA kroz dve faze: Fazu 1 (uspostavljanje ISAKMP SA, kroz *Main Mode* ili *Aggressive Mode*) i Fazu 2 (uspostavljanje IPsec SA, kroz *Quick Mode*). *Aggressive Mode*, kao brža ali kriptografski slabija alternativa *Main Mode*-u, prenosi identitet učesnika u prvoj poruci pre uspostavljanja enkripcije — arhitektura protokola je takva i odluka koja je, kao što je detaljno analizirano kroz poglavlje posvećeno IKEv1 protokolu u okviru ovog magistarskog rada, osnov za niz poznatih ranjivosti. Za potrebe ovog naučno-istraživačkog rada, relevantno je da IKEv1 implementacije, posebno kada su u pitanju starije implementacije (dugo neažurirane implementacije na enterprise VPN gateway uređajima) često sadrže programski kod nasleđen iz perioda pre uvođenja savremenih memorijskih zaštita (ASLR, stack canaries, CFG/CET), što ih čini disproporcionalno pogodnijim za ROP eksploataciju. Dokumentovan primer, jeste CVE-2026-50751/50752 kombinacija kod *Check Point* uređaja, gde je logička ranjivost u validaciji sertifikata unutar IKEv1 razmene specijalno dizajniranih poruka, omogućila potpuno zaobilazanje autentifikacije bez ijedne memorijske ranjivosti (*memory corruption vulnerability*) pokazujući da IKEv1 arhitektura generiše rizik i kroz logičke, a ne samo memorijske propuste. IKEv2, definisan kroz RFC 7296, konsoliduje IKEv1-ovu dvofaznu arhitekturu u pojednostavljenu razmenu poruka: *IKE_SA_INIT* (uspostavljanje kriptografskih parametara i razmena *Diffie-Hellman* vrednosti) i *IKE_AUTH* (autentifikacija i uspostavljanje prve *Child SA*). Značajno za ovaj rad je naknadno uvedeni *IKE_INTERMEDIATE* mehanizam (RFC 9242), koji omogućava umetanje dodatnih razmena poruka između *IKE_SA_INIT* i *IKE_AUTH* postao deo arhitekture protokola i osnova za integraciju postkvantnih KEM algoritama kroz RFC 9370, jer omogućava prenos obimnog PQC kriptografskog materijala bez oslanjanja na IP fragmentaciju. Svaka dodatna razmena poruka, međutim, predstavlja i dodatni kod za parsiranje i obradu payload-a [2],[10],[51].

Dokumentovan primer memorijske ranjivosti (*memory corruption vulnerability*) direktno u IKEv2 obradi jeste CVE-2025-9242 kod *WatchGuard Fireware OS*-a, gde napadač putem vektora napada cilja verziju firmvera korišćenjem prilagođenog *Vendor ID* payload-a u *IKE_SA_INIT* odgovoru, potom pregovara transformacije (*AES-256, Diffie-Hellman Group 14*) i šalje preveliki identifikacioni payload u *IKE_SA_AUTH* poruci, izazivajući promene u

okviru registara i preuzimanje kontrole toka izvršavanja. Zajednička karakteristika i IKEv1 i IKEv2 protokola, iz perspektive memorijske bezbednosti, jeste da se pregovaranje odvija kroz niz strukturiranih payload-a (*Security Association, Key Exchange, Identification, Certificate, Vendor ID, Notify*, i drugi) čiju dužinu i sadržaj delimično određuje udaljeni učesnik razmene kriptografskog materijala. Parsiranje ovih payload-a, posebno u implementacijama pisanim u memorijski nebezbednim jezicima poput programskog jezika C, koji dominira u *firmware*-u mrežnih uređaja (*FortiOS, WatchGuard Firewall*) i u sistemskim komponentama operativnih sistema (*Windows IKEEXT servis*) otvara prostor za klasične memorijske ranjivosti: prekoračenje bafera na steku (*stack-based buffer overflow*), prekoračenje bafera na heap-u (*heap-based buffer overflow*) i *out-of-bounds write* operacije. Upravo ove kategorije ranjivosti čine empirijsku osnovu za sve dokumentovane ROP eksploatacije IKE/IPsec implementacija analizirane u ovom radu.

Navedena i naučno dokazana činjenica, da je površina napada direktno proporcionalna količini i kompleksnosti payload-a koje protokol definiše — predstavlja polaznu tačku za analizu odnosa između postkvantne kriptografske migracije i memorijsko-izvršnog rizika, jer uvođenje PQC KEM algoritama u IKEv2 (*posebno onih sa većim ključevima, poput ML-KEM-1024*) nužno povećava obim i broj payload-a koje implementacija mora ispravno parsirati, validirati i obraditi [92; BSI TR-02102-1.],[92. BSI TR-02102-1].

Analiza mehanizama *Return-Oriented Programming* (ROP) eksploatacije u kontekstu IKE/IPsec implementacija, a zatim sistematizuje tri dokumentovana slučaja, *Windows IKE ekstenziju, WatchGuard Firewall OS i FortiOS SSL-VPN/IPsec stack*, kroz procesnu perspektivu. ROP predstavlja tehniku eksploatacije koja zaobilazi zaštitu DEP/NX (*Data Execution Prevention / No-eXecute*), koja onemogućava izvršavanje koda. Umesto ubacivanja i izvršavanja sopstvenog *shellcode*-a, napadač konstruiše lanac ("*ROP chain*") od kratkih sekvenci instrukcija ("*gadget-a*") koje se već nalaze unutar legitimnog, izvršivog koda ciljnog programa, a koje se završavaju instrukcijom povratka (*return*). Precizno postavljanje pokazivača steka omogućava napadaču da izvršava proizvoljnu logiku isključivo kombinovanjem postojećih *gadget*-a, bez unošenja novog izvršivog koda čime se DEP/NX zaštita u potpunosti zaobilazi.

Proces ROP eksploatacije IKE/IPsec implementacije tipično sledi sledeću procesnu sekvencu: (1) identifikacija memorijske ranjivosti u parsiranju IKE payload-a (*stack ili heap-based buffer overflow, out-of-bounds write*); (2) precizna kontrola sadržaja memorije u blizini targetiranog opsega, često putem "*heap grooming*" ili "*stack grooming*" tehnika koje dovode memorijski raspored u predvidljivo stanje; (3) pronalaženje upotrebljivih *gadget*-a unutar binarnog fajla cilja, uključujući "*stack pivot*" gadget koji preusmerava pokazivač steka na memoriju pod kontrolom napadača; (4) konstrukcija ROP lanca koji poziva funkcije poput *mprotect* (za označavanje memorijske stranice kao izvršive) ili direktno izvršava sistemske pozive za pokretanje *shell*-a; i (5) isporuka finalnog *shellcode*-a ili *payload*-a, čime se ostvaruje remote code execution (RCE) sa privilegijama procesa koji je IKE izvršavao (*Local System* ili *root* nivo).

Ključna implikacija ove sekvence za predmet ovog magistarskog rada jeste da nijedan korak procesa ne zavisi od kriptografskog algoritma koji se u okviru IKE razmene pregovara. ROP lanac se konstruiše i izvršava pre, ili nezavisno od, uspostavljanja finalnog sesijskog ključa, jer se ranjivost tipično nalazi u fazi parsiranja pregovaranih payload-a (npr. *IKE_SA_INIT* ili *IKE_SA_AUTH* poruka), a ne u samom kriptografskom izračunavanju.

6.7.1. Cve-2026-33824 — windows ike extension (ikeext)

CVE-2026-33824 predstavlja kritičnu ranjivost udaljenog izvršavanja koda (*remote code execution*) u Windows IKE ekstenziji, servisu koji implementira IKE funkcionalnost neophodnu za uspostavljanje Windows-baziranih VPN i IPsec konekcija. Ranjivost omogućava neautentifikovanom napadaču izvršavanje koda preko mreže na pogođenim sistemima pre bilo kakve autentifikacije, sa CVSS ocenom 9,8 — što je klasifikuje među najozbiljnijim ranjivostima ove kategorije dokumentovanim u 2026. godini.

Tehnički mehanizam eksploatacije, dokumentovan u analizama objavljenim tokom aprila 2026. godine, pokazuje da ranjivost dovodi do formiranja ROP lanca koji onemogućava *Control Flow Guard* (CFG) i *Control-flow Enforcement Technology* (CET), dve savremene hardversko-softverske zaštite dizajnirane specifično da otežaju ROP eksploataciju — nakon čega se izvršavanje preusmerava na memoriju pod kontrolom napadača radi pokretanja proizvoljnog *shellcode*-a ili PE *payload*-a unutar konteksta IKEEXT procesa, što je ekvivalentno privilegijama *Local System* naloga. Rezultat je potpuna SYSTEM komandna *shell* bez prekida rada servisa, što napadaču omogućava da izbegne detekciju zasnovanu na monitoringu dostupnosti servisa. Ova ranjivost je posebno pogodna za inicijalni pristup *internet-facing* VPN/IPsec hostovima u korporativnim okruženjima. (neophodna je implementacija kompleksnih sistema zaštite i primena *DMZ-Demilitarized Zone*).

Iz procesne perspektive, značajno je da CVE-2026-33824 demonstrira da čak i savremene, namenski dizajnirane zaštite protiv ROP tehnike (CFG, CET) mogu biti sistematski onesposobljene kao deo samog ROP lanca — što ukazuje da odbrana isključivo na nivou platforme, bez odgovarajuće bezbednosti implementacije protokola, nije dovoljna i da je neophodna implementacija višestrukih mehanizama zaštite informaciono-komunikacionog sistema i procesni pristup.

6.7.2. Cve-2025-9242 — watchguard firewall os (ikev2)

CVE-2025-9242, objavljena pod WatchGuard advisory oznakom WGS-2025-00015, predstavlja *out-of-bounds write* ranjivost u Firewall OS-u koja omogućava daljinsko neautentifikovano izvršavanje proizvoljnog koda putem IKEv2 VPN konekcija na *Firebox* uređajima, sa CVSS 4.0 ocenom 9,3. Ranjivost pogađa više verzija firmvera (od 11.10.2 do 12.11.3, kao i 2025.1), izlažući rizika hiljade malih i srednjih preduzeća koja koriste *WatchGuard* perimetarsku zaštitu.

Proces eksploatacije počinje analizom verzije firmvera (od strane napadača na informaciono-komunikacioni sistem) putem prilagođenog Vendor ID payload-a unutar IKE_SA_INIT odgovora, koji sadrži *base64*-kodirane podatke o verziji i build broju uređaja — korak koji napadaču omogućava preciznu prilagođavanje ROP lanca konkretnoj verziji binarnog fajla, s obzirom da se adrese *gadget*-a razlikuju između verzija firmvera. Nakon "*fingerprint*" faze prikupljanja informacija od značaja za kreiranje vektora napada, napadač pregovara transformacije (*AES-256*, *Diffie-Hellman Group 14*) i šalje preveliki identifikacioni payload u IKE_SA_AUTH poruci, čime se utiče na rad *registry* procesora i preuzima kontrola nad tokom izvršavanja, dovodeći do *segmentation fault*-a ili formiranja ROP lanca. Dokumentovana demonstracija eksploatacije pokazuje da se lanac *gadget*-a koristi za pozivanje *mprotect* funkcije radi označavanja regiona steka kao izvršivog, nakon čega se isporučuje *reverse TCP shellcode* koji pokreće root Python interpreter, omogućavajući dalje akcije poput *remount* operacije fajl sistema ili preuzimanja dodatnih BusyBox alata radi potpunog pristupa mrežnom uređaju.

Ovaj slučaj je posebno relevantan jer ranjivost eksploatiše upravo mehanizam utvrđivanja verzije putem Vendor ID payload-a unutar IKE_SA_INIT razmene — iste faze protokola u koju se, kroz IKE_INTERMEDIATE mehanizam i RFC 9370, uvode dodatni postkvantni KEM *payload*-i. Veći i brojniji *payload*-i povezani sa PQC migracijom ne uklanjaju ovaj vektor fingerprint-ovanja niti tip greške (*out-of-bounds write pri obradi identifikacionog payload-a*), već, naprotiv, uvode dodatne prilike za sličnu klasu grešaka u kodu koji mora parsirati veće strukture podataka [91. NIST IR 8547.];[92. BSI TR-02102-1.];[93. BSI TR-02102-3.].

6.7.3. Rop niz u fortios ssl-vpn/ipsec stack-u (cve-2022-42475, cve-2023-27997, cve-2024-21762)

Treći dokumentovani slučaj ne predstavlja izolovanu ranjivost, već niz od tri hronološki povezane ROP-eksploataбилne ranjivosti u FortiOS SSL-VPN/IPsec implementaciji, dokumentovane između 2022. i 2024. godine, koje zajedno ilustruju obrazac ponovljene eksploatacije istog arhitektonskog obrasca unutar iste kodne baze.

CVE-2022-42475 predstavlja *heap-based buffer overflow* u sslvpnd komponenti, za koju je Fortinet potvrdio aktivnu eksploataciju u praksi. Dokumentovana rekonstrukcija eksploatacije pokazuje da je napadač, nakon pronalaska *stack pivot gadget*-a, konstruisao ROP lanac čiji je cilj bio pronalaženje adrese *mprotect* funkcije unutar *Procedure Linkage Table* (PLT) binarnog fajla FortiOS init procesa — pri čemu je autor eksploatacije eksplicitno napomenuo da se adresa PLT unosa razlikuje između verzija firmvera, što je zahtevalo zasebnu analizu za svaku ciljanu verziju firmvera.

CVE-2023-27997 (poznata i pod neformalnim nazivom “Xortigate”), *heap-based buffer overflow* u sslvpnd komponenti, eksploatisana je putem sličnog obrasca — dokumentacija pokazuje da veliki, monolitni *FortiGate* binarni fajl (preko 70 MB), sadrži veliki broj upotrebljivih *gadget*-a, što eksploataciju čini tehnički izvodljivom uprkos odsustvu klasičnog *shellcode* injection pristupa; autor javno dostupne eksploatacije eksplicitno navodi da implementacija RCE putem ROP-a, u takvim uslovima, nije tehnički zahtevna.

CVE-2024-21762, *out-of-bounds write* ranjivost u istoj komponenti, nastavlja isti obrazac primene kompromitacije bezbednosnih mehanizama. Zajednička karakteristika sve tri ranjivosti jeste da SSL-VPN komponenta FortiOS-a, koja u praksi deli veliki deo koda sa IPsec/IKE obradom unutar iste binarne datoteke, ne implementira ASLR (*Address Space Layout Randomization*) na način koji bi konzistentno onemogućio predvidljivost adresa *gadget*-a, okolnost koju dokumentacija jedne od analiziranih eksploatacija eksplicitno navodi kao olakšavajuću okolnost za konstrukciju ROP lanca.

Procesno posmatrano, ovaj niz od tri ranjivosti unutar iste kodne baze, ponavljane kroz period od najmanje dve godine, ukazuje na sistemski, a ne izolovan problem: arhitektura velikog, monolitnog binarnog fajla koji objedinjuje SSL-VPN, IPsec i IKE funkcionalnost stvara veliki broj ROP *gadget*-a i, istovremeno, otežava potpunu primenu memorijskih zaštita kroz čitavu kodnu bazu.

Sva tri analizirana slučaja dele zajednički procesni obrazac: (1) ranjivost se nalazi u fazi parsiranja *payload*-a koja prethodi ili je nezavisna od finalnog kriptografskog izračunavanja ključa; (2) uspešna eksploatacija zahteva poznavanje specifične verzije ciljnog binarnog fajla (za pronalaženje odgovarajućih adresa *gadget*-a), što napadači rešavaju kroz “*fingerprint*”

fazu verzije putem samog IKE protokola; (3) rezultat je *remote code execution* sa visokim nivoom privilegija, tipično pre bilo kakve autentifikacije. Ovaj obrazac, dokumentovan nezavisno na tri različite platforme (*Windows*, *WatchGuard*, *Fortinet*) tokom perioda 2022–2026, predstavlja empirijsku potvrdu da ROP eksploatacija IKE/IPsec infrastrukture nije teorijska mogućnost, već aktivna, ponovljiva i kontinuirano dokumentovana pretnja, nalaz koji direktno podržava hipotezu o značaju i ulozi procesnog pristupa u analizi bezbednosnih mehanizama IKE protokola.

6.7.4. Mehanizam byovd tehnike: zloupotreba modela poverenja u potpisane drajvere

BYOVD predstavlja tehniku eskalacije privilegija i zaobilaženja odbrambenih mehanizama (*defense evasion*) u kojoj napadač, umesto da pokuša da eksploatiše nepoznatu ranjivost u samom operativnom sistemu ili bezbednosnom softveru, instalira legitiman, digitalno potpisan drajver treće strane za koji je već poznato (dokumentovano, npr. kroz *LOLDrivers* projekat koji katalogizuje ovakve drajvere) da sadrži eksploatabilnu ranjivost. Mehanizam se oslanja na fundamentalnu karakteristiku Windows modela poverenja: *Driver Signature Enforcement* zahteva da svaki drajver koji se učitava u kernel bude digitalno potpisan, ali ne proverava da li potpisani drajver sadrži poznate bezbednosne propuste. Napadač sa administrativnim privilegijama tako može učitati stariji, ranjiv, ali i dalje validno potpisan drajver, uključujući drajvere čiji je sertifikat istekao ili čak povučen, jer operativni sistem u praksi nastavlja da učitava takve drajvere usled propusta u primeni *Driver Signature Enforcement*-a. *Bring Your Own Vulnerable Driver* (BYOVD) tehnike i njenu dokumentovanu primenu u kontekstu VPN/IPsec infrastrukture, sa fokusom na slučaj koji eksplicitno povezuje IKE-baziran inicijalni pristup sa naknadnom BYOVD eskalacijom — čime se, u skladu sa procesnim pristupom i formuliše koherentan dvofazni lanac vektora napada.

Nakon učitavanja ranjivog drajvera, napadač eksploatiše poznate bezbednosne propuste u cilju realizacije proizvoljnog čitanja/pisanja kernel memorije sa privilegijama kernela (Ring 0) — najvišim nivoom privilegija u Windows arhitekturi. Sa tim nivoom pristupa, napadač može terminirati procese EDR (*Endpoint Detection and Response*) i antivirusnog softvera, uticati na procese u okviru *kernel callback*-a, i onemogućiti monitoring agente, čime se obezbeđuje da nijedna naredna faza napada — eksfiltracija podataka, lateralno kretanje, ili implementacija ransomware enkripcije — ne bude detektovana ili prekinuta. U MITRE ATT&CK okviru, BYOVD se mapira na tehniku T1068 (*Exploitation for Privilege Escalation*) i često se preklapa sa T1562.001 (*Impair Defenses: Disable or Modify Tools*).

Kritična karakteristika BYOVD tehnike, koja je čini posebno kompleksnim bezbednosnim izazovom i teško detektabilnom, jeste da napadač ne mora da eksploatiše nikakvu ranjivost u samom operativnom sistemu ili bezbednosnom softveru koji pokušava da zaobiđe — sam čin instalacije digitalno potpisanog drajvera, čak i ranjivog, tipično prolazi standardne provere integriteta operativnog sistema, s obzirom da je potpis sam po sebi validan, samo izdat za softver koji sadrži naknadno otkrivenu ranjivost [27],[29],[49].

Slučaj dokumentovan tokom februara 2026. godine, analiziran kroz telemetriju upravljanog SIEM sistema, predstavlja posebno relevantan primer u okviru ovog magistarskog rada, jer eksplicitno povezuje IKE/IPsec-baziran inicijalni pristup sa naknadnom BYOVD eskalacijom unutar jednog kompleksnog vektora napada. Analiza VPN autentifikacionih logova pokazala je da je napadač uspešno autentifikovan na *SonicWall* SSL-VPN sa eksterne IP adrese, čime je ostvaren inicijalni pristup korporativnoj mreži.

Nakon uspostavljanja pristupa, napadač je implementirao alat za onesposobljavanje EDR zaštite ("*EDR killer*") koji zloupotrebljava legitiman forenzički drajver kompanije *Guidance Software (EnCase)* sa povučenim digitalnim sertifikatom, radi terminacije bezbednosnih procesa sa nivoa kernela — klasična primena BYOVD tehnike. Sertifikat EnCase drajvera istekao je još 2010. godine i naknadno je povučen (*revoked*), ali je operativni sistem, usled propusta u primeni *Driver Signature Enforcement*-a, i dalje učitavao ovaj drajver, propust koji napadači kontinuirano eksploatišu. Napad je otkriven i prekinut pre implementacije *ransomware* enkripcije, ali slučaj ilustruje obrazac koji je, prema dokumentaciji, postao standardna komponenta savremenog *ransomware playbook*-a "*repurposing*" legitimnog forenzičkog alata potpisanog pre više od petnaest godina radi zaobilaženja savremene *endpoint* zaštite.

Procesna analiza ovog slučaja pokazuje jasnu dvofaznu strukturu koja direktno dokumentuje nalaze naučno-istraživačke analize ovog magistarskog rada: Faza 1 (inicijalni pristup) ostvarena je kompromitacijom VPN/SSL-VPN autentifikacionog sloja, funkcionalno analognog IKE autentifikacionoj fazi, dok je Faza 2 (*eskalacija privilegija i onemogućavanje detekcije*) ostvarena isključivo kroz BYOVD tehniku, nezavisno od bilo kakvog svojstva kriptografskog protokola korišćenog u Fazi 1. Sveobuhvatna analiza objavljena u martu 2026. godine, koja je kvantifikovala obim BYOVD ekosistema, identifikovala je 54 različita *EDR-killer* alata koji zloupotrebljavaju 35 potpisanih, legitimnih drajvera radi zaobilaženja *endpoint* zaštite. Ovaj nalaz predstavlja kvalitativnu promenu u odnosu na ranije stanje, kada je BYOVD bila specijalizovana tehnika koju su pretežno koristili napredni državno-sponzorisani akteri (APT grupe) danas predstavlja lako dostupan alat unutar šireg *ransomware* ekosistema [34],[36],[38].

Istraživanje objavljeno od strane Cisco Talos i Trend Micro tokom aprila 2026. godine potvrđuje da *ransomware* grupe *Qilin* i *Warlock* primenjuju BYOVD tehniku kao standardni predenkripcijski korak, a ne kao povremenu ili graničnu taksonomsku pojavu nalaz koji direktno korespondira sa *Check Point* dokumentacijom koja povezuje *Qilin* ransomware afilijate sa IKEv1 autentifikacionim zaobilaženjem kod *Check Point* VPN uređaja (CVE-2026-50751). Ova podudarnost aktera — isti ransomware alat dokumentovan i u kontekstu IKE-baziranog inicijalnog pristupa i u kontekstu BYOVD eskalacije — pruža dodatnu, indirektnu ali značajnu empirijsku potvrdu koherentnosti dvofaznog lanca napada koji je predmet ovog rada. Učestalo zloupotrebljavani drajveri u dokumentovanoj literaturi uključuju *RTCore64.sys*, *gdrv.sys*, *mhyprot2.sys* i *procexp.sys*, korišćene od strane ransomware operatera poput *BlackByte*, *AvosLocker* i *LockBit*, kao i APT grupa, radi terminacije EDR procesa, onemogućavanja bezbednosnih alata i tampering procesa u okviru kernel struktura.

Sinteza nalaza iz ovog i prethodnog poglavlja omogućava formulisanje jedinstvenog, dvofaznog procesnog modela primenljivog na savremenu VPN/IPsec infrastrukturu: Faza 1 (inicijalni pristup) ostvaruje se kroz ROP eksploataciju IKE/IPsec implementacije, primeri CVE-2026-33824, CVE-2025-9242, *FortiOS* niz) ili kroz logičku/autentifikacionu ranjivost (*Check Point* CVE-2026-50751) ili kroz kompromitovane kredencijale (u slučaju *SonicWall*-a); Faza 2 eskalacija privilegija i onemogućavanje detekcije, ostvaruje se kroz BYOVD tehniku, nezavisno od mehanizma kojim je Faza 1 ostvarena. Ova nezavisnost dve faze — gde tehnika korišćena u Fazi 2 ne zavisi od toga da li je Faza 1 ostvarena eksploatacijom memorijske ranjivosti, logičkim zaobilaženjem autentifikacije, ili neovlašćenim korišćenjem kredencijala drugih lica predstavlja ključni argument u prilog tezi da je bezbednosni rizik savremene VPN/IPsec infrastrukture funkcija kombinovane, a ne izolovane analize

kriptografskog i memorijsko-izvršnog sloja [14],[16],[18].

6.8. Objedinjena cve tabela i povezanost sa rop/byovd tehnikama

Prethodna dva podpoglavlja analizirala su ROP i BYOVD tehnike zasebno, svaku kroz sopstveni skup dokumentovanih slučajeva. Ovo poglavlje sistematizuje te nalaze kroz tri komplementarne tabele — CVE tabelu ROP-eksploatabilnih ranjivosti, tabelu zloupotrebljenih BYOVD drajvera, i tabelu koja eksplicitno povezuje obe tehnike u jedinstven, dvofazni procesni lanac — praćeno komparativnom analizom trendova koji iz ovih podataka proizlaze.

6.8.1. Metodologija sistematizacije

Kriterijumi uključivanja CVE unosa u tabeli 10 bili su sledeći: (a) ranjivost mora direktno pogađati IKE, IPsec ili funkcionalno neposredno povezanu VPN autentifikacionu komponentu (SSL-VPN deljenu sa IPsec stack-om); (b) mora postojati javno dostupna tehnička dokumentacija mehanizma eksploatacije (bilo kroz vendor advisory, CISA KEV katalog, ili nezavisnu bezbednosnu analizu); (c) ranjivost mora biti klasifikovana kao remote code execution ili authentication bypass sa CVSS ocenom 9,0 ili višom, odražavajući fokus rada na kritične, praktično eksploataibilne slučajeve. Sedam unosa u tabeli 10 zadovoljava sva tri kriterijuma, pri čemu šest predstavlja memorijske (ROP-eksploataibilne) ranjivosti, a jedan (Check Point CVE par) logičku ranjivost uključenu radi kompletnosti procesne slike IKEv1 rizika uspostavljene u Poglavlju 2.

Kriterijum uključivanja drajvera u tabeli 11 bio je dokumentovana zloupotreba u kontekstu ransomware ili APT kampanje sa jasno opisanim mehanizmom kernel-nivo eksploatacije, dok je tabela 12 konstruisana isključivo od slučajeva gde postoji eksplicitna ili visoko-verovatna veza između faze inicijalnog pristupa (analizirane kroz IKE/IPsec ili srodnu VPN komponentu) i naknadne BYOVD faze.

Tabela 10. Objedinjena CVE tabela — ROP-eksploatabilne i autentifikacione ranjivosti IKE/IPSEC infrastrukture

CVE oznaka	Proizvođač / Proizvod	Komponenta / Protokol	CWE kategorija	CVSS	Mehanizam / Vektor	God.
CVE-2026-33824	Microsoft / Windows IKE Extension	IKEEXT servis (IKE/IPsec)	CWE-787 (Out-of- bounds Write)	9,8	ROP lanac onesposobljava CFG/CET, RCE pre autentifikacije	2026
CVE-2025-9242	WatchGuard / Firewall OS (Firebox)	IKEv2 (IKE_SA_INI T/AUTH)	CWE-787 (Out-of- bounds Write)	9,3	Vendor ID fingerprint + ROP preko mprotect	2025
CVE-2022-42475	Fortinet / FortiOS	SSL-VPN / IPsec (sslvpn)	CWE-122 (Heap- based Buffer Overflow)	9,3	ROP preko PLT adrese mprotect funkcije	2022
CVE-2023-27997	Fortinet / FortiOS, FortiProxy	SSL-VPN / IPsec (sslvpn)	CWE-122 (Heap- based Buffer Overflow)	9,2	"Xortigate" — obilje gadget-a u monolitnom binarnom fajlu	2023
CVE-2024-21762	Fortinet / FortiOS	SSL-VPN / IPsec	CWE-787 (Out-of- bounds Write)	9,6	Nastavak obrasca iz CVE-2023-27997, RCE bez autentifikacije	2024
CVE-2025-0282	Ivanti / Connect Secure, Policy Secure, ZTA	VPN gateway (pre-auth stack)	CWE-121 (Stack- based Buffer Overflow)	9,0	Stack overflow, neautentifikovan RCE, aktivno eksploatisano	2025
CVE-2026-50751 / CVE-2026-50752	Check Point / Security Gateway	IKEv1 (Remote Access/Mobil e Access)	CWE-287 (Improper Authenticat ion)	9,3	Logička greška u validaciji sertifikata (bez memorijske korupcije), MITM na site-to-site	2026

Analiza Tabele 10 otkriva nekoliko obrazaca značajnih za hipoteze ovog rada. Prvo, dominantna CWE kategorija su memorijske ranjivosti pisanja izvan granica dodeljenog bafera (CWE-787, tri od sedam unosa) i heap-based prekoračenje bafera (CWE-122, dva unosa) — obe kategorije klasične za implementacije pisane u memorijski nebezbednim jezicima, potvrđujući da površina napada IKE/IPsec infrastrukture ostaje suštinski vezana za kvalitet implementacije parsera payload-a, a ne za snagu pregovorenih kriptografskih parametara. Drugo, CVSS ocene svih sedam unosa kreću se u opsegu 9,0–9,8, što ukazuje da ranjivosti ove klase sistematski spadaju u najkritičniju kategoriju rizika, nezavisno od proizvođača ili generacije protokola (IKEv1 kod Check Point slučaja, IKEv2 kod WatchGuard i Windows slučajeva). Treće, hronološka distribucija (2022–2026) pokazuje kontinuitet, a ne opadajući trend — što sugerise da industrija mrežne bezbednosti nije sistematski rešila osnovni arhitektonski problem (veliki, monolitni binarni fajlovi sa nedovoljno doslednom primenom memorijskih zaštita) uprkos ponovljenim, javno dokumentovanim incidentima.

Tabela 11. BYOVD drajveri dokumentovani u kompromitacijama VPN/IPSEC infrastrukture

Drajver	Poreklo / Vendor	Tip ranjivosti / Status sertifikata	Zloupotrebljen od strane	Dobijena privilegija
EnCase forenzički drajver	Guidance Software	Sertifikat istekao 2010, naknadno povučen; i dalje učitavan	EDR-killer nakon SonicWall SSL-VPN pristupa (2026)	Kernel-mode (Ring 0), terminacija EDR procesa
RTCore64.sys	MSI (Micro-Star Int.)	Proizvoljno čitanje/pisanje kernel memorije	BlackByte, AvosLocker i drugi ransomware operateri	Kernel-mode (Ring 0)
gdrv.sys	Gigabyte	Proizvoljno čitanje/pisanje fizičke memorije	LockBit i srodne ransomware kampanje	Kernel-mode (Ring 0)
mhyprot2.sys	miHoYo (anti-cheat drajver)	Terminacija proizvoljnog procesa iz kernela	Ransomware akteri (dokumentovano od 2022)	Kernel-mode (Ring 0), proces kill primitivi
procexp.sys	Microsoft Sysinternals	Legitiman alat zloupotrebljen za terminaciju procesa	Više APT i ransomware grupa	Kernel-mode (Ring 0)

Podaci u tabeli 12 ukazuju da zloupotrebljeni drajveri poreklom nisu ograničeni na jednu kategoriju softvera — obuhvataju forenzičke alate (EnCase), hardverske upravljačke drajvere (RTCore64.sys, gdrv.sys), softver za sprečavanje varanja u igrama (mhyprot2.sys) i legitimne systemske dijagnostičke alate (Sysinternals procexp.sys). Ova heterogenost porekla direktno potvrđuje opštu prirodu BYOVD tehnike opisanu u Poglavlju 4: napadaču je irelevantna funkcionalna namena drajvera — jedini relevantan kriterijum jeste postojanje validnog digitalnog potpisa u kombinaciji sa poznatom kernel-nivo ranjivošću. Ovo ima direktnu implikaciju za odbrambenu strategiju: liste blokiranih drajvera (blocklists) moraju se ažurirati kontinuirano i ne mogu se ograničiti na kategorije softvera tipično povezane sa bezbednošću ili mrežnom infrastrukturom.

Tabela 12. Objedinjeni dvofazni procesni lanac napada

Slučaj	Faza 1 (inicijalni pristup)	Faza 2 (eskalacija / evazija)	Povezani akter / napomena
SonicWall / EnCase	Kompromitovane VPN kredencijale, SSL-VPN autentifikacija	BYOVD (EnCase drajver) — terminacija EDR pre ransomware faze	Prekinuto pre enkripcije (2026)
Check Point / Qilin	CVE-2026-50751/50752 — logičko zaobilaženje IKEv1 autentifikacije	BYOVD (industrijalizovana praksa dokumentovana kod istog aktera)	Qilin ransomware afilijat (srednja pouzdanost atribucije)
FortiOS niz	ROP RCE preko SSL-VPN/IPsec steka (CVE-2022-42475 i dr.)	Nije direktno dokumentovana BYOVD faza u istom izvoru, ali arhitektonski kompatibilna	Obrazac konzistentan sa ostalim slučajevima
Windows IKEEXT	CVE-2026-33824 — ROP RCE, zaobilaženje CFG/CET	Pun SYSTEM shell omogućava naknadnu BYOVD instalaciju bez dodatne autentifikacije	Dokumentovano kao red-team/pentest scenario

Podaci u tabeli 12 predstavljaju centralni analitički doprinos ovog poglavlja — eksplicitno mapiranje četiri dokumentovana ili arhitektonski utemeljena slučaja na dvofazni procesni model uspostavljen u Poglavlju 4.4. Značajno je da se Faza 1 ostvaruje kroz tri različita mehanizma (memorijska ROP eksploatacija, logičko zaobilazjenje autentifikacije, kompromitacija kredencijala), dok Faza 2 u dokumentovanim slučajevima dosledno koristi BYOVD tehniku nezavisno od mehanizma Faze 1 — empirijska potvrda tvrdnje iz Poglavlja 4 da su dve faze arhitektonski nezavisne. Slučaj Check Point/Qilin posebno je vredan pažnje jer povezuje dva nezavisna izvora (Check Point Research analizu IKEv1 ranjivosti i Cisco Talos/Trend Micro analizu BYOVD prakse) preko zajedničkog aktera, čime se indirektno, ali metodološki validno, potvrđuje da isti akteri koji eksploatišu IKE/IPsec ranjivosti kao inicijalni vektor takođe rutinski primenjuju BYOVD kao narednu fazu.

6.8.2. Komparativna i trend analiza

Posmatrano kroz vremenski period, CVE tabela pokazuje da su ROP-eksploatabilne ranjivosti IKE/IPsec infrastrukture dokumentovane kontinuirano u periodu od 2022. do 2026. godine sa prosečno jednim do dva značajna javno dokumentovana slučaja godišnje među analiziranim proizvođačima. Ovo je u kontrastu sa BYOVD ekosistemom, koji pokazuje eksponencijalni, a ne linearni rast, od tehnike ograničene na uzak krug naprednih aktera do dokumentovanih 54 EDR-killer alata i 35 zloupotrebljenih drajvera u periodu od svega godinu dana (2025–2026). Ova razlika u dinamici rasta dve tehnike ima važnu implikaciju: dok ROP eksploatacija IKE/IPsec implementacija zahteva specijalizovano tehničko znanje (identifikacija memorijske ranjivosti, konstrukcija ROP lanca specifičnog za verziju binarnog fajla), BYOVD tehnika je, nakon početnog istraživačkog napora utrošenog na identifikaciju ranjivog drajvera, trivijalno ponovljiva i lako distribuirana kroz širi krug manje sofisticiranih aktera — što objašnjava zašto se u tabeli 12 Faza 2 dosledno oslanja na BYOVD, a ne na ponovljenu memorijsku eksploataciju.

Distribucija po proizvođačima pokazuje da nijedan pojedinačni vendor nije imun — Microsoft, Fortinet, WatchGuard, Ivanti i Check Point svi imaju bar jedan dokumentovan kritičan slučaj u periodu obuhvaćenom analizom. Fortinet se izdvaja sa tri odvojena unosa (CVE-2022-42475, CVE-2023-27997, CVE-2024-21762) u istoj funkcionalnoj komponenti (sslvpn), što — kao što je već napomenuto u Poglavlju 3.4 — ukazuje na sistemski, arhitektonski problem specifičan za taj proizvod, a ne na izolovan propust u pojedinačnoj verziji koda. Dodatno, uočljivo je da su tri od sedam CVE unosa (43%) dokumentovana kao aktivno eksploatisana u realnim uslovima pre objavljivanja zakrpe (CVE-2022-42475, CVE-2025-0282, CVE-2026-50751), što ukazuje da ROP-eksploatabilne i autentifikacione ranjivosti IKE/IPsec infrastrukture nisu isključivo teorijski, laboratorijski rizik, već aktivno korišćen vektor u stvarnim kompromitacijama.

6.8.3. Ograničenja sistematizacije

Metodološki je važno eksplicitno navesti ograničenja sprovedene sistematizacije. Prvo, podaci u tabeli 10 obuhvataju isključivo javno dokumentovane, objavljene CVE unose — postoji neizbežna verovatnoća da dodatne, još neotkrivene ili neobjavljene (*zero-day*) ranjivosti iste kategorije postoje u analiziranim hardverskim (ili softverskim) komponentama informaciono-komunikacionih sistema i još uvek su nedokumentovane (ili neotkrivene) ili drugim proizvodima koji imaju uticaj na bezbednosne karakteristike, tako da sistematizacija predstavlja donju granicu, a ne potpun popis stvarnog rizika. Drugo, veza uspostavljena u tabeli 12 između Faze 1 i Faze 2 za slučaj *Check Point/Qilin* zasniva se na atribuciji srednje pouzdanosti (prema izvornoj *Check Point Research* dokumentaciji) i na vremenskoj/tematskoj

podudarnosti sa nezavisnom BYOVD analizom, a ne na jedinstvenom izveštaju koji eksplicitno prati istog aktera kroz obe faze unutar istog incidenta — stepen izvesnosti ove veze stoga treba tumačiti kao indikativan, a ne kao definitivno utvrđenu uzročnu vezu. Treće, odsustvo dokumentovane BYOVD faze u *FortiOS* nizu (tabela 12), ne znači da takva faza ne postoji u praksi, već da dostupna javna dokumentacija analiziranih incidenata nije eksplicitno izvestila o njoj tj. neophodno je naglasiti da odsustvo dokaza ovde nije nepobitan dokaz kvalitativnih svojstava bezbednosnih mehanizama, već ograničenje dostupnosti pouzdanih izvora informacija na osnovu kojih se može bazirati naučno-istraživački rad [14].

6.8.4. Implikacije za procenu rizika mrežne infrastrukture

Nalazi sistematizovani u ovom poglavlju imaju direktnu praktičnu implikaciju za administratore i timove u oblasti informacione bezbednosti koji upravljaju IKE/IPsec infrastrukturom: procena rizika koja se oslanja isključivo na verziju kriptografskog protokola (npr. “IKEv2” je bezbedniji od “IKEv1”) ili isključivo na kriptografske parametre (dužina kriptografskog ključa, specifikirani kriptografski algoritam itd.) sistematski previđa dimenziju rizika dokumentovanu u Tabeli 1, jer kao što pokazuje slučaj *WatchGuard Firewall* (CVE-2025-9242), IKEv2 implementacija podjednako je podložna ROP eksploataciji kao i IKEv1 implementacija *Check Point* uređaja, samo kroz drugačiji specifičan mehanizam. Praktična preporuka koja proizlazi iz ove analize jeste da procena rizika mora biti dvodimenzionalna — obuhvatajući i kriptografski sloj (algoritam, dužina ključa, otpornost na kvantne napade) i implementacioni/memorijski sloj (istorija CVE ranjivosti konkretnog proizvoda, prisustvo memorijskih zaštita poput ASLR/CFG/CET, veličina i modularnost binarnog fajla) princip koji će biti formalizovan kroz prošireni višekriterijumski model [38],[42].

Dodatna implikacija odnosi se na prioritizaciju odbrambenih resursa: s obzirom da podaci u tabeli 11 ukazuju da BYOVD tehnika koristi drajvere potpuno nepovezane sa mrežnom ili VPN funkcionalnošću (anti-cheat softver, forenzički alati), odbrana isključivo fokusirana na hardening IKE/IPsec komponente — koliko god bila metodološki opravdana s obzirom na nalaze iz tabele 10 — ostaje nedovoljna bez paralelnog, sistemskog upravljanja listom dozvoljenih/blokiranih kernel drajvera na nivou celog operativnog sistema uređaja koji IKE/IPsec funkcionalnost implementira [16],[18],[19],[38].

Sistematizacija sprovedena u ovom poglavlju kroz tri tabele potvrđuje tri centralna nalaza: (1) ROP-eksploatabilne ranjivosti IKE/IPsec infrastrukture predstavljaju kontinuiranu, a ne opadajuću pretnju, dosledno klasifikovanu u najkritičniju CVSS kategoriju; (2) BYOVD tehnika je, u periodu 2025–2026, prešla put industrijalizacije koji je čini standardnom, lako dostupnom komponentom napadačkog arsenala u konstruisanju kompleksnih vektora napada nezavisno od sofisticiranosti aktera; i (3) direktna, empirijski dokumentovana veza između ova dva toka — ilustrovana tabelom 12 — potvrđuje hipotezu ovog rada da ROP i BYOVD tehnike, kombinovane, čine koherentan dvofazni lanac napada primenljiv na savremenu VPN/IPsec infrastrukturu nezavisno od generacije IKE protokola. Nalazi predstavljaju naučnu osnovu za nastavak analize (pregled konkretnih ranjivih hardverskih uređaja) i podrazumeva interdisciplinarni pristup (odnos prema postkvantnoj kriptografskoj zaštiti).

6.9. Pregled konkretnih ranjivih hardverskih uređaja

Analizirane su ROP i BYOVD tehnike kroz apstraktan mehanizam i sistematizovanu CVE/drajver tabelu. Ovo poglavlje kompletira procesnu sliku fokusirajući se na konkretnu hardversku i platformsku realnost (*produkciono okruženje*) tj. uređaje i operativne sisteme na kojima se dokumentovane ranjivosti manifestuju, njihovu ulogu u tipičnoj mrežnoj arhitekturi, i obim izloženosti koji njihova rasprostranjenost implicira [6],[7].

6.9.1. Fortinet fortigate (fortios)

FortiGate predstavlja liniju *next-generation firewall* (NGFW) uređaja kompanije Fortinet, koji objedinjuju firewall, IPsec/SSL-VPN gateway, intrusion prevention i druge bezbednosne funkcije unutar jednog uređaja i jedinstvenog operativnog sistema (*FortiOS*). Arhitektura i bezbednosne karakteristike FortiOS-a relevantne za ovaj rad: SSL-VPN i IPsec funkcionalnost dele veliki deo koda unutar istog, monolitnog binarnog fajla tj. činjenica koja objašnjava zašto se tri odvojene ROP-eksploataбилne ranjivosti (CVE-2022-42475, CVE-2023-27997, CVE-2024-21762) pojavljuju unutar iste funkcionalne komponente (sslvpn) tokom perioda od svega dve godine. *FortiGate* uređaji se u praksi masovno koriste kao perimetarska zaštita malih, srednjih i velikih preduzeća, kao i kao IPsec *site-to-site gateway* između poslovnih lokacija i uloga koja ih čini *internet-facing* uređajima po definiciji, i time direktno izloženim neautentifikovanoj eksploataciji ranjivosti.

Rizik povezan sa FortiGate uređajima dodatno je uvećan njihovom dugom prisutnošću u proizvodnji (mnogi uređaji ostaju u operativnoj upotrebi 5-7 godina ili duže) u kombinaciji sa administrativnom praksom odlaganja ažuriranja firmvera zbog operativnog rizika od prekida VPN konektivnosti — obrazac koji je, prema dokumentaciji CISA-inog *Known Exploited Vulnerabilities*) kataloga, doprineo produženom periodu aktivne eksploatacije nakon objavljivanja bezbednosnog *update*-a za sve tri analizirane FortiOS ranjivosti.

6.9.2. Watchguard firebox (fireware os)

Firebox predstavlja liniju UTM (*Unified Threat Management*) i NGFW uređaja kompanije *WatchGuard*, tipično implementiranih u segmentu malih i srednjih preduzeća, sa Fireware OS operativnim sistemom koji implementira IKEv2-baziranu VPN funkcionalnost (CVE-2025-9242). Značajna karakteristika *WatchGuard* tržišnog pozicioniranja jeste fokus na jednostavnost administracije i centralizovano upravljanje (*WatchGuard Cloud*), što u praksi znači da veliki broj *Firebox* uređaja upravlja spoljni MSP (*Managed Service Provider*) davalac usluga umesto internog IT tima klijenta — arhitektura koja, kada je ranjiva, potencijalno multiplikuje uticaj jedne ranjivosti kroz veliki broj klijentskih mreža istog MSP-a.

Opseg pogođenih verzija firmvera dokumentovan za CVE-2025-9242 (11.10.2 do 12.11.3, kao i 2025.1) obuhvata firmver koji je bio aktuelan tokom višegodišnjeg perioda, što implicira da je veliki deo instalirane baze *Firebox* uređaja bio istovremeno izložen u trenutku objavljivanja ranjivosti — okolnost koja delimično objašnjava zašto je *WatchGuard* advisory (WGSA-2025-00015) klasifikovan kao kritičan prioritet koji u značajnoj meri utiče na bezbednosne karakteristike informaciono-komunikacionih sistema.

6.9.3. Ivanti connect secure, policy secure i zta gateway

Ivanti Connect Secure (ranije poznat kao *Pulse Connect Secure*) predstavlja SSL-VPN/IPsec *gateway* rešenje pretežno korišćeno u *enterprise* i vladinim okruženjima, uključujući, prema javno dostupnim CISA advisory dokumentima, agencije od nacionalnog bezbednosnog značaja u više jurisdikcija. Ivanti proizvodna linija ima dokumentovanu istoriju ponovljenih kritičnih pre-autentifikacionih ranjivosti (uključujući i ranije slučajeve van opsega ovog rada), a CVE-2025-0282, nastavlja taj obrazac kroz *stack-based buffer overflow* koji omogućava neautentifikovan RCE.

Kontekst posebno relevantan za procenu rizika Ivanti uređaja jeste njihova dokumentovana upotreba kao meta naprednih državno-sponzorisanih aktera (APT grupa) usled prirode klijentele koja koristi Ivanti uređaje (*vladine agencije, odbrambeni sektor, kritična*

infrastruktura). Na osnovu tih informacija se može zaključiti da ranjivosti poput CVE-2025-0282 nose disproportionalno visok bezbednosno-obaveštajni značaj u odnosu na njihovu tehničku CVSS ocenu, jer eksploatacija ranjivosti otvara pristup računarskim mrežama i bazama podataka visokog stepena tajnosti.

6.9.4. Check point security gateway

Check Point Security Gateway uređaji predstavljaju liniju enterprise firewall/VPN rešenja, sa posebno rasprostranjenom upotrebom IKEv1-bazirane *Remote Access* i *Mobile Access* VPN funkcionalnosti analizirane kroz CVE-2026-50751/50752. Za razliku od prethodna tri proizvođača, čije analizirane ranjivosti su memorijske (ROP-eksploataбилne) prirode, Check Point slučaj demonstrira da rizik IKEv1 komponente proizlazi i iz logičkih grešaka u validaciji sertifikata — kategorija ranjivosti koja ne zahteva sofisticiranu ROP konstrukciju, ali proizvodi ekvivalentno kritičan ishod (zaobilaženje autentifikacije, MITM napade na *site-to-site* vezama).

Prisustvo Check Point uređaja u kritičnoj infrastrukturi i finansijskom sektoru, u kombinaciji sa dokumentovanom vezom analiziranog CVE para sa Qilin ransomware afilijatom, čini ovaj slučaj posebno ilustrativnim za dvofazni procesni model — Faza 1 (IKEv1 logičko zaobilaženje) direktno omogućava pristup mrežama visoke vrednosti u kojima naredna BYOVD faza ostvaruje maksimalan destruktivni potencijal.

6.9.5. Windows server: ike extension (ikeext) hostovi

Za razliku od prethodna četiri slučaja, koji se odnose na namenske mrežne bezbednosne uređaje (*firewall/VPN appliance*), CVE-2026-33824 targetira Windows Server (i Windows desktop) instalacionu bazu koja implementira IKE funkcionalnost kroz sistemski IKEEXT servis (*komponentu koja podržava Windows-baziranu IPsec i VPN konektivnost*) uključujući *DirectAccess*, *Always On VPN* i *site-to-site* IPsec konfiguracije unutar *Active Directory* domenskih okruženja. Ova arhitektonska razlika ima važnu implikaciju za obim izloženosti: dok su FortiGate, Firebox, Ivanti i Check Point uređaji namenski bezbednosni proizvodi sa relativno ograničenim, specijalizovanim tržišnim udelom, Windows Server predstavlja dominantan operativni sistem (enterprise domenske infrastrukture), čime CVE-2026-33824 potencijalno pogađa značajno veći skup organizacija.

Dodatna otežavajuća okolnost jeste da IKEEXT servis na Windows Server platformi tipično izvršava sa *Local System* privilegijama unutar domenskog okruženja, što uspešnu ROP eksploataciju direktno pretvara u domenski relevantan kompromitujući događaj, potencijalno otvarajući put ka eskalaciji na nivo domenskog kontrolera kroz naredne, van opsega ovog rada, tehnike lateralnog kretanja napadača na informaciono-komunikacione sisteme tj. lateralno kretanje unutar *Active Directory* infrastrukture.

Sistematski pregled pet analiziranih platformi pokazuje da rizik dokumentovan kroz ovaj rad nije ograničen na jednu kategoriju uređaja, arhitekturu ili tržišni segment. Namenski bezbednosni uređaji (*FortiGate, Firebox, Ivanti, Check Point*) dele zajedničku karakteristiku direktne *internet-facing* izloženosti kao funkciju njihove osnovne namene, dok opšta platforma (Windows Server IKEEXT) unosi drugačiju dimenziju rizika kroz obim instalirane baze i kroz dubinu integracije (sa domenskom infrastrukturom). Ova heterogenost potvrđuje centralnu tezu rada da bezbednosni rizik IKE/IPsec infrastrukture ne može biti adekvatno procenjen kroz analizu jedne platforme ili jednog proizvođača, već zahteva sistemski, procesni pristup primenjiv kroz čitav sistem uređaja koji IKE/IPsec protokole implementiraju tj. nalaz koji direktno priprema teren analizu u kojem će biti analizirano da li postkvantna kriptografska migracija ovih pet platformi na jednak način utiče na memorijsko-izvršni rizik

dokumentovan u ovom poglavlju.

6.10. Postkvantna kriptografija i granica njene zaštite

6.10.1. Rfc 9370 i ml-kem integracija u ikev2 protokolu

RFC 9370 (*Multiple Key Exchanges in IKEv2*), objavljen od strane IETF-a, definiše mehanizam koji omogućava kombinovanje više nezavisnih razmena ključeva unutar jedne IKEv2 SA_INIT sekvence — arhitektura rešenja je osmišljena specifično za hibridnu tranziciju ka postkvantnoj kriptografiji, u kojoj se klasičan Diffie-Hellman (ECDH) kombinuje sa jednim ili više postkvantnih *Key Encapsulation Mechanism* (KEM) algoritama, poput ML-KEM (*Module-Lattice-Based KEM*, standardizovan kroz NIST FIPS 203). Kombinovanje klasičnog i postkvantnog mehanizma, umesto potpune zamene, odražava konzervativan pristup migraciji — čak i ako bi ML-KEM algoritam u budućnosti pokazao neočekivanu kriptografsku slabost, sigurnost veze ostaje zaštićena klasičnom ECDH komponentom, i obrnuto [93; BSI TR-02102-3].

Tehnička implementacija ovog mehanizma zahteva IKE_INTERMEDIATE razmenu (RFC 9242) kao nosioca dodatnih KEM public key i ciphertext struktura, jer standardni IKE_SA_INIT payload nije dimenzionisan za obiman kriptografski materijal koji ML-KEM algoritmi generišu — ML-KEM-768, na primer, generiše enkapsulacioni ključ veličine približno 1184 bajta i ciphertext od približno 1088 bajtova, dok ML-KEM-1024 generiše proporcionalno veće strukture. Za razliku od klasične ECDH razmene (tipično 32-64 bajta po ključu), ove dimenzije zahtevaju dodatne razmene poruka (IKE_FOLLOWUP_KEY, uvedene upravo za ovu namenu) kako bi se izbegla fragmentacija IP paketa, koja sama po sebi nosi dodatne bezbednosne implikacije (kao što je na primer izloženost UDP fragmentation napadima) [75; RFC 9867].

StrongSwan, jedna od vodećih open-source IPsec/IKEv2 implementacija koja se koristi i kao referenca u enterprise i istraživačkim okruženjima, implementirala je podršku za hibridnu ML-KEM razmenu u skladu sa ovim standardima, čime PQC migracija IKEv2 infrastrukture prelazi iz teorijske specifikacije u praktično dostupnu, deployable funkcionalnost.

Centralni analitički alat ovog poglavlja jeste eksplicitno razdvajanje dva sloja bezbednosti IKE/IPsec uređaja, uvedeno konceptualno u uvodnom poglavlju, a ovde formalizovano kroz slojeviti (*layered*) model. Kriptografski sloj obuhvata matematičku sigurnost algoritma za razmenu ključeva, što podrazumeva otpornost na kriptozanalizu, uključujući, u slučaju ML-KEM, otpornost na napade kvantnim računarom putem Shor-ovog algoritma. Memorijsko-izvršni sloj obuhvata integritet procesa koji taj algoritam implementira ispravnost parsiranja payload-a, upravljanje memorijom, i otpornost na tehnike poput ROP koje ne napadaju kriptografski algoritam već implementaciju. Ključni analitički uvid na osnovu naučno-istraživačke analize jeste da ROP eksploatacija IKE/IPsec implementacije po pravilu cilja fazu parsiranja pregovaranih payload-a koja prethodi ili je paralelna sa kriptografskim izračunavanjem, a ne sâmo izračunavanje. Konkretno, u sva tri ROP slučaja analizirana u Poglavlju 3 (CVE-2026-33824, CVE-2025-9242, FortiOS niz), ranjivost se nalazi u obradi identifikacionih, vendor ID ili autentifikacionih payload-a — strukturama koje postoje nezavisno od toga da li se razmena ključeva odvija putem klasičnog Diffie-Hellman-a ili hibridnog ML-KEM mehanizma. Iz ovoga sledi direktan zaključak koji potvrđuje da karakteristike kriptografskih algoritama i otpornosti na kriptozanalizu (uključujući postkvantne kriptografske algoritme i kvantnu otpornost) uspostavljenog ključa ne utiče na verovatnoću uspešne ROP eksploatacije, iz razloga što se te dve operacije realizuju na arhitekturno

nezavisnim slojevima(u kontekstu obrade podataka) [75; RFC 9867].

Argument u prilog tezi da PQC migracija ne utiče na ROP/BYOVD rizik: PQC KEM algoritmi menjaju isključivo matematičku operaciju izvođenja deljene tajne (*shared secret*) i format ključnog materijala koji se prenosi tj. ne menjaju arhitekturu parsiranja identifikacionih, autentifikacionih ili *vendor payload*-a u kojima su dokumentovane ranjivosti. Prema ovom argumentu, uređaj ranjiv na CVE-2025-9242 pre PQC migracije ostaje podjednako ranjiv i nakon migracije, jer se ranjivost nalazi u kodnoj putanji koja nije modifikovana uvođenjem ML-KEM podrške u kontekstu povećanja stepena zaštite.

Argument u prilog tezi da PQC migracija marginalno povećava rizik: uvođenje ML-KEM podrške u praksi zahteva netrivialne izmene koda IKE implementacije — parsiranje novih tipova payload-a (KE payload sa novim *Transform ID* vrednostima za ML-KEM grupe, kako su definisane u IANA registru), implementaciju IKE_INTERMEDIATE i IKE_FOLLOWUP_KE state mašina koje ranije nisu postojale, i uspostavljanje konekcije uslovljava značajno većim strukturama podataka nego što je klasična IKEv2 implementacija bila projektovana da obrađuje. Svaka od ovih izmena predstavlja novi kod koji nosi sopstveni, nezavisan rizik od memorijskih grešaka — princip dobro utemeljen u opštoj literaturi bezbednosti softvera, gde je gustina defekata (*defect density*) po liniji koda relativno stabilna metrika nezavisno od funkcije koda koji se piše. Konkretno, WatchGuard slučaj (CVE-2025-9242) direktno ilustruje ovaj rizik obrazac: ranjivost proizlazi iz obrade identifikacionog payload-a čija je dužina delimično određena pregovorenim parametrima — arhitekturno identičan rizik postoji, i po svemu sudeći se uvećava, kada IKE_FOLLOWUP_KE razmena mora obraditi ML-KEM strukture reda veličine 1-2 kilobajta po poruci, u poređenju sa desetinama bajtova kod klasične ECDH razmene.

Treći argument predstavlja sintezu prethodna dva: PQC migracija ne utiče na rizik od ranjivosti u postojećem, nepromenjenom kodu (*te ranjivosti ostaju identično eksploataбилne kao i pre migracije*), ali istovremeno otvara novi, dodatni prostor rizika u novom kodu koji migracija unosi. To znači da je efekat PQC migracije u kontekstu memorijsko-izvršne ranjivosti povećan, suprotno intuitivnom, ali pogrešnom očekivanju da implementacija postkvantnih kriptografskih algoritama implicira "bezbedniji hardverski uređaj" u celini.

6.10.2. Mogućnost zaobilaženja ili narušavanja pqc zaštite primenom pop i byovd tehnika

Analiza ovog pitanja zahteva preciznu distinkciju između dva različita smisla u kojima se "zaobilaženje" PQC zaštite može razumeti. Prvi smisao — kriptanalitičko zaobilaženje, odnosno slamanje matematičke sigurnosti ML-KEM algoritma — nije predmet ovog magistarskog rada i nije ono što ROP ili BYOVD tehnike čine; nijedan od dokumentovanih slučajeva analiziranih u ovom radu ne uključuje napad na sâm kriptografski algoritam. Čineći kriptografsku zaštitu irelevantnom zaobilaženjem sloja na kojem ona operiše predstavlja upravo ono što ROP i BYOVD tehnike sistematski realizuju, i predstavlja centralni nalaz ovog poglavlja.

ROP eksploatacija, kao što je pokazano kroz sva tri slučaja, ostvaruje cilj (*remote code execution*) u fazi koja prethodi ili je paralelna sa uspostavljanjem finalnog session ključa tj. u praksi, napadač koji uspešno izvrši ROP lanac protiv (IKE_SA_INIT ili IKE_AUTH) obrade dobija kontrolu nad procesom pre nego što je PQC-zaštićena SA uopšte uspostavljena, ili neposredno nakon toga, sa punim pristupom memoriji procesa u kojoj se ključni materijal (uključujući dešifrovan ML-KEM *shared secret*) nalazi u kriptografski (čitljivom)

nezaštićenom obliku (plaintext) radi upotrebe u daljem šifrovanju saobraćaja.

Ovo je arhitekturno neizbežna posledica svakog kriptografskog sistema tj. kriptografski ključ mora u nekom trenutku postojati u *plaintext* obliku unutar memorije procesa koji ga koristi za enkripciju/dekripciju — i PQC migracija ovu fundamentalnu činjenicu ne menja niti može promeniti. Sledstveno, napadač sa ROP-ostvarenim RCE pristupom IKE procesu ima pristup i samom uspostavljenom ključu, čineći pitanje "da li je ključ kvantno-otporan" bezpredmetnim za taj specifičan vektor napada — kriptografska snaga ključa štiti od napadača koji presreće saobraćaj, ali ne i od napadača koji je već kompromitovao proces koji taj ključ upotrebljava [40],[75; RFC 9867].

BYOVD tehnika ostvaruje analogan, ali arhitektonski dublji oblik irelevantnosti kriptografske zaštite: kernel-nivo pristup ostvaren BYOVD tehnikom (Poglavlje 4) nadilazi granice pojedinačnog procesa i operativnog sistema u celini, omogućavajući napadaču pristup memoriji svih procesa, uključujući IKE demon i sve procese koji koriste podatke dešifrovane putem uspostavljene IPsec SA. U tom kontekstu, PQC zaštita razmene ključeva postaje irelevantna ne zato što je algoritam slomljen, već zato što napadač operiše na sloju privilegija (Ring 0) koji je hijerarhijski iznad bilo kog korisničkog procesa čiju bezbednost kriptografija štiti — model pretnje za koji nijedan algoritam za razmenu ključeva, klasičan ili postkvantan, nije dizajniran da pruži zaštitu [75; RFC 9867].

6.10.3. Formulacija centralnog nalaza: nezavisnost slojeva kao strukturno svojstvo

Sinteza analize sprovedene u ovom poglavlju omogućava sledeću formulaciju : kriptografski sloj (uključujući njegovu postkvantnu dimenziju) i memorijsko-izvršni sloj (*čiju ranjivost eksploatišu ROP i BYOVD tehnike*) predstavljaju strukturno nezavisne dimenzije bezbednosnog rizika IKE/IPsec infrastrukture. Ova nezavisnost nije slučajna karakteristika trenutnog stanja implementacija, već proizlazi iz fundamentalne arhitekture tj. činjenice da se kriptografska operacija (izračunavanje deljene tajne) i memorijska operacija (parsiranje payload-a, upravljanje baferima, izvršavanje koda) odvijaju kao odvojeni, sekvencijalni koraci unutar iste softverske implementacije. Poboljšanje jednog koraka (jača kriptografija, primer primene postkvantnih algoritama za enkripciju) ne implicira automatsko poboljšanje drugog (bezbednija implementacija parsiranja) [31],[38].

Ovaj nalaz ima dve važne, na prvi pogled kontraintuitivne implikacije. Prvo, PQC migracija, uprkos svom nesumnjivom značaju za dugoročnu otpornost na kvantne napade na presretnuti saobraćaj ("harvest now, decrypt later" scenario), ne predstavlja i ne treba da bude predstavljena kao mera koja unapređuje otpornost uređaja na ROP ili BYOVD kompromitaciju — dva bezbednosna cilja koja zahtevaju odvojene, namenske mere (*memory-safe programski jezici, formalna verifikacija implementacije parsera, kernel-nivo drajver whitelisting*). Drugo, i posledično, organizacije koje sprovode PQC migraciju svoje IKE/IPsec infrastrukture ne treba da tretiraju tu migraciju kao priliku za smanjenje investicije u naučno-istraživački rad i višestruke slojeve bezbednosti (redovno ažuriranje firmvera, monitoring memorijskih ranjivosti, EDR/kernel integritet) naprotiv, kao što je pokazano, sama migracija privremeno uvećava memorijsko-izvršni rizik kroz uvođenje novog, još netestiranog programskog koda.

Nalazi u potpunosti potvrđuju hipoteze ovog magistarskog rada, i pruža empirijski i logički utemeljen odgovor na centralno istraživačko pitanje postavljeno u analizi bezbednosnih mehanizama.

Ovo poglavlje formalizuje kvalitativne nalaze kroz kvantitativni višekriterijumski model, nadograđujući Indeks Rizika od Napredne Lateralne kompromitacije (IRNL) — originalni model razvijen u okviru teze, gde su ROP i BYOVD tehnike ocenjene vrednostima 3,95/10 i 7,55/10 respektivno — dodatnom, petom dimenzijom eksplicitno posvećenom sposobnosti tehnike da učini irelevantnom postkvantnu kriptografsku zaštitu. Prošireni model, u ovom radu označen kao IRNL-PQC, omogućava sistematsko poređenje rizika kako između tehnika (ROP naspram BYOVD), tako i između (specificiranih) uređaja analiziranih u ovom konkretnom poglavlju.

Originalni IRNL model, primenjen u tezi na analizu lateralnog kretanja nakon inicijalne mrežne kompromitacije, sistematizovao je rizik kroz kriterijume tehničke izvodljivosti, realizovane eskalacije privilegija, rasprostranjenosti primene i detektabilnosti. Ograničenje originalnog modela za potrebe ovog rada jeste odsustvo eksplicitne dimenzije koja bi kvantifikovala nalaz da tehnika može biti visokorizična ne samo zbog svoje tehničke izvodljivosti, već i zbog stepena u kojem čini kriptografsku investiciju (uključujući skupu i tehnički zahtevnu PQC migraciju) u određenim okolnostima irelevantnom. Na osnovu toga, naučno-istraživačka analiza metodološki opravdava uvođenje kriterijuma K3 (*PQC Bypass kapacitet*), čime se broj kriterijuma proširuje sa četiri na pet kriterijuma.

6.11. Post-kvantna kriptografija u ike sistemima

Poslednji tematski odeljak ovog poglavlja posvećen je bezbednosnom izazovu koji se kvalitativno razlikuje od svih prethodno analiziranih rizika: za razliku od implementacionih propusta (prva tematska celina), pitanja optimalnog izbora parametara unutar postojeće matematičke paradigme (druga tematska celina), i implementaciono-konfiguracionih rizika u zaštiti podataka i upravljanju identitetom, izazov razmatran u ovom odeljku proističe iz mogućnosti da čitava matematička osnova na kojoj počiva savremena asimetrična kriptografija – uključujući Diffie-Hellman razmenu analiziranu kroz čitav ovaj rad – bude fundamentalno i neopozivo narušena razvojem kvantnih računara dovoljnog kapaciteta. Analiza bezbednosnih karakteristika sistematski razmatra prirodu ove pretnje, put standardizacije post-kvantnih mehanizama unutar IKEv2 protokola, i praktične izazove njihove implementacije, uz oslanjanje na analitičke nalaze iz svih prethodnih poglavlja ovog rada.

Teorijska osnova kvantne pretnje po klasičnu asimetričnu kriptografiju leži u Shor-ovom algoritmu, kvantnom algoritmu objavljenom 1994. godine, koji, izvršen na dovoljno moćnom i dovoljno stabilnom kvantnom računaru, rešava problem faktORIZACIJE velikih brojeva i problem diskretnog logaritma – u oba matematička konteksta, konačnim poljima i eliptičkim krivama, u polinomijalnom vremenu, za razliku od eksponencijalne ili subeksponencijalne kompleksnosti koju ovi problemi zahtevaju na klasičnim računarima. Praktična realizacija ove teorijske pretnje zahteva tzv. kriptografski relevantan kvantni računar (*Cryptographically Relevant Quantum Computer* – CRQC) – uređaj sa dovoljnim brojem logičkih (kvantno korigovanih) kubita i dovoljno niskom stopom greške da izvrši Shor-ov algoritam na kriptografski relevantnim veličinama parametara (na primer, RSA modulima od 2048 bita ili ekvivalentnim eliptičkim krivama). Iako se procene o vremenskom horizontu do pojave CRQC-a znatno razlikuju među stručnjacima i institucijama, konsenzus u kriptografskoj i širokoj bezbednosnoj zajednici – uključujući NIST, NSA, i IETF radne grupe zadužene za standardizaciju – jeste da priprema mora otpočeti znatno pre pouzdane realizacije CRQC-a, upravo usled strategije napadača poznate kao „*harvest now, decrypt later*“ (HNDL), već

pomenute u ranijim delovima ovog istraživanja: podaci enkriptovani danas klasičnom Diffie-Hellman razmenom, ukoliko budu presretnuti i arhivirani od strane napadača sa dovoljnim resursima i strpljenjem, ostaju potencijalno dekriptabilni u trenutku kada CRQC postane dostupan, bez obzira na to koliko je taj trenutak vremenski udaljen od trenutka presretanja [93; BSI TR-02102-3].

Značaj HNDL strategije za IKE ekosistem, konkretno, proističe iz prirode podataka koje IKE/IPsec infrastruktura tipično štiti: komunikacije državnih institucija, kritične infrastrukture, i organizacija sa dugoročnim zahtevima za poverljivošću podataka (na primer, medicinski podaci, poslovne tajne sa dugim ekonomskim vekom, ili, od posebnog značaja za kontekst ovog rada, komunikacije relevantne za nacionalnu bezbednost i obaveštajni rad) – kategorije podataka za koje zahtevani period poverljivosti često prevazilazi jednu ili čak dve decenije, period koji je, prema većini stručnih procena razmotrenih u okviru NIST i IETF standardizacionih aktivnosti, uporediv sa ili čak kraći od procenjenog vremenskog horizonta do pojave CRQC-a. Ova okolnost čini IKE/IPsec infrastrukturu, uz TLS protokol, jednim od prioritetnih konteksta za rano usvajanje post-kvantnih mehanizama zaštite, uprkos tome što CRQC u trenutku pisanja ovog rada (sredina 2026. godine) i dalje ne postoji u praktično upotrebljivom obliku [92; BSI TR-02102-1],[93; BSI TR-02102-3].

Odgovor kriptografske zajednice na ovu pretnju materijalizovao se kroz višegodišnji proces standardizacije koji je Američki nacionalni institut za standarde i tehnologiju (NIST) sproveo tokom perioda 2016–2024. godine, uključujući javni, više rundi trajući konkurs za post-kvantne algoritme razmene ključeva i digitalnog potpisa, sa učešćem kriptografa iz čitavog sveta. Proces je rezultirao objavljivanjem tri federalna standarda u avgustu 2024. godine: FIPS 203, koji standardizuje (akronim) ML-KEM (*Module-Lattice-Based Key-Encapsulation Mechanism*, prethodno poznat pod imenom CRYSTALS-Kyber) kao mehanizam enkapsulacije ključa zasnovan na problemu učenja sa greškom u strukturiranim rešetkama (*Module Learning With Errors*, akronim: MLWE); FIPS 204, koji standardizuje ML-DSA (*Module-Lattice-Based (Digital Signature Algorithm)*, prethodno CRYSTALS-Dilithium) za digitalne potpise; i FIPS 205, koji standardizuje SLH-DSA (*Stateless Hash-Based Digital Signature Algorithm*, prethodno SPHINCS+), zasnovan na kriptografskim heš funkcijama kao alternativan, matematički nezavisan pristup digitalnom potpisu. Za potrebe ovog magistarskog rada, od direktne relevantnosti za IKEv2 razmenu ključeva jeste ML-KEM (FIPS 203), dok ML-DSA i SLH-DSA postaju relevantni u kontekstu post-kvantne zaštite same autentifikacije sertifikatima, sprovedene u okviru naučno-istraživačke analize, ali čija detaljna obrada izlazi iz uskog obuhvata ovog odeljka.

Vredno je, radi potpunosti naučne analize, eksplicitno napomenuti i epizodu koja ilustruje da proces post-kvantne standardizacije nije bio linearan niti bez rizika: NIST-ov konkurs je u jednoj od ranijih rundi razmatrao i SIKE (*Supersingular Isogeny Key Encapsulation*), algoritam zasnovan na matematici izogenija superingularnih eliptičkih krivih, koji je dospeo do poslednje runde razmatranja kao jedan od kandidata za standardizaciju. U julu 2022. godine, međutim, istraživači su objavili napad koji je, koristeći isključivo klasičan (ne kvantni) računar, uspeo da izračuna privatni ključ SIKE algoritma za standardne parametre u roku od nešto više od sat vremena na običnom personalnom računaru – potpun kriptanalitički kolaps algoritma koji je do tog trenutka prošao kroz nekoliko godina javne kriptanalize bez otkrivanja ove slabosti. Ova epizoda predstavlja izuzetno značajnu metodološku pouku direktno relevantnu za širi analitički okvir ovog rada: nova, matematički inovativna kriptografska konstrukcija, čak i kada prođe kroz formalni, višegodišnji proces javne kriptanalize u okviru renomirane standardizacione procedure, ne pruža istu vrstu

dugoročno potvrđene pouzdanosti kao matematički problemi (poput diskretnog logaritma) koji su bili predmet kriptanalize kroz višedecenijski period, analogno obrascu identifikovanom u okviru ovog rada da zrelost i dužina javnog testiranja predstavljaju nezavisnu, i ne uvek intuitivno očiglednu dimenziju bezbednosnog rizika, nezavisnu od formalne matematičke sofisticiranosti same konstrukcije.

Upravo iz razloga ilustrovanog SIKE epizodom, IETF radna grupa zadužena za IKEv2 standardizaciju (IPsecME) opredelila se za hibridni, a ne isključivo post-kvantni pristup migraciji – strategiju kojom se post-kvantni mehanizam kombinuje sa, a ne zamenjuje, postojećom klasičnom *Diffie-Hellman* razmenom. Prvi korak u ovom pravcu predstavljao je RFC 8784 (2020. godina), koji definiše mehanizam unapred deljenih post-kvantnih ključeva (Post-Quantum-Preshared-Keys akronim PPK), kojim se dodatni, van protokola distribuiran deljeni tajni materijal kombinuje sa standardnim SKEYSEED izvođenjem ključeva analiziranim u ranijim delovima ovog istraživanja, pružajući otpornost na HNDL napad bez oslanjanja na bilo koji konkretan post-kvantni algoritam razmene ključeva – pristup koji, iako operativno jednostavan, zahteva postojanje bezbednog, van-protokolarnog kanala za prethodnu distribuciju deljenog materijala, što ograničava njegovu praktičnu skalabilnost u odnosu na scenarije udaljenog pristupa sa velikim brojem heterogenih klijenata.

Suštinski značajniji korak predstavlja RFC 9370 (maj 2023. godine), koji definiše opšti okvir za više uzastopnih razmena ključeva (*Multiple Key Exchanges*) unutar iste (IKE_SA_INIT/IKE_AUTH) arhitekture analizirane u okviru ovog istraživanja, uvodeći dve nove pomoćne razmene, uvodeći IKE_INTERMEDIATE (definisanu ranije, u RFC 9242 iz 2022. godine, prvobitno radi drugih svrha, ali iskorišćenu kao nosilac dodatnih razmena ključeva) i uvodeći IKE_FOLLOWUP_KE (za slučaj *rekeying*-a ili uspostavljanja dodatnih neophodnih Child SA) kroz koje se, pored standardne Diffie-Hellman razmene u IKE_SA_INIT poruci, mogu razmeniti do sedam dodatnih parova ključnog materijala, čiji se rezultati zajednički „kombinuju“ (kroz uzastopnu primenu PRF funkcije analizirane u delu ovog istraživanja u kontekstu SKEYSEED izvođenja) u konačni ključni materijal IKE SA. Ova arhitektura, važno je naglasiti, direktno se oslanja na uniformnost i proširivost arhitekture (IKE_SA_INIT/IKE_AUTH) razmene analiziranu kao centralnu bezbednosnu prednost IKEv2 u odnosu na IKEv1, tačno onu vrstu proširivosti bez izmene osnovnog toka protokola koja je razmatrana kao jedna od arhitekturnih prednosti IKEv2 dizajna [93; BSI TR-02102-3].

RFC 9370 sam po sebi definiše samo generički okvir, a ne konkretnu instancijaciju sa ML-KEM algoritmom – zadatak koji je, u trenutku pisanja ovog rada (sredina 2026. godine), predmet IETF Internet-Draft dokumenta u okviru IPsecME radne grupe (draft-ietf-ipsecme-ikev2-mlkem, u svojoj petoj reviziji od marta 2026. godine), koji precizira kako se konkretno ML-KEM enkapsulacija i dekapulacija integrišu u IKE_INTERMEDIATE razmenu, uključujući i eksplicitne bezbednosne zahteve poput obavezne provere tipa šifrovanog teksta (*ciphertext*) pre operacije dekapulacije, radi sprečavanja određenih klasa napada specifičnih za implementacije na određene bezbednosne kontekste kriptografije i kriptanalize. Status ovog dokumenta kao Internet-Draft-a, a ne još uvek objavljenog RFC-a, sam po sebi ilustruje da je proces konkretne, interoperabilne standardizacije ML-KEM podrške u IKEv2 protokolu, iako značajno uznapredovao, u trenutku pisanja ovog rada i dalje u završnoj fazi, sa realnim mogućnostima manjih izmena specifikacije pre konačnog objavljivanja.

Praktični izazovi implementacije hibridnog pristupa razmotrenog u prethodno navedenim primerima zaslužuju eksplicitnu analizu, budući da direktno povezuju ovaj odeljak sa nalazima iz ranijih delova ovog rada. Prvi i najznačajniji izazov odnosi se na veličinu poruka:

dok X25519 (ECP Grupa 31, analizirana u okviru ovog rada) zahteva prenos javne vrednosti od svega 32 bajta, ML-KEM-768 (varijanta koja odgovara približno AES-192 nivou klasične bezbednosti) zahteva prenos javnog ključa od približno 1184 bajta i enkapsulisanog šifrovanog teksta slične veličine – uvećanje veličine (IKE_SA_INIT) poruke za red veličine u odnosu na čisto klasičnu *Diffie-Hellman* razmenu. Ova okolnost direktno aktivira zabrinutost razmotrenu u odeljku 7 ovog rada u kontekstu izbora *Diffie-Hellman* grupa: veća IKE_SA_INIT poruka povećava verovatnoću premašivanja MTU vrednosti mrežne putanje i posledične potrebe za IKE fragmentacijom (RFC 7383), mehanizmom čija je implementaciona osetljivost eksplicitno dokumentovana kroz analizu CVE-2026-33824 u ovom poglavlju. Drugim rečima, migracija ka post-quantnoj otpornosti, upravo usled povećanja veličine poruka koje ta migracija nužno nosi, može posredno povećati izloženost IKE infrastrukture jednoj od najozbiljnijih kategorija implementacionih ranjivosti identifikovanih u prvoj tematskoj celini ovog rada – nalaz koji predstavlja originalan doprinos ovog istraživanja, budući da direktno povezuje naizgled odvojene tematske celine rada (implementacione ranjivosti i post-quantnu migraciju) kroz zajednički uzročni mehanizam (veličina IKE_SA_INIT poruke i fragmentacija).

Drugi izazov odnosi se na računarske kapacitete neophodne u slučaju ML-KEM operacija u odnosu na klasičnu ECP *Diffie-Hellman* razmenu. Iako je ML-KEM, zahvaljujući svojoj rešetkastoj matematičkoj strukturi, projektovan da bude računarski efikasan (u pojedinim merenjima brži od RSA operacija ekvivalentne klasične bezbednosti), hibridni pristup po definiciji zahteva izvršavanje i klasične i post-quantne operacije, čime se ukupan računarski resursi neophodni za IKE_SA_INIT razmene neizbežno povećavaju u odnosu na scenario koji koristi isključivo jedan mehanizam – kompromis koji je, prema eksplicitnoj filozofiji hibridnog pristupa ilustrovanog SIKE epizodom, namerno prihvaćen radi postizanja odbrane u dubinu (*defense in depth*): bezbednost hibridne konstrukcije zavisi od toga da bar jedan od dva mehanizma – klasičan ili post-quantni – ostane u stanju bezbednosti, čime se hibridni pristup štiti i od scenarija u kojem bi CRQC postao dostupan pre nego što se očekuje, i od scenarija, analognog SIKE epizodi, u kojem bi post-quantni algoritam bio kriptanalitički probijen klasičnim sredstvima pre nego što CRQC uopšte postane dostupan.

Treći izazov, od posebnog značaja za institucionalni i državno-bezbednosni kontekst razmatran u uvodnom odeljku ovog rada, odnosi se na regulatorni vremenski okvir migracije. Američka Nacionalna bezbednosna agencija (NSA), kroz svoj CNSA 2.0 (*Commercial National Security Algorithm Suite 2.0*) skup zahteva, propisuje obavezno usvajanje ML-KEM mehanizama za sisteme koji štite komunikacije od nacionalnog bezbednosnog značaja do 2030. godine, dok šire NIST preporuke (uključujući NIST IR 8547) predviđaju postepeno isključivanje klasičnih, isključivo *Diffie-Hellman* zasnovanih mehanizama za savezne sisteme Sjedinjenih Država do 2035. godine. Ovi regulatorni vremenski okviri, iako formalno primenjivi u prvom redu na jurisdikciju Sjedinjenih Država, u praksi oblikuju i šire, globalno tržište IKE/IPsec opreme, budući da proizvođači mrežne opreme sa globalnim tržišnim prisustvom po pravilu implementiraju regulatorne zahteve najstrožih relevantnih jurisdikcija kao podrazumevanu funkcionalnost dostupnu svim korisnicima – obrazac koji ima direktnu posledicu i za planiranje bezbednosne modernizacije IKE infrastrukture u jurisdikcijama van Sjedinjenih Država, uključujući i institucionalne sisteme relevantne za nacionalnu bezbednost razmatrane u kontekstu ovog istraživanja [91; NIST IR 8547.], [93; BSI TR-02102-3].

Na osnovu naučno-istraživačke analize sprovedenu u ovom poglavlju, post-quantna migracija IKE sistema predstavlja bezbednosni izazov kvalitativno različite prirode od svih prethodno analiziranih rizika u ovom radu tj. ne implementacionu grešku koju je moguće otkriti i

primeniti *security update*, niti pitanje optimalnog izbora unutar poznate i stabilne matematičke paradigme, već fundamentalnu promenu same matematičke osnove bezbednosti IKE protokola i bezbednosnih mehanizama, čije puno ostvarenje (primena CRQC) tek predstoji, ali čije se posledice (kroz HNDL strategiju) potencijalno ostvaruju već danas. Analiza sprovedena u ovom poglavlju pokazuje da odgovor IKE sistema na ovaj izazov jeste hibridni pristup formalizovan kroz RFC 9370 i konkretizovan kroz tekuću ML-KEM standardizaciju i predstavlja metodološki oprezan, (na iskustvu SIKE epizode utemeljen pristup), ali da njegova praktična implementacija istovremeno reaktivira i pojačava rizike identifikovane u ranijim delovima ovog rada, konkretno rizik fragmentacije IKE_SA_INIT poruke povezan sa CVE-2026-33824 iz dela naučno-istraživačke analize ovog rada. Ovaj nalaz sam po sebi ilustruje širi metodološki zaključak magistarskog rada: pojedinačni bezbednosni mehanizmi i izazovi IKE sistema ne mogu biti adekvatno analizirani izolovano, već isključivo u međusobnoj, sistemskoj interakciji, što je i bio vodeći analitički princip primenjen kroz sve odeljke ovog istraživanja.

7. Zaključak

Ovo završno poglavlje sintetizuje ukupne nalaze istraživanja sprovedenog kroz ovu tezu, sa primarnim fokusom na potvrđivanje glavne hipoteze naučno-istraživačkog rada u okviru ove magistarske teze o značaju procesnog pristupa kao metodološke osnove bezbednosne analize kriptografskih protokola za razmenu ključeva. Sinteza obuhvata rezultate primene integrativnog procesno-strukturnog okvira na IPsec arhitekturu u celini, i na IKEv1 i IKEv2 protokole pojedinačno, dopunjenu analizom dodatne klase bezbednosnih pretnji — *Return-Oriented Programming* (ROP) eksploatacije i BYOVD (*Bring Your Own Vulnerable Driver*) napada — koji postaju relevantni u fazi lateralnog kretanja nakon što je napadač ostvario početni pristup informaciono-komunikacionom sistemu, uključujući slučajeve gde je taj početni pristup ostvaren upravo kroz eksploataciju ranjivosti IKE protokola analiziranih u naučno-istraživačkom radu.

Struktura zaključka prati logiku uspostavljenu od centralnog nalaza i potvrđivanje glavne hipoteze kroz procesni pristup, preko testiranja posebnih hipoteza formulisanih u uvodnom poglavlju, do proširenja analize na širi kontekst lanca napada koji uključuje ROP i BYOVD tehnike relevantne za fazu lateralnog kretanja. Ova struktura odražava nameru da zaključak bude sveobuhvatna sinteza koja povezuje tehnički fokusirane rezultate analize IKE/IPsec protokola sa širim, praktično relevantnim kontekstom savremenih lanaca napada kakve primenjuju sofisticirani akteri poput državno sponzorisanih hakerskih grupa koje primenjuju slične ili identične tehnike koji primenjuju proizvođači komercijalnog spyware-a.

7.1. Potvrđivanje glavne hipoteze kroz procesni pristup

Glavna hipoteza ovog istraživanja tvrdi da sistematska primena integrativnog procesno-strukturnog pristupa — koji bezbednosni protokol analizira istovremeno kroz arhitekturni, procesni, strukturno-sintakski i kriptografsko-matematički nivo — omogućava identifikaciju kritičnih bezbednosnih ranjivosti koje nastaju na preseku više, pojedinačno konfiguracija koje ponaosob ne dovode informaciono-komunikacioni sistem u nebezbedno stanje, i koje ostaju neotkrivene kada se protokol analizira isključivo kroz jednodimenzionalne metode. Sistematska primena ovog okvira u toku naučno-istraživačkog rada magistarske tezu — na IPsec arhitekturu u celini, i na IKEv1 i IKEv2 protokole pojedinačno — pruža višestruko potvrđenu empirijsku osnovu za potvrdu ove hipoteze i značaju procesnog pristupa u pravovremenom otkrivanju ranjivosti informaciono-komunikacionog sistema i prednosti primene procesnog pristupa u slučaju kada napadač ima status zaposlenog i kada dolazi do zloupotrebe pristupa (*napad insajdera na IKT sistem*) i takođe u slučaju kompleksnih vektora napada koji primenjuju ROP i BYOVD tehnike neovlašćenog pristupa informaciono-komunikacionom sistemu.

EksPLICITNA potvrda glavne hipoteze proizlazi iz analize kritične ranjivosti kombinacije *Aggressive Mode* razmene i *Pre-Shared Key* autentifikacije u okviru IKEv1 protokola. Izolovana arhitektonska analiza *Aggressive Mode*-a pokazala bi isključivo da se identitet prenosi u prvoj poruci pre uspostavljanja enkripcije — podatak koji, sam po sebi, ukazuje na narušavanje zaštite identiteta, ali ne nužno na da će IKT sistem biti doveden u nebezbedno stanje. Izolovana kriptografska analiza PSK metode autentifikacije pokazala bi isključivo da je HMAC-zasnovana konstrukcija SKEYID izvođenja matematički korektna i, uz dovoljnu entropiju, kriptografski otporna na kriptanalizu koje karakteriše primena sada raspoloživih tehničko-tehnoloških kapaciteta jer kvantni računari efikasnije izvršavaju kriptanalizu.

Nijedan od ova dva izolovana nalaza, sam za sebe, ne otkriva praktično eksploatabilnu ranjivost. Tek eksplicitno povezivanje procesnog nalaza (neenkriptovan prenos u *Aggressive Mode*-u) sa strukturnim nalazom (tačna pozicija HASH_R vrednosti unutar payload strukture) i kriptografskim nalazom (direktna zavisnost HASH_R vrednosti od PSK-izvedenog SKEYID-a) otkriva kompletan uzročni lanac koji čini offline PSK *cracking* napad praktično izvodljivim. Ovaj nalaz, detaljno razrađen kroz analizu sprovedenu u poglavlju posvećenom IKEv1 protokolu, predstavlja višestruko potvrđenu glavnu hipotezu istraživanja.

Analogna potvrda proizlazi iz analize IPsec arhitekture na širem nivou, iznad samog IKE protokola. Izolovana analiza AH i ESP protokola (*koji ostvaruju stvarnu zaštitu korisničkog saobraćaja*) ne otkriva zavisnost njihove bezbednosti od ispravnog funkcionisanja IKE protokola kao mehanizma za uspostavljanje ključeva; izolovana analiza IKE protokola ne otkriva uvek do kraja praktične posledice kompromitacije IKE Faze 1 na sve naknadno pregovorene IPsec bezbednosne asocijacije. Tek procesno praćenje čitavog lanca — od uspostavljanja ISAKMP SA, preko izvođenja SKEYID_d komponente, do KEYMAT izvođenja za konkretnu IPsec SA — otkriva da kompromitacija bilo koje faze u ovom lancu (*najkritičnije, same Faze 1 autentifikacije*) ugrožava kompletnu bezbednosnu arhitekturu IPsec tunela, nezavisno od toga koliko su AH/ESP algoritmi enkripcije sami po sebi kriptografski robusni. Ovaj nalaz, koji je moguće dobiti isključivo kroz procesnu perspektivu koja prati tok kriptografskog materijala kroz čitavu arhitekturu, dodatno potvrđuje centralnu vrednost procesnog pristupa.

Treća, komparativna potvrda glavne hipoteze proizlazi iz analize sprovedene kroz poglavlja posvećena IKEv2 protokolu i komparativnoj analizi sa IKEv1. Primena identičnog, četvoroslojnog analitičkog okvira na oba protokola omogućila je precizno lociranje tačaka u kojima IKEv2 arhitektura eliminiše specifične strukturne slabosti IKEv1 protokola — ne kroz uopštenu tvrdnju da je 'IKEv2 bezbedniji', već kroz eksplicitno mapiranje svake IKEv1 slabosti (*izbor moda razmene, neformalna proširenja, nedostatak standardizovane DoS zaštite*) na konkretan, identifikovan odgovor u IKEv2 standardu (jedinствена IKE_SA_INIT/IKE_AUTH sekvenca, formalizovana EAP/konfiguracijski payload integracija, COOKIE notifikacija). Ova preciznost mapiranja, ostvarena isključivo zahvaljujući doslednoj primeni procesno-strukturnog okvira na oba protokola, predstavlja treći, nezavisan stub potvrde glavne hipoteze.

Četvrta potvrda glavne hipoteze proizlazi iz metodološkog iskustva stečenog kroz razvoj originalnih analitičkih modela unutar ove teze — pokušaj da se IKBZ model kvantitativne evaluacije konstruiše isključivo na osnovu izolovanih kriterijuma (npr. samo kriptografska snaga kripto-varijabli, bez razmatranja načina na koji se ta snaga manifestuje kroz konkretan procesni tok) pokazao se nedovoljnim za formiranje smislene, diskriminativne ocene. Tek uključivanje kriterijuma koji eksplicitno premošćuju arhitekturni, procesni i implementacioni nivo (npr. 'otpornost PSK na offline napade', koji po definiciji zahteva razumevanje i kriptografske konstrukcije i procesnog konteksta *Aggressive Mode* razmene) omogućilo je da IKBZ model proizvede ocenu koja stvarno diskriminiše između bezbednosno različitih konfiguracija — dodatna, metodološki izvedena potvrda da izolovani kriterijumi ne mogu adekvatno uhvatiti suštinu bezbednosnog rizika, dok kriterijumi koji eksplicitno integrišu više analitičkih nivoa to mogu.

Peta, sintezna potvrda proizlazi iz same strukture ove teze kao celine — dosledna primena identičnog četvoroslojnog okvira na IPsec arhitekturu, IKEv1 protokol, i IKEv2 protokol, omogućila je ne samo analizu svakog protokola pojedinačno, već i sistematsko poređenje

između njih zasnovano na uporedivim, metodološki konzistentnim kriterijumima. Ova sistematičnost, koja bi bila nemoguća bez doslednog pridržavanja procesno-strukturnog okvira kroz čitavu tezu, sama po sebi predstavlja empirijsku demonstraciju praktične vrednosti procesnog pristupa — vrednost koja se ne ogleda samo u pojedinačnim tehničkim nalazima, već u sposobnosti okvira da organizuje i poveže te nalaze u koherentnu, uporedivu celinu.

Šesta, završna potvrda proizlazi iz direktnog poređenja rezultata testiranja posebnih pomoćnih hipoteza (*detaljno razrađenog u narednom odeljku ovog zaključka*) — činjenica da su ova četiri, nezavisno formulisane i testirane hipoteze rezultovale nijansiranim, diferenciranim ishodima, predstavlja dodatnu indikaciju metodološke robustnosti prednosti primenjenog procesnog pristupa analizi IPsec i IKE protokola.

Sveukupno, šest nezavisnih linija potvrde iznetih u ovom odeljku : primer *Aggressive Mode/PSK kombinacije*, šira IPsec arhitekturna analiza, komparativna preciznost mapiranja IKEv1→IKEv2 poboljšanja, metodološki konzistentna analiza razvoja IKBZ modela, sistematičnost celokupne strukture magistarske teze, i nijansiran obrazac rezultata testiranja hipoteza — zajedno formiraju snažnu, višestruko utemeljenu empirijsku osnovu za potvrdu glavne hipoteze ovog istraživanja. Nijedna od ovih linija dokaza, posmatrana izolovano, ne bi bila dovoljna za potpunu potvrdu hipoteze ovog obima i značaja; tek njihova kombinovana, međusobno potkrepljujuća snaga pruža uverljivu, rigoroznu naučnu osnovu za zaključak da je glavna hipoteza ovog istraživanja empirijski potvrđena.

7.2. Testiranje pomoćnih hipoteza

Posebna hipoteza H1 (viši nivo zaštite identiteta u IKEv2) potvrđena je kroz procesnu analizu IKE_SA_INIT/IKE_AUTH sekvence — za razliku od IKEv1, gde izbor *Aggressive Mode*-a dozvoljava prerano otkrivanje identiteta, IKEv2 arhitektura strukturno ne dozvoljava prenos identiteta pre uspostavljanja DH-izvedenog enkripcionog materijala, ni u jednoj dozvoljenoj konfiguraciji protokola. Ova hipoteza potvrđena je bez izuzetka, potvrđujući da IKEv2 eliminiše samu mogućnost konfiguracionog izbora koji ugrožava zaštitu identiteta.

Posebna hipoteza H2 (eliminacija PSK/nezaštićeni-mod ranjivosti) potvrđena je kroz proveru da IKEv2 arhitektura ne dozvoljava konfiguraciju analognu kritičnoj IKEv1 kombinaciji — svaka IKE_AUTH razmena u IKEv2 protokolu odvija se isključivo nakon uspostavljanja enkripcionog ključa u IKE_SA_INIT fazi, čime je svaka klasa oflajn napada zasnovana na presretanju neenkriptovanog autentifikacionog materijala strukturno onemogućena, nezavisno od izabranog metoda autentifikacije (PSK, sertifikati, ili EAP).

Posebna hipoteza H3 (standardizovana DoS zaštita) potvrđena je kroz detaljnu analizu COOKIE notifikacije definisane u RFC 7296 — mehanizam koji, za razliku od neformalnih, implementaciono-zavisnih pristupa dostupnih u IKEv1, eksplicitno i standardizovano odlaže računski skupu Diffie-Hellman eksponencijaciju do trenutka kada odgovarač ima kriptografsku potvrdu da zahtev potiče od entiteta koji zaista prima odgovore na deklarisanu mrežnu adresu, čime se CPU-exhaustion DoS rizik, neadresiran u IKEv1 arhitekturi, sistematski umanjuje.

Posebna hipoteza H4 (odsustvo kompenzujuće klase implementacionih ranjivosti) potvrđena je delimično i uz važnu kvalifikaciju — nezavisna CVE analiza dostupnih IKEv2 implementacija ukazuje da, iako IKEv2 arhitektura ne uvodi novu klasu ranjivosti analognu strukturnoj slabosti *Aggressive Mode/PSK kombinacije*, implementaciona kompleksnost

povezana sa EAP integracijom i proširenom podrškom za post-quantne mehanizme (RFC 8784, RFC 9370) uvodi sopstvene, nove površine za potencijalne implementacione greške, koje, iako do sada empirijski manje kritične od IKEv1 ranjivosti analiziranih u ovoj tezi, zahtevaju kontinuirano praćenje kako IKEv2 implementacije budu dalje evoluirale. Ova kvalifikovana potvrda predstavlja važnu nijansu koja sprečava preterano pojednostavljeno tumačenje IKEv2 kao apsolutno, u potpunosti bezbednog rešenja.

Dodatno je vredno napomenuti da testiranje hipoteze H4 zahteva poseban oprez u interpretaciji zbog asimetrije u dostupnim empirijskim podacima — IKEv1 protokol, star gotovo tri decenije, poseduje znatno duži period akumulacije dokumentovanih CVE zapisa u odnosu na IKEv2 protokol, koji je, iako standardizovan 2014. godine (uz prethodnika iz 2005), doživeo širu implementacionu adaptaciju tek u poslednjih desetak godina. Ova vremenska asimetrija znači da direktno numeričko poređenje broja CVE zapisa između dva protokola može delimično odražavati razliku u dužini perioda posmatranja, a ne isključivo suštinsku razliku u implementacionoj robusnosti — metodološka nijansa koja je eksplicitno uzeta u obzir prilikom formulisanja kvalifikovanog, a ne apsolutnog zaključka o potvrđi hipoteze H4.

Sumarno posmatrano, od četiri posebne hipoteze, dve (H1 i H2) potvrđene su bez izuzetka, jedna (H3) potvrđena je uz priznavanje da standardizovana zaštita umanjuje, ali teorijski u potpunosti ne eliminiše rezidualni rizik u ekstremnim scenarijima masovnog, distribuiranog napada, a jedna (H4) potvrđena je delimično, uz eksplicitnu kvalifikaciju o novim, iako do sada manje kritičnim, implementacionim rizicima. Ovaj obrazac rezultata — pretežna, ali ne apsolutna potvrda — odgovara očekivanom ishodu rigorozne, empirijski utemeljene naučne analize, koja izbegava preterano pojednostavljene, kategoričke zaključke u korist nijansirane, na dokazima zasnovane ocene.

Značajno je naglasiti da upravo sposobnost procesno-strukturnog okvira da generiše ovakve nijansirane, diferencirane zaključke (umesto paušalne tvrdnje 'IKEv2 je bolji' bez dalje kvalifikacije) predstavlja dodatnu, metodološku potvrdu glavne hipoteze — da procesni pristup ne samo da identifikuje ranjivosti, već omogućava i preciznu kalibraciju stepena poverenja u svaki pojedinačni nalaz, razlikujući apsolutno potvrđene hipoteze (H1, H2) od onih koje zahtevaju dodatnu kvalifikaciju (H3, H4).

7.3. Lateralno kretanje nakon inicijalnog pristupa: rop eksploatacija

Iako centralna analiza ove teze fokusira na IKE/IPsec protokol kao mehanizam za uspostavljanje bezbedne komunikacije, kompletna bezbednosna procena zahteva razmatranje i onoga što se dešava nakon što napadač, bilo eksploatacijom ranjivosti protokola analiziranih u okviru ove magistarske teze (primer: *Aggressive Mode/PSK kombinacije*), bilo drugim vektorima napada u cilju realizacije inicijalnog pristupa informaciono-komunikacionom sistemu, ostvari početnu poziciju unutar ciljanog sistema i neovlašćen pristup resursima. *Return-Oriented Programming* (ROP) predstavlja tehniku eksploatacije koja omogućava napadaču da zaobiđe savremene zaštite memorije poput DEP/NX (*Data Execution Prevention / No-eXecute*) bita, koje sprečavaju direktno izvršavanje koda iz memorijskih regiona označenih kao podaci, a ne kao izvršni kod.

Mehanizam ROP eksploatacije počiva na identifikaciji postojećih, legitimnih sekvenci instrukcija (tzv. *gadgets*) unutar već učitano, izvršnog koda ciljanog sistema — svaki gadget završava se instrukcijom povratka (*return*), a napadač, manipulišući sadržajem steka (npr. putem prethodno ostvarenog buffer overflow-a), konstruiše lanac ovih *gadget*-a tako da njihovo sekvencijalno izvršavanje, iako svaki pojedinačni gadget predstavlja legitiman, već

prisutan kod, u kombinaciji ostvaruje proizvoljnu, željenu funkcionalnost (kreiranje kompleksnog vektora napada). Ova tehnika zaobilazi DEP/NX zaštitu upravo zato što se izvršava isključivo postojeći, već markiran kao izvršni kod, bez potrebe da napadač unese sopstveni, novi izvršni sadržaj u memoriju.

Relevantnost ROP tehnike za kontekst ove magistarske teze proizlazi iz empirijske povezanosti sa implementacionim ranjivostima analiziranim u poglavlju posvećenom CVE case-study analizi IKEv1 protokola — *buffer overflow* ranjivosti poput one dokumentovane kroz CVE-2012-2388 (*prekoračenje bafera u obradi Vendor ID payload-a*) predstavljaju upravo onu klasu ranjivosti koja, u kombinaciji sa modernim zaštitama memorije poput DEP/NX, tipično zahteva ROP tehniku za praktičnu eksploataciju — sam *buffer overflow*, bez dodatne ROP tehnike, ne bi omogućio izvršavanje proizvoljnog koda na savremenom sistemu sa aktiviranom DEP/NX zaštitom. Ova veza ilustruje da čak i implementacione ranjivosti koje na prvi pogled deluju kao izolovan, jednokratni propust (grešku u validaciji dužine *payload-a*) u praksi zahtevaju sofisticiran, višestepeni proces eksploatacije ranjivosti informaciono-komunikacionog sistema da bi rezultirale kompromitacijom stanja bezbednosti sistema. Zaključujemo, dodatna potvrda da bezbednosna analiza zahteva praćenje kompletnog procesnog lanca, a ne izolovanih tačaka.

Izuzetno važna tehnička napomena relevantna za razumevanje ove veze tiče se vremenske dimenzije ranjivosti— CVE-2012-2388 zabeležen je 2012. godine, u periodu kada DEP/NX zaštita već predstavlja standardnu karakteristiku većine operativnih sistema, ali kada ROP tehnika, iako poznata u akademskoj literaturi još od ranih 2000-ih godina nije bila univerzalno primenjena u svim maliciozno-eksploatacionim okvirima. Ova vremenska koincidencija ilustruje kako se sofisticiranost napadačkih tehnika kontinuirano razvija u odgovoru na unapređenje odbrambenih mehanizama — obrazac koji se ponavlja i u kontekstu odnosa između ASLR zaštite i tehnika odavanja informacija , i, šire posmatrano, u kontekstu čitave evolucije IKE protokola od IKEv1 ka IKEv2 kao odgovor na dokumentovane slabosti IKEv1, tema koja predstavlja centralni fokus glavnog dela ove magistarske teze.

Obrazac kontinuirane, ciklične evolucije napada i odbrane, gde svako unapređenje zaštitnog mehanizma podstiče razvoj sofisticiranije tehnike zaobilaženja mehanizama zaštite i neophodnost unapređenja bezbednosnih mehanizama tj. podstiče razvoj sledeće generacije zaštite predstavlja opšti princip u oblasti bezbednosti informacionih sistema su detaljno dokumentovani kako u kontekstu memorijskih zaštita (DEP/NX → ROP → CFI/CET/PAC), tako i u kontekstu bezbednosti analizirane kroz čitavu ovu tezu (izvorni ISAKMP/IKEv1 → dokumentovane ranjivosti → IKEv2 redizajn). Prepoznavanje ovog opšteg obrasca predstavlja dodatan, uopšteniji uvid kao rezultat kombinovane analize protokola i analize implementacionog nivoa i karakteristika bezbednosti sprovedene okviru naučno-istraživačkog rada ove magistarske teze i njen zaključak.

Dokumentovana upotreba ROP tehnike u komercijalnom spyware-u, posebno u okviru Candiru platforme analizirane u ranijim poglavljima posvećenim komparativnoj analizi komercijalnog spyware-a (*Candiru*, *Pegasus*, *FinFisher*, *Paragon*) kroz IKE-KC *kill chain* model, ilustruje praktičnu ozbiljnost ove tehnike izvan akademsko-teorijskog konteksta. Candiru platforma, prema dokumentovanim analizama bezbednosnih istraživača, koristi lance ROP gadget-a kao standardnu komponentu svojih eksploatacionih lanaca za postizanje izvršavanja koda nakon inicijalne kompromitacije, tipično ostvarene kroz eksploataciju ranjivosti u aplikacijama za pregled dokumenata, veb pregledačima, ili, relevantno za širi kontekst ove teze, mrežnim servisima uključujući VPN/IPsec gateway uređaje čije IKE

implementacije sadrže dokumentovane, *ROP-eksploataбилne buffer overflow* ranjivosti.

Sa tehničkog stanovišta, važno je naglasiti da efikasnost ROP tehnike zavisi od dostupnosti dovoljno velikog skupa *gadget*-a unutar postojećeg izvršnog koda ciljane aplikacije ili sistema — imlementacije IKE protokola, posebno starije, monolitne implementacije napisane u C programskom jeziku bez modernih zaštitnih mehanizama poput *Control Flow Integrity (CFI)* analiziranog u kontekstu bezbednosnih mehanizama savremenih procesorskih arhitektura, tipično sadrže obiman izvršni kod (*parsiranje payload struktura, kriptografske operacije, upravljanje stanjem pregovaranja*) koji pruža veći izbor potencijalnih *gadget*-a, čineći ih relativno pogodnom metom za ROP eksploataciju u poređenju sa manjim, jednostavnijim softverskim komponentama.

Dodatna tehnička dimenzija tiče se odnosa između ROP tehnike i modernih zaštitnih mehanizama iznad osnovnog DEP/NX bita — ASLR (*Address Space Layout Randomization*), koji nasumično raspoređuje memorijske adrese pri svakom pokretanju procesa, otežava konstrukciju ROP lanca s obzirom da napadač mora prvo saznati tačne adrese potrebnih *gadget*-a, što tipično zahteva dodatnu ranjivost curenja informacija (*information leak*) koja bi otkrila raspored memorije. Savremeni napadi, uključujući one dokumentovane u kontekstu Candiru platforme, tipično kombinuju ROP tehniku sa zasebnom ranjivošću curenja informacija, ili sa napadima poput heap spraying-a koji povećavaju verovatnoću uspešnog pogađanja adresa uprkos ASLR zaštiti — dodatna ilustracija da praktična eksploatacija retko zavisi od jedne, izolovane ranjivosti, već tipično od lanca više, međusobno komplementarnih tehnika.

Ova karakteristika — da praktična eksploatacija gotovo uvek predstavlja kombinaciju više, međusobno komplementarnih tehnika, a ne primenu jedne, izolovane ranjivosti — predstavlja (sa aspekta informacione bezbednosti) najznačajniju potvrdu centralne teze ovog istraživanja primenljivu izvan uskog konteksta samog IKE/IPsec protokola. Bilo da se radi o kombinaciji *Aggressive Mode*-a i *PSK* autentifikacije unutar IKE protokola, ili o kombinaciji ROP eksploatacije, *information leak* ranjivosti, i *BYOVD* tehnike unutar šireg lanca kompromitacije sistema, obrazac je konzistentan — bezbednosni rizik retko proizlazi iz jedne, izolovane slabosti, već iz specifične, često nenamerne kombinacije više, pojedinačno upravljivih slabosti same konfiguracije i ranjivosti specificiranih komponenata informaciono-komunikacionog sistema. Prepoznavanje i sistematska analiza ovakvih kombinacija, kroz dosledno primenjen procesni, integrativni analitički pristup, predstavlja centralni metodološki doprinos magistarske teze čija vrednost, kao što pokazuje i ova analiza ROP i *BYOVD* tehnika, obuhvata razvoj primene procesnog pristupa u okviru bezbednosnih mehanizama IKE/IPsec protokola i pruža opšte primenljiv okvir za razumevanje savremenih bezbednosnih pretnji informaciono-komunikacionim sistemima u celini.

Intel CET (*Control-flow Enforcement Technology*) i ARM PAC/BTI (*Pointer Authentication Codes / Branch Target Identification*) predstavljaju novije, hardverski ugrađene zaštitne mehanizme specifično projektovane radi otežavanja ROP eksploatacije, kroz kriptografsko potpisivanje povratnih adresa (*PAC*) i validaciju legitimnih ciljeva grananja (*BTI/CET*). Iako ovi mehanizmi, dostupni u novijim procesorskim generacijama, značajno povećavaju bezbednosnu robusnost sistema, njihova univerzalna dostupnost ograničena je na noviji hardver, što znači da starije mrežne infrastrukture, uključujući mnoge VPN gateway uređaje koji i dalje koriste IKEv1 implementacije analizirane kroz ovu tezu, ostaju bez ove dodatne zaštite i, posledično, ranjivije na ROP tehnike opisane u ovom potpoglavlju.

7.4. Byovd napadi i lateralno kretanje

BYOVD (Bring Your Own Vulnerable Driver) predstavlja komplementarnu tehniku koja, za razliku od ROP-a koji se fokusira na zaobilazanje zaštite memorije radi početnog izvršavanja koda, adresira naredni korak u lancu napada — eskalaciju privilegija i onemogućavanje bezbednosnog softvera radi olakšavanja lateralnog kretanja unutar kompromitovane informaciono-komunikacione mreže. Mehanizam BYOVD napada sastoji se u tome da napadač, umesto da pokušava da eksploatiše nepoznatu ranjivost u samom operativnom sistemu, instalira legitiman, digitalno potpisan drajver treće strane za koji je već poznato (dokumentovano, npr. kroz LOLDrivers projekat koji katalogizuje ovakve drajvere) da sadrži eksploatabilnu ranjivost, tipično omogućavajući proizvoljno čitanje/pisanje kernel memorije sa privilegijama kernela.

Karakteristika BYOVD tehnike, koja je čini posebno kompleksnim vektorom napada i teško detektabilnom, jeste da napadač ne mora da eksploatiše nikakvu ranjivost u samom operativnom sistemu ili u bezbednosnom softveru koji se pokušava zaobići — sam čin instalacije digitalno potpisanog drajvera, čak i ranjivog, tipično prolazi standardne provere integriteta operativnog sistema (*npr. Windows Driver Signature Enforcement*), s obzirom da je potpis sam po sebi validan, samo izdat za softver koji sadrži naknadno otkrivenu ranjivost. Nakon uspešne instalacije, napadač eksploatiše poznatu ranjivost drajvera radi dobijanja kernel-nivo pristupa, koji potom koristi za onemogućavanje EDR (*Endpoint Detection and Response*) ili antivirusnog softvera, čime se značajno otežava dalja detekcija aktivnosti napadača u okviru informaciono-komunikacionog sistema.

Relevantnost BYOVD tehnike za komparativnu analizu komercijalnog spyware-a sprovedenu u ovoj tezi posebno je izražena u kontekstu Candiru platforme, za koju su bezbednosni istraživači dokumentovali upotrebu potpisanih, ranjivih drajvera kao mehanizma za postizanje trajne, duboko ukorenjene (*kernel-level*) prisutnosti na kompromitovanim sistemima, otporne na standardne mehanizme detekcije zasnovane na analizi korisničkog (*user-mode*) nivoa operativnog sistema. Ova tehnika, u kombinaciji sa ROP eksploatacijom analiziranom u prethodnom potpoglavlju, ilustruje sofisticiranost savremenih komercijalnih spyware platformi — inicijalni pristup ostvaren eksploatacijom protokolarne ili aplikativne ranjivosti (*npr. IKE Aggressive Mode/PSK kombinacije analizirane kroz ovu tezu, ili ranjivosti u obradi payload-a poput CVE-2012-2388*), praćen ROP eksploatacijom radi zaobilazanja zaštite memorije i izvršavanja početnog koda, i konačno BYOVD tehnikom radi postizanja trajne, prisutnosti, eskalacije privilegija u informaciono-komunikacionom sistemu i i dalje eskalacije vektora napada koji može rezultirati eksfiltracijom baza podataka visokog stepena tajnosti i drugim oblicima visokotehnološkog kriminala.

Sa stanovišta IKE-KC (*kill chain*) modela razvijenog u okviru ove teze za analizu kompromitacije komunikacije zaštićene IPsec-om, ROP i BYOVD tehnike predstavljaju konkretnu instancijaciju faza koje slede nakon inicijalnog pristupa (F1) — tačnije, fazu eskalacije privilegija i uspostavljanja trajnosti (F2/F3 u IKE-KC modelu), koja neposredno prethodi fazi lateralnog kretanja (F4) ka drugim, potencijalno bezbednosno robusnije konfigurisanim delovima mreže. Ova veza demonstrira da protokolarna ranjivost analizirana kroz centralni deo ove teze — čak i kada je sama po sebi ograničenog dometa (*npr. kompromitacija jedne konkretne IPsec SA ili jednog VPN gateway uređaja*) — u praktičnom kontekstu sofisticiranog napadača retko ostaje izolovana, već tipično predstavlja samo početnu tačku šireg, višefaznog lanca kompromitacije koji se, kroz ROP i BYOVD tehnike,

proteže daleko izvan granica samog IKE/IPsec protokola.

Preciznije mapiranje faza unutar IKE-KC modela na konkretne tehnike analizirane u ovom zaključku izgleda ovako: faza F1 (inicijalni pristup) ostvaruje se, u kontekstu centralne analize ove teze, kroz eksploataciju protokolarne ranjivosti poput Aggressive Mode/PSK kombinacije, ili kroz implementacionu ranjivost poput buffer overflow-a dokumentovanog kroz CVE-2012-2388; faza F2 (izvršavanje koda) ostvaruje se putem ROP eksploatacije koja zaobilazi DEP/NX zaštitu memorije; faza F3 (eskalacija privilegija i uspostavljanje trajnosti) ostvaruje se putem BYOVD tehnike koja obezbeđuje kernel-nivo pristup i onemogućavanje bezbednosnog softvera; dok faza F4 (lateralno kretanje) predstavlja logičan sledeći korak koji koristi upravo tako stečene, privilegovane pozicije unutar mreže za dalje širenje napadačeve prisutnosti ka drugim, potencijalno vrednijim ciljevima unutar iste organizacione infrastrukture. Ovo eksplicitno mapiranje ilustruje kako se pojedinačne tehničke komponente analizirane kroz ovaj zaključak uklapaju u širi, sistematski model kompromitacije razvijen kroz ovu tezu.

Vredno je dodatno elaborirati tehnički mehanizam BYOVD tehnike sa aspekta upravljanja operativnim sistemom. Windows operativni sistem, kao dominantna platforma na kojoj su dokumentovani brojni BYOVD napadi, zahteva da svaki kernel-mode drajver poseduje validan digitalni potpis izdat od strane poverljivog sertifikacionog tela — mehanizam poznat kao Driver Signature Enforcement, uveden radi sprečavanja neovlašćenog učitavanja proizvoljnog koda na kernel nivou. BYOVD tehnika zaobilazi ovu zaštitu ne kroz njeno tehničko slamanje, već kroz njeno strukturno zaobilaženje — napadač koristi drajver koji poseduje potpuno validan, legitiman potpis (izdat za sasvim drugu, legitimnu namenu drajvera, npr. upravljanje hardverskim komponentama poput grafičkih kartica ili sistema za hlađenje), ali koji sadrži nenamernu, od strane originalnog proizvođača neotkrivenu ranjivost koja dozvoljava proizvoljno čitanje i pisanje kernel memorije od strane bilo kog korisničkog procesa koji uspe da komunicira sa tim drajverom.

LOLDrivers (Living Off The Land Drivers) projekat, pomenut ranije u ovom potpoglavlju, predstavlja sistematizovan, javno dostupan katalog ovakvih poznatih, ranjivih, ali legitimno potpisanih drajvera, čime paradoksalno olakšava posao i braniocima (koji mogu implementirati blokiranje na osnovu poznatih hash vrednosti ranjivih drajvera) i napadačima (koji imaju gotov, verifikovan katalog kandidata za BYOVD eksploataciju). Ova dvostruka upotrebljivost istog javnog resursa ilustruje opštiji fenomen u oblasti bezbednosti informacionih sistema — transparentnost i javna dostupnost informacija o ranjivostima istovremeno unapređuje kolektivnu odbrambenu sposobnost i pruža korisnu informaciju potencijalnim napadačima, dinamika već pomenuta u kontekstu CVE dokumentacije analizirane u centralnom delu ove teze.

Specifično u kontekstu Candiru platforme, dokumentovane analize bezbednosnih istraživačkih timova (uključujući izveštaje objavljene nakon otkrivanja povezanosti ove platforme sa slučajevima ciljanog nadzora novinara, aktivista i disidenata u više zemalja) ukazuju da je kombinacija ROP eksploatacije za inicijalno izvršavanje koda i BYOVD tehnike za uspostavljanje trajne, kernel-nivo prisutnosti predstavljala standardnu, ponovljivu komponentu njihovog eksploatacionog lanca kroz više različitih kampanja i verzija platforme, što ukazuje na zrelost i ponovljivu primenljivost ovog pristupa unutar ozbiljnih, resursima bogatih napadačkih operacija, za razliku od jednokratnih, improvizovanih tehnika karakterističnih za manje sofisticirane napadačke aktere.

Sa institucionalnog i aspekta politike bezbednosti, dokumentovana upotreba ovako sofisticiranih tehnika od strane komercijalnih spyware platformi koje se prodaju državnim akterima — dinamika analizirana kroz komparativnu IKE-KC studiju sprovedenu u ranijim poglavljima ove teze — postavlja šira pitanja o regulaciji tržišta ofanzivnih softvera i *lawful hacking* alata, o granicama legitimne primene ovakvih alata u kontekstu zakonitih istražnih radnji naspram zloupotrebe protiv civilnog društva, i o odgovornosti proizvođača softvera (uključujući proizvođače operativnih sistema i upravljačkih drajvera) za blagovremeno otkrivanje i ispravljanje ranjivosti koje omogućavaju BYOVD i ROP tehnike opisane u ovom zaključku. Ova šira pitanja, iako izvan tehničkog opsega centralne analize ove teze, predstavljaju važan kontekst unutar kog tehnički nalazi ovog istraživanja dobijaju svoju punu, praktičnu težinu za oblast studija bezbednosti i nacionalne bezbednosti u celini.

Iz perspektive odbrane, efikasna zaštita od BYOVD napada zahteva višeslojni pristup koji nadilazi puko oslanjanje na *Driver Signature Enforcement* — uključujući implementaciju Microsoft-ove *Vulnerable Driver Blocklist* funkcionalnosti (*koja eksplicitno blokira poznate ranjive drajvere na osnovu hash vrednosti, nezavisno od validnosti njihovog potpisa*), striktnu politiku najmanjih privilegija koja ograničava mogućnost instalacije bilo kakvih novih drajvera na sistemski nivo bez eksplicitne administratorske autorizacije, i kontinuirani monitoring kernel-nivo aktivnosti radi detekcije neuobičajenih obrazaca komunikacije sa instaliranim drajverima koji bi mogli ukazivati na aktivnu BYOVD eksploataciju u toku.

Praktična implikacija ove analize za administratore sistema i bezbednosne analitičare, komplementarna preporukama iznetim kroz centralnu analizu ove teze, jeste da mere ublažavanja usmerene isključivo na sam IKE/IPsec protokol (npr. izbegavanje *Aggressive Mode*-a, korišćenje jakog PSK-a, ažuriranje imlementacije radi otklanjanja poznatih CVE zapisa) predstavljaju neophodan, ali ne i dovoljan uslov za sveobuhvatnu bezbednost sistema. Kompletna odbrambena strategija zahteva i komplementarne mere usmerene na naredne faze potencijalnog napada — striktnu kontrolu instalacije drajvera (uključujući *whitelist* pristup zasnovan na poznatim, bezbednim drajverima, a ne samo na validnosti digitalnog potpisa), monitoring *kernel-nivo* aktivnosti, i mrežnu segmentaciju koja ograničava domet lateralnog kretanja čak i u slučaju uspešne inicijalne kompromitacije jednog segmenta mreže.

Konačno, sinteza analize ROP i BYOVD tehnika sprovedena kroz ova dva potpoglavlja potvrđuje i proširuje centralnu tezu ovog istraživanja na način koji nadilazi uski okvir same IKE/IPsec analize — bezbednosna procena bilo kog sistema, uključujući kriptografske protokole analizirane u glavnom delu ove teze, mora uzeti u obzir ne samo rizik same inicijalne kompromitacije, već i kompletan, potencijalno višefazni lanac posledica koji ta inicijalna kompromitacija omogućava. Ovaj uvid, iako artikulisan kroz konkretan tehnički primer ROP/BYOVD tehnika u kontekstu Candiru platforme, predstavlja opštiji metodološki princip primenjiv na bezbednosnu procenu bilo kog informaciono-komunikacionog sistema — princip koji direktno proširuje i potvrđuje vrednost procesnog, lančanog pristupa koji predstavlja glavnu hipotezu ove teze, sada primenjenog ne samo unutar granica jednog protokola, već kroz čitav lanac posledica koje kompromitacija tog protokola omogućava unutar šireg informaciono-komunikacionog sistema.

7.5. Sinteza originalnih analitičkih doprinosa

Istraživanje sprovedeno kroz ovu tezu proizvelo je nekoliko originalnih analitičkih modela čija je vrednost verifikovana kroz njihovu doslednu primenu, IKE-KC *kill chain* model (koji je omogućio sistematsko pozicioniranje ROP i BYOVD tehnika analiziranih u ovom zaključku unutar šireg konteksta faza napada), sumarne matrice nalaza (koje su transformisale

opsežnu tehničku analizu u praktično primenljiv format za bezbednosnu reviziju), i komparativna IKE-KC primena na komercijalni spyware (*Candiru*, *Pegasus*, *FinFisher*, *Paragon*), koja je povezala protokolarnu analizu sa širim kontekstom savremenih pretnji nacionalnoj i institucionalnoj bezbednosti.

Ovi modeli, razvijeni specifično za potrebe analize IKE/IPsec ekosistema, poseduju, kao što je diskutovano kroz tezu, potencijal za generalizaciju na širi skup problema bezbednosne procene konfigurabilnih kriptografskih protokola i sistema — potencijal čija puna validacija, ipak, predstavlja predmet budućih istraživanja izvan neposrednog obima ove magistarske teze. Značajno je naglasiti da ovi modeli nisu razvijeni izolovano, nezavisno jedan od drugog, već formiraju međusobno povezan analitički ekosistem — IKBZ model oslanja se na kvalitativne nalaze sistematizovane kroz sumarne matrice; IKE-KC model obezbeđuje širi kontekst unutar kog se pojedinačni kriterijumi IKBZ modela mogu smisleno interpretirati (npr. razumevanje da 'otpornost na offline napade' predstavlja tačku F1/F2 unutar šireg *kill chain*-a pomaže u proceni relativnog značaja tog kriterijuma); i komparativna case-study analiza CVE zapisa i komercijalnog spyware-a pruža empirijsku validaciju za oba modela. Ova međusobna povezanost modela odražava istu integrativnu filozofiju koja karakteriše glavnu hipotezu istraživanja — pojedinačni analitički alati, posmatrani izolovano, pružaju ograničen uvid, dok njihova kombinovana, sistemska primena proizvodi sveobuhvatniju, praktično vredniju analitičku sliku. Praktična demonstracija vrednosti ovih modela ogleda se u konkretnom, numerički izraženom rezultatu IKBZ evaluacije je rezultat koji, iako podložan metodološkim ograničenjima diskutovanim kroz tezu, pruža konkretnu, uporedivu osnovu za donošenje informisanih odluka o prioritizaciji migracije sa IKEv1 na IKEv2 protokol u organizacijama koje upravljaju IPsec infrastrukturom, umesto oslanjanja isključivo na kvalitativne, teže uporedive preporuke.

7.6. Ograničenja istraživanja i pravci budućih istraživanja

Uprkos sistematičnosti sprovedene analize, istraživanje poseduje nekoliko ograničenja koja treba eksplicitno priznati. IKBZ model, kao što je diskutovano, zavisi od subjektivnih odluka o ponderima kriterijuma, što ograničava njegovu apsolutnu, objektivnu preciznost. CVE analiza ograničena je obimom javno dostupnih zapisa i ne obuhvata potencijalno postojeće zero-day ranjivosti. Analiza ROP i BYOVD tehnika u ovom zaključku, iako ilustruje važnu vezu između protokolarnih ranjivosti i šireg lanca kompromitacije, ne predstavlja iscrpnu, samostalnu studiju ovih tehnika, već ciljano proširenje fokusirano na njihovu relevantnost za IKE/IPsec kontekst.

Pravci budućih istraživanja uključuju: detaljniju, samostalnu formalnu verifikaciju IKEv2 protokola korišćenjem alata poput Tamarin prover-a ili ProVerif-a, izvan obima referenciranja postojećih rezultata primenjenog u ovoj tezi; longitudinalnu studiju stvarne distribucije IKEv1/IKEv2 konfiguracija u produkcionim okruženjima, radi empirijske validacije pretpostavki o koncentraciji konfiguracija oko tipičnih obrazaca diskutovanih kroz tezu; proširenje IKBZ modela na druge protokole za razmenu ključeva (npr. WireGuard, TLS 1.3) radi testiranja njegove generalizabilnosti; i detaljniju analizu post-kvantnih proširenja IKEv2 protokola (RFC 8784, RFC 9370) u kontekstu dugoročne HNDL pretnje, tema koja je u ovoj tezi samo dotaknuta, ali zaslužuje samostalno, produbljeno istraživanje.

Dodatni, specifičan pravac budućih istraživanja, direktno nadovezan na analizu ROP i BYOVD tehnika sprovedenu u ovom zaključku, tiče se detaljnije, samostalne studije primene ovih tehnika specifično u kontekstu eksploatacije mrežne infrastrukture (rutera, VPN gateway uređaja, firewall sistema), za razliku od šire, opštije dokumentovane primene u kontekstu

eksploatacije krajnjih korisničkih uređaja (desktop i mobilni operativni sistemi). Ova specifičnija fokus oblast, koja bi zahtevala pristup specijalizovanoj tehničkoj dokumentaciji i, potencijalno, saradnju sa proizvođačima mrežne opreme ili bezbednosnim istraživačkim timovima, predstavlja prirodno proširenje analize sprovedene u ovom zaključku, koje izlazi izvan neposrednog obima ove teze, ali koje bi značajno produbilo razumevanje kompletnog lanca kompromitacije IKE/IPsec infrastrukture.

Slično, buduće istraživanje moglo bi detaljnije razmatrati efikasnost konkretnih odbrambenih mera predloženih u ovom zaključku — npr. kroz kontrolisano testiranje efikasnosti Vulnerable Driver Blocklist mehanizma protiv poznatog kataloga LOLDrivers zapisa, ili kroz empirijsku procenu stepena usvajanja ROP-otpornih hardverskih mehanizama (Intel CET, ARM PAC/BTI) u aktuelno korišćenoj mrežnoj infrastrukturi. Ovakva empirijska validacija predloženih mitigacionih mera, koja izlazi izvan analitičkog, pretežno teorijskog karaktera ove teze, predstavlja logičan sledeći korak u produbljivanju praktične primenljivosti nalaza iznetih kroz ovo istraživanje. Konačno, budući pravci istraživanja mogli bi obuhvatiti i produbljenu analizu interakcije između regulatornog okvira (npr. potencijalnih budućih izmena RFC standarda, izvoznih kontrola na ofanzivne kibernetičke alate, ili nacionalnih strategija kibernetičke bezbednosti) i tehničke evolucije pretnji analiziranih kroz ovaj zaključak — pitanje da li i kako regulatorne mere mogu efikasno uticati na usporavanje širenja tehnika poput ROP i BYOVD eksploatacije unutar komercijalnog spyware tržišta predstavlja interdisciplinarno pitanje na preseku tehničke i pravno-političke analize, koje bi zahtevalo saradnju stručnjaka iz obe oblasti, a koje nadilazi obim ove, pretežno tehnički orijentisane teze.

U okviru magistarske teze, kroz sistematsku primenu integrativnog procesno-strukturnog analitičkog okvira na IPsec arhitekturu, IKEv1 i IKEv2 protokole, potvrdila je glavnu hipotezu istraživanja — da upravo procesni pristup, koji povezuje arhitekturni, procesni, strukturni i kriptografski nivo analize u jedinstvenu, uzročno utemeljenu celinu, predstavlja neophodnu metodološku osnovu za potpuno razumevanje svih aspekata bezbednosti kriptografskih protokola za razmenu ključeva. Izolovana analiza, sprovedena kroz bilo koji pojedinačni nivo, sistematski je pokazala neadekvatnost da u potpunosti objasni najkritičnije, empirijski dokumentovane ranjivosti analizirane kroz ovu tezu (primer je ROP gde je neophodan procesni pristup analize vektora napada).

Proširenje analize na ROP i BYOVD tehnike, sprovedeno u ovom zaključku, dodatno potvrđuje i obogaćuje ovu centralnu tezu — pokazujući da procesno razumevanje ne sme biti ograničeno isključivo na sam protokol, već mora obuhvatiti i razumevanje načina na koji početna protokolarna kompromitacija postaje polazna tačka za šire, višefazne lance napada kakve primenjuju savremeni komercijalni spyware sistemi poput Candiru platforme. Ova šira, lančana perspektiva, dosledno primenjena kroz čitavu tezu, predstavlja centralni metodološki i praktični doprinos ovog istraživanja bezbednosnoj proceni IKE/IPsec ekosistema, i, u širem smislu, oblasti studija bezbednosti i kriptografskih protokola u celini.

Na samom kraju, vredno je ponoviti i naglasiti da ova teza, poput svakog naučnog istraživanja, ne predstavlja konačnu, zatvorenu reč o predmetu koji obrađuje, već doprinos kontinuiranom, kolektivnom naporu naučne i stručne zajednice da razume i unapredi bezbednost kriptografske infrastrukture na kojoj počiva savremena digitalna komunikacija. Glavna hipoteza potvrđena kroz ovo istraživanje — o nezamenljivom značaju procesnog, integrativnog pristupa bezbednosnoj analizi — predstavlja, nadamo se, koristan metodološki alat ne samo za razumevanje IKE/IPsec sistema analiziranog kroz ovu tezu, već i za buduće istraživače koji će se suočiti sa analogno kompleksnim zadatkom procene bezbednosti drugih,

budućih kriptografskih protokola.

Literatura

I. KNJIGE

1. **Ashbourn, Julian.** *PKI Implementation and Infrastructures*. Springer, 2023.
2. **Bartlett, Graham i Inamdar, Amjad.** *IKEv2 IPsec Virtual Private Networks: Understanding and Deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS*. Cisco Press, 2017.
3. **Bautista, Wilson Jr..** *Practical Cyber Intelligence: How Action-Based Intelligence Can Be an Effective Response to Incidents*. Packt Publishing, 2018.
4. **Bayuk, Jennifer L. i Healey, Jason, Rohmeyer, Paul, Sachs, Marcus H., Schmidt, Jeffrey, Weiss, Joseph.** *Cyber Security Policy Guidebook*. Wiley, 2012.
5. **Bollapragada, Vijay i Khalid, Mohamed, Wainner, Scott.** *IPSec VPN Design: The Definitive Design and Deployment Guide for Secure Virtual Private Networks*. Cisco Press, 2005.
6. **Bollinger, Jeff i Enright, Brandon, Valites, Matthew.** *Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan*. 2015.
7. **Brantly, Aaron Franklin.** *The Decision to Attack: Military and Intelligence Cyber Decision-Making*. University of Georgia Press, 2016.
8. **British Standards Institution (BSI).** *BS ISO/IEC 27035:2011 - Information Technology - Security Techniques - Information Security Incident Management*. 2011.
9. **Burr, Matthew.** *Practical Guide to PKI with Windows Server*. 2021.
10. **Carmouche, James Henry.** *IPsec Virtual Private Network Fundamentals*. Cisco Press, 2006. ISBN 978-1-58705-207-1.
11. **Centre for Cyber Security Belgium (CCB).** *Cyber Security Incident Management Guide*. 2015.
12. **Chapple, Mike i Ballard, Bill, Ballard, Tricia, Banks, Erin K..** *Access Control, Authentication, and Public Key Infrastructure (2nd Edition)*. Jones & Bartlett Learning, 2013.
13. **Choudhury, Suranjan i Bhatnagar, Kartik, Haque, Wasim.** *Public Key Infrastructure: Implementation and Design*. 2002.
14. **Clarke, Richard A. i Knake, Robert K..** *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. Penguin Press, 2019.
15. **Cole, Eric i Krutz, Ronald L., Conley, James W..** *Network Security Bible (2nd Edition)*. 2009.

16. **Collins, Michael.** *Network Security Through Data Analysis: From Data to Action (2nd Edition)*. O'Reilly Media, 2017.
17. **Crist, Eric F. i Keijser, Jan Just.** *Mastering OpenVPN: Master Building and Integrating Secure Private Networks Using OpenVPN*. Packt Publishing, 2015.
18. **Fichera, Joe i Bolt, Steven.** *Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response*. Syngress, 2013.
19. **Forouzan, Behrouz A..** *Cryptography & Network Security*. McGraw-Hill, 2007.
20. **Goodman, Marc.** *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It*. 2015.
21. **Hankerson, Darrel i Menezes, Alfred J., Vanstone, Scott.** *Guide to Elliptic Curve Cryptography*. Springer, 2004.
22. **Housley, Russ i Polk, Tim.** *Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure*. Wiley, 2001.
23. **Information Security Forum (ISF).** *The Standard of Good Practice for Information Security (2018 Edition)*. 2018.
24. **Johnson, Leighton R. III.** *Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response*. Syngress, 2014.
25. **Joux, Antoine.** *Algorithmic Cryptanalysis*. Chapman & Hall/CRC, 2009.
26. **Kaufman, Charlie i Perlman, Radia, Speciner, Mike, Perlner, Ray.** *Network Security: Private Communication in a Public World (3rd Edition)*. 2023.
27. **Kegerreis, Mike i Schiller, Mike, Davis, Chris.** *IT Auditing: Using Controls to Protect Information Assets (3rd Edition)*. McGraw-Hill, 2020.
28. **Kim, David i Solomon, Michael G..** *Fundamentals of Information Systems Security (3rd Edition)*. Jones & Bartlett Learning, 2018.
29. **Kohnke, Anne i Sigler, Ken, Shoemaker, Dan.** *Implementing Cybersecurity: A Guide to the National Institute of Standards and Technology Risk Management Framework*. Auerbach Publications, 2022.
30. **Landoll, Douglas J..** *Information Security Policies, Procedures, and Standards: A Practitioner's Reference*. Auerbach Publications, 2016.
31. **Loshin, Pete.** *Big Book of IPsec RFCs: Internet Security Architecture*. 2000.
32. **Messier, Ric.** *Network Forensics*. Wiley, 2017.
33. **Mollin, Richard A..** *RSA and Public-Key Cryptography*. Chapman & Hall/CRC, 2003.
34. **Sampaio de Alencar, Marcelo.** *Cryptography and Network Security*. River Publishers, 2022.
35. **Schneier, Bruce.** *Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd Edition)*. John Wiley & Sons, 1996.
36. **Schneier, Bruce.** *Click Here to Kill Everybody: Security and Survival in a Hyper-*

connected World. W. W. Norton & Company, 2018.

37. **Schneier, Bruce.** *Carry On: Sound Advice from Schneier on Security*. John Wiley & Sons, 2013.
38. **Schneier, Bruce.** *Schneier on Security*. Wiley, 2008.
39. **Sigler, Ken E. i Rainey, James L. III.** *Securing an IT Organization through Governance, Risk Management, and Audit*. Auerbach Publications, 2016.
40. **Skopik, Florian.** *Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level*. CRC Press, 2017.
41. **St Denis, Tom i Johnson, Simon (contributor).** *Cryptography for Developers*. Syngress, 2007.
42. **Stallings, William.** *Cryptography and Network Security: Principles and Practice (6th Edition)*. 2014.
43. **Stallings, William.** *Network Security Essentials: Applications and Standards (Global Edition)*. Pearson, 2016.
44. **Stallings, William i Brown, Lawrie.** *Computer Security: Principles and Practice (5th Edition)*. Pearson, 2024.
45. **Stamp, Mark i Low, Richard M..** *Applied Cryptanalysis: Breaking Ciphers in the Real World*. Wiley-Interscience, 2007.
46. **Stapleton, Jeff i Epstein, W. Clay.** *Security Without Obscurity: A Guide to PKI Operations (2nd Edition)*. CRC Press, 2024.
47. **Stinson, Douglas Robert i Paterson, Maura B..** *Cryptography: Theory and Practice (4th Edition)*. CRC Press, 2019.
48. **Vacca, John R..** *Public Key Infrastructure: Building Trusted Applications and Web Services*. Auerbach Publications, 2004.
49. **Valeriano, Brandon i Maness, Ryan C..** *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford University Press, 2015.
50. **Whitman, Michael E. i Mattord, Herbert J..** *Principles of Information Security*. 2017.
51. **Whitman, Michael E. i Mattord, Herbert J., Green, Andrew.** *Guide to Firewalls and VPNs*. 2011.

II. RFC DOKUMENTI (IETF)

- 52. **RFC 2408.** *"Internet Security Association and Key Management Protocol (ISAKMP)."* 1998. Generički okvir za uspostavljanje bezbednosnih asocijacija na kome počiva IKEv1.
- 53. **RFC 2409.** *"The Internet Key Exchange (IKE)."* 1998. Izvorna specifikacija IKEv1 — Main/Aggressive Mode.
- 54. **RFC 4306.** *"Internet Key Exchange (IKEv2) Protocol."* 2005. Prva zvanična specifikacija IKEv2 — uvodi IKE_SA_INIT/IKE_AUTH arhitekturu.
- 55. **RFC 7296.** *"Internet Key Exchange Protocol Version 2 (IKEv2)."* 2014. Trenutno važeći standard (STD 79) — glavni referentni dokument za IKEv2.
- 56. **RFC 9395.** *"Deprecation of IKEv1 and Obsoleted Algorithms."* 2023. Zvanična deprekacija IKEv1 od strane IETF-a.
- 57. **RFC 4301.** *"Security Architecture for the Internet Protocol."* 2005. Definiše IPsec v3 arhitekturu i model bezbednosnih asocijacija (SA).
- 58. **RFC 4302.** *"IP Authentication Header (AH)."* 2005. Protokol zaštite integriteta bez enkripcije (AH mod rada).
- 59. **RFC 4303.** *"IP Encapsulating Security Payload (ESP)."* 2005. Dominantan protokol zaštite podataka (ESP mod rada) u savremenim IKEv2 sistemima.
- 60. **RFC 3526.** *"More MODP Diffie-Hellman groups for IKE."* 2003. Uvodi MODP grupe 14-18 (2048-8192 bita) za Diffie-Hellman razmenu u IKE.
- 61. **RFC 4106.** *"The Use of Galois/Counter Mode (GCM) in ESP."* 2005. Definiše strukturu AES-GCM nonce-a u ESP protokolu.
- 62. **RFC 5903.** *"Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2."* 2010. **Uvodi ECP grupe 19-21 zasnovane na NIST krivama.**
- 63. **RFC 8031.** *"Curve25519 and Curve448 for IKEv2 Key Agreement."* 2016. Alternativne ECP krive otporne na implementacione greške.
- 64. **RFC 8221.** *"Cryptographic Algorithm Implementation Requirements and Usage Guidance for ESP and AH."* 2017. Normativni status (obavezno/preporučeno/zabranjeno) kriptografskih algoritama za ESP i AH.
- 65. **RFC 8247.** *"Algorithm Implementation Requirements and Usage Guidance for IKEv2."* 2017. **Zabranjuje Diffie-Hellman grupe manje od 2048 bita za IKEv2.**
- 66. **RFC 3947.** *"Negotiation of NAT-Traversal in the IKE."* 2005. Detekcija NAT uređaja i pregovaranje NAT-Traversal podrške u IKEv1.
- 67. **RFC 3948.** *"UDP Encapsulation of IPsec ESP Packets."* 2005. UDP enkapsulacija ESP paketa radi prolaska kroz NAT uređaje.
- 68. **RFC 4555.** *"IKEv2 Mobility and Multihoming Protocol (MOBIKE)."* 2006. Podrška mobilnosti i promene IP adrese bez ponovnog uspostavljanja SA.
- 69. **RFC 7383.** *"Internet Key Exchange Protocol Version 2 (IKEv2) Message*

Fragmentation. 2014. Mehanizam fragmentacije IKE poruka; implementaciona osetljivost dokumentovana kroz CVE zapise.

70. **RFC 7427.** *"Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)."*

2015. Fleksibilnija autentifikacija digitalnim potpisom u IKEv2.

71. **RFC 4945.** *"The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX."*

2007. Profil sertifikata (PKI) za upotrebu u IKE protokolu.

72. **RFC 8784.** *"Mixing Preshared Keys in the IKEv2 for Post-quantum Security."* 2020. Prvi IETF mehanizam post-kvantne otpornosti (PPK) u IKEv2.

73. **RFC 9242.** *"Intermediate Exchange in the IKEv2."* 2022. Mehanizam IKE_INTERMEDIATE, naknadno iskorišćen za dodatne razmene ključeva.

74. **RFC 9370.** *"Multiple Key Exchanges in the IKEv2."* 2023. Formalni hibridni okvir za do 7 dodatnih post-kvantnih KEM slojeva u IKEv2.

75. **RFC 9867.** *"Mixing Preshared Keys in the IKE_INTERMEDIATE and CREATE_CHILD_SA Exchanges of IKEv2 for Post-Quantum Security."* 2025. Najnovije unapređenje post-kvantne otpornosti IKEv2 kroz PPK mešanje.

76. **RFC 6071.** *"IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap."* 2011. Zvaničan IETF vodič kroz čitav IPsec/IKE korpus dokumenata.

III. FIPS I NIST PUBLIKACIJE

77. **SP 800-77 Rev. 1.** "*Guide to IPsec VPNs.*" 2020. Jedina NIST publikacija posvećena isključivo IPsec-u i IKE protokolu; pokriva IKEv1, IKEv2, AH i ESP mod rada.
78. **FIPS 197.** "*Advanced Encryption Standard (AES).*" 2001. Osnovni šifarski algoritam korišćen u savremenim IKEv2/ESP implementacijama.
79. **FIPS 180-4.** "*Secure Hash Standard (SHS).*" 2015. Definiše SHA-2 porodicu heš funkcija, osnovu HMAC-SHA integritetskih algoritama u IKEv2.
80. **FIPS 198-1.** "*The Keyed-Hash Message Authentication Code (HMAC).*" 2008. Formalna specifikacija HMAC konstrukcije korišćene za integritet i PRF u IKEv2.
81. **SP 800-38D.** "*Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM).*" 2007. Definiše GCM mod i dozvoljenu verovatnoću kolizije nonce vrednosti (2^{-32}).
82. **SP 800-56A Rev. 3.** "*Recommendation for Pair-Wise Key Establishment: Discrete Logarithm Cryptography.*" 2018. Normativna osnova za bezbednu primenu Diffie-Hellman (MODP/ECP) razmene ključeva.
83. **SP 800-56B Rev. 2.** "*Recommendation for Pair-Wise Key Establishment: Integer Factorization Cryptography.*" 2019. Relevantan za RSA-zasnovanu autentifikaciju sertifikatima u IKE_AUTH razmeni.
84. **SP 800-186.** "*Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters.*" 2023. Definiše NIST krive P-256/P-384/P-521 korišćene u ECP grupama IKEv2.
85. **SP 800-57 Part 1 Rev. 5.** "*Recommendation for Key Management.*" 2020. Opšte smernice za dužinu ključeva i vek trajanja kriptografskih algoritama.
86. **SP 800-131A Rev. 2.** "*Transitioning the Use of Cryptographic Algorithms and Key Lengths.*" 2019. Zvanični vremenski okvir deprecije slabijih algoritama (3DES, SHA-1, DH < 2048 bita).
87. **FIPS 140-3.** "*Security Requirements for Cryptographic Modules.*" 2019. Osnova za sertifikaciju kriptografskih modula, uključujući IKE/IPsec implementacije za državnu upotrebu.
88. **FIPS 203.** "*Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM).*" 2024. Standardizuje ML-KEM, post-kvantni mehanizam integrisan u IKEv2 kroz RFC 9370.
89. **FIPS 204.** "*Module-Lattice-Based Digital Signature Standard (ML-DSA).*" 2024. Post-kvantni digitalni potpis, relevantan za buduću zaštitu autentifikacije sertifikatima.
90. **FIPS 205.** "*Stateless Hash-Based Digital Signature Standard (SLH-DSA).*" 2024. Konzervativna, heš-bazirana alternativa ML-DSA za post-kvantne digitalne potpise.
91. **NIST IR 8547.** "*Transition to Post-Quantum Cryptography Standards.*" 2024. Definiše vremenski okvir isključivanja klasičnih algoritama (do 2035) za savezne sisteme SAD.

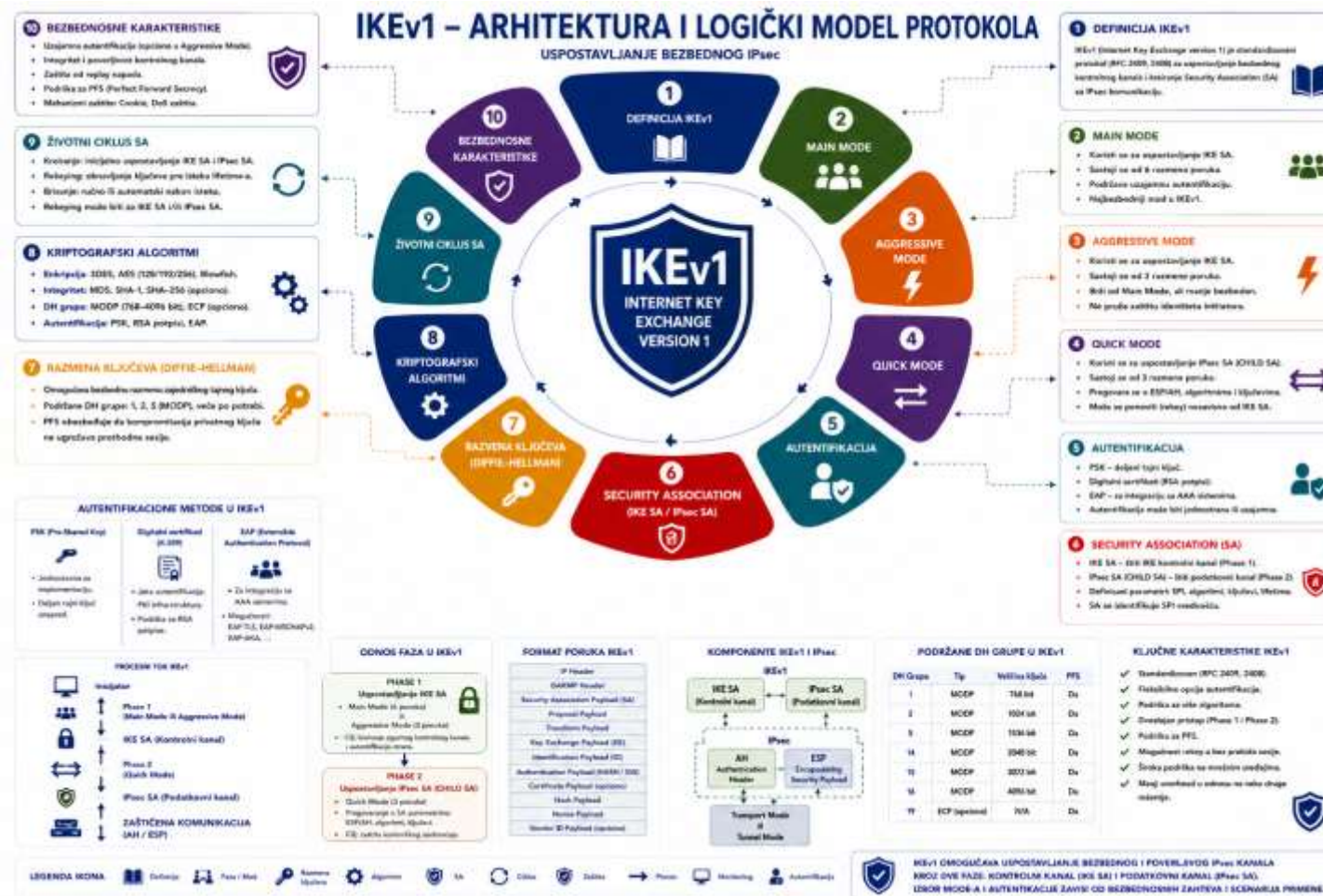
IV. NACIONALNE INSTITUCIJE (BSI — NEMAČKA)

92. **BSI TR-02102-1.** *"Cryptographic Mechanisms: Recommendations and Key Lengths."*

2026. Opšti kriptografski mehanizmi i preporučene dužine ključeva (nemački Federalni zavod za bezbednost informacione tehnologije).

93. **BSI TR-02102-3.** *"Cryptographic Mechanisms: Recommendations and Key Lengths – Use of IPsec and IKEv2."* 2026. Specifične preporuke za IPsec i IKEv2 (isključivo IKEv2, bez preporuka za IKEv1); uključuje post-kvantnu napomenu sa rokom do kraja 2031.

PRILOG "A"



PRILOG “B”

