UNIVERZITET SINGIDUNUM

-MASTER STUDIJSKI PROGRAM-
SAVREMENE INFORMACIONE TEHNOLOGIJE

Bezbednost računarskih mreža

- Master rad -

Mentor:
Prof. dr. Mladen Veinović

Student:
Raško Marković
Br. indeksa: 2013/410660

Univerzitet Singidunum

Beograd

S A D R Ž A J :

UVODNA RAZMATRANJA 5
1. Uvod 5
KLJUČNA RAZMATRANJA 7
1. Principi računarskih telekomunikacija 7
1.1. Osnovni elementi računarskih komunikacija 7
1.2. Prenos podataka 8
1.3. Protokoli 10
1.4. Kategorizacije računarskih mreža 12
2. Sigurnosne arhitekture i modeli 13
2.1. Osnove sigurnosnih arhitektura 13
2.1.1. Zaštitni mehanizmi 13
2.1.2. Apstrakcija i koncept skrivanja informacija: 14
2.1.3. Domeni zaštite i zaštitni prstenovi 14
2.1.4. Sigurnosne oznake: 16
2.1.5. Sigurnosni režimi: 16
2.1.6. Distribuirane arhitekture 17
2.1.7. Ranjivosti u sigurnosnoj arhitekturi i procedure oporavka 18
2.1.8. Procedure oporavka: 19
2.1.9. Kriterijumi ocenjivanja: 20
2.2. DITSCAP I NIACAP: 22
3. Osnovne bezbednosti u računarskim mrežama: 23
3.1. Neki tipovi i modeli napada: 23
3.1.1. Kriptoanaliza: 24
3.1.2. Razbijanje šifrata primenom sirove sile: 24
3.1.3. Napad posredovanjem u komunikaciji: 27
3.1.4. Napad uskraćivanjem usluge: 28
3.2. Popularni sistemi za zaštitu komunikacije: 30
3.2.1. Zaštita na nivou aplikativnog protokola: 30
3.2.1.1. Zaštita elektronske pošte: 31
3.2.2. Zaštita na nivou transportnog protokola: 34
3.2.3. Zaštita na nivou mrežnog protokola 35
3.2.3.1. Internet Protocol Security sistem zaštite 36
3.2.3.1.1. Režimi rada 37
3.2.3.1.2. Protokol Authentication Header 37

3.2.3.1.3. Protokol Encapsulationg Security Payload 38
3.2.3.1.4. Implementacija IPsec protokola 39
3.2.3.1.5. Internet Key Exchange protokol 40
3.2.4. Firewall (Fajervol) 41
3.2.5. Sistemi za otkrivanje i sprečavanje napada 42
3.3. Standardni šifarski algoritni 43
3.3.1. Advanced Encryption Standard, AES 44
3.3.2. Data Encryption Standard (DES, 3DES) 45
3.3.3. RSA 46
3.4. Trendovi 47
4. Pretnje, napadi, sigurnost i metode zaštite 48
4.1. Napadi i pretnje 48
4.1.1. Modelovanje pretnji 53
4.1.2. Najčešće primenjivani napadi i pretnje 54
4.2 Šta je sigurnost 55
4.2.1 Sigurnosni ciljevi: 57
4.2.2. Sigurnosne usluge 58
4.2.3. Strategije ostvarivanja sigurnosti 59
4.2.4. Slojevita zaštita 60
4.2.5. Sigurnosni modeli: 61
4.2.6. Klasifikovanje informacija 62
4.2.6.1. Klasifikovanje tajnosti informacija: 63
4.2.6.2. Drugi načini klasifikacije: 64
4.3. Metode zaštite: 65
4.4. Različiti aspekti zaštite: 66
4.5. Primeri: 67
4.6. Pristup organizacije (ISC)2: 68
4.7. Projektovanje sistema zaštite: 69
5. Nadzor računarskih mreža: 71
5.1. Uvodne napomene: 71
5.2. Simple Network Management Protocol (SNMP): 71
5.2.1. Razvoj protokola SNMP: 73
5.2.2. Delovi sistema za upravljanje mrežom: 74
5.2.3. Management Information Base (MIB): 75
5.2.4. Opis rada protokola SNMP: 75
5.2.5. Posrednički SNMP agent - proksi konfiguracija: 76
5.2.6. SNMPv3: 77
5.3. Alati za nadzor mreža: 78
5.3.4 Nadzor na operativnim sistemima Windows: 79
6.1. Organizacione metode zaštite: 81

6.1.1. Kadrovski aspekti: 81
6.1.2. Analiza rizika i upravljanje njime: 83
6.1.2.1. Analiza rizika: 83
6.1.2.2. Upravljanje rizikom: 85
6.2. Fizičke metode zaštite: 85
6.2.1. Pretnje po fizičku sigurnost: 85
6.2.2. Mere zaštite: 86
6.2.3. Biometrija 86
6.2.3.1. Biometrija zasnovana na fizičkim kakrakteristikama: 87
6.2.3.3. Biometrija, fizička sigurnost i privatnost: 90
ZAKLJUČNA RAZMATRANJA 91
LITERATURA: 92

UVODNA RAZMATRANJA

1. Uvod:

U ranijim fazama razvoja tehnologija na kojima se baziraju računarske mreže fokus je bio postavljen na omogućavanje što veće brzine prenosa podataka sa što manjom verovatnoćom greške. Mala baza korisnika, sastavljena uglavnom od tehnički obrazovanih korisnika, i retke praktične primene omogućile su brz razvoj tehnologija i dovele računarske mreže do potencijala kojim prete da u potpunosti zamene ostale popularne sisteme komunikacije kao što su telefonija i televizija. Međutim, rastom popularnosti računarske mreže su izašle iz čisto tehničko - tehnološkog domena i sve više na njihov razvoj i primenu imaju ekonomski i socijalni faktori.

Najveća račuarska mreža današnjice je internet koja ima milione korisnika zahvaljujući mnogim servisima koji nudi svojim korisnicima razne vrste usluga, čak se obavljaju online sastanci i finansijske transakcije, prenosi se dosta državnih a i ostalih bitnih informacija. Računarska mreža prenosi više informacija u današnje vreme nego što su telefon i televizor ikada prenosili. Problem kod tolikog protoka informacija je ujedno rizik koji je srazmeran lakoći prenosa tih istih bitnih informacija, a cilj računarskih mreža je eliminisati taj rizik ili ga smanjiti što je više moguće sa datim resursima. Rešenja sigurnosti i zaštićenosti podataka unutar neke velike mreže računara su uglavnom kompleksna ali nekad mogu biti i jednostavna instaliranjem uredjaja koji sam automatski rešava date probleme uz malo monitoringa.

Greške koje se javljaju na računarskim mrežama i kod resursa koji su putem njih dostupni možemo podeliti u četiri kategorije na osnovu uzroka njihovog pojavljivanja:

1. Greške koje se pojavljuju usled propusta u definiciji hardveskih i softverskih komponenti računarskih mreža,
2. Greške koje se javljaju kod posledica neadekvatnog dizajniranja računarskih mreža i nenamenske upotrebe korišćenih komponenti,
3. Greške koje se javljaju usled neadekvatnog korišćenja računarskih mreža od strane korisnika nedovoljno obučenih za rad,
4. Greške koje se javljaju kao posledica iskorišćenja propusta u definiciji hardverskih/softverskih komponenti računarskih mreža, njihovom dizajnu i (ne)pažnji

korisnika može se iskoristit od strane zlonamernih korisnika i u cilju ostvarivanja određene koristi od napada na računarsku mrežu ili resurs.

Greške gore pomenutih kategorija mogu imati razne vrste posledica na mrežu od kojih neke mogu biti i katastrofalne po mrežu. Ovaj rad se bavi napadima na računarske mreže, tipovima napada i merama koje se mogu preduzeti protiv toga.

KLJUČNA RAZMATRANJA

1. Principi računarskih telekomunikacija:

Računarske telekomunikacije predstavljaju jedan od oblika komunikacija, odnosno komunikaciju na daljinu ostvarenu putem korišćenja računara. Iako se često uzimaju za jedan od najsavremenijih rezultata razvoja razvoja civilizacije, one ne rešavaju nijedan od suštinskih problema vezanih za komunikaciju već predstavljaju strogo tehnološki napredak. Ipak, takav napredak je posredno doveo do mnogih napredaka u oblastima nevezanim za računarske tehnologije, kao i do određenih sociooloških, kulturoloških i drugih fenomena.

Osnovni principi računarskih telekomunikacija uslovljeni su principima vezanim za komunikaciju uopšte i principima vezanim za računarstvo uopšte. U ovom poglavlju su predstavljeni osnovni principi računarskih telekomunikacija, prvenstveno sa aspekta principa računarskih sistema i tehnologija za komunikaciju na daljinu.

1.1. Osnovni elementi računarskih komunikacija:

Kao osnovni elementi računarske mrežne komunikacije mogu se izdvojiti:

- Korisničke aplikacije
- Hardver računara,
- Operativni sistem,
- Komunikacioni vod

Kod direktne komunikacije između računara svi učesnici poseduju navedene elemente, osim u slučajevima kada komunikacija počinje i završava se na nivou operativnog sistema ili jednog računara, ili kada je komunikacija na nivou mrežnog hardvera. Međutim u drugim

slučajevima komunikacija može biti posredna i odvijati se preko nekih jednostavnijih mrežnih uređaja, koji se često sastoje od hardvera sa ugrađenim funkcijama i interfejsima ili preko više složenijih mrežnih uređaja koji u sebi sadrže specijalizovane mrežne operativne sisteme.

Komunikacioni vodovi i drugi elementi koji ih povezuju u računarskim mrežama sa mrežnim interfejsima uređaja ili računara nazivaju se vrstom pasivne opreme. Uređaji koje koristimo u mreži a koji u sebi sadrže i firmver ili neku vrstu softeva sposobnu za analize i promene iliti modifikacije nosećih signala pripadaju aktivnoj mrežnoj opremi. Komunikacija se vrši između uređaja po pravilima koja se nazivaju protokoli.

Uspešne komunikacije izmedju članova mreže koji se nalaze na krajevima same mreže zahtevaju obezbeđenu funkcionalnost na svim komunikacionim nivoima. Komunikacije neće biti moguća izmedju tih računara ako računari nemaju dovoljno hardverske i softverske podrške.

Sledeće komponente čine pasivnu mrežnu opremu, opremu koja nema uticaj na mrežu osim na samu fizičku povezanost mreže:

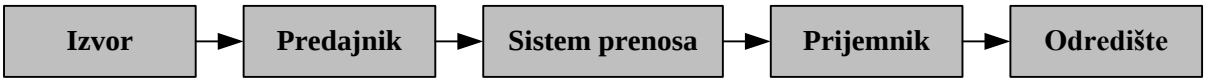
- Rek ormani,
- Kablovi,
- Patch paneli,
- Patch kablovi,
- Kanalice,
- Utičnice

1.2. Prenos podataka:

Računarska mreža je vrsta sistema komunikacije gde se informacije generisane na jednoj strani dostavljaju drugoj strani iliti od izvora do željenog odredišta.Osnovni elementi jednog takvog sistema su:

- Izvor –mesto odakle se generišu podaci
- Predajnik –transformiše podatke ili signale u željen oblik koji je pogodan za prenošenje
- Prenosni sistem –nekad je prost pravolinijski put nekad može komplikovana mreža
- Prijemnik –uzima dostavljen signal i vraća ga iz predajnikove transformacije u željen oblik

- Odredište-mesto na kraju puta koje prihvata podatke kada prijemnik završi sa konvertovanjem.



Slika 1. Model komunikacionog sistema

Ključni poslovi u komunikacionom sistemu su:

- Povezivanje uređaja na komunikacioni sistem,
- Generisanje signala –stvaranje signala i uslova komunikacije
- Sinhronizacija predajnika i prijemnika,
- Razmena podataka prema odgovarajućim protokolima,
- Otkrivanje i ispravljanje grešaka prilikom slanaja datoteka
- Kontrola toka - usaglašavanje brzine slanja i brzine prijema podataka,
- Adresovanje i usmeravanje – dodeljivanje adresa izmedju više učesnika
- Oporavak - mogućnost nastavka transfera podataka od mesta prekida
- Formatiranje podataka – predvidja dužinu podataka izmedju izvora i odredišta
- Zaštita na prenosnom putu provera autentičnost podataka i održava
- Upravljanje mrežom – mreža uglavnom nije prosta vrsta sistema ona zahteva održavanje i konfigurisanje različitih uredjaja prema budućim namenama.

1.3. Protokoli:

Protokoli predstavljaju pravila za prenos podataka i standard za ostvarivanje veze i kontrolu veze kao i prenos podataka između dva računara, dve firme iliti dve krajnje destinacije. Protokolima se obavlja prenos podataka kroz mrežu, oni su ujedno i pravila koja su poznata svim učesnicima u mreži. Protokol koji predstavlja skup pravila za signalizaciju, kontrolu grešaka i proveru autentičnosti se naziva komunikacioni protokol. Ključni elementi protokola kojim se dogovara spremnost za slanje, spremnost za prijem, format podataka i sl. su:

1. Semantika
2. Tajming
3. Sintaksa

Razmena podataka u računarskoj mreži je izuzetno složena. Kada je u pitanju veliki broj umreženih računara koji komuniciraju povećava se i broj zahteva za usavršenijim uslugama i servisima, ujedno je neophodno i usavršavanje protokola a i cele opreme koja radi sa njim. Svaki sloj protokola je napravljen sa određenom funkcijom i određenim poslom koji treba da radi.Većina umrežavanja je bila rešena od strane jednog proizvodjača u prošlosti. Uvođenje standarda za celu mrežnu opremu je dovelo to toga da se više proizvođača pojavi na tržištima širom sveta. Standardi omogućuju kombinovanje različitih proizvodjača softvera i hardvera ali to i dalje ne radi u praksi dobro kao što bi trebalo u teoriji i po datim reklamnim materijalima.

Jedna od važnijih stvari kod umrežavanje je pravilno odrađeno adresovanje unutar mreže. Ako posmatramo mrežu od svega dva računara tu nema potrebe za adresovanjem jer će informacije biti poslate na drugi računar kome su i namenjene bez nekih većih problema. Kada je više računara sa istim adresama dešava se da se informacije šalju deo po deo pri čemu nikad ne stignu svi delovi na jedan računar nego budu podeljene na više računara. U većim mrežama adresovanje je jedna od najbitnih stvari jer utiče na brzinu informacija a ujedno i na primanje informacija od strane željenog primaoca,u prevodu ako se pošalju željene informacije postoji rizik da sve informacije ne stignu na namenjenu lokaciju.

Protokol izvršava sledeće stvari na predajnom računaru:

- Deli podatke u manje celine, nazvani paketi, koje može da obrađuje,
- Paketima dodaje adresne informacije tako da odredišni računar na mreži može da odluči da li oni pripadaju njemu,
- Priprema podatke za prenos kroz mrežnu karticu i dalje kroz mrežni kabl.
- Na prijemnom računaru protokoli sprovode isti niz koraka, ali obrnutim redosledom:
- Preuzimaju se podaci sa kabla,
- Kroz mrežnu karticu unose se paketi podataka u računar,
- Iz paketa podataka uklanjaju se sve informacije o prenosu koje je dodao predajni računar,
- Kopiraju se podaci iz paketa u prihvatnu memoriju (bafer) koja služi za ponovno sklapanje i
- Ponovno sklopljeni podaci prosleđuju se aplikacije u obliku koji ona može da koristi.[21]

Osnovne stvari u dizajnu protokola su pouzdanost, efikasnost i prilagodljivost. U slučaju slanja i primanja podataka potrebno je da primaoc i pošiljalac svaki korak izvedu na isti načina kako bi podaci ostali u formi kao pre slanja. U jednoj računarskoj mreži je poželjno da više protokola rade kao tim zajedno. Zajednički rad podataka obezbeđuje ispravnu pripremu podataka kao i prenos do odredišta. Ako rad više protokola nije usaglašen događaće se nekompletne operacije ili će biti dostavljena dokumenta koja nema dovoljan broj bajtova iliti polomljene fascikle.

Uspostavljanje veze, prenos podataka i raskid veze određeni su setom protokola od kojih je svaki nadležan za jedan od sledećih poslova:

- *Handshaking* - uspostavljanje veze,
- Pregovaranje o različitim karakteristikama veze,
- Definisanje početka i kraja poruke,
- Definisanje formata poruke,
- Definisanje pravila za obradu oštećenih ili nepravilno formatiranih poruka (ispravka grešaka),
- Utvrđivanje neočekivanog prekida veze i definisanje daljih koraka u tom slučaju,
- Prekid veze .[21]

1.4. Kategorizacije računarskih mreža:

U današnje vreme postoji više vrsta mreža i više pravila po kojima se mreže prave, realizuju i koriste. Računarske mreže su postale jedan od glavnih komunikacionih delova jedne organizacije ili čak poslovno orjentisanih objekata, što je doprinelo ozbiljnijem shvatanju rešavanja raznih problema i njihovom rešavanju u mrežama. Interesovanje za poboljšavanjem mreža je raslo kada i njihova upotreba. Računarske mreže imaju više podela.

U skladu sa medijumom koji se koristi za prenos podataka računarske mreže mogu biti:

1. Kablirane mreže
2. Bežične mreže.

Po topologiji računarske mreže mogu da imaju podelu:

1. Topologijom magistrale,
2. Topologijom zvezde,
3. Topologijom prstena,
4. Kombinovanom topologijom.

Po vremenskoj postojanosti računarske mreže mogu biti:

1. Fiksne
2. Privremene.

Po prostoru na kome se prostiru računarske mreže mogu biti:

1. (MAN)- Metropolitan Area Network,
2. (WAN)- Wide Area Network
3. (LAN)- Local Area Network,
4. (PAN)- Personal Area Network,
5. (Internet)

Po arhitekturi (funkcionalnom odnosu članova) računarske mreže mogu biti:

1. *Host-based*,
2. Klijent-server i
3. *Peer-to-peer*.

Po specifičnoj funkciji koju obavljaju računarske mreže mogu biti:

1. *Storage area network*,
2. *Server farm network*,
3. *Process control network*,
4. *Value added network*,
5. *SOHO network*,
6. *Wireless community network* i
7. *XML appliance network*.

Treba imati u vidu da su računarske mreže jedna dinamična oblast u kojoj su česte promene tako da je svaki pokušaj striktne kategorizacije osuđen na kratkotrajnu ispravnost.

2. Sigurnosne arhitekture i modeli:

2.1. Osnove sigurnosnih arhitektura:

Kao što je rečeno, **sigurnosna arhitektura** jednog sistema je osnova uvodjenja sigurnosnih mera. Zavisno od toga o koliko strogoj sigurnosnoj politici je reč,u zavisnosti od tipa sistema otvorenog ili zatvorenog, distribuiranom centralizovanom ili distribuiranom - gradi se odgovarajuća sigurnosna arhitektura i primenjuju se odgovarajuće metode zaštite. U ovom delu biće opisani neki zaštitni mehanizmi, sigurnost u distribuiranim arhitekturama, kriterijumi ocenjivanja, ranjivost i metode seftifikacije i akreditacije. [4]

2.1.1. Zaštitni mehanizmi:

Računarska baza od poverenja je kombinacija raznih zaštitnih mehanizama softvera, hardvera i firmvera koja primenjuje sigurnosna pravila. *Security perimeter* (sigurnosna ograda ili granica) je granica izmedju baze od poverenja i ostalih sistema ili ostatka sistema. Korisnik zaobilazi sve zabrane tako što koriste sigurne puteve (trusted path) koji su u velikom broju slučajeva vrsta tunela do sigurnosne baze. Računarski sistem da bi bio od poverenja mora da koristi određene mere hardverskog i softverskog obezbeđenja nekad i na više nivoa.

2.1.2. Apstrakcija i koncept skrivanja informacija:

Jedan od uobičajenih formalnih pristupa problemu zaštite jeste korišćenje apstrakcije. **Apstrakcija** (engl. *abstraction*) znači posmatranje sistemskih komponenata na višem nivou, to jest ignorisanje njihovih detalja na nižim nivoima (tj. na nivou detalja). Ovaj pristup olakšava (pojednostavljuje) razumevanje složenih sistema i usredsređivanje na bitne probleme na višem nivou, bez ulaženja u detalje pojedinačnih elemenata sistema. U objektno orijentisanom programiranju, na primer, metode i podaci su enkapsulirani (zatvoreni) u neki objekat koji može da se posmatra kao apstrakcija. Ovaj koncept se ponekad zove **sakrivanje informacija** (engl. *information hiding*) zbog toga što su detalji funkcionisanja objekta sakriveni. Sa ovim objektima se komunicira preko poruka na koje objekat odgovara kako je to definisano njegovim internim metodama.

2.1.3. Domeni zaštite i zaštitni prstenovi:

U računarskom sistemu istovremeno može biti aktivno više procesa (konkurentni procesi). Pristup odredjenim memorijskim lokacijama ima svaki proces i mogćnost izvršavanja podskupova računarskih instrukcija. Izvršavanje procesa i memorijsko područje koje je dodeljeno svakom procesu zove se **zaštitni domen** (engl. *protection domain*). Ovaj domen može da se proširi na virtuelnu memoriju, što prividno povećava radnu memoriju tako što se koristi prostor na disku. Smisao uspostavljanja zaštitnog domena jeste da se programi zaštite od neovlašćene izmene ili ometanja tokom izvršenja.

Jedna od šema koja podržava višestruke domene zaštite jeste korišćenje zaštitnih prstenova (engl. *protection rings*). Prstenovi su realizovani tako da je domen s najvećim pravima u centru prstena, a da je domen s najmanjim pravima spoljašnji, tj. periferni prsten. [10]

Jezgro operativnog sistema obično se nalazi u prstenu 0 i ima pravo da pristupi svim domenima u sistemu. **Sigurno jezgro** (engl. *security kernel*) čine hardverski, firmverski i softverski elementi računarske baze od poverenja, koji implementiraju koncept monitora referenci (engl. *reference monitor*). **Monitor referenci** je komponenta sistema koja forsira pristupe objektima. Prema tome možemo reći da je monitro referenci vrsta apstraktne mašine u posredovanju izmedju subjekata i objekata.

Sigurno jezgro mora da:

- Posreduje u svim pristupima,
- Bude zaštićeno od izmena,
- Bude verifikovano kao ispravno.

U konceptu prstena, prava pristupa se smanjuju kako raste broj prstena. Znači, najveći skup prava obezbeđuje prsten u centru. Sistemske komponente su smeštene u odgovarajući prsten po principu najmanjih potrebnih prava. Prema tome, procesi imaju minimum prava nužnih za izvršavanje njihovih funkcija.

Postoje i drugi pristupi zaštiti, zasnovani na jezgru i srodnim mehanizmima:

- Korišćenje posebnog hardverskog uređaja koji proverava sve reference u sistemu i objavljuje ih kao važeće,
- Implementiranje nadgledanja iliti monitora virtuelne mašine (virtual machine monitor) koji može predstavljati veliki broj virtuelni mašina.Svaka od tih mašina može raditi na različitom sigurnosnom nivou.
- Korišćenje softverski sigurnog jezgra koje radi u vlastitom domenu zaštite.

2.1.4. Sigurnosne oznake:

Sigurnosna oznaka (engl. *security label*) dodeljuje se nekom resursu. Sigurnosna oznaka može ukazati na potrebu za posebnim načinom (režimom) rukovanja (rukovanje objektom uz primenu dodatnih sigurnosnih mehanizama), ili se može koristiti za kontrolu pristupa. Dodeljene oznake se obično ne mogu izmeniti, pa predstavljaju efektivan, tj. delotvoran mehanizam kontrole pristupa. Pošto se oznake moraju podeliti i vertifikovati u skladu s politikom sigurnosti, njihova primena će izazvati dodatan utrošak režijskog vremena u sistemu. [1]

2.1.5. Sigurnosni režimi:

Informacioni sistemi rade u različitim sigurnosnim režimima koji su određeni nivoima klasifikacije informacija, profilima korisnika i njihovim ovlašćenjima (engl. *clearance*). Glavna razlika u radu informacionih sistema jeste između sistemskog visokog nivoa (režima rada) i sigurnosnog režima sa više nivoa. U **sistemski - visokom režimu rada** (engl. *sustem high mode of operation*), sistem radi na najvišem nivou klasifikacije (sigurnosti), gde svi korisnici moraju imati ovlašćenja za najviši nivo. Međutim, neće svi korisnici imati potrebu da znaju, tj. vide sve podatke. **Režim rada s više nivoa** (engl. *multilevel mode of operation*) podržava korisnike s različitim ovlašćenjima i podatke različitih nivoa klasifikacije. Slede opisi dodatnih režima rada:

- **Namenski**
- **Odeljeni**
- **Kontrolisani**
- **Ograničen pristup**

2.1.6. Distribuirane arhitekture:

Migracija od centralizovanih modela računarskih sistema ka klijent/server modelu i ka višeslojnim modelima, stvorila je nov skup problema za profesionalce u oblasti sigurnosti informacioniih sistema. Situaciju je dodatno komplikovala sve veća primena stonih i prenosnih računara. Na takvim računarima se mogu nalaziti bitna dokumenta koja su osetljiva za posao kojima se bave neke organizacije. [20] U velikom broju slučajeva, korisnik obavlja poslove administratora sistema, programera i operatera na ovakvom personalnom računaru. Glavni razlozi za brigu su sledeći:

- Stoni prenosni računari mogu sadržati osetljive informacije, čije otkrivanje može biti rizično,
- Korisnici mogu, uopšteno govoreći, biti nedovoljno svesni problema sigurnosti,
- Ova vrsta računara obično služi kao sredstvo za pristup kompaniskim mrežama i informacionim sistemima na kojima se nalaze bitni podaci,
- Modemi i drugi uređaji za povezivanje stonih i prenosnih računara na korporativne mreže podložni su različitim tipovima napada,
- Preuzimanje podataka sa Interneta (engl. *download*) i drugih javnih sistema, povećava rizik da se korporativni sistemi inficiraju zlonamernim kodom ili nenamernim izmenama u bazama podataka,
- Stoni sistemi i njihovi diskovi često nisu zaštićeni od fizičkog upada ili krađe,
- Neredovna izrada rezervniih kopija podataka.

Segurnosni mehanizmi se koriste da bi se izborili sa sigurnosnim slabostima koje mogu postojati u distribuiranim sistemima. Takvi mehanizmi su:

- Pravila o elektronskoj pošti i preuzimanju ili slanju datoteka,
- Robusna kontrola pristupa koja uključuje biometrijske mere da bi se ograničio pristup,
- Mehanizmi grafičkih korisničkih interfejsa koji su usmereni na ograničenje pristupa bitnim podacima,
- Šifrovanje,

- Razdvajanje procesa koji se izvršavaju u privilegovanom i neprivilegovanom režimu rada procesora,
- Domeni zaštite,
- Zaštita osetljivih diskova tako što se fizički montiraju na nepokretne kontejnere i zaključavaju (uklanja se mogućnost da ih neko isključi i odnese) te fizičko osiguranje stonih računara, prenosnih računara i mobilnih uređaja,
- Različito označavanje diskova i drugih materijala zavisno od klasifikacije njihove poverljivosti i osetljivosti,
- Centralizovani sistemi arhiviranja i izrade rezervnih kopija podataka,
- Redovna obuka usmerena na održavanje i podizanje svesti o problemima sigurnosti,
- Kontrola softvera instaliranog na računarske sisteme i uređaje,
- Šifrovanje, kontrolni zbirovi i korićenje heš funkcija prilikom slanja i skladištenja informacija,
- Praćenje obavljenih transakcija i prenosa podataka i vođenje evidencije o njima,
- Primena drugih odgovarajućih fizičkih, logičkih i administrativnih mera kontrole pristupa,
- Sistemi za upravljanje bazama podataka koji ograničavaju pristup osetljivim informacijama,
- Zaštita od oštećenja i uništenja računara i medijuma usled uticaja iz okruženja,
- Korišćenje formalnih metoda za razvoj softvera i aplikacija, koje uključuju biblioteke, kontrolu izmena (engl. *change control*) i upravljanje konfiguracijama (engl. *configuration management*),
- Izrada i primena planova za oporavak od nesreće (engl. *disaster recovery*) i planova za kontinuirano odvijanje posla (engl. *business continuity plans*).

2.1.7. Ranjivosti u sigurnosnoj arhitekturi i procedure oporavka:

Ranjivosti (engl *vulnerability*) u sistemskoj sigurnosnoj arhitekturi mogu voditi ka narušavanju sistemske sigurnosne politike. Među uobičajene ranjivosti arhitekture spada i sledeće:

- **Skivreni kanal** (engl. *covert shannel*) - Nenamerni komunikacioni kanal između dva ili više subjekata koji dele zajednički resurs, koji podržava prenos podataka na način koji

narušava sistemsku sigurnosnu politiku. Podaci se obično prenose preko zajedničkog skladišta podataka ili pristupanjem zajedničkom putu koji se koristi kao deljivi kanal za komunikaciju za koju nije predviđen,

- **Nepostojanje provere perimetra** (engl. *lock of perimeter checking*) - Greška ili nepostojanje provere ulaznih tokova koji su određeni parametrima. Napadi prekoračenja bafera eksploatišu ovu slabost u određenim operativnim sistemima i programima,
- **„Maintenance hook" ranjivost** - Hardverski ili softverski mehanizam koji je instaliran da bi se dozvolilo održavanje sistema i koji preskače sistemske sigurnosne mehanizme zaštite,
- **„Time of Check to Time of Use" (TOC/TOU) napad** - Napad koji iskorišćava razliku između vremena kada su sigurnosne kontrole primenjene i vremena kada je korišćena usluga provere identiteta i iskorišćeno neko pravo.

2.1.8. Procedure oporavka:

Kada grešku prouzrokuje hardverska ili softverska komponenta sistema od poverenja, veoma je važno da ta greška ne kompromituje zahteve sigurnosne politike tog sistema. Dodatno, procedura oporavka ne treba da ostavi mogućnost za narušavanje sigurnosne politike sistema. Ako se zahteva restartovanje sistema, sistem mora biti restartovan u sigurnom stanju. Sistem se mora pokrenuti u **režimu održavanja** (engl. *maintenance mode*), koji dozvoljavaju pristup samo privilegovanim korisnicima s privilegovanih terminala. Ovaj režim podržava povratak (oporavak) sistemskog stanja i sugurnosnog stanja. [8]

Kada se javi grška na računaru ili mrežnoj komponenti, a računar ili mreža nastavi da radi, takav sistem se smatra **optornim na greške** (engl. *Fault - tolerant system*). Da bi sistem otporan na greške radio, mora biti u stanju da otkrije grešku i da je onda ispravi ili da nastavi da radi bez obzira na grešku. U sistemu koji je **bezbedan u slučaju otkaza** (engl. *Fail - safe system*), izvršenje programa se prekida i sistem je zaštićen od kompromitovanja kada se pojavi i detektuje hardverska ili softverska greška. U sistemu koji je **elastičan u slučaju otkaza** (engl. *resilient*), tj. „*fail - soft*", određeni procesi koji nisu kritični prekidaju se kad se javi i otkrije hardverska ili softverska greška. Računar ili mreža nastavljaju da rade sa slabijim

performansama tj. na nižem nivou. Izraz „*fail - over*“ odnosi se na prebacivanje tokom rada na rezervne komponente.

Hladni start (engl. *cold start*) nastaje u sistemu kada se javi TCB greška ili greška na medijima i kada procedure oporavka ne mogu da vrate sistem u poznatom, pouzdano, sigurno stanje. U ovom slučaju, TCB i delovi softvera i podataka mogu biti nekonsistentni pa će biti neophodna spoljna intervencija. U tom slučaju, obično se mora iskoristiti režim održavanja sistema da bi se sistem oporavio.

2.1.9. Kriterijumi ocenjivanja**:**

Osiguranje (engl. *assurance*) definiše se kao stepen poverenja i zadovoljenja sigurnosnih potreba. U ovom delu poglavlja sumirani su osnovni zahtev i standardi kojima se procenjuje i prihvata čvrstina, to jest garantuju sigurnosni aspekti i karakteristike sistema.

Tokom 1985. godine, Nacionalni centar za računarsku sigurnost (*National Computer Security Center,* NCSC) uveo je **kriterijum za procenu računarskih sistema od poverenja** (*Trusted Computer System Evaluation Cretiria*, TCSEC) s namerom da obezbedi vodeće smernice za ocenjivanje određenih sigurnosnih standarda proizvoda različitih proizvođača. **TCSEC** pruža sledeće:

- Osnovu za uspostavljanje zahteva u pogledu sigurnosti u procesu definisanja specifikacija,
- Standard za sigurnosne usluge koje proizvođači treba da obezbede za različite klase sigurnosnih zahteva,
- Načine i sredstva za merenje pouzdanosti i poverljivosti, tj. stepena poverenja koji se može ukazati informacionom sistemu.

Ostale klase kojima se ITSEC bavi jesu integritet, to jest celovitost, i visoka raspoloživost.

TCSES, ITSEC i Canadian Trusted Computer Product Evaluation Criteria (CTC-PEC) revolvirali su u jedan kriterijum procene koji se zove Zajednički kriterijum. Zajednički kriterijum (engl. *Common Criteria*) definiše profil zaštite (engl. *protection profile*) koji specificira sigurnosne zahteve i zaštitu proizvoda koji treba da se ocene. Funkcionalni zahtevi Zajedničkog kriterijuma organizovani su oko TCB entiteta. Među te entitete spadaju fizičke i logičke kontrole, podizanje sistema i oporavak, referentna medijacija i privilegovana stanja. Kao i u slučaju TCSEV-a i ITSEC-a, rangiranja Zajedničkoj kriterijuma takođe su hijerarhijska. [11]

2.1.10. Sertifikacija i akreditacija:

U mnogim okruženjima moraju se primeniti formalne metode da bi se osiguralo postavljanje prikladnih metoda zaštite informacionog sistema, kao i to da one funkcionišu prema specifikaciji. Dodatno, neki autoritet mora preuzeti odgovornost za stavljanje sistema u operativno stanje. Ove akcije su poznate kao sertifikacija i akreditacija.

Formalno, definicije su sledeće:

- **Sertifikacija** (engl. *certification*) predstavlja opsežnu procenu tehničkih i netehničkih sigurnosnih karakteristika informacionog sistema i drugih zaštitnih mehanizama koji treba da podrže proces akreditacije, da ustanove varijacije, tj. prihvatljiva proširenja - proširenja u okviru kojih određena arhitektura i njena implementacija zadovoljava skup specificiranih sigurnosnih zahteva,
- **Akreditacija** (engl. *adreditation*) je vrsta formalne deklaracije koja može da daje ovlašćena organizacija i po kojom je dozvoljeno nekom informacionom sisetemu da radi u odredjenom sigurnosnom režimu sa skupom propisanih mehanizama zaštite.

Sertifikacija i akreditacija sistema moraju biti proverene posle definisanog perioda ili kada se dese promene na sistemu ili u njegovom okruženju. Onda se zahtevaju resertifikacija i reakreditacija.

2.2. DITSCAP I NIACAP:

Za procenu važnih informacionih sistema postoje dva američka odbrambena i državna sertifikaciona i akreditaciona standarda. To je vrsta procesa sertifikacija i akreditacija sigurnosti odbramenih informacionih tehnologija i proces sertifikacije i akreditacije državnih informacionih tehnologija. DITSCAP je skraćenica za *Defense Information Technology Security Certification and Accreditation Process* a NIACAP je *National Information Assurance Certification and Accreditation Process.*

DITSCAP ustanovljava proces standardizacije, skup aktivnosti, opšte opise zadataka i upravljačku strukturu da bi se sertifikovali i akreditovali IT sistemi koji će održavati zahtevano sigurnosno stanje. Ovim procesom se sertifikuje da IT sistem zadovoljavaju zahteve akreditacije i da će sistem održavati akreditovano sigurno stanje kroz svoj žitovni ciklus. Ovo su faze DITSCAP procesa:

- **Faza 1**, definicija. Faza 1 se fokusira na razumevanje misije, okruženja i arhitekture kako bi se odredili zahtevi u pogledu sigurnosti i nivo truda potrebnog da se dostigne akreditacija,
- **Faza 2**, verifikacije. U fazi 2 verifikuje se da sistem u razvoju ili modifikovani sistem odgovara informacijama navedenim u ugovoru o autorizaciji sigurnosti sistema (*System Security Authorization Agreement*, SSAA). Cilj je da se koristi SSAA kako bi se uspostavila saglasnost o izgradnji i razvoju sigurnosti, pre nego što razvoj počne i pre nego što se sprovedu izmene sistema. Posle akreditacije, SSAA postaje osnovni dokument o sigurnosnoj konfiguraciji,
- **Faza 3**, validacija. U fazi 3 vrednuje se usklađenost potpuno integrisanog sistema sa informacijama navedenim u SSAA,
- **Faza 4**, postakreditacija. Faza 4 obuhvata aktivnosti koje su nužne za nastavak rada akreditovanog IT sistema u računarskom okruženju, i za brigu o izmenjenim opasnostima s kojima se sistem suočava tokom životnog ciklusa.

NIACAP u SAD uspostavlja minimalni nacionalni standard za sertifikaciju i akreditaciju nacionalnih sigurnosnih standarda. Ovaj proces daje standardni skup aktivnosti, opštih zadataka i upravljačke strukture, neophodnih da bi se sertifikovali i akreditovali sistemi koji održavaju obezeđenje informacija i stanje sigurnosti sistema ili lokacije. NIACAP sertifikuje da

informacioni sistem zadovoljava zahteve akreditacije i da će nastaviti da održava akreditovano sigurno stanje tokom životnog ciklusa sistema.

Postoje tri tipa NIACAP akreditacije:

1. **Akreditacija lokacije** (engl. *site accreditation*). Procenjuje aplikacije i sisteme na određenoj samosadržanoj (engl. *selfcontained*) lokaciji,
2. **Akreditacija tipa** (engl. *type accreditation*). Procenjuje aplikaciju ili sistem koji se distribuira na određeni broj lokacija,
3. **Akreditacija sistema** (engl. *sustem accreditation*). Procenjuje glavnu, tj. osnovnu (engl. *major*) aplikaciju ili opšti sistem podrška.

NIACAP se sastoji od četiri faze - definicija, verifikacija, validacija i postakreditacija, one su, u suštini, identične onima u DITSCAP-u.

Razvija se i proces za analizu sigurnosti komercijalnih informacionih sistema (*Commercial Information Security Analysis Process*, SIAP) u kome se, korišćenjem NIACAP metodologije, procenjuju kritični komercijalni sistemi.

3. Osnovne bezbednosti u računarskim mrežama:

3.1. Neki tipovi i modeli napada:

Danas u praksi postoji veliki broj različitih tipova napada na računarske sisteme i komunikacione kanale. Postoje različiti tipovi napada a oni se (uglavnom) mogu podeliti u suštinski različite grupe u okviru kojih različiti napadi koriste iste principe, a razlikuju se u praktičnoj realizaciji i meti napada. U okviru ovog dela knjige biće predstavljena tri suštinski različita tipa napada - razbijanje šifrata primenom sirove sile, posredovanje u komunikaciji i uskraćivanje usluge.

3.1.1. Kriptoanaliza:

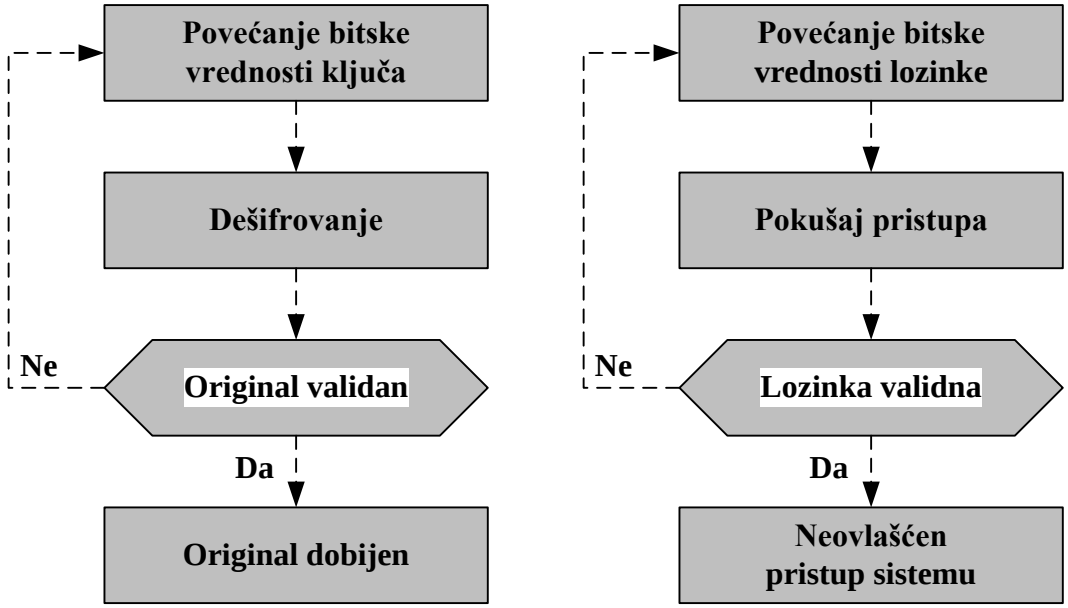
Termin kriptoanaliza odnosi se na deo kriptologije vezan za analizu i dekriptiranje šifrata bez poznavanja jednog ili više parametara (ključeva, transformacije i sl.) pomoću kojih je on kreiran. Iako je kriptoanaliza suprotstavljena kriptografiji (koja je usmerena na razvoj šifarskih sistema) ona ipak čini i izuzetno važan alat za proveru efikasnosti šifarskih sistema. Kriptoanaliza predstavlja najsloženiju oblast kriptologije.

Rezultat uspešne kriptoanalize jeste dobijanje originala na osnovu šifrata. Ukoliko proces kriptoanalize da takav rezultat, analizirani šifarski sistem se smatra „probijenim“. Ukoliko se kriptoanaliza primenjuje na digitalne potpise, njeni ciljevi mogu biti falsifikovanje potpisa ili pronalaženje tajnog ključa.

Jedan od značajnih primera kriptoanalize jeste njena primena na *RSA* algoritam koji danas predstavlja *de facto* standard u asimetričnom šifrovanju. Noseće funkcije ovog algoritma već decenijama su predmet analize matematičara i profesionalaca na polju bezbednosti. Do sada nisu objavljeni rezultati kriptoanalize ovog algoritma, što nije slučaj sa mnogim šifarskim algoritmima koji su se ranije koristili, ili se još uvek koriste .[21]

3.1.2. Razbijanje šifrata primenom sirove sile:

Jedan od najelementarnijih načina za otkrivanje zaštićenih pristupnih parametara sistemu ili originalu šifrata (korisničkog imena i lozinke, tajnog ključa i sl.) jeste korišćenjem tzv. „sirove sile“ (engl. *brute farce attack*). Ovaj pristup u osnovnoj varijanti podrazumeva redno isprobavanje različitih pristupnih parametara sve do pogađanja odgovarajućih .[21]



Slika 2. Algoritam metoda „sirove sile“

Glavni nedostatak primene metoda „sirove sile“ jeste vreme potrebno za razvijanje lozinki i ključeva veće bitske dužine, jer svaki dodatni bit lozinke ili ključa duplira potrebno vreme (eksponencijalni rast). Iz tog razloga se u praksi (uglavnom kod razbijanja pristupnih lozinki) često koriste modifikovani algoritmi i rečnici često korišćenih izraza. [2]

Principi i mogućnosti odbrane od ovog tipa napada znatno se razlikuju u zavisnosti od toga da li se štiti pristup sistemu ili šifrovani podaci koji se prenose putem mreže. Za slučaj zaštite sistema od neovlašćenog pristupa kao primer se može uzeti *UNIX* operativni sistem, njegovi bezbednosni mehanizmi i njihova evolucija.

U ranim fazama razvoja računara, njihova procesorska snaga i broj korisnika bili su (sa bezbednosnog aspekta) zanemarljivi te su pristupne lozinke korisnika čuvane u šifrovanom obliku (heš funkcije) u javno dostupnom fajlu /*etc/passwd*. Međutim, uporedo sa razvojem procesorske snage računara i rastom broja korisnika javili su se prvi slučajevi zloupotrebe pristupnih parametara ostalih korisnika sistema koji su bili otkriveni primenom metoda „sirove sile“ na šifrate lozinke. Iz ovog razloga šifrati lozinki su izmešteni u fajl /*etc/shadow* kome je pristup odobren samo administratoru sistema i procesu koji vrši prijavljivanje korisnika na sistem.

Sledeći bezbednosni problem koji se javio jeste pojava alata koji su za metod primene „sirove sile“ iskoristili sistemsku naredbu za promenu identiteta *su* i na taj način iskoristili posredan pristup heš vrednosti lozinke putem procesa za prijavljivanje korisnika na sistem. Ovi alati su omogućivali maksimalno iskorišćavanje performansi sistema za razvijanje heš vrednosti lozinke time što se moglo ispitati više desetina, stotina ili hiljada vrednosti (u zavisnosti od procesorske snage računara) u toku jedne sekunde. Ovaj bezbednosni problem je rešen izmenom sistema za prijavu korisnika na sistem tako da su dodata čekanja od po nekoliko sekundi između dva pokušaja prijavljivanja.

Na *MS Windows* operativnim sistemima postoji i opcija da se nalazi automatski zaključavaju nakon nekoliko neuspešnih pokušaja prijavljivanja. Isti princip se koristi i kod tzv. „pametnih„ kartica i njima pridruženim pristupnim *PIN* kodovima. Ovaj metod zaštite, iako efikasan u zaštiti od neovlašćenog pristupa, često se može zloupotrebiti od strane napadača u cilju onemogućavanja normalnog funkcionisanja sistema i rada legalnih korisnika. [17]

Za razliku od zaštite sistema od neovlašćenog pristupa, kod prenosa podataka računarskim i telekomunikacionim mrežama zaštitu nije moguće zasnovati na nedostupnosti šifrata napadaču. U takvoj situaciji se kao rešenje najčešće predlaže korišćenje ključeva veće bitske dužine. Postoje različite preporuke za izbor dužine ključa u cilju odbrane od napada metodom primene „surove sile“ a u zavisnosti od načina šifrovanja, oblasti primene, važnosti podataka i slično.

Vreme potrebno za razbijanje šifrata primenom „sirove sile“ u opštem slučaju zavisi od dva parametra - dužine korišćenog ključa (veličine skupa iz koga se bira ključ) i frekvencije kojom se isprobavaju različiti ključevi. Očekivana verovatnoća da će ključ biti pogođen iznosi 2^{N-1} proverenih kombinacija gde je *N* bitska dužina ključa.

U cilju ostvarivanja što kraćeg vremena za razbijanje šifrata najčešće se koriste brzi računari sa više procesora, klasteri računara ili namenski uređaji. Primer namenskog uređaja za razbijanje šifrata primenom „sirove sile“ je uređaj *COPACOBANA* razvijen na nemačkim univerzitetima *Bochum* i *Kiel*.

Ovaj uređaj je namenjen razbijanju svih simetričnih sistema šifrovanje koji koriste ključeve dužine do 64 bita. U sistem je ugrađena podrška za *DES* algoritam a sistem se može

proširiti i sopstvenim modulima. Takođe, moguće je i serijsko povezivanje do 127 *COPACOBANA* uređaja koji bi paralelno radili na istom zadatku. Prosečna brzina pretrage sistema je oko 43 milijarde ključeva u sekundi a snaga sistema je 2006. godine upotređena sa 22.865 *Pentium* 4 računara. Cena jednog uređaja je oktobra 2006. godine iznosila 8.980 evra. Po današnjim merilima 2015. godine korišćenje čak i starijih sistema kao Blue Genie super računar može razvijati stotine milijardi ključeva u sekundi ili čak delovima sekunde.

Kao što je ranije pomenuto i prikazano, u literaturi i od strane različitih organizacija koje se bave bezbednošću komunikacija, kao podrazumevani metod zaštite od razvijanja šifrata primenom sirove sile navodi se korišćenje ključeva veće bitske dužine, jer se polazi od osnovne pretpostavke da je razbijanje šifrata simetričnih algoritama moguće samo primenom „sirove sile“. Međutim, jedna od čestih teza eksperta na polju zaštite u računarskim mrežama jeste da veće bitske dužine mogu predstavljati prepreku za napadače koji za razbijanje koriste računarske sisteme skromnijih proceskih moći ali ne i za napadače koji raspolažu klasterima super-računara ili namenskih uređaja.

3.1.3. Napad posredovanjem u komunikaciji:

Jedan od najopasnijih napada u računarskim i telekomunikacionim mrežama jeste napad putem posredovanja između strana koje komuniciraju (engl. *Man in the middle attack*). Uzeti u obzir to da današnje globalne računarske i telekomunikacione mreže najčešće podrazumevaju veliki broj infrastrutkurnih posrednika u komunikaciji (ruteri, repetitori i sl.), mogućnosti za izvršavanje ovakvog tipa napada su sve veće.

Napad posredovanja u komunikaciji se, pre svega, odnosi na zaštićene (šifrovane) i autorizovane komunikacije. Kod nezaštićenih i neautorizovanih komunikacija su podrazumevano ostvareni svi preduslovi za uspešan napad. Osnovni rezultati posredovanja u komunikaciji jesu mogućnost prisluškivanja (odnosno snimanja) komunikacije i mogućnost izmene njenog sadržaja. Preduslov za uspešno izvršavanje napada jeste uspešno lažno predstavljanje kod obe strane, odnosno, simuliranje identiteta druge strane .[21]



Slika 3. Struktura napada sa posredovanjem u komunikaciji

Proces izvođenja napada posredovanja u komunikaciji podrazumeva prihvatanje, čitanje, eventualnu izmenu, i prosleđivanje poruka koje strane razmenjuju. Kod uspešno izvedenog napada regularne komunikacione strane imaju iluziju da komuniciraju direktno i nemaju nikakvu mogućnost da utvrde da je došlo do prisluškivanja. [18]

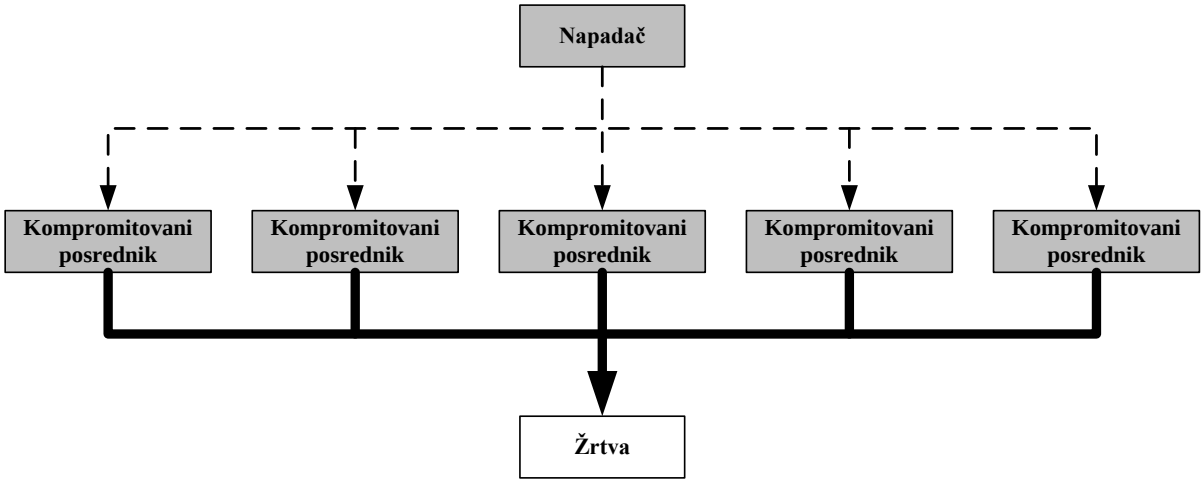
Postoji više mehanizama za odbranu od napada posredovanja u komunikaciji: korišćenje *PKI* infrastruktura, tajnih ključeva, posebnih kanala za razmenu, itd. U ovom delu su opisana rešenja koja se baziraju na upotrebi simetričnih algoritama sa tajnim ključevima koji se razmenjuju odvojenim komunikacionim kanalima. Takav pristup se može smatrati bezbednim od napada posredovanja u komunikaciji.

3.1.4. Napad uskraćivanjem usluge:

Onemogućavanje usluge (engl. *Denial of Service, DoS*) je tip napada usmeren ka komunikacionoj strukturi, odnosno, njenom kapacitetu (propusnoj moći). Cilj napada ovog tipa nije da napadaču omogući pristup ili kontrolu nad udaljenim sistemom (ili podacima) već da zauzimanjem svih komunikacionih kapaciteta onemoguće pristup sistemu od strane regularnih korisnika.

Postoji više tipova napada sa ciljem onemogućavanja usluge. Najjednostavniji tipovi napada ovog tipa se baziraju na slanju što veće količine podataka žrtvi u što manjem vremenskom periodu. Nešto napredniji tip napada je napad sa modifikovanim paketima mrežnog nivoa. Primer ovakvog tipa napada je tzv. reflektovani napad. Kod ovog tipa napada napadač posredniku (koji nije kompromitovan - pod napadačevom kontrolom) šalje pakete koji zahtevaju odgovor a kod kojih je za izvorišna adresa (adresa napadača) zamenjena adresom žrtve. Ovo je ujedno i najprimitivniji oblik sakrivanja izvora napada.

Jedan od najopasnijih tipova napada sa ciljem onemogućavanja usluge je distribuirani napad sa ciljem onemogućavanja usluga (engl. *Distributed Denial of Service, DDoS*). Glavna karakteristika ovakvih napada je to što napadač ne zavisi od kapaciteta sopstvenih komunikacionih kanala već za napad može istovremeno koristiti kapacitete hiljada kompromitovanih posrednika .[21]



Slika 4. Model distribuiranog napada sa ciljem onemogućavanja usluge

Kod ovog tipa napada samom napadu prethodi proces kompromitovanja što većeg broja posrednika (koji se ponekad nazivaju i „zombijima“). Za kompromitovanje posrednika najčešće se koristi maliciozni softver. Na kompromitovane posrednike se instalira softver za udaljenu kontrolu koji, kada napadač dobije adresu žrtve, započinje slanje podataka. Dva značajna problema pri odbrani od ovog tipa napada su ta što se javlja veliko opterećenje komunikacionih kanala i što postoji veliki broj izvora napada. [16]

Sredinom 2008. godine primećen je novi tip napada sa ciljem onemogućavanja usluge. Ovaj napad nije usmeren na zagušivanje komunikacionog kanala žrtve već na njen mrežni interfejs. Redosled koraka u izvršavanju ovog tipa napada je sledeći:

1. Korisnički program na strani napadača sa nivoa *IP* protokola šalje žrtvi *IP* datagram sa sadržajem koji je indentičan sadržaju *TCP* paketa za otvaranje soketa (iniciranje veze),
2. Napadnuti računar nakon prijema datagrama prosleđuje sadržaj transportnom nivou - *TCP* protokolu - koji otvara novi soket smatrajući da se radi o regularnom zahtevu,
3. Proces se ponavlja dok se komunikacija sa napadnutim računarom ne onemogući preveliki broj otvornih soketa .[21] mozda prevelikim brojem otvorenih soketa

Napadi sa ciljem onemogućavanja usluge mogu prouzrokovati obziljne probleme korisnicima koji zavise od komunikacionih kanala visoke propusne moći (Internet provajderi,

veliki poslovni subjekti, on-lajn poslovanja i sl.). Postoje različiti načini odbrane od ovakvih napada (konfiguracija rutera, alternativni linkovi itd.).

3.2. Popularni sistemi za zaštitu komunikacije:

Danas se u praksi reklamira i sreće veliki broj različitih sistema zaštite. Ovi sistemi su projektovani u skladu sa različitim namenama, okruženjima i načinima upotrebe. Neki od njih su projektovani za krajnje korisnike, a neki pre predstavjaju radne okvire za razvoj sopstvenih bezbednosnih konfiguracija. Kategorizaciju sistema zaštite moguće je obaviti po više kriterijuma:

- Sistemi za zaštitu izdvojenih sistema i sistema za zaštitu mreža,
- Sistemi sa dostupnim izvornim kodom i zatvoreni sistemi,
- Sistemi koji koriste javne algoritme i sistemi sa sopstvenim algoritmima i drugi .[22]

Pregledom postojećih sistema zaštite komunikacije za potrebe ovog dela izvršena je kategorizacija na osnovu sloja *OSI i TCP/IP* referentnih modela na kome ti sistemi funkcionišu. U skladu sa tim, dat je pregled sistema zaštite komunikacije koji funkcionišu na nivou aplikativnog protokola, nivou transportnog protokola i nivou mrežnog protokola.

3.2.1. Zaštita na nivou aplikativnog protokola:

Aplikativni sloj predstavlja najfleksibilnije područje za razvoj sopstvenih sistema za zaštitu komunikacije iz tog razloga što se pri razvoju protokola na ovom nivou ne mora voditi računa o kompatibilnosti sa protokolima viših nivoa. Bezbednost sopstvenog sistema zaštite na aplikativnom sloju zavisi prvenstveno od nivoa zaštite koji nude korišćeni algoritmi, procedure i okruženje u kome se sistem primenjuje. [4]

Osnovni nedostatak integracije bezbednosnih sistema na nivou aplikativnog protokola jeste taj što se razvojem/integracijom jednog bezbednosnog sistema pokriva samo jedan aplikativni protokol. [5]

Ukoliko korisnici komunikaciju vrše putem različitih protokola, tada se za svaki od protokola mora izvršiti zaseban razvoj/integracija. Dodatno, u takvoj situaciji se set softvera koji

koriste krajnji korisnici mora ograničiti da ne bi došlo do razmene važnih podataka protokolima koji nisu zaštićeni .[21]

3.2.1.1. Zaštita elektronske pošte:

Elektronska pošta predstravlja jedan od najčešće korišćenih servisa na Internet mreži. Jedna od značajnih karakteristika ovog servisa je ta da se u okviru mrežnog saobraćaja koji se njime ostvaruje nalazi najveći procenat podataka generisanih od strane korisnika. U skladu sa tim postoji više sistema za zaštitu podataka koji se prenose putem servisa elektronske pošte. Ovi sistemi se uglavnom baziraju na šifrovanju podataka. Jedan od najpopularnijih sistema zaštite elektronske pošte jeste *OpenPGP*.

OpenPGP sistem obezbeđuje usluge zaštite i intergriteta podataka elektronske pošte i fajlova korišćenjem digitalnih potpisa, šifrovanja, kompresije i *Radix*/64 konvertovanja [RFC 4880]. Dodatno, ovaj sistem obezbeđuje i servise za upravljanje ključevima i sertifikatima. *OpenPGP* kombinuje simetrično i asimetrično šifrovanje za obezbeđenje poverljivosti. Kod simetričnog šifrovanja jedan ključ se koristi samo jednom, za šifrovanje jedne poruke ili fajla. Novi sesijski ključ generiše se kao (pseudo) slučajan broj i šalje se uz poruku, šifrovan javnim ključem primaoca. Koraci u korišćenju *OpenPGP* sistema zaštite su:

1. Pošoljalac kreira poruku,
2. *OpenPGP* generiše (pseudo) slučajan broj kao simetrični ključ za šifrovanje poruke,
3. *OpenPGP* šifruje sesioni ključ javnim ključem primaoca i takav šifrat stavlja na početak poruke,
4. *OpenPGP* šifruje sadržaj poruke i njime nastavlja poruku započetu šifratom sesionog ključa,
5. Primalac svojim tajnim ključem dešifruje sesijski ključ pridružen poruci,
6. Primalac korišćenjem dešifrovanog sesijskog ključa dešifruje sadržaj poruke .[21]

Ukoliko je u osnovnoj poruci definisano više primalaca, za svakog od njih se na početak poruke stavlja sesijski ključ šifrovan njegovim javnim ključem. Ukoliko se u sistemu koristi i digitalno potpisivanje, digitalni potpis poruke se izračunava pre šifrovanja, a zatim se šifruje po istom principu kao i sadržaj poruke. Proces digitalnog potpisivanja podrazumeva sledeće poruke:

1. Pošoljalac kreira poruku,
2. Sistem izračunava heš vrednost poruke,
3. Sistem izračunava digitalni potpis korišćenjem heš vrednosti i tajnog ključa pošiljaoca,
4. Digitalni potpis se pridružuje poruci,
5. Primalac prihvata poruku i izračunava njenu heš vrednost,
6. Izračunata heš vrednost se uparuje sa javnim ključem pošiljaoca i upoređuje sa dobijenim digitalnim potpisom.

OpenPGP sistem zaštite nudi i mogućnost kompresovanja poruke. Kompresovanje se vrši nakon izračunavanja digitalnog potpisa, a pre šifrovanja sadržaja. U zaglavlje poruke se postavlja identifikacioni broj algoritma za kompresovanje:

ID	**Algoritam**
0	Nema kompresovanja
1	*ZIP* [RFC 1951]
2	*ZLIB* [RFC 1950]
3	*BZip2*
100-110	Privatni i eksperimentalni algoritmi

Tabela 1. Algoritmi za kompresovanje podataka u *OpenPGP* sistemu

Kao algoritmi za izračunavanje heš vrednosti poruka koriste se sledeći algoritmi (identifikacioni broj algoritma se postavlja u zaglavlje poruke):

ID	**Algoritam**
1	*MD5*
2	*SHA-1*
3	*RIPE-MD/160*

4	Rezervisano
5	Rezervisano
6	Rezervisano
7	Rezervisano
8	*SHA256*
9	*SHA384*
10	*SHA512*
11	*SHA224*
100-110	Privatni i eksperimentalni algoritmi

Tabela 2. Algoritmi za izračunavanje heš vrednosti u *OpenPGP* sistemu

Kao simetrični šifarski algoritmi koriste se:

ID	**Algoritam**
0	nema šifrovanja
1	*IDEA*
2	*3DES (168bit)*
3	*CAST5 (128bit) [RFC 2144]*
4	*Blowfish (128bit)*
5	Rezervisano
6	Rezervisano
7	*AES (128 bit)*
8	*AES (192bit)*
9	*AES (256bit)*
10	*Twofish (256bit)*
100-110	Privatni i eksperimentalni algoritni

Tabela 3. Simetrični šifarski algoritmi u *OpenPGP* sistemu

Kao asimetrični algoritmi za šifriranje se koriste:

ID	**Algoritam**

1	*RSA* (šifrovanje i potpisivanje)
2	*RSA* (samo šifrovanje)
3	*RSA* (samo potpisivanje)
16	*Elgamal* (samo šifrovanje)
17	*DSA*
18	rezervisano
19	rezervisano
20	rezervisano
21	rezervisano
100-110	Privatni i eksperimentalni algoritmi

3.2.2. Zaštita na nivou transportnog protokola:

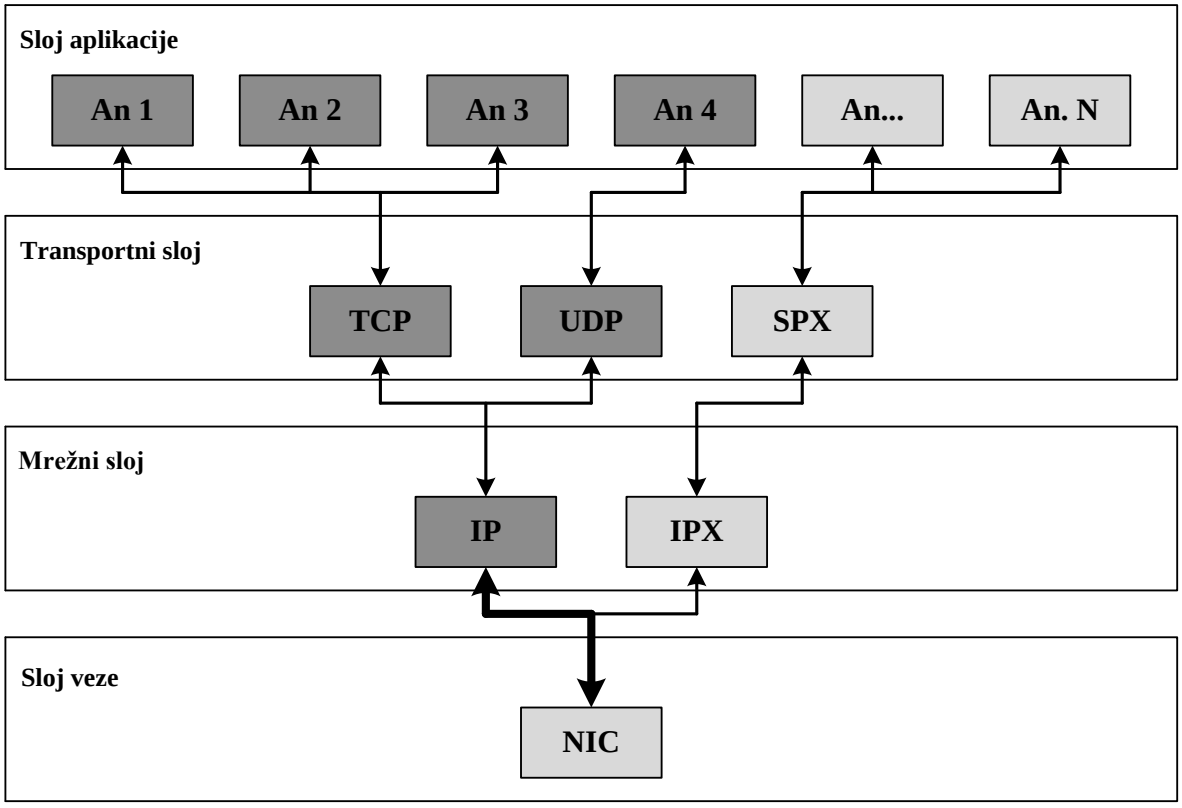
Realizacija sistema zaštite komunikacije na nivou transportnog protokola *OSI* i *TCP/IP* referentnih modela, umesto na nivou aplikativnog protokola, omogućava širu primenu jer se na taj način jednom realizacijom mogu obezbediti komunkacije većeg broja aplikacija.

Na primer, ugradnjom bezbednosnih funkcija u *TCP* protokol mogao bi se zaštititi ogroman broj aplikativnih protokola koji koriste pomenuti transportni protokol. Međutim, izmena samog *TCP* protokola predstavlja veoma složen zahvat koji bi mogao imati značajne posledice vezane za upotrebljivost okruženja u kome bi se tako izmenjen protokol primenjivao. Na primer, izmenjena varijanta *TCP* protokola, sa ciljem komunikacije preko nebezbedne mreže (npr. Interneta), mogla bi dovesti do prestanka rada servisa lokalne mreže na kojima je prisutna originalna verzija *TCP* protokola (npr. servisa za mrežno štampanje dokumenata).

Najrasprostranjeniji protokol za zaštitu podataka na transportnom nivou jeste *TLS* (engl. *Transport Layer Security*). On je razvijen na osnovu vezije 3.0 popularnog *SSL* (engl. *Secure Sockets Layer*) protokola. Prethodna verzija *SSL* protokola (verzija 2.0 i ranije) sadrže ozbiljne bezbednosne propuste vezane za integritet poruka, *Man-in-the-middle* napad na napad odsecanjem podataka. Dodatno, izvozne regulative kod ranijih verzija ograničavaju korišćene ključeve na dužinu od 40 bitova .[21]

3.2.3. Zaštita na nivou mrežnog protokola

Mrežni sloj *OSI* referentnog modela predstavlja najpogodniji sloj za realizaciju bezbednosnih sistema. Razlozi za to su višestruki: mrežni sloj donosi odluku o posrednicima u komunikaciji, popularni protokoli na mrežnom sloju imaju jasnu strukturu i lako se mogu proširivati i drugo. [13]



Slika 5. Zaštita na nivou mrežnog protokola

Ogromna prednost u realizaciji sistema zaštite na nivou mrežnog protokola je i činjenica da se realizacijom sistema na tom novou štite i podaci protokola viših nivoa - transportnog i aplikativnog, odnosno da se na ovaj način mogu zaštititi komunikacije svih korisničkih aplikacija. Vodeći sistem zaštite na mrežnom sloju je *Internet Protocol Security* .[21]

3.2.3.1. Internet Protocol Security sistem zaštite

Internet Protocol Cesurity (IPsec) protokol je rešenje za zaštitu podataka koji se prenose korišćenjem *IP* protokola. Ovaj sistem je realizovan setom protokola kojima se ostvaruje šifrovanje, provera autentičnosti izvora i integriteta poruka koje se prenose. Dodatno, *IPsec* sistem koristi i protokol za razmenu ključeva na početku sesije.

IPsec sistem se može koristiti za zaštitu komunikacije između krajnjih učesnika, između krajnjeg učesnika, sa jedne strane, i podrazumevanog mrežnog prolaza, sa druge strane, ili između podrazumevanih mrežnih prolaza sa obe strane. U skladu sa tim *IPsec* podržava dva režima rada: transportni i tunelski.

Jedna od značajnih prednosti *IPsec* sistema zaštite u odnosu na druge popularne sisteme zaštite (*SSL,TLS...)* je rad na niskom nivou u odnosu na *OSI* i *TCP/IP* referentne modele. Ovakva pozicija obezbeđuje fleksibilnost u pogledu zaštite velikog broja protokola viših nivoa.

Osnovne komponente *IPsec* sistema zaštite su *Internet Key Exchange* (*IKE, IKE*2) - sistem za upravljanjem ključevima i uspostavljanje bezbednosnih acosijacija, *Authentication Header (AH)* - protokol za obezbeđivanje autentičnosti i integriteta i *Encapsulating Security Payload (ESP)* - protokol za obezbeđivanje poverljivosti, autentičnosti i integriteta. [8]

Joj jedna značajna karakteristika *IPsec* sistema zaštite je i podrška za *IPv6* protokol. U stvari, *IPsec* je podrazumevani deo ovog protokola i inicijalno je i razvijan na njemu a naknadno je portovan na verziju 4.

Za uspešno korišćenje *IPsec* protokola neophodno je uspostavljanje pravilnih bezbednosniih asocijacija. Bezbednosne asocijacije predstavljaju pravila po kojima će se uspostaviti bezbedna komunikacija između učesnika. U bezbednosnim asocijacijama mogu biti direktno postavljeni ključevi koji će se koristiti za šifrovanje a u tu svrhu se može iskoristiti i protokol za razmenu ključeva putem Interneta.

IPsec sistem zaštite se može posmatrati kao jednostavno i efikasno rešenje za zaštitu komunikacija baziranih na *IP* protokolu. Važna karakteristika ovog sistema jeste otvorenost i dokumentovanost kroz *RFC* i druge dokumente. Izbor *IPsec* sistema zaštite kao nosioca realizacije sopstvenog rešenja baziranog na sopstvenom algoritmu, rezultat je dugotrajnog i temeljnog ispitivanja postojećih alternativa .[21]

3.2.3.1.1. Režimi rada

Jedna od značajnih karakteristika *IPsec* sistema zaštite jeste podrška za dva osnovna režima rada: transportni i tunelski. Osnovna razlika između ova dva režima rada leži u tome da li se šifruju samo podaci protokola višeg nivoa ili kompletan *IP* datagram.

U slučaju tunelskog režima rada za svaki *IP* datagram kreira se novi *IP* datagram koji je sačinjen od novog zaglavlja i podataka u vidu šifrata originalnog *IP* datagrama. Osnovna potreba za tunelskim režimom rada proizilazi iz potrebe za prevođenjem mrežnih adresa (engl. *Network Address Translation*) i kreiranjem virtualnih privatnih mreža (engl. *Virtual Private Network*) .[21].

Za potrebe integracije sopstvenih kriptoloških sistema u *IPsec*, razlike između opisanih režima rada mogu se zanemariti, pre svega iz razloga što, gledano sa aspekta integracije sopstvenog šifarskog algoritma, isti principi važe za oba režima rada a ceo proces promene režima rada obavlja se automatski u okviru implementacije. [15].

3.2.3.1.2. Protokol Authentication Header

AH (Authentication Header) zaglavlje se u okviru *IPsec* protokola koristi za obezbeđivanje integriteta podataka i autentičnosti izvora *IP* datagrama [*RFC 2402*]. Dodatno, ovaj protokol omogućava i zaštitu od ponovljenih slanja istih datagrama. *AH* protokolom su pokriveni svi statični delovi *IP* datagrama - podaci protokola višeg nivoa i nepromenljiva polja zaglavlja.

AH protokol se može koristiti nezavisno ili u kombinaciji sa *ESP (Encapsulating Security Payload*) protokolom. Takođe, ovaj protokol se može koristiti u komunikaciji između krajnjih učesnika u komunikaciji, između mrežnih prolaza ili između krajnjeg učesnika, sa jedne strane, i podrazumevanog prolaza, sa druge strane.

Razlika između *AH* i *ESP* protokola na polju obezbeđivanja integriteta podataka i autentičnosti izvora ogleda se u tome što *ESP* protokol podržava samo rad sa podacima *IP* datagrama, odnosno ne podržava rad sa poljima zaglavlja (osim u slučaju tunelskog režima rada).

Struktura *IP* datagrama sa korišćenim *AH* protokolom razlikuje se u zavisnosti od toga da li se *IPsec* protokol koristi u transportnom ili tunelskom režimu rada.

Polje *SPI* (*Security Parameters Index*) ima dužinu od 32 bita. U ovom polju se nalazi bezbednosna asocijacija koja se koristi za dekapsulaciju paketa. Polje *Sequence Number* koristi se za zaštitu od tzv. *reply* napada. Polje *Authentication Data* sadrži *HMAC* (*hash message authentication data*) dužina 96 bita. Korišćenjem sadržaja ovog polja prijemna strana može (uz poznavanje tajnog ključa) utvrditi da li je došlo do izmena na *IP* datagramu u toku prenosa .[21].

3.2.3.1.3. Protokol Encapsulationg Security Payload

ESP (*Encapsulating Security Payload*) je ključni protokol *IPsec* arhitekture i dizajniran je da obezbedi više bezbednosnih servisa [*RFC* 2406]. Ovaj protokol se može koristiti nezavisno ili u kombinaciji sa *AH (Authentication Header*) protokolom. Takođe, ovaj protokol se može koristiti u komunikaciji između krajnjih učesnika, između mrežnih prolaza ili između krajnjeg učesnika, sa jedne strane, i podrazumevanog prolaza, sa druge strane.

Servisi koje će *ESP* protokol obezbediti određuju se kod podešavanja bezbednosne asocijacije za komunikaciju. Osnovni zadatak *ESP* protokola je da obezbedi poverljivost podataka koji se prenose korišćenjem *IP* i *IPsec* protokola. Dodatno, *ESP* obezbeđuje i proveru autentičnosti izvora, integritet poruka (datagrama, ne i celokupnog sadržaja komunikacije) a nudi i zaštitu od *reply* napada.

ESP protokol se može koristiti i za obezbeđivanje pojedinačnih servisa. Na primer, moguće je iskoristiti samo servis poverljivosti bez korišćenja servisa integriteta i provere autentičnosti izvora (bilo putem ESP ili AH protokola). Međutim, ovakva konfiguracija korišćenih servisa može dovesti do ugrožavanja servisa poverljivosti.

Servisi provere autentičnosti i integriteta poruka se često zajedno stavljaju pod servis autentičnosti. Bez uključivanja ovih servisa nije moguće iskoristiti *ESP* protokol za zaštitu od *reply* napada.

ESP protokol se može koristiti i da *IPv4,* i sa *IPv6* protokolom. *ESP* zaglavlje se umeće na kraju zaglavlja *IP* datagrama u transportnom režimu rada, odnosno pre enkapsuliranog zaglavlja originalnog *IP* datagrama u tunelskom režimu rada.

SPI (Security Parameters Index) polje zaglavlja ima dužinu od 32 bita i koristi se u kombinacii sa *ESP* protokolom i odredišnom *IP* adresom za jedinstveno određivanje bezbednosne asocijacije datagrama. Vrednosti od 1 do 255 su rezervisane za buduću upotrebu *SPI* polje zaglavlja je obavezno kod korišćenja *ESP* protokola. Vrednost 0 je rezervisana za lokalnu upotrebu i na mreži se ne smeju pojaviti datagrami koji je sadrže.

Polje *Sequence Number* je, takođe, dužine 32 bita i povećava se sa svakim poslatim datagramom. Ovo polje je obavezno čak i u slučajevima kada se ne podrazumeva zaštita od *reply* napada. Vrednost ovog polja se postavlja na 0 na početku komunikacije .[21].

3.2.3.1.4. Implementacija IPsec protokola:

S obzirom na to da *IPsec* predstavlja *de facto* standard za obezbeđivanje komunikacija zasnovanih na *IP* protokolu, postoji veliki broj implementacija za različite operativne sisteme, uređaje, protokole i sl.

Sa aspekta operativnih sistema često se koristi princip integrisanja implementacije u jezgro operativnog sistema a korišćenje konfiguracionih alata (*ISAKMP/IKE*) iz korisničkog prostora. Osim ovoga pristupa postoje i primeri korišćenja *IPsec* implementacija nezavisnih od jezgra operativnih sistema.

Linuks operativni sistem poseduje sopstvenu implementaciju *IPsec* protokola u okviru jezgra počev od verzije 2.6. Pre ove implementacije na Linuks operativnom sistemu su najčešće korišćene *FreeS/WAN, Openswan* i *strongSwan* implementacije koje su funkcionisale u vidu procesa odvojenih od jezgra operativnog sistema.

Kompanija Majkrosoft je počela sa integracijom sopstvene *IPsec* implementacije u operativne sisteme počev od 2000. godine. Danas, integrisanu podršku za ovaj sistem zaštite imaju operativni sistemi *Windows Vista, Windows Server* 2008, *Windows Server* 2003, *Windows XP, i Windows* 2000. Takođe, pomenuta *IPsec* implementacija je integrisana i u *Active Directory* servis.

Na *BSD* grupi operativnih sistema (*FreeBSD, NetBSD, OpenBSD*) uglavnom se koristi *KAME* implementacija. Ista implementacija se koristi i na *Mac OS X* operativnom sistemu. *OpenBSD* sistemi koriste i *NRL* (*United States Naval Research Laboratory*) implementaciju, odnosno, sopstvenu implementaciju baziranu na kodu pomenute implementacije.

Proizvodi kompanije *Cisco* koriste sopstvenu implementaciju u *IOS* operativnom sistemu. Operativni sistemi kompanije *IBM (AIX, z/OS)* koriste sopstvene implementacije. *Solaris*, operativni sistem kompanije *Sun*, koristi sopstvenu implementaciju .[21]

3.2.3.1.5. Internet Key Exchange protokol:

Protokol *IKE* (engl. *Internet Key Exchange*) je komponenta *IPsec* protokola koja je koristi za međusobnu proveru autentičnosti učesnika u komunikaciji i za uspostavljanje i upravljanje zaštićenim vezama (bezbednosnim asocijacijama, engl. *Security Associations, SA*). Trenutno aktuelna verzija ovog protokola je 2 (*IKEv2*).

Uspostavljanje zaštićenih veza jedna je od osnovnih funkcija *IKE* protokola. Kroz uspostavljanje zaštićene veze definišu se bezbednosni parametri neophodno za rad *ESP* i *AH* protokola, odnosno šifarskih algoritama koji obezbeđuju komunikaciju. [9].

Sve komunikacije *IKE* protokola podrazumevaju dve poruke - zahtev i odgovor. Ovaj par poruka naziva se razmenom (engl. *exchange*). Za obezbeđivanje pouzdanosti komunikacije zadužena je strana koje šalje zahtev - ukoliko se odgovor ne dobije u određenom vremenskom periodu strana koja šalje zahtev dužna je da zahtev ponovi ili prekine vezu. Prvi par poruke *IKE* protokola pri uspostavljanju veze (*IKE_SA_INIT*) služi za utvrđivanje parametara zaštićene veze, vremensku sinhronizaciju i razmenu *Diffie-Hellman* vrednosti. Drugi par poruka (*IKE_AUTH*) razmenjuje identitete učesnika, potvrđuje poznavanje deljene tajna i uspostavlja zaštićenu vezu.

IKE protokol podrazumevano radi na portu 500 ili 4500. Za razmenu poruka koriste se datagrami *UDP* protokola transportnolg nivoa. S obzirom da ovaj protokol ne nudi pouzdan prenos podataka sam *IKE* protokol sadrži funkcije za prepoznavanje i rešavanje gubitka paketa, višestruku isporuku istog paketa i falsifikovanje paketa.

Poruke *IKE* protokola su projektovane da budu kratke. Međutim, gornja granica poruka nije eksplicitno ograničena (osim specifikacijom da implementacije moraju da održe dužinu od 1.280 bajtova a preporučeno je da imaju mogućnost obrade poruka dužine do 3.000 bajtova, ili većih). Sam *IKE* protokol ne poseduje mogućnost fragmentovanja poruka.

Pri uspostavljanju bezbedne veze *IKE* protokol pored seta bezbednosnih protokola koji će biti korišćeni (*ESP, AH*) utvrđuje i koji će šifarski algoritmi biti korišćeni za te protokole. Inicijalno se lista podržanih šifarskih algoritama (transformacija) razmenjuje u vidu predloga. Za

svaki od algoritama mogu se javiti atributi ukoliko sam naziv algoritma nije dovoljan za jednoznačno određivanje željene transformacije (npr. dužina ključa kod algoritama koji podržavaju različite dužine) .[21].

Šifarski ključ koji se ugovori *IKE* protokolom može se koristiti ograničen period vremena, za šifrovanje ograničene količine podataka. Ova ograničenja ujedno predstavljaju i životni vek zaštićene veze za koju je ključ iskorišćen. Ukoliko se dostigne bilo koje od pomenuta dva ograničenja zaštićena veza se više ne sme koristiti, a ukoliko postoji potreba za daljim prenosom podataka mora se uspostaviti nova zaštićena veza. Za uspostavljanje nove zaštićene veze koristi se termin *rekeying*. Nova zaštićena veza se uspostavlja nešto ranije u odnosu na sam istek tekuće zaštićene veze, u cilju eliminisanja prekida u prenosu podataka.

3.2.4. Firewall (Fajervol):

Jedan od boljih načina zaštite računara i računarskih mreža je korišćenje *firewall*-sistema za kontrolu pristupa.Ovakav sistem radi po sistemu prihvatanja ili odbijanja zahteva za mrežnu komunikaciju.Postoji više vrsta *firewall* sistema neka rešenja su čak i hardverski vezana kao Cisco ASA uredjaji.Postoje 3 generacije *firewall* sistema.

Firewall-ovi se dele na namenske uredjaje i računarski softver.Uredjaji se češće koriste da zaštite veće mreže dok se softver koristi u obe svrhe nekad čak kombinovano sa uredjaj firewall-om radi još veće sigurnosti.

Prednost namenskog hardvera jeste što nema daljih instalacija softvera po ostalim računarima i delovima mreže,ali oni imaju svoju boljku jer ne štite sistem od napada iz unutrašnjosti,većina softverskih firewall-ova traži administratorske šifre što sprečava korisnike unutra mreže ako ne znaju šifre da instaliraju neželjene softver.U bilo kojoj većoj mreži bez dobro napravljene same mreže sa dobro odredjenim aktivnim direktorijumom i dalje ne sprečava korisnike da stavljaju ne odobrene softvere.

Osnove razlike izmedju generacija firewallova su:

-Sistemi **prve generacije** proveravaju pakete uz pomoću paket filtera koji gleda adresu I portove sa kojih je paket poslat i odredjuje da li će paket biti pušten ili blokiran.Primer prve generacije firewall-ova je Gufw firewall.Prve generacije rade uglavnom samo na 3 lejera OSI referentnog modela koje uglavnom obuhvataju jako malo gledanja u transportni lejer.

-Sistemi **druge generacije** rade do četvrtog nivoa lejera OSI modela ovo postižu tako što zadržavaju pakete dok im se ne odredi tačno stanje.Bombardovanje paketima je slabost ovih firewall ova jer im usporavaju rad eventualno se dešava da takav system mora da se resetuje ili slično da bi nastavio sa normalnim radom.

-Sistemi **treće generacije** gledaju čak do aplikativnog nivoa ,sedmog nivoa OSI modela .Glavna prednost ovih firewall-ova je što mogu da nauče kojim aplikacijama pripadaju koji portovi i koje protokole koriste aplikacije da bi ostale neželjene konekcije bile zaustavljene.

Firewall-ovi se mogu podeliti na osnovu uloga koje rade u mreži na lične i mrežne.Mrežni firewall se nalazi najčešće na mrežnim ulazima kod manjih mreža ili na bitnim spojnim tačkama kod većih,lični firewall štiti samo lokalni računar od pretnji.

3.2.5. Sistemi za otkrivanje i sprečavanje napada:

Za razliku od fajervol sistema koji svoje odluke o dozvoli ili zabrani određene mrežne komunikacije baziraju na statičnim polisama, sistemi za sprečavanje napada (engl. *Intrusion Prevention System, IPS*) su sofisticiraniji i za izvršavanje svoga zadatka - sprečavanje upada na sistem(e) koji štiti - koriste detaljniju analizu (sličnu fajervol sistemima treće generacije) a ponekad i „inteligentne“ algoritme koji imaju mogućnost da razviju model „normalnog“ ponašanja i da odbiju sve zahteve koji ne spadaju pod taj model. Kao i fajervol sistemi, *IPS* sistemi mogu biti dizajnirani za zaštitu jednog računara (*Host based IPS, HIPS*) ili cele mreže (*Network based IPS, NIPS*).

Osim potrebe za odbranom od napada, u računarskim mrežama postoji i potreba za utvrđivanjem da li je do napada došlo i da li je napad uspešno obavljen. Iako na prvi pogled ove potrebe deluju manje važno, treba uzeti u obzir da cilj napada ne mora biti konačna akcija na napadnutom računaru već i kontinualna izmena podataka, sabotiranje obrade ili korišćenje resursa. Sa druge strane, uspešni napadi koji omogućavaju potpunu kontrolu napadnutog računara omogućavaju takvu izmenu log fajlova i alata za uvid u stanje sistema nakon koji više

nije moguće utvrditi ne samo da je računar bio napadnut već i da je računar još uvek pod kontrolom napadača. Na Unidž sistemima postoje tzv. rootkit alati koji iz log fajlova uklanjaju sve zapise o aktivnostima napadača a alate za uvid u stanje sistema (npr. uvid u liste procesa i fajlova na sistemu) zamenjuju izmenjenim alatima koji iz prikaza takođe izostavljaju procese i fajlove napadača. Računar na kojem je instaliran rootkit može godinama biti pod kontrolom napadača (što otvara mogućnost stalnog preuzimanja, izmene ili uklanjanja podataka i korišćenja resursa) a da nadležni administrator ne dobije ni najmanji nagoveštaj da je računar pod tuđom kontrolom. Uloga sistema za otkrivanje napada (engl. *Intrusion Detection System, IDS*) sistema je da prepozna uspešno obavljene napade, o tome obavesti administratora i eventualno ukloni zaostale komponente napada. *IDS* sistemi se veoma razlikuju i najčešće su strogo vezani za određeni operativni sistem ili okruženje. Sistem rada ovih sistema se kreće od jednostavne provere adekvatnih elemenata sistema putem alata koji se nalaze van dometa napadača do korišćenja „inteligentnih“ algoritama sposobnih da razviju model normalnog ponašanja u sistemu i na osnovu njega prepoznaju sve akcije korisnika koje odstupaju od tog modela. Pitanje koje se postavlja kod *IDS* sistema jeste zašto se sistemi koji imaju mogućnost da utvrde da je napad ostvaren ne iskoriste preventivno. Odgovor na ovo pitanje leži u oblasti rada *IDS* sistema jer *IDS* sistemi najčešće ne analiziraju mrežni saobraćaj već interne aktivnosti sistema do kojih dolazi, osim kod regularnog korišćenja, tek kada je napad ostvaren. Takođe, *IDS* sistemi najčešće imaju mogućnost da obustave sve aktivnosti na sistemu i obaveste o tome administratora ukoliko utvrde da je napad ostvaren .[21].

3.3. Standardni šifarski algoritni:

Osnovna podela šifarskih algoritama definiše dva tipa: simetrične i asimetrične šifarske algoritme. Simetrični šifarski algoritmi (šifrovanje tajnim ključem) rezultat su razvoja klasične kriptografije. Za uspešno korišćenje simetričnog šifrovanja korisnici pre toga moraju razmeniti ključ koji će biti korišćen za šifrovanje i dešifrovanje sadržaja. Osnove bezbednosti koju nude simetrični šifarski algoritmi leže u tajnosti ključa i nemogućnosti dobijanja originala bez njegovog poznavanja. U najpopularnije simetrične šifarske algoritme spadaju *AES, DES, RC4* i *Blowfish*.

Osnovna prednost simetričnih šifarskih algoritama je njihova brzina. Sa druge strane, osnovni problem kod njihovog korišćenja jeste uspostavljanje tajnog ključa, odnosno

neophodnost da se tajni ključ bezbedno dostavi do obe strane. U tu svrhu se najčešće koriste odvojeni komunikacioni kanali. To može biti značajan problem kod većih komunikacionih mreža jer se za potrebe bezbedne komunikacije mora izvršiti *n*-1 razmena ključeva (*n* je broj članova mreže). Jedno od rešenja za ovaj problem može biti centralno telo koje izdaje ključeve za komunikacione sesije.

Koncept asimetričnog šifrovanja predstavljen je 1976. godine od strane Vajtfilda Difija i Martina Helmana. U svom prvom radu kao osnovnu motivaciju ovi autori su naveli „eliminisanje potrebe za odvojenim komunikacionim kanalima za razmenu ključeva i stvaranje ekvivalenta pisanom potpisu“. Kod asimetričnog šifrovanja svaka strana ima par kljujčeva, *e* (javni ključ) i *d* (tajni ključ). Javni ključ je javno dostupan dok se tajni ključ čuva van dometa ostalih korisnika. Podaci šifrovani javnim ključem mogu se dešifrovati samo uparenim tajnim ključem. Sa druge strane, tajni ključ se može iskoristiti za potpisivanje digitalnog sadržaja, a javni ključ se u tom slučaju koristi za proveru autentičnosti potpisa. Podrazumeva se nemogućnost izračunavanja tajnog ključa na osnovu njegovog javnog para. Najpoznatiji predstavnici asimetrične kriptografije jesu Difi-Helman sistem razmene ključeva i *RSA* algoritam.

U poređenju sa simetričnim akvivalentima asimetrični sistemi za šifrovanje su uglavnom sporiji i nude niži nivo bezbednosti za istu dužinu ključeva (odnosno, zahtevaju korišćenje ključeva veće dužine. Sa druge strane, oni ne zahtevaju odvojene kanale za distribuciju ključeva, a nude i specifičnosti u pogledu elektronskih potpisivanja dokumenata. U praksi se često sreće mešovita upotreba simetričnog i asimetričnog šifrovanja - asimetrično šifrovanje koristi se za distribuciju ključeva simetričnih algoritama .[21].

3.3.1. Advanced Encryption Standard, AES*:*

Šifarski algoritam *Advanced Encryption Standard (AES)* jedan je od najpopularnijih šifarskih algoritama danas. Ovaj algoritam je odobren od strane *NIST*-a kao federalni standard za procesiranje informacija. U pitanju je simetrični blokovski algoritam za šifrovanje i dešifrovanje podataka. U praksi postoje različite softverske, firmverske i hardverske realizacije ovog algoritma.

AES algoritam može koristiti ključeve dužine 128, 196 i 256 bitova. Inicijalna specifikacija algoritma omogućavala je i druge veličine ključeva ali one nisu ušle u standard. Osnovna jedinica za obradu podataka kod *AES* algoritma je bajt, što znači da se ulazni podaci,

izlazni podaci i ključ za šifrovanje obrađuju u jedinicama od jednog bajta. Kod *AES* algoritma dužina ulaznog bloka, izlaznog bloka i stanja je 128 bitova. Interno, operacije *AES* algoritma izvršavaju se pod dvodimenzionalnim nizovima bajtova koji se nazivaju stanja. Ovi nizovi sadrže po četiri reda bajtova od kojih svaki sadrži *N* bajtove (*N* je veličina bloka podeljena sa 32).

Izvršavanje kod *AES* algoritma, odnosno broj rundi (engl. *number of rounds*), zavisi od dužine ključa. Za dužinu ključa od 128 bitova broj rundi je 10, za dužinu od 196 bitova je 12, a za dužinu ključa od 256 bitova broj rundi je 14. Za procese šifrovanja i dešifrovanja podataka *AES* algoritam koristi sledeće transformacije:

1. Zamena bajtova na osnovu tabele,
2. Smicanje redova matrice stanja po različitim veličinama,
3. Mešanje podataka u okviru kolone matrica stanja i
4. Dodavanje *Round Key* vrednosti (vrednost izračunata na osnovu ključa) matrici stanja .[21].

Na očetku procesa šifrovanja ulazni niz se kopira u matricu stanja. Nakon dodavanja *Round Key* vrednosti matrica stanja se transformiše korišćenjem funkcije zaokruživanja 10, 12 ili 14 puta, u zavisnosti od dužine ključa. Nakon zaokruživanja, matrica stanja se kopira u izlazni niz. Jedan od parametara funkcije zaokruživanja je jednodimenzionalni niz reči od po četiri bajta, dobijen na osnovuj *Key Expansion* rutine. Rutina *Key Expansion* na osnovu glavnog ključa generiše tzv. raspored ključeva (engl. *key schedule*) dužina *Nr* reči (*Nr* je broj ciklusa) od četiri bajta.

3.3.2. Data Encryption Standard (DES, 3DES)*:*

Šifarski algoritam *Data Encryption Standard (DES)* je simetrični blokovski šifarski algoritam, odobren od strane *NIST*-a kao jedan od federalnih standarda za procesiranje informacija. Ovaj algoritam je projektovan za šifrovanje i dešifrovanje podataka u blokovima dužine 64 bita. Ključevi koji se koriste za rad sa *DES* algoritmom takođe imaju dužinu od 64 bita od čega se 56 koriste za šifrovanje i dešifrovanje dok se preostalih 8 bitova koristi za prepoznavanje grešaka.

Prvi korak u šifrovanju podataka kod *DES* algoritma podrazumeva inicijalnu permutaciju (*Ip*). Nad rezultatom inicijalne permutacije se, zatim, vrše složene računske operacije (oznaka *f*) u kojima kao parametar učestvuje i ključ (nad kojim je izvršena funkcija za izračunavanje pod-ključa, *key scheduling, KS*) kojim se vrši šifrovanje. Nad rezultatom ovih operacija se izvršava proces reverzan inicijalnoj permutaciji (Ip^{-1}). Rezultatom ovih operacija dobija se šifrat, a reverznim operacijama vrši se njegovo dešifrovanje, odnosno dobija se original .[21].

Samo uvođenje *DES* algoritma kao standarda za šifrovanje pratili su različiti problem i nejasnoće. Razvoj ovog algoritma inicirao je *NIST* (tadašnji *NBS, National Bureau of Standards*) početkom sedamdesetih godina prošloga veka. Međutim, ispostavilo se da ni jedna od predloženih realizacija nije ispoštovala postavljene visoke standarde. Nakon konsultacija sa *NSA* agencijom prihvaćeno je rešenje koje je ponudila kompanija *IBM* a bazirano je na prethodno razvijenom *Lucifer* algoritmu autora Horsa Fistela. [20]

DES algoritam je kritikovan i od strane Martina Helmana i Vajtfilda Difija koji su ukazali na skraćivanje ključeva i misteriozne *S* boksove, kao posledice uticaja *NSA* agencije na razvoj algoritma. Pretpostavlja se da je bilo u pitanju namerno oslabljivanje algoritma u cilju omogućavanja razbijanja šifrata od strane vladinih agencija. I pored svih navedenih problema sa ovim algoritmom on se i danas u praksi često sreće u svojoj *3DES* varijanti.

3.3.3. RSA*:*

Šifarski algoritam *RSA* dobio je ime po svojim autorima Ronu Rajvestu, Adiju Šamiru i Leonardu Adlemanu (*Rivest-Shamir-Adleman*). U pitanju je asimetrični šifarski algoritam koji se, osim za šifrovanje podataka, može koristiti i za pitpisivanje elektronskih dokumanata.

Asimetrični rad *RSA* algoritma podrazumeva postojanje dva ključa - javnog i tajnog. Javni ključ se sastoji od dva pozitivna cela broja - modula i javnog eksponenta. Privatni ključ *RSA* algoritma može se predstaviti na dva načina: preko modula i tajnog eksponenta (pozitivni celi brojevi), ili prako sedam parametara - prvi faktor, drugi faktor, prvi faktgor *CRT* (*Chinese Remainder Theorem*) eksponenta, drugi faktor *CRT* eksponenta, prvi *CRT* koeficijent, *i*-ti faktor, *i*-ti faktor *CRT* eksponenta, *i*-ti faktor *CRT* koeficijenta.

Šifarski algoritam *RSA* predstavlja grupu asimetičnih algoritama. Osnovna prednost ovih algoritama, u odnosu na simetrične šifarske algoritme, jeste mogućnost da se između dve strane izvrši razmena šifrovanih podataka a da nije neophodna prethodna razmena ključa zaštićenim

kanalom. Sa druge strane, simetrični šifarski algoritmi obično nude bolje performanse u radu, a njihova bezbednost ne zavisi od protokola za inicijalnu razmenu ključa . [21]

3.4. Trendovi:

Trendovi vezani za bezbednost su u direktnoj vezi sa opštim trendovima na polju računarskih i telekomunkacionih mreža, odnosno sa vrednostima realnog sveta koje se prenose njihovim kanalima. Na osnovu različitih istraživanja kao najvažnije oblasti za ispitivanje bezbednosnih trendova izdvajaju se:

1. Neovlašćeni pristup,
2. Problem insajdera i
3. Krađa identiteta .[21]

Još jedna značajna karakteristika izdvojenih oblasti jeste njihovo često preplitanje, odnosno povezan uticaj različitih faktora. Na primer, neovlašćeni pristup resursima često se dešava kao posledica saradnje sa insajderima, ili kao posledica krađe elektronskog identiteta osobe koja je ovlašćena za pristup elektronskim resursima. [10]

Anketa koju je 2004. godine vodio *CSO* magazin u saradnji sa Američkom bezbednosnom službom i koordinacionim centrom *CERT*-a, pokazuje da bivše ili trenutno zaposlene ili privremeno angažovane osobe predstavljaju drugu po redu najznačajniju pretnju poslovnim sistemima. Jedan od značajnih faktora koji utiče na ovaj problem jeste sve veća mogućnost ostvarivanja materijalne koristi putem neovlašćenog prisvajanja elektronskih podataka umesto materijalnih dobara. Počinioci kriminalnih radnji baziranih na insajderima u velikoj većini slučajeva podrazumavaju insajdere - zaposlene - kao direktne počinioce a u ostatku slučajeva zaposleni najčešće omogućava spoljnom napadaču pristup određenim informacijama ili funkcijama.

Po rečima bezbednosnog eksperta Garija Barneta iz firme Ovum jedna od karakteristika 2009. godine će biti i primena bezbednosnih lekcija naučenih ranijih godina u poslovnim sistemima. Sa sledećim Barnetovim stavom slaže se i Majk Gilespi, direktor bezbednosti konsultantske firme Adventim - u 2009. godini će se znatno poraditi i na zaštiti podataka od slučajnog ili namernog uništavanja ili tzv. „curenja“ u javnost.

Oliver Fridrih, menadžer u kompaniji Simantek, ukazuje i na bezbednosne probleme koji se mogu javiti kao posledica ubrzane primene koncepta virtualizacije računara. „Brzina i lakoća kojom se mogu uvoditi virtualni računari može uspavati ljude po pitanju razmatranja pravilnog obezbeđivanja virtualnih računara i okruženja u kome se nalaze“ navodi Fridrih. [7]

Bezbednosni koncepti koji se predstavljaju u ovom radu podrazumevaju uključivanje malog broja ljudi u proces ostvarivanja i održavanja bezbednosti. Dodatno, predstavljeno rešenje se bazira na nižim slojevima *OSI* i *TCP/IP* modela i potpuno je van vidljivosti i upravljanja od strane krajnjih korisnika. Ove osobine znatno smanjuju rizik koji potiče od insajdera.

4. Pretnje, napadi, sigurnost i metode zaštite:

4.1. Napadi i pretnje:

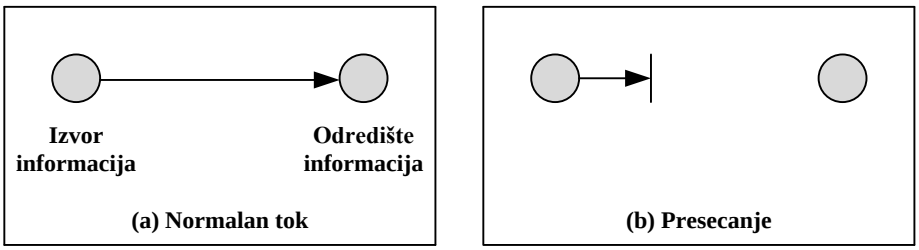
Da bi se što bolje zaštitile neke organizacije i da bi se odabrali odgovarajuće sigurnosne mere procedure i rešenja ljudima koji su odgovorni za sigurnost mreže u firmi potrebno je sistematično definisati zahteve ,jedan od pristupa je da se razmotre tri aspekta sigurnosti informacija.Ta tri aspekta su napad na sigurnost,sigurnosni mehanizam i sigurnosna usluga.

1. **Sigurnosna usluga-**(security service) je usluga koja povećava sigurnost sistema ona ujedno uključuje upotrebu više sigurnosnih mehanizama ako je potrebno
2. **Napad na sigurnost-**je bilo koja vrsta napada ili akcije koja ugrožava sigunost informacija.
3. **Sigurnosni mehanizam** je mehanizam koji treba da detektuje ili predupredi napade nekad ujedno da oporavlja sisteme od napada.

Napadi su u osnovi prosto akcije koje ugrožavaju računarske sisteme i mreže . Delimo vrste napada u četiri kategorije:

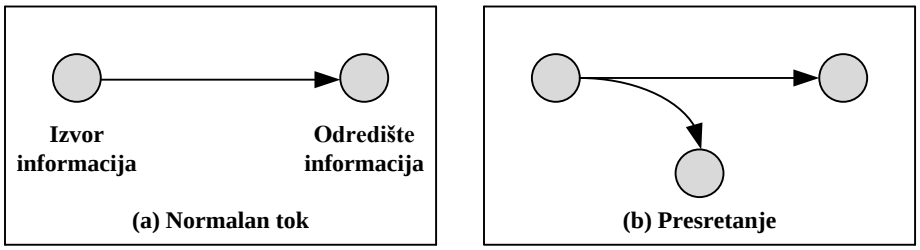
1. **Presecanje**, tj. **prekidanje** (engl. *intgerruption*) predstavlja napad na **raspoloživost** (engl. *availability*). Presecanjem se prekidaju tokovi informacija ujedno se

onemogu'avaju pristupi odredjenim uslugama ili funkcionisanja sistema,presecanje spada u aktivnu vrstu napada.



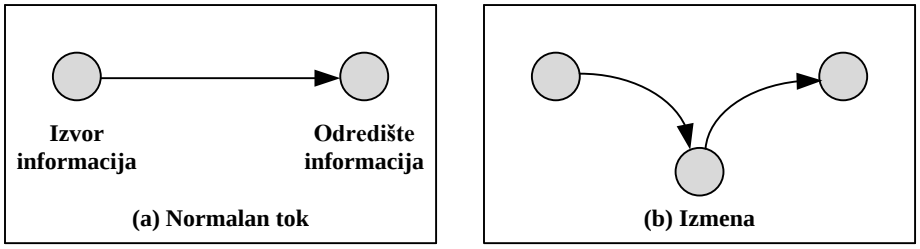
Slika 6. Presecanje

2. **Presretanje** (engl. *interception*) predstavlja vrstu napada koja služu više kao mera nadgledanja i čuvanja tudjih bitnih informacija to je vrsta pasivnog napada zato je teže otkriti.Kao svako presretanje informacija ono može služiti radi poboljšanja drugih možda ne aktivnih napada.



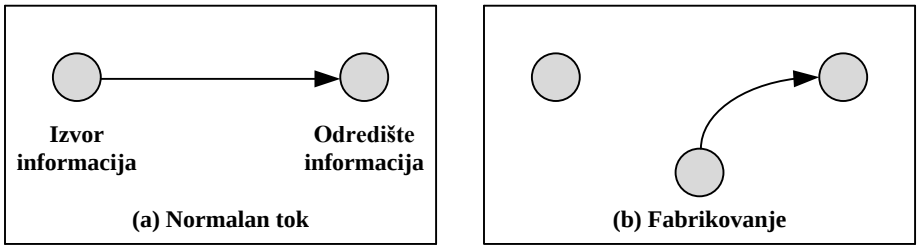
Slika 7. Presretanje

3. **Izmena** je vrsta napada koja predstavlja napad na integritet. Kada se ova vrsta napada dešava na prenosnom putu onda se može računati kao **covek u sredini** (man in the middle) vrsta napada. Ova vrsta napada se može izvesti i sa unutrašnje strane tako što menja date privilegije odredjenom računaru korisniku. Iako ova vrsta napada menja podatke često ostaje neprimećena zbog korišćenosti složenih tehnika prilikom napada.



Slika 8. ***Izmena***

4. **Fabrikovanje** (engl. *fabrication*), slika 9, predstavlja napad na **autentičnost** (engl. *authenticity*). Napadač izvodi ovaj aktivni napad tako što generiše lažne podatke, lažni saobraćaj ili izdaje neovlašćene komande. Veoma često se koristi i lažno predstavljanje korisnika, usluge, servira, Web strane ili nekog drugog dela sistema.

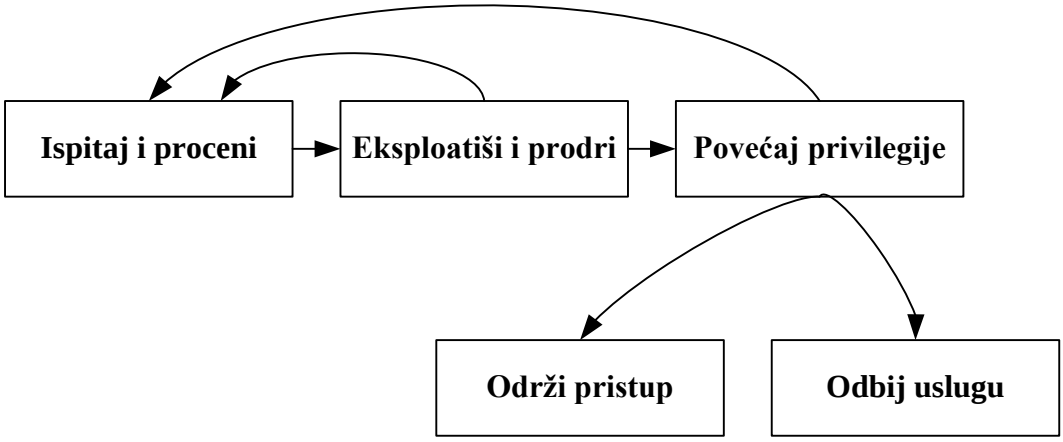


Slika 9. Fabrikovanje

Anatomija napada:

Ako se shvata napadacev pristup koji koristi da prodre u neku vrstu sistema lakše je odbraniti se od njega ko se znaju metode koje bi koristio.

Ispitaj i proceni je prvi korak koji napadač preduzima.Ispitaj i proceni se zasniva na istraživanju mete procene njenih karakteristika.Ispitaj i proceni je vrsta pripreme pred prave aktivne vrste napada.



Slika 10. Osnovni koraci napada

1. **Eksploatiši i prodri** Posle ispitivanje slabosti ili ranjivosti neke mreže napadač pokušava da iskoristi ranjivost i prodre u sistem.Ako je mreža ili umreženei računar potpuno osigran napadač može koristiti aplikaciju ili internet stranica za prijavljivanje na odredjenje sajtove .
2. **Povećaj privilegije** Ovaj korak se dešava kada napadač udje u sistem, jedna od prvih stvari koju će raditi je sa mesta ulaza je da proširi sebi dostupnost podacima tako što ce sebi dati više privilegije ako je moguće čak i da uzme administratorske privilegijeDobro definisane privilegije mogu usporiti ovakvu vrstu napada znatno ili čak davanje privilegija koje aktivnim direktorijum ogranicava da će biti aktivne tek nakon 24h uz pomoću polisa bez pravog administratora i više provera.
3. **Održavanje pristupa-**Jednom kada uspe napadač da udje u sistem napadač će preuzeti mere da prikrije tragove i olakša buduće ulaženje u sistem . Jedan od češćih načina je korišćenje back-door programa ili postojećih naloga koji nisu zaštićeni. Jedna od najčešćih stvari je brisanje dnevnih logova i pravljenja nevidljivih aplikacije koje se mogu pronaći najčešće u servisimsa.Analize logova mogu otkriti uzrok problema pa čak i samog napadača.
4. **Odbijanje usluga-**Napadaci koji ne mogu da se izbore sa merama bezbednosti jedne mreže će pokušati da zaustave rad aplikacije iliti **odbijanje usluga**(**denial of service** attack DOS). Neki napadači, DoS je jedina vrsta napada koju koriste.

Pretnje i jednačina rizika:

Rizik je, u kontekstu sigurnosti računarskih sistema i mreža, mera opasnosti, tj. mogućnost da nastane oštećenje ili gubitak neke informacije, hardvera, intelektualne svojine, prestiža ili ugleda. Rizik treba definisati eksplicitno, na primer, „rizik od narušavanja integriteta bez klijenata“ ili „rizik odbijanja usluga od strane *on-line* portala banke“. Rizik se obično izražava u obliku jednačine rizika, gde je: Rizik = Pretnja x Vrednost imovine. [14]

Pretnja (engl. *threat*) jeste protivnik, situacija ili splet okolnosti s mogućnošću i/ili namerama da se eksploatiše ranjivost. Ova definicija pretnje stara je nekoliko decenija i konsistentna je s opisom terorista. Pretnja može biti strukturirana ili nestrukturirana. Strukturirane pretnje su protivnici s formalnom metodologijom, finansijskim sponzorom i definisanim ciljem. Takve pretnje su karakteristične za ekonomsku špijunažu, organizovani kriminal, strane obaveštajne službe i takozvane „informatičke ratnike“. Pretnje se dele na pasivne i aktivne.

Ranjivost (engl. *vulnerability*) predstavlja slabost neke strukture,vrednosti ili čak u vrsti programa ili bilo čega na šta se odnosi specificno kod mreža i aplikacije ranjivost se odnosi na par stvari:

- **Loše projektovanje** je greška projektanta sistema. Loše projektovanje softvera ili čak hardvera koji se lako pregreva i kvari je ono što gradi tržište ili nesigurnih softvera koji su puni bug-ova.Napadač koji zna takve klasične mane nekih proizvedenih softvera sistema može da ih i iskoristi da uruši nestabilnu bazu podataka ili da preseče jedan deo mreže od drugog dela mreže jer je bilo naročito lako doći do drugih uredjaja.
- **Instaliranje iliti implementacija** je odgovornost ososbe koja instalira proizvod.I pored silnih dokumentacije nekad je jednostavno najbolje pozvati ljude specijalizovane za takve stvari.
- **„Zagađenje“** se odnosi na pogrešne pristupe nekih aplikacija recimo paragraf lex i neki drugi programi zahtevaju konstantne administratorske privilegije u odredjenim aspektima što može dati dobrom hakeru ili programeru moć da ih iskoristi da upadne preko njih i njihove baze podataka gde će mu sve biti na poslužavniku.Prosto neke aplikacije zahtevaju više privilegija nego što odredjeni aspekti samih tih aplikacije bi trebali da daju krajnjim korisnicima.

Vrednst imovine je mera uloženih resursa vremena koji bi trebali da se vrate prilikom havarije.Problem je što iako je lako definisati neki podaci koji nigde nisu bili backupovani koji su permanentno izgubljeni posle par godina mogu biti po definiciji cene zamene van bilo kakve vrednosti iliti ne zamenjive.Stvar je prosta kod pregrejanog dela hardvera miningom ili nečim sličnim može biti monetarno vraćena/zamenjena olako.

4.1.1. Modelovanje pretnji:

Modelovanje pretnji nikada ne bi trebao da bude proces koji se obavi i posle toga se više ne radi na tom aspektu zaštite.Ljudi brzo zaboravljaju kako tehnologija brzo napreduja ujedno tako se i broj i vrste napadača povećavaju. Ažuriranje aplikacija treba da bude stalan proces pogotovo za borbu protiv nekih counter aplikacija kao virusa i sličnih.**Proces modelovanja** pretnji odvija se u šest faza, a može se primeniti i za postojeće aplikacije i za aplikacije koje se tek razvijaju.

1. **Identifikovanje vrednosti** se zasniva na odredjivanju ciljeva i utvrdjivanju stvari koje sistem treba da zaštiti
2. **Izrada pregleda arhitekture**. Korišćenjem jednostavnih dijagrama i tabela, dokumantuje se aplikacija, uključujući podstisteme, granice poverenja i tokove podataka,
3. **Dekompozicija aplikacije**. Kada je gotova aplikacija onda je vreme da se ponovo dekomponuje da vi se videlo kako najbolje napraviti sigurnosni profil.
4. **Identikovanje pretnji**. Imajući u vidu ciljeve napadača i poznajući arhitekturu i moguće ranjivosti aplikacije, identifikuju se pretnje koje mogu da ugroze aprikaciju,
5. **Dokumentovanje pretnji**. Normalno se pretnje identifikuju i stavljaju u šablone po nekim karakteristikama koje ih definišu.
6. **Rangiranje pretnji**,Pretnje se rangiraju prema vrsti napada,štete koju mogu da čine.To pomaže pravljenju redosleda iliti rangiranju pretnji ,da bi se prvo rešavale najznačajnije pretnje.

4.1.2. Najčešće primenjivani napadi i pretnje:

Razlićite vrste napada na računarski sistem i mreže se mogu uraditi na mnogo načina,devedesetih je bio ogroman problem sa worm programima iliti crvima.Najčešće vrsta napada na računar su njuškanje,ubacivanje zlonamernih programa,lažiranje IP adresa.

- **Odbijanje usluga** je vrsta napada koja izaziva prestanak rada programa odredjenih servisa.DoS napadi se najlakše vrše na transportnom sloju slanjem velikog broja zahteva za konekciju,zaštita se postiže kontrolisanjem broja zahteva u jedinici vremena.
- **Lažiranje IP adresa** Napadač menja svoju adresu u kodu i predstavlja se kao računar iz mreže.Lažiranje IP adresa uspeva da radi zahvaljujći tome što DNS servis ne proverava odakle dolaze informacije.Najbolja zaštita od ove vrste napada je rutiranje ,router ce odbijate sve pakete koji sadrže adrese lokalne mreže a stižu na javni interfejs rutera.
- **Njuškanje** (*sniffing*). Njuškanje se zasniva na presretanju TCP/IP paketa koji dolaze do odredjenog računara i pregledanja sadržaja tih paketa.Vrste njuškanja su trojanski konji,vrste prelivanja bafera.
- **Trojanski konj** (*trojan horse*) je segment kods,podmetnut u neki program koji može da menja funkcija ili da utiče negativno na rad nekog programa.Specijalne varijante trojanskog konja su napravljene koje oponašaju procedure prijavljivanja na sistem ili mrežu,prosto rečeno skida podatke od pravog korisnika da bi napadač obezbedio ulaz na tudj računar/server ili pristup nekoj aplikaciji.
- **Klopka** (*trap door*). Kreator programa može greškom ostaviti prazna mesta u kodu. Na primer, zaokruživanjem iznosa transakcija u odredjenim aplikacijama,može predstavljati vrstu klopke u slučaju da se ostali deo iznosa prenosi na račune programera.Klopka je komplikovana vrsta prevare koja zahteva pregled celog koda da bi bila otkrivena.
- **Buffer overflow**-iliti prekoračenje bufera je vrsta anomalije gde prgraom dok piše podatke u bufferu predje granice bufera i utiče negativno na dinamičku memoriju.Prekoračenja bufera mogu da utiču na sistem rada programa i da stvaraju česte plave ekrane zbog pada sistema.
- **Crvi** su samostalna zlonamerna vrsta programa koja se širi po sistemu i može sa računara na računar obično ima lake metode da zavara korisnika da pokrene takav program.Crv utiče na rad računara na više načina smanjuje slobodno mesto i mahom povećava

procenat korišćenja svih komponenti,u poslednje vreme postoje miner programi koji u isto vreme koriste komponente da se bave data-miningom bitcoine.

4.2 Šta je sigurnost:

Sigurnost je proces održavanja jednog stanja mreže u kom se minimalizuju pretnje koje i samo treba da se stalno updatuje novinama. Organizacija ili institucija ne može se smatrati „sigurnom“ ni u jednom trenutku posle izvršene poslednje provere usklađenosti s vlastitim sigurnosnim pravilima. Jednostavno rečeno, ako vas iko pita o sigurnosti mreže treba uvek reći da je uradjeno maksimum sa datim resursima jer bilo šta preko toga bi bilo suviše reći.

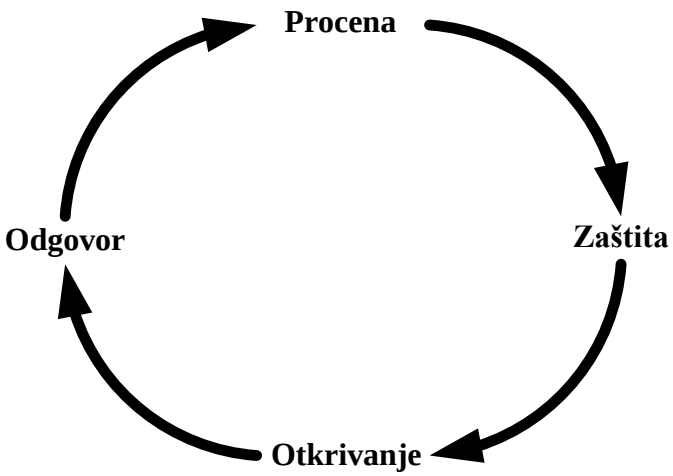
Svetske kompanije često reklamiraju svoje proizvode kao sigurna rešenja proverena iako se retko ko posmatra da u toku kupovine je to rešenje samo trenutno može imati reklamiran status odbrane.Čak i da je proizvod bio srebrni metak u jednom periodu do perioda kupovine ako nije neka vrsta usluge koja se konstantno dopunjuje sa novinama izmenama iliti update-uje mala šansa da pruža reklamirane mere zaštite.Iz toga možemo reći da je sigurnost dugotrajan proces koj treba stalno dogradjivati i unapredjivati i kao svaka druga sigurnost,sigurnost mreže nikad ne može biti potpuna i apsolutna samo da je efikasno napravljena.

Prosto govoreći veća ulaganja u sigurnost računarskih mreža i sistema smanjuje rizik iliti pravilo da ako mnogo jeftiniji uredjaj štititi skuplji da je velika šansa da će skuplji uredjaj da permanentno prestane sa radom.Zato je veoma bitno da se što bolje iskoriste uložene pare,savršene kanalice ništa ne vrede ako je sam provodnik u njima slabog kvaliteta jer je on sam sebi opasnost.

Ujedno kako se povećava sigurnost i smanjuje opasnost od havarija i upada u sistem ili ko računarskih mreža to može dovesti do usporenosti rada i može da poveća vreme potrebno da se urade odredjene operacija čak i onemogući. Pitanje balansa kao i uvek ako je sistem pre-zaštićena da stalno prolazi kroz stres od više procedura za naj sitnije radnje i mnogo usporava posao tada je to podjednako loše zbog produktivnosti kao virus iliti neke od vrsta napada na samu računarsku mrežu.

Sigurnost kao proces koji traje se zasniva na sledecim osnovnim koracima:procena,zaštita,otkrivanje i odgovor.

1. **Procena** se oduvek smatra ključnom pre odlučivanja za odredjene mere zaštite, jer loša procena može dovesti do većih problema prilikom samog kreiranja nekog informacionog sistema ili mreže.
2. **Zaštita** ili prevencija je sledeći logički korak koji se zasniva na primeni prtivmera.Vremenom većina zaštita zakaže što nas vodi do sledećeg koraka to je otkrivanje.



Slika 11. Sigurnost kao proces

3. **Otkrivanje** iliti detekcija se zasniva na detektovanju povreda sigurnosnih mera updaa ili uopsteno povreda sigurnosnih pravila jednog sistema.Sama detekcija po sebi ne može da spreči pretnju što nas vodi do sledećeg koraka a to je sprečavanje iliti odgovor na pretnje.
4. **Odgovor** je vrsta reakcije koja ujedno sprečava problem i prati ga do odredišta da bi se permananentno rešila tog problema.Ujedno odgovor uključuje i oporavak samog sistema od posledica upada/virusa i nekih drugih štetnih stvari po mrežu ili neki informatički sistem.Pravna sredstva su uvek bila način rešavanja takvih stvari pa se i danas koriste

4.2.1 Sigurnosni ciljevi:

Tri fundamentalna kriterijuma kroz koja se posmatraju sigurnosni ciljevi su (Confidentiality,Integrity,Availability) skraćeno CIA:

1. **Poverljivost** (*confidentiality*). Poveljivost obuhvata sve vrste pokušaja da se spreči namerno i neovlašćeno otkrivanje i korišćenje.
2. **Integritet** (*integrity*). U okviru sigurnosti informacija, koncept integriteta se zasniva na tome da podatke ne smeju menjati neovlašćena lica ili procesi,lica ne smeju obavljati promene za koje nisu autorizovana,podaci su medjusobno konzistentni.
3. **Raspoloživost** (*availability*). Koncept raspoloživosti obezbedjuje uslove da se može lako pristupati željenim informacijama,uredjajima u mreži ili resursima. Prosto rečeno raspoloživost znači da svi sistemi rade kao što im je predvidjeno.

4.2.2. Sigurnosne usluge:

Sigurnosna usluga je usluga koja povećava sigurnost kao što smo pre rekli usluga koja povećava sigurnost sistema.Sigurnosni mehanizmi se menjaju konstantno dolaskom novih tehnologija i novim sistemima zaštite.Da bi se izabrale prave mere stanje na tržištu bi se moralo proveravati redovno.

U sigurnosne usluge spadaju:

Provera identiteta je usluga koja zahteva od svakog korisnika da se predstavi sistemu pre nego što uradi nešto,ona ujedno obezbedjuje načina identifikacije nečega ili nekoga uz pomoć ID,pinovam,korisničkih imena kartica pa čak i bio skenera.Provera identiteta ujedno može d asadrži istoriju promena koje je željeni korisnik uradio za svoj interval vremena proveden u zaštićenoj ustanovi/prostoru.

Poverljivost iliti privatnost je značajna sigurnosta usluga a takodje se ciljevi mnogih savremenih projektovanja zasnivaju na njoj.Privatnost u najopštijem smislu je skrivanje informacije od javnosti i njihovog curenja u javnost.Privatnost može biti vezana za anonimnost,privatnost najviše cene ljudi koji su izloženi javnosti.Prosto rečeno privatnost je sigurnosna usluga koja drži informacije u zatvorenom krugu korisnika i nikome više.Privatnost dobija na značaju u sukobu više suprostavljenih interesnih grupa.Po ISO standardu je poverljivost iliti privatnost informacija definisana kao usluga obezbedjivanja pristupa informacijama za one korisnike koji su ovlašćeni da pristupe tim datim informacijama. Podaci se moraju štititi kad su uskladišteni, tokom obrade i prilikom prenosa,

Integritet je usluga koja obezbedjuje sigurnost podataka kao jedne celine kojoj ne bi trebala da se desi promena sa strane napadača a da pritom ostane neprimećena sama promena.Integritet je vrsta usluge koja sprečava modifikovanje poruke tokom obrade,transporta ili čak skladištenja a sistem bi trebao da izvršava predvidjene operacije iliti usluge bez spoljašnjeg manipulisanja.

Neporicanje, priznavanje (*non-repudiation*) je koja koriniku obezbedjuje prilikom izmena podataka uvid ko je to uradio i da bi osoba odgovorna za date promene bila lakše utvrdjena.Takva vrsta sigurnosne usluge sprečava sporove iznošenjem jasnih dokaza.

Kontrola pristupa kontrola pristupa je sigurnostna usluga koje sprečavan neovlašćenu upotrebu odredjenih resursa.Pomoću ove kontrole se dozvoljava objektu sa proverenim identitetom i odgovarajućim ovlašćenjima da pristupi radu na odredjenim stvarima ili raznim uslugama.Kontrola pristupa naj prostije rečeno odredjuje ko i kada ima pristup čemu i na kakav način.

Raspoloživost, upotrebljivost (engl. *availability*) - usluga kojom se obezbeđuje dostupnost podataka i raspoloživost sistema koji pruža neke usluge. Primeri takvih usluga su sprečavanje DoS napada i sprečavanje napada virusa koji brišu ili oštećuju datoteke.

4.2.3. Strategije ostvarivanja sigurnosti:

Softverska i hardverska rešenja sama po sebi ne znače uopšte puno ako se ne koriste sa strane obučenog osoblja i za stvari za koje su sami urejdaji namenjeni da rade. Da bi se postigli željeni rezultati treba imati obučene ljude jer neke male greške kao pogrešna adresiranja ili korišćenja routera kao switch mogu dovesti do problema prilikom dodavanja novih delova mreže iliti dodatnih mrežnih uredjaja.Mreža ujedno mora biti zaštićena i fizički,server sala bi trebala da bude dobro obezbedjena protiv havarija uključujući i fizički obezbedjena.

4.2.4. Slojevita zaštita:

Više slojna zaštita je jedna od najviše upotrebljenih vrsta zaštite u mreži, koja se zasniva na formiranju više odgovora na više pretnji i njihovom usporavanju.. Korisnik u slučaju prolaska kroz više slojeva zaštite mora zadovoljavati sve sigurnosne mehanizme koji zadržavaju napadača ili minimiziraju njegovu mogućnost pristupa kritičnim resursima. Više slojni pristup treba da obezbedi kombinaciju sigurnosnih mehanizama i tehničkih rešenja koji obuhvataju dovoljno širok asortiman sigurnosnih zahteva. Trebalo bi onemogućiti da probijanje jednog sloja ima katastrofalne posledice po sigurnost celog sistema. Verovatnoća da bude probijeno više slojeva mnogo je manja od verovatnoće probijanja jednoslojne zaštite.

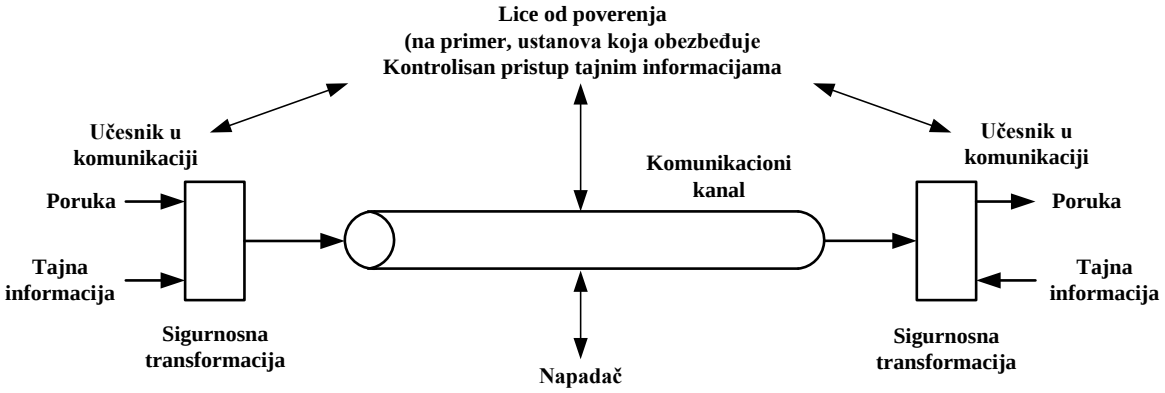
1. Spoljašnji sloj je granica između jednog sistema i spoljašnjeg sveta u slučaju računarskih mreža uglavnom interneta.Spoljašnjem sloju glavne provere vrše firewall,router i DNS server.Sloj ovakve vrste je uglavnom lako dostupan deo neke privatne mreže,mogao bi da bude i javno pristupan deo mreže.
2. Treći zaštitni sloj štiti sistem od unutrašnjih vrsta napada i čine ga vrste razne mrežne barijere,VPN,anyconnect i uopsta vrste sigurnih tunela.
3. Drugi sloj su praktično najnoviji update i zakrpe operativnih sistema,serverske opreme koje sprečavaju stvaranja kvarova,pored svega toga sama oprema treba biti fizički zaštićena.

4. Unutrašnji sloj štiti informacije i vrste podataka koji se čuvaju na databazama u samom sistemu.Sigurnosni mehanizmi u ovom slojuu čine lozinke,kartice i PIN provere,kontrola provera pristupa na osnovu IP adrese sa koje neki korisnik pristupa i praćenje istih.

4.2.5. Sigurnosni modeli:

Prema mestu sigurnosne transformacije i funkcija koje ta transformacija obavlja delimo uočavaju se dva sigurnosna modela.

Prvi model je prikazan na slici broj 12 on pokazuje kada se protok informacija dešava preko nesigurno komunikacionog kanala izmedju dva učesnika uz postojanje napadača. Učesnici primenjuju sigurnosne transformacije sa ciljanim vrstama tajnih informacija koje obezbeduju lica kojima veruju oba učesnika u komunikaciji. Ovo je jedan od načina kako zaštiti komunikacioni kanal od napadača jer u ovakvom slučaju napadač ne bi mogao da dobije skrivenu informaciju. Jedna od vrsti sigurnosnih transformacija može da bude šifrovanje sa javnim ključem, a lice od poverenja bi mogla da bude neka institucija koja će učesnicima u razmeni podataka iliti komunikaciji distribuirati neke vrste javnih ključeve i time obezbediti potvrdu usaglašenosti identiteta učesnika i ključa. (Jedan od načina je i izdavanje odgovarajućih sertifikata.)



Slika 12. Model s nesigurnim komunikacionim kanalom

Druga vrsta modela je kontrolisana vrsta pristupa resursima i podacima računarskog sistema u slučaju prisustva napadača ili potencijalnih napadača. Unutar samog sistema se kontroliše pristup (na primer, mrežna barijera koja obezbeđuje pristup na odredjen način samo određenim mrežnim servisima) čime se postiže sigurnost. Jedan od načina zaštite u ovom modelu je korišćenje kriptografskih tehnika.

4.2.6. Klasifikovanje informacija:

Koncept vlasništva je jedan od bitnijih koncepta politike zaštite informacija. Ovaj koncept obezbeđuje da su skoro svi računarski resursi - glavni informacioni entiteti (razne vrste baza podataka,vrste prenosnih puteva i etc) –imaju vlasnika, koji:

- Vrši klasifikovanje informacije u jednu od klasa koje su na raspolaganju,
- Označava lica koja imaju pristup podacima,
- Odgovara za podatke i zaštitu istih.

4.2.6.1. Klasifikovanje tajnosti informacija:

U zavisnosti od značaja informacije se dele u četiri osnovne klase koje su nastale pre dolaska informatičkog doba ali su i dalje validne: javne, interne, poverljive i tajne informacije.

1. **Javne informacije** – Javne informacije su one čije otkrivanje ne bi trebalo da nnesu štetu preduzeću. Ovakvoj vrsti informacija integritet nije važan. Nedostupnost ovakvih vrsta podataka , u nekim slučajevima, može biti i kažnjiva, zavisno od regulativa zemlje u kojoj se kompanija nalazi. Objave osnovnih podataka o preduzeću, javnih nabavki, ugovora na sajtovima javnih preduzeća su jedna od vrsta javnih informacija.
2. **Interne informacije** – Pristup ovakvim informacijama je selektivan iako neke od njih mogu postati javne informacije. Nivo klasifikacije treba da bude označen na svakom dokumentu. Sprovođenje ovakvog načina rukovanja sprečava javno iznošenje informacija. Neki od primera su: interni telefonski imenici, radni dokumenti (npr. nacrti tenderskih dokumentacija), projekti koji su u toku, itd.
3. **Poverljive informacije** – Ovoj klasi pripadaju podatci koji se moraju zaštititi od spoljnog pristupakoji su zaključani. U savremenom poslovanju oni su dostupni u svim pačunskim centrima, pa je neophodno da računari budu u prostorijama koje se zaključavaju. Originali dokumenta se čuvaju na bezbednim mestima a moraju se šifrovati u slučaju slanja preko interneta. U zavisnosti od vrste, dokumenti se arhiviraju ili uništavaju kada više ne budu aktuelni. Loša politika pristupa takvim informacijama može naneti velike gubitke kompanijama ili čak ugroziti odredjene vrste institucija.Primeri su: ugovori u nekim od preduzeća (izuzetak su javna preduzeća), podaci o zaposlenima i njihovim platama, tehničke specifikacije odredjenih projekata.
4. **Tajne informacije** – Pristup ovakvim podacima ima mali broj ljudi unutar institucije, jer bi neodgovorno odnosno neovlašćeno pristupanje dovelo do njenog razaranja. Integritet je veoma važan i proporcionalan vrednosti podataka. Podaci i dokumenta moraju da budu strogo čuvani sa izuzetno jakim lozinkama, nekad i šifrovani, i dobro fiziči zaštićeni. Gubitak ovakvih informacija dovodi do urušavanja institucija, ponekad i država. Najbolji primer toga su vojni podaci.

4.2.6.2. Drugi načini klasifikacije:

Rangirano od najnižeg na više u sistemima informacija na državnom nivou:

1. **Neklasifikovano** (engl. *unclassified*) – Podaci koji nisu toliko osetljivi i čije otkrivanje neće povrediti poverljivost
2. **Osetljivo ali neklasifikovano** (engl. *sensitive but unclassified, SBU*) – To su vrste malih tajni ali ne prave značajnu štetu ako su otkriveni. Primer su rešenja ispita i testova.
3. **Poverljivo** (engl. *confidential*) – Otkrivanje ovih informacija može izazvati štetu po predvidjene korisnike, može imati i ozbiljan uticaj i na nacionalnu sigurnost.
4. **Tajna** (engl. *secret*) – Podaci koji mogu da naprave štetu po državnu bezbednost ako budu neovlašćeno otkriveni ili date članovima konfliktnih grupa.
5. **Strogo poverljivo** (engl. *top secret*) – Ovakve informacije su na samom vrhu po klasifikaciji i rangiranju bitnosti informacija i one utiču na cele države i mogu da imaju fatalne posledice.

Sledeća terminologija koristi se za klasifikaciju informacija namenjenih privatnom sektoru:

1. **Javne** (*public*) –Razne vrste neklasifikovanih informacija koje ne spadaju u neku od dole navedenih kategorija se mogu računati kao javne informacije. Informacije ovakve vrste ne treba uvek da budu otvorene. Međutim u slučaju kada su otvorene, očekuje se da neće imati ozbiljan ili negativan uticaj na preduzeće.
2. **Oseljive** (*sensitive*) - Informacije bitnije od onih u grupi običnih podataka. Da bi se očuvalo poverenje u preduzeće ovakve informacije se zaštićuju od otkrivanja. Neophodna je i zaštita od neovlašćenih izmena.
3. **Privatne** (*private*) - Informacije privatne prirodekoje se isključivo koriste u firmi. Otkrivanje/objavljivanje informacija se negativno odražava na firmu i zaposlene. Primer su lični podaci o zaposlenim, njuhova primanja.

4. **Poverljive** (*confidential*) – Najosetljivije informacije i samo u internoj primeni. One predstavljaju izuzetak i ne podležu obavezi javnog objavljivanja prema Aktu o slobodi informacija (*Freedom of Information Act*). Otkrivanje informacija najčešće ozbiljno urušava preduzeće. Primer: razvoj novog proizvoda, preuzimanje/spajanje sa drugim preduzećem, smatra se poverljivim informacijama.

Jedna od jednostavnijih klasifikacija informacija a koristi se u privatnom i komercijalnom sektoru:

1. **Javna upotreba** - Informacije koje su otvorene za javnost,
2. **Samo interna upotreba** - Informacije koje se koriste samo u preduzeću,
3. **Informacije poverljive za preduzeće** - Osetljive informacije i njima raspolažu samo pojedinci, koji mogu i moraju da imaju saznanje.

4.3. Metode zaštite:

Za metode zaštite takođe postoji nekoliko pristupa i podela. S vremenom ove klasifikacije se unapređuju i menjaju sa razvojem tehnologije i računarskih sistema i mreža. Jedna od klasifikacija podrazumeva četiri grupe metoda zaštite:

- Kriptografske metode,
- Programske metode,
- Organizacione metode i
- Fizičke metode.

Obzirom sa se prema većini autora ovakva podela smatra zastarelom sve je masovnija primena šeme **deset domena sigurnosti** koju je definisala organizacija (ISC)2. Autori, koji definišu takozvane metode odbrane, klasifikuju ih na:

- Šifrovanje,
- Softverska kontrola pristupa (ograničenja u bazi podataka /operativnom sistemu),
- Hardverska kontrola pristupa (pametne kartice /biometrijske metode),
- Zaštitne polise (uvođenje pravila o učestalom menjanju lozinke),
- Fizička kontrola pristupa.

Kao što je već rečeno, kontrola pristupa dozvoljava korišćenje određenih usluga sistema samo objektu čiji je identitet proveren (ko ima pravo pristupa i na koji način):

- Kontrola pristupa je obavezna i neizostavna,
- Korisnici koji pristupaju objektu moraju da budu ovlašćeni ,
- Korisnici mogu da svoja prava nad objektima dodele drugim korisnicima,
- Korisnicima sistema nije dozvoljena upotreba/menjanje tuđih prava.

4.4. Različiti aspekti zaštite:

Vidovi zaštite su određeni odnosu na položaj u informacionom sistemu/računarskoj mreži:

- **Zaštita na nivou aplikacije**. Ova zaštita obuhvata: softversku zaštitu aplikacije (na primer zaštitu od prekoračenja bafera), izolovanje važnih aplikacija na serverima i umreženim računarima, primenu specifičnih protokola,
- **Zaštita na nivou operativnog sistema**. Zaštita obuhvata vezu aplikacija sa operativnim sistemom, vezu prema mreži.
- **Zaštita na nivoju mrežne infrastrukture**. Zaštita se odnosi na:uvođenje mrežnih barijera (engl. *firewalls*), blokiranje nepotrebnih portova (priključaka), šifrovanje putanje, izolovanje putanje pomoću komutatora i rutera ili određene infrastrukture ,
- **Proceduralna i operaciona zaštita**. Zaštita obuhvata: definisanje i sprovođenje pravila zaštite, procedure i politike, otkrivanje napada, preventivno delovanje u cilju zaštite i smanjivanja ranjivosti sistema, upravljanje konfiguracijom sistema, podizanje svesti o problemima i obrazovanje korisnika.

Posebne delove u metodama zaštite čine zaštita od elementarnih nepogoda (požara, poplava, zemljotresa) i zaštita od terorizma ili drugih rušilačkih akcija. Neophodno je voditi računa i o regulativi, etici, psihologiji i kvalitetu života pojedinaca.

4.5. Primeri:

Situacije i primeri iz prakse u gde se primenjuju različite metode i tehnike zaštite su:

- Formiranje demilitarizovane zone (DMZ). DMZ je zona između privatne mreže i javne mreže, koju formiraju računarski hardver i softver. Sačinjava je kombinacija rutera, mrežnih barijera, posredničkih servera (engl. *proxy servers*) i softverskih sistema za otkrivanje i sprečavanje napada,
- Ispitivanje softvera. Pre instraliranja softvera u operativnom okruženju, on treba da bude ispitan u razvojnom okruženjusoftver se ispituje instaliranjem, npr. Web servera, ftp servera, servera za e-poštu i sistema za upravljanje bazama podataka. Neophodno je uključivanje zakrpa (*patch*), radi obezbeđenja sigurnosti u radu.
- Zaštita vitalnih kompanijskih podataka. Postoje posebne baze podataka u kojima se čuvaju poverljiva dokumenta kao što su podaci o finansijskim transakcijama, primanjima zaposlenih, podaci o komitentima. Ograničeno je povezivanje ovih baza sa spoljašnjim sistemima.
- Obezbeđivanjem FTP i TELNETa omogućava se pristup serverskoj opremi samo ovlašćenim licima,
- Korišćenje lozinki. Neophodna je upotreba korisničke lozinke i koje ne treba da sadrže očigledne elemente kao što su lična imena iz porodice i okruženja, brojeve telefona, važne datume,... Ne treba koristiti ni složene lozinke, teške za pamćenje.
- Ažuriranje softvera. Neophodno je korišćenje najnovijih verzija softvera obzirom da postoji opasnost od grešaka u starijim verzijama.
- Politika zaštite informacija. Obaveza svake organizacije a naročito u javnom sektoru je da sačini Akt o proceni rizika kojim se definišu rizici i načini i sredstva za njihovo suzbijanje.

4.6. Pristup organizacije (ISC)2:

Information Systems Security Certification ISD-2 se satoji od nekoliko severnoameričkih udruženja čiji članovi imaju visok nivo stručnosti. Organizacija ISC-2 razvija i koristi ujedno i administriraju razne vrste programa i sertifikacija.CISSP je titula koja označava da je neko profesionalac za sigurnost sistemaUloge ovakvih organizacija je da kreiraju i održavaju jedan skup znanja poznatiji kao CBK koji obuhvata deset vrsta protekcije:

- Sistemi za kontrolu pristupa,
- Sigurnost razvoja aplikacija i sistema,
- Obezbedjenja neprekidnosti poslovanja i planiranje rekonstrukcije sistema
- Kriptografija,
- Etički i pravni aspekti sigurnosti
- Fizička sigurnost,
- Sigurnost operative,
- Upravljanje sigurnosnim sistemima,
- Sigurnosni modeli i arhitekture
- Sigurnost računarskih mreža i komunikacionih mreža

Navedeno se često upotrebljava kod klasifikacija različitih zaštitnih metoda. Za CISSP sertifikat postoje seminari, koje pohađaju kandidati sa minimumom 3 godine prakse; ujedno su dužni da potpišu *Code of Ethics(ISC-2)*. Code of Ethics je vrsta vrsta etičkog kodeksa koja je

postala standard za ISC-2 udruženje.

4.7. Projektovanje sistema zaštite:

Zaštita mora da bude jednostavna, dosledna i primenjuje se i na nižim nivoima sistama.

Projektovanje sistema zaštite podrazumeva:

- Osobu odgovornu za projekat,
- Različite načine prepoznavanja terminala i korisnika.
- Strukture šema ovlašćenja,
- Načine otkrivanjua nedozvoljenih pristupa,
- Načine integrisanja zaštite u sistemske programe,
- Postupak rekonstrukcija posle oštećenja datoteke,
- Postupak rekonstrukcije nakon otkaza sistema,
- Metode nadzora,
- Odlučiti se za korišćenje kriptografije,
- Odlučiti se za vrstu konrola koje treba ugraditi radi analiziranja i korišćenja statističkih datoteka,
- Odlučiti se koju kontrolu treba primeniti kod operacija pregledanja datoteka.

Principi projektovanja sistema zaštite su sledeći:

- Ekonomičnost zaštite,
- Pouzdanost zaštite,
- Potpuna provera,
- Javnost projekta,

- Razdvajanje prava,
- Najmanja prava,
- Smanjenja broja zajedničkih mehanizama,
- Psihološka prihvatljivost (veza između računara i čoveka),
- Radni faktor,
- Evidencija ugrožavanja.
-

Kod projektovanja zaštite mora se voditi računa o performansama računarskog sistema. Često performanse slabe sa povećanjem stepena zaštite iako je cena u tom slučaju veća. Korišćenjem beležnice (enleski *one-time pad*) u kriptografskom protokolu povećaće se sigurnost ali će oslabiti performanse.

Postavlja se pitanje koja zaštita je efikasnija, softverska ili hardverska. Rešenje zavisi i određuje se od problema do poroblema, a najčešća je kombinacije U praksi se, međutim, najčešće koristi kombinacija softverske i hardverske zaštite. Ako ima potrebe za šifrovanjem podataka u jednoj instituciji treba kupiti različita softverska rešenja ka GnuPG. U zavisnoste koje se metode koriste identifikovanja zaposlenih i ako se koristi biometrijska zaštita nužno kupiti odredjene vrste čitača(čitače rožnjače ili otisaka prstiju).Predloživo je kupiti za zažtitu mreže pametne routere ili ASA firewall uredjaji koji saradjuju sa ruterima,radi interne zaštite se postavljaju uredjaji kao Linksysov IronPort C170 ili jači modeli.

5. Nadzor računarskih mreža:

5.1. Uvodne napomene:

Međunarodna organizacija za standrde ISO podelila je upravljanje mrežom u pet funkcinalnih domena.

1. **Upravljanje kvarovima** – ima za cilj identifikaciju, izolovanje i uklanjanje grešaka u mreži,
2. **Upravljanje obračunavanjem troškova** – koristi za obračunavanje i naplaćivanje troškova za korišćenje mrežnih resursa,
3. **Upravljanje konfiguracijom** koristi se za skupljanje podataka od upravljivih delova mreže i za odašiljanje podataka objektima u mreži kojima se upravljakoji su potrebni za neprekidan rad sistema/mreže.
4. **Upravljanje performansama** koristi se za prikazivanje statusa mrežnih objekata kojima se upravlja i kvaliteta međusobne komunikacije,

5.2. Simple Network Management Protocol (SNMP):

Softver za mrežno upravljanje (engl. *network management software*) se sastoji od:

1. **Softver za predstavljanje upravljačkih podataka korisnicima**. Mrežno upravljanje raznim softverima se odvija kroz korišćenje interfejsa namenjenog korisnicima takav

interfejs se naziva korisnički interfejs,ujedno daje mogućnost korisniku da nadgleda i upravlja mrežom,Cisco kompanija je patentirala poslednjih goidna softver u tom domenu koj nadgleda sve cisco uredjaje od telefona do wi-fi uredjaje i automatski ih prepoznaje. Takav interfejs omogućava korisniku nadzor i upravljanje mrežom. Bitno je da pored sinhronizovanog rada takvih uredjaja sa istim brendom podržavaju i mrežne uredjaje drugih proizvodjača.

2. **Softver za upravljanje mrežom** (engl. *network management software*). Arhitektura ovog softvera može biti relativno složena i prilagođena, kako OSI tako i TCP/IP mrežnoj arhitekturi. Aplikacija kojima se upravlja mrežom čine najviše slojeve u takvom softveru, svaka od tih aplikacija pokriva neke odredjene delove mreže pokrivene OSI standardima. Rad malog broja aplikacija može da podržava veliki broj aplikacionih elemenata(SQL baze za ERP softvere i etc).
3. **Softver za podrku aplikaciji mrežnog upravljanja** Služi da omogući da aplikacija mrežnog upravljanja pristupa MIB-u i ostvaruje vezu sa udaljenim elementima mreže.MIB je drugi naziv za *Managemenet Information Base* iliti baze za upravljanje informacijama.

SNMP obuhvata integrisanu kolekciju alata koji služe za nadzor mreže i upravljanje mrežom. Osnovne karakteristike SNMP-a su jedinstven operatorski interfejs i minimalna količina posebne opreme (softverske i mrežno-komunikacione mogućnosti i sposobnosti ugrađene su u postojeću opremu).

Ključni elementi SNMP-a su integrisani skup alata za nadgledanje i kontrolu mreže, upravljačka stanica, upravljački agenti, upravljačka informaciona baza i protokol za upravljanje mrežom.

U ovom kontekstu, upravljanje mrežom može obuhvatati nekoliko skupova tj. tipova značajnih operacija, kao što su definisanje pojedinih parametara, preusmeravanje saobraćaja, rekonfigurisanje, distribuirani nadzor i upravljanje.

Kada govorimo o sigurnosti i pitanjima nadzora i upravljanja mrežama, pretnje možemo podeliti na dve osnovne grupe: primarne i sekundarne. U **primarne pretnje** spadaju modifikacija sadržaja poruke (sistem za upravljanje zaštitom mora da obezbedi sredstva za otkrivanje neovlaćene promene sadržaja poruka u prenosu) i lažno predstavljanje (potrebno je da

se obezbedi nedvosmislena identifikacija pošiljaoca poruke). **Sekundarne pretnje** su promena toka podataka (promena redosleda poruka, unošenje dodatnog kašnjenja i dupliranje poruka) i prisluškivanje.

5.2.1. Razvoj protokola SNMP:

Glavni stručnjaci, odgovorni za razvoj SNMP-a, jesu: Keith McCloghrie, Marshall Rose, Jeffrey D. Case, Mark Fedor, Martin Lee Schoffstall i James R. Davin. Dosad su napravljene tri verzije SNMP-a: SNMPv1, SNMPv2 i SNMPv3.

RFC 1052 postoji od 1988 godine i on pripada zahtevnim specifikacijama za mrežno upravljanje kojom je objašnjeno sve ono što obezbedjuje mrežno upravljanje.Dokument odredjuje formate poruka i komunikacionog protokola kao i vrste poruka koje se razmenjuju i ujedno omogućavaju alarmiranje različitih korisnika(administratora).

SNMPv1, rana verzija ovog protokola, praktično i nije vodio računa o sigurnosti. SNMPv1 ne koristi nikakve mehanizme sigurnosti i zaštite podataka. Ovaj protokol mogu ugroziti praktično sve vrste napada koji se mogu izvesti u računarskoj mreži. SNMPv1 je protokol bez uspostavljanja veze (koristi UDP kao protokol transportnog sloja). UDP se koristi zato što je efikasniji od protokola TCP (ne troši se režijsko vreme na slanje potvrde o prijemu paketa ili na ponovno uspostavljanje izgubljenih veza), a od protokola za upravljanje mrežom očekuje se visoka efikasnost.

U aprilu 1993., verzija 2.0^2 (SNMPv2) postala je standard. U drugu verziju protokola uneta su neka poboljšanja, kao što su: novi tipovi podataka, očuvanje integriteta i redosleda skupova, bolje definicije tekstualnih konvencija, bolje upravljanje dodavanjem i brisanjem redova u tabelama, izjave o sposobnosti proizvođača i dobavljača opreme, bolje definicije tipova objekata, zahtevi za usklađenost MIB baza itd.

U drugu verziju SNMP protkola unete su novine koje u određenoj meri obezbeđuju sigurnost i zaštitu poruka i učesnika u saobraćaju i nadzoru. SNMPv2 omogućava zaštitu integriteta poruke, proveru identiteta pošiljaoca, šifrovanje poruke, korišćenje proizvoljnih mehanizama digitalnog potpisa, simetričnih i asimetričnih algoritama šifrovanja podataka za realizaciju mehanizama zaštite. SNMPv2 koristi heš funkciju MD5 i algoritam DES za širfovanje podataka. U ovoj verziji je, takođe, dozvoljena upotreba TCP protokola za pouzdan prenos.

Godine 1997, formirana je radna grupa koja je napravila treću verziju protokola SNMP. Verzija SNMPv3 objavljena je u maju 1998. godine.

5.2.2. Delovi sistema za upravljanje mrežom:

SNMP je protokol a ujedno i deo sistema za upravljanje mrežom (engl. *network management system*) se sastoji od:

- **Upravljačka stranica** (engl. *network management station*) jeste mrežni računar koji ima sposobnost procesuiranja ekvivalentnu za izvršavanje upravljačke aplikacije. **Upravljačka aplikacija**, koju nazivaju SNMP menadžer (engl. *manager*) ili samo menadžer, računarski je program koji nadgeda upravljane elemente na čvorovima mreže koji su upravljani i upravlja njima u skladu s polisama upravljanja (engl. *management policy*) koju je definisao čovek - upravnik računarske mreže,
- **Upravljani čvor** (engl. *managed node*) mrežni je uređaj čijim se stanjima, ili stanjima nekih njegovih delova koji se nazivaju upravljavim elementima ,upravlja ili se ona samo konrolišu. U odnosu na složenost i funkciju,pomenuti čvorovi često su raznovrsni i raznorodni, na primer razne vrste mrežnih računara, serveri, terminali, ruteri, modemi, mrežni štampači.**SNMP** agent je vrsta protokola koja radi na aplikativnom nivou koja je definisana za RFC 1157 za razmenu informacija izmedju uredjaja u mreži.
- **Upravljačke informacije** (engl. *management information*) služe za dobijanje infromacija o statusu na upravljenim elementima u upravljanom čvoru. Preuzimajući te informacije sa upravljanih elemenata, SNMP menadžer vrši monitoring elemenata, a eventualnom promenom njihovih vrednosti menja ta stanja. Upavljačke informacije, koje su fizički smeštene u SNMP agentima, SNMP menadžer vidi kao skup korisnuči upravljanih elemenata smeštenih u virtuelnom skladištu informacija koje se naziva baza upravljačkih informacija. Za prenos upravljačkih informacija između SNMP agenata i menadžera koristi se protokol SNMP,
- Protokol SNMP je protkol za upravljanje uredjaja na IP mrežama

5.2.3. Management Information Base (MIB):

Protokol SNMP, koji je opisan u prethodnom delu ovog poglavlja, bavi se komunikacijom između upravljačkih stanica (na primer konzola) i upravljanih objekata (kao što su ruteri, mrežni prolazi, komutatori) koristeći MIB baze. Poseban softverski modul na upravljanim objektima (SNMP agent) komunicira sa SNMP upravljačkim softverom. Kao što je ranije navedeno, SNMP koristi zadati skup komandi i uputa. MIB baza treba da sadrži informacije o ovim komandama i skup komandi i upita. MIB baza treba da sadrži informacije o ovim komandama i ciljnim objektima (upravljivim entitetima ili potencijalnim izvorima informacija o statusu), s posebnim osvrtom na podešavanje mreže i transporta podataka radi poboljšanja i unapređenja. [1]

MIB (*Management Information Base*) je vrsta baze podataka koja se koristi za upravljanje raznim uredjajima u komnikaciji mreže,sama se sastoji od upravljanih objekata.Najčešće je asocirana sa SNMP protkolom iako je bila predvidjena da se bavi svim informacijama i najčešće se odnosi na MIB-module.Ova baza adresira svaki ulazak kroz OID.OID(*Object indentifier*) je vrsta identifikatora za odredjene objekte u mreži.MIB hierarhija se prikazuje kao stablo bez kore,nikada deca i roditelji u tom stablu ne mogu imati celobrojne vrednosti.

Svaki upravljani objekat ima bazu podataka, tj. vrednosti, za svaku definiciju zapisanu u MIB-u. Postoje dve vrste upravljanih objekata: skalarni i tabelarni. Skalarni objekti definišu pojedinačne instance objekata. Tablični definišu više povezanih instanci objekata koje su grupisane u MIB tabelu.

5.2.4. Opis rada protokola SNMP:

Protokol kojim se kontroliše i upravlja mrežama.Preko prikpupljenih informacija o elementima mreže kreiraju se informacije koje se prosledjuju administratoru SNMP radi uz pomoć UDP-a (*User Datagram Protocol*). UDP se moze opisati na sledeći način:

- Agent sluša na UDP portu 161,
- Odgovori se šalju na NMS port (1961),

- Gornja vrednost SNMP poruke ograničena je gornom vrednošću UDP poruke,
- Sve SNMP implementacije moraju primiti pakete najmanje dužine 484 bajta,
- Ako nastane greška prilikom prenosa, prima se poruka na NMS portu 162.

Svaki mrežni uredjaj primenjuje SNMP agenta - tačnije, koristi programske module koji skupljaju informacije o tom uredjaju u mreži, njegovim karakteristikama, saobraćaju kroz njega, greškama i sličnim informacijama.

Upravljačka konzola sakuplja podatke od SNMP agenta od svih upravljivih uredjaja i čuva ih organizovane u bazi podataka .Baza podataka u kojo cuva podatke je MIB.Zapisi u MIB bazi jedinstvenog su formata, tako da je lako upravljačkim jedinicama SNMPa da prezentuju administratorima sistema i to obično na upravljačkoj konzoli.

SNMP se zasniva na modelu menadžer/agent. SNMP je jednostavan jer agent zahteva minimalan softver. Da bi bio jednostavan, SNMP sadrži ograničen skup naredba i odgovora: get next i set za dobijanje pojedinačnih ili grupnih promenljivih ili za utvrđivanje vrednosti pojedinačnih promenljivih. Agent šalje odgovor na te poruke. Agent, takođe, šalje *trap* poruke upravljačkom sistemu ako je nastala greška.

Postoji pet osnovniih poruka tj. jedinca podataka SNMP protokola:

1. *Get request* - zahteva vrednost jedne ili više promenljivih u MIB bazi,
2. *Get next request* – koristi se za iščitavanje redova tabele ili omogućava korisniku da dodje do sledećih vrednosti u nizu
3. *Set request* – ažurira MIB promenjive ilit update-uje njihovo stanje
4. *Get response* - vraća odgovor na get request, get next request ili set reguestl,
5. *Trap* – alaramira o nastanku značajnih promena ili dogadjaja u mreži

5.2.5. Posrednički SNMP agent - proksi konfiguracija:

Neki mrežni uređaji nemaju mogućnost za korišćenje SNMP programa pa su zato napravljeni proksiji koji im pružaju te mogućnosti.

SNMP zahteva da svi agenti u NMS-u podržavaju jedinstven stek protokola.Taj stek protkola treba da bude zasnovan an UDP i IP protokolima. Takav pristup onemogućava primenu SNMP upravljanja u uređajima u kojima nisu implementirani protokoli TCP/IP steka (kao što su, na primer, neki komutatori i modemi). Zbog ograničenih procesnih mogućnosti nije poželjno u

takve sistema ugrađivati dodatni softver koji podržava SNMP, agentsku logiku i održavanje MIB-ova. [18]U mreži su neki uredjaji prezauzeti da bi podržavali i SNMP protokole i da bi ona bila instalirana na njih. Da bi problem bio rešen po tom pitanju uvedeni su proksi agenti koji posreduju u upravaljanju mrežom Posrednički agent može posmatrati više uredjaja. Agent se zasniva na komunikaciji izmedju uredjaja i upravljačke stanice. Upravljačka stanica šalje SNMP upite posredničkom agentu, a on ih pretvara u poruke upravljačkog protokola koji koristi zastupani uređaj. Kada upravljačka stanica postavi upite SNMP on šalje odgovore vezane za uredjaje,taj odgovor dolazi u obliku SNMP poruke. Posrednički agent može upravljačkoj stanici slati i poruke *Trap*. Posrednički agent može služiti kao veza izmedju uredjaja sa starijim SNMP verzijama i novijim SNMP verzijama v3. Veći deo cisco uredjaja danas koristi SNMP v3.Ako se koriste posrednički agenti to može samo pozitivno uticati na mrežu tako što će smanjiti probleme vezane za sigurnost.

5.2.6. SNMPv3:

SNMPv1 i SNMPv2 su raniji protokoli koji su ranjivi na čitanje paketa sa strane neovlašćenih lica. SNMPv3 je promenio tok stvari jer je počeo da rešava problem vezan za NMS.Provere su bile kvalitetnije što se tiče identiteta korisnika i samo šifrovanja SNMP poruke.

Svaki SNMPv3 ima svoj pogon iliti *engine* i odvojenog dela SNMP **aplikacija**. SNMPv3 *engine* sastoji od 4 podsistema a to su sledeći:

1. Dispečerski podsistem je sistem koji obradjuje poruke i odredjuje njihove verzije ujedno šalje i prima poruke.
2. Podsistem za obradu poruka je sistem koji šalje poruke drugim objektima i koristi podatke iz SNMP poruka od drugih objekata

3. Sigurnosni podsistem izvršava usluge provere identiteta i radi deo šifrovanja informacija. U proveri identiteta koristi se mehanizam zajednica odnosno SNMPv3 korisnička (engl. *user-based*) provera identiteta. Provera verodostojnosti korisnika zasniva se na upotrebi algoritama SHA ili MDS. Provera identiteta u SNMPv3 ima mogućnost se provera verodostojnosti korisnika izvršava bez slanja lozinki u čitljivom obliku,pri šifrovanju se koriste algoritmi DES za šifrovanje i dešifrovanje poruka.
4. Upravljanje pristupom se kontroliše uz pomoću četvrtog podsistema,ovaj sistem odredjuje pristup korisniku nad pojedinacnim objektima i ujedno daje autorizacije šta bi smelo da se radi nad tim objektima.

Drugi deo entiteta su aplikacije:

- Generator naredba generiše zahteve **get, get-next, get-bulk** i **set** i obrađuje odgovore
- Generator odgovora ,njegova svrha je da odgovara na zahteve **get, get-next, get-bulk** i **set**
- Generator obaveštenja generiše SNMP zamke (engl. *traps*) i obaveštenja iliti notifikacije
- Prijemnik obaveštenja prima zamke i poruke
- Posrednik za prosleđivanje (engl. *proxy forwarder*) olakšava prosleđivanje SNMP poruka između entiteta,
- Ostale aplikacije.

5.3. Alati za nadzor mreža:

Softverski alati za nadzor računarskih mreža primenjuju se sve češće. Dve grupe srodnih alata postoje prva vrsta samo nadgleda računarske mreže druga vrsta upravlja njima to su *network monitoring* i *network management tools* Ove dve grupe alata imaju srodnu namenu i u tesnoj su vezi. Mnogi ih često mešaju, pogotovu zbog ekraćenice NMS koja se u engleskoj literaturi koristi za oba tipa alata. Ovi alati se u novije vreme najčešće koriste zajedno s drugim alatima koji obezbeđuju i štite računarske sistema i mreže, kao što su alati za kontrolu pristupa, za zaštitu od zlonamernih programa, otkrivanje i sprečavanje upada i slično

5.3.4 Nadzor na operativnim sistemima Windows:

Microsoft je u svoj operativni sistem, Windows, počevši od Windowsa NT, počeo da dodaje vremenom i novijim verzijama alate za posmatranje procesa unutar sistema i podršku za različite vrste protokola kao OID,MIB i slične.Kasnije su developeri windowsa razvili program koji nadgleda performanse (*Peformance Monitor*), koji se pokreće naredbom **perfmon** ili iz MMC-a dodatkom snap-in.MMC je mikrosftova konzola za nadgledanje komponenti windowsa koja utiče i na nadgledanje antivirus programa kao i njihovo update-ovanje.Bitnije stvari kojoj je doprinela MMC konzola je regulisanje grupnih polisa,posmatranje sertifikata i event viewer programom na osnovu čijih dump fajlova mogu se videti logovi greški koje su se dešavale.

Ovaj sistem je proširiv i omogućava pisanje tj. programiranje vlastitih monitora, definisanje brojača, dodavanje zamki (engl. *traps*), tj. pragova za određene merače i brojače, koji će pokrenuti predviđenu akciju u određenim okolnostima.

Primera radi, može se programirati da se administratoru sistema pošalje poruka elektronskom poštom ili SMS poruka (ako ima takvih mogućnosti) u slučaju da slobodan prostor na disku padne ispod 10% ukupnog kapaciteta ili, recimo, kada se uoči da su za određeno korisničko ime bila 3 neuspela pokušaja prijavljivanja u određenom vremenskom intervalu. Može se, recimo, bez uzbunjivanja administratora, aktivirati i skript koji će obrisati nepotrebne zapise sa diska ukoliko preti opasnost od prepunjenja. [10]

U operativnom sistemu Windows moguće je dodati i drajver za nadzor mreže, to se obavlja preko dijaloga za svojstva LAN veze.

Preporučuje se da detaljnije informacije o ovoj temi potražite u dokumentaciji uz biblioteku MSDN (Microsoft Developer Network) i u raspoloživim resursima na Microsoftovoj Web lokaciji i lokacijama brojnih drugih proizvođača.

6. METODE ZAŠTITE

Metode zaštite mogu biti fizičke organizacione i pravne.

6.1. Organizacione metode zaštite:

Prilikom projektovanja i realizovanja informacionih sistema i računarskih mreža, treba voditi računa o skupu mera za povećanje sigurnosti i održavanje rizika na prihvatljivom nivou, uz prihvatljive troškove i uticaj na performanse sistema. Potrebno je definisati:

- Odgovornost u projektovanju tehnika i postupaka zaštite i
- Odgovornost za zaštitu pri svakodnevnom radu.

Radi ostvarivanja **odgovornosti u projektovanju tehnika i postupaka zaštite**, neophodno je uspostaviti sledeće elemente odgovornosti:

- Za tehnički aspekt projekta uz ukupnu koordinaciju
- Za kontrolu procedura,
- Za kontrolu rada programa i programera,
- Za fizičku zaštitu,
- Za proveru funkcionisanja sistema zaštite.

Potrebno je definisati i odgovornost za sledeće procedure:

- Operativne kontrolne,
- Rad u prostoriji s računarima,
- Pravila kojima se štite podaci,
- Koje se koriste kod uvodjenje novog sistema umesto starog
- Koje primenjujemo u slučajevima havarije

Bitni segmenti organizacionih metoda zaštite, o kojima će dalje u ovom poglavlju biti reči, jesu kadrovski aspekt, kao i analiza rizika i upravljanje njima.

6.1.1. Kadrovski aspekti:

Prilikom izbora kadrova za rad na osetljivim mestima i obavljanje funkcija u kviru informacionog i komunikacionog sistema, kao i računarske mreže, potrebno je voditi računa o stručnosti, poverenju i lojalnosti. Kandidati za neke službe moraju proći posebnu proveru sa

stanovišta bezbednosti - proverava se šta su radili na ranijim mestima te njihova stručna i lična prošlost.

U svakodnevnom radu, posebno odgovornost za zaštitu imaju:

- **Rukovodilac računarskog centra**. Zadužen je za raspodelu odgovornosti u oblasti zaštite i odgovoran je za striktnu i neprekidnu primenu mera zaštite,
- **Administrator zaštite.** Administrator zaštite vodi računa o tabeli obaveštenja lozinkama i zaštitnim kodovima kod primene ovlašćenja. U njegove aktivnosti spadaju: vođenje dnevnika povreda zaštite i dnevnika aktivnosti operatera, pregledanje statistike aktivnosti sistema, izveštaja čuvara i lista prekovremenog rada. Administrator zaštite takođe odgovorana ukoliko dodje do povrede zaštite ,njegova obaveza je da proceni delotvornost opredeljenih mera zaštite, uočava propuste u zaštiti i metode za njeno narušavanje i pronalazi nove metode za poboljšanje zaštite,
- **Lokalni službenici zaštite**. Veći distribuirani sistem može imati više lokalnih službenika zaštite. Oni se brinu o slanju izveštaja ukoliko dodje do povrede procedura zaštite.
- **Vlasnici datoteka.** Njihov rad je opcion, što znači da može (ali i ne mora) postojati vlasnik datoteke odnosno baze podataka. Međutim, ako postoje tj. ako su određeni, vlasnici su odgovorni za zaštitu datoteka, tačnost datoteka i za rekonstrukciju datoteka ukoliko se one oštete ili unište,
- **Kontrolori zaštite**. Kontrolori zaštite obavljaju sledeće zadatke: povremeno proveravaju sve aspekte zaštite, obavljaju regularne obimne analize svih aspekata zaštite, sastavljaju izveštaje o slabostima i propustima u sistemu zaštite, pronalaze rešenja za otklanjanje otkrivenih propusta, proveravaju fizički i sistemski nivo zaštite.

Prilikom realizacije zaštite, potrebno je obaviti čitav niz mera, kao što su:

- Opšta kontrola i raspitivanje,
- Korišćenje upitnika i anketa,
- Povremene najavljene i nenajavljene provere,
- Namerna primena pogrešnih transakcija i generalno „provociranje“ reakcije na grešku,
- Pokušaji narušavanja integriteta, tajnosti i raspoloživosti elemenata sistema i sistema u celini,
- Raznovrsna ispitivanja, pilot sistemi, specijalni programi za nadzor, analize, simulacije,

- Procedure za traženje grešaka (engl. *troubleshooting*)..

Navedene mere kao i brojne druge, poboljšavaju celokupnu sigurnost računarskih sistema, mreža i informacionih sistema u celini. Potrebno je osmisliti i povremeno sprovoditi kompletno ili delimično ispitivanje radi provere zaštite. Ova ispitivanja se obavljaju u određenim intervalima, a mogu ih sprovoditi ljudi iz internog sastava, prema unapred pripremljenim planovima, ali vrlo često i spoljni saradnici ili za to ovlašćene i osposobljene firme ili organizacije. Danas su ispitivanje mogućnosti upada u računarske mreže (engl. *penetration testing*) i informacione sisteme, kao i takozvano etično hakerisanje (engl. *ethical hacking*) postali posebna poslovna grana u okviru računaskih delatnosti. O tome će biti još reči kasnije u ovoj knjizi.

6.1.2. Analiza rizika i upravljanje njime:

U definisanju politike sigurnosti postoji potreba da se znaju rizici u informacionom sistemu. Izazovi i napadi su izvori potencijalnih sigurnosnih problema, dok se rizik odnosi na verovatan ishod i njemu pridružen trošak zbog nastanka posebnog događaja. U pretnje iz okruženja i unutar samog IT sistema spadaju i zlonamerni ljudi i prirodni neprijatelji kao što su vatra, voda, zemljotres, nestanak električne energije itd. Moguće su obe vrste incidenata i namerne štete. Drugo dolaze iznutra - od korisnika, ili spolja - od hakera. Nedavna istraživanja potvrđuju da korisnici lakše mogu da pristupe sistemu i često znaju gde da traže najosetljivije ili najvažnije podatke, pa su mnogo opasniji često su izvor velikih problema u domenu ugrožavanja sigurnosti. [20]

6.1.2.1. Analiza rizika:

Svakom projektovanju sistema zaštite treba prići respektujući analizu rizika. Ovo omogućava procenu sredstava za realizaciju kao i budzet potreban za tekuće funkcionisanje.

Osetljivost sistema na neki događaj definiše se iskazuje kao eventualni gubitak u finansijskim sredstvima koja bi pretrpela institucija ukoliko do dogadjaja dodje. Rizik se definiše kao proizvod verovatnoće dešavanja i osetljivosti na taj dogadjaj. Verovatnoće rizika određuje vremenski interval u kom se može očekivati vrsta takvog dešavanja.

Navodimo primer izračunavanja izloženosti sistema. Ako je procenjeno da neki događaj može da izazove gubitak od 1.000.000 dinara, a verovatnoća njegovog dešavanja u jednoj godini iznosi 0,5%, onda je izloženost sistema: I = P h V = 0,005 x 1.000.000 = 5.000 dinara.

Ukupna izloženost neke organizacije jednaka je zbiru **parcijalnih izloženosti** za razne događaje. Projektant zaštite treba da vodi računa o tome da događaji, čije istovremeno dešavanje može da izazove narušavanje integriteta podataka, učini **nezavisnim**, tako da rezultantna verovatnoća dešavanja bude mala. Verovatnoće se ne mogu množiti (za dva ili više događaja) ako događaji nisu nezavisni. [15]

Napomenimo da se verovatnoća uspeha smišljenog napada na pojedine tačke sistema ili ceo sistem može znatno smanjiti tako što će s raznim aspektima sistema - pre svega sa samim metodama zaštite - biti upoznate samo one osobe koje to treba da znaju.

Procena rizika je zanimljiva disciplina u oblasti finansijskog menadžmenta. Kompanije koje se bave osiguranjem imovine i lica imaju viševekovno iskustvo u procenjivanju rizika. Međutim, troškove nemilog rizičnog događaja u IT oblasi moraće da snosi firma koja definiše svoju sigurnosnu politiku, a u proceni ne može da koristi stvarne (aktuelne) podatke o materijalnoj šteti. Pri proračunu i proceni troškova ne treba uzeti u obzir samo stvarno izgubljen novac, već i više od toga. Potrebno je vrednovati i potencijalne štet od gubitka privatnosti, narušavanja ugleda tj. reputacije, pravne obaveze, neželjenu izloženost masovnim medijima tj. gubitak poverenja i reputacije, troškove raščišćavanja, oporavka i sve drugo.

Jedan od načina procene rizika je da se pripišu troškovi „najgoreg scenarija“. U određenim slučajevima možda ćete poželeti da na najgori mogući trošak dodate verovatnoću da će događaj nastati tokom određenog perioda, kako biste ukazali na to koliki su izdaci potrebniza zaštitu od takvog događaja.

6.1.2.2. Upravljanje rizikom:

Upravljanje rizikom je proces izvršavanja zadataka uz minimalne troškove a s minimalnom opasnošću za izloženost riziku.

Kada korisnik odlučuje kako će reagovati na rizik, izabraće jednu od tri mogućnosti:

- **Prihvatljiv rizik** je onaj kod koga je izloženost riziku mala a troškovi zaštite uvećani.
- **Dodeliti rizik**. U nekim slučajevima manji su troškkovi tj. isplativije je prihvatanje rizika s kojim bi se neko drugi suočio nego direktna zaštita od njega. Primer su preduzeća koja se opredeljuju za kupovinu zaštitnih komercijalnih sredstava umesto da ih sama grade.
- **Izbeći rizik**. Ovo uključuje uspostavljanje na potrebnom mestu takvih neophodnih sigurnosnih mera da incident uopšte neće nastati ili takvih mera da incident postaje mnogo manje verovatan.

6.2. Fizičke metode zaštite:

Domen fizičke sigurnosti sistema bavi se pretnjama, ranjivostima i merama koje se mogu primeniti kako bi se fizički zaštitili resursi i poverljive informacije neke kompanije, organizacije ili institucije. U resurse koji se fizički štite spadaju osoblje, prostorije u kojima osoblje radi, računarske i komunikacione opreme, medijumi s kojima se radi i pomoćna infrastruktura. Fizička sigurnost se najčešće odnosi na mere koje se preduzimaju kako bi se proizvodni i poslovni sistemi zaštitili od pretnji kao što su provale i krađe resursa i poverljivih informacija, pa se najjednostavnije može definisati kao proces kontrole osoblja, opreme i podataka uključenih u proces obrade informacija. [19] U ovom segmentu se, taođe, analiziraju i metode zaštite od elementarnih nepogoda i nesrećnih slučajeva, kao što su požar, poplava, zemljotresi, ratovi i slično.

6.2.1. Pretnje po fizičku sigurnost:

Pre nego što se pozabavimo fizičkim metodama zaštite i njihovom ispravnom implementacijom, treba da analiziramo aspekte okruženja koji predstavljaju potencijalnu pretnju po računarsku infrastrukturu. „Veliko trojstvo“ sigurnosti (poverljivost, integritet i rapoloživost - CIA) izloženo je riziku iz fizičkog okruženja pa se mora zaštititi. Rizik predstavljaju:

- Prekidi u obezbeđivanju računarskih usluga (raspoloživost),

- Fizičko oštećenje sistema ili pomoćne infrastrukture (raspoloživost),
- Neovlašćeno razotkrivanje informacija (poverljivost),
- Gubitak kontrole nad sistemom (integritet),
- Krađa podataka i/ili opreme (poverljivost, integritet i raspoloživost).

Navodimo i nekoliko primera pretnji po fizičku sigurnost:

- Hitni slučajevi (požari i zagađenje dimom, oštećenje građevine, eksplozije, prekid snabdevanja električnom energijom ili grejanja, oštećenja izazvana pucanjem vodovodnih cevi, ispuštanje toksičnih materija),
- Prirodne katastrofe (zemljotresi, klizišta, poplave),
- Ljudska intervencija (sabotaže, vandalizam, ratovi, državni udari)

6.2.2. Mere zaštite:

Jedan segment fizičke zaštite je **fizička kontrola pristupa** prostorijama u kojima se nalaze računari, računarska i komunikacona oprema. Ovde se mogu koristiti različite metode kontrole - čuvari, brave sa šiframa, kartične kontrole pristupa i biometrijske provere identiteta. U tipične biometrijske karakteristike koje se mogu iskoristiti da bi se jednoznačno utvrdio identitet neke osobe spadaju: otisak prsta, snimak rožnjače oka, crte lica, geometrija šake, glas i svojeručni potpis.

6.2.3. Biometrija:

Biometrija se najčešće koristi za proveru identiteta, ali je upotrebljiva i u drugim oblastima, na primer, u prepoznavanju govora. Biometrijska provera identiteta obuhvata postupke prikupljanja i analize fizičkih karakteristika (na primer, otisci prstiju i snimak rožnjače oka) i drugih karakteristika koje se teško mogu oponašati, a skoro jednoznačno identifikuju čoveka (na primer, rukopis). Karaktetistike se prikupljaju, tj. „snimaju“ pomoću specijalnih

uređaja, digitalizuju i obrađuju softverski (pomoću programa koji se delom oslanjaju na principe veštačke inteligencije).

Karakteristike kojima se opisuju biometrijske metode su sledeće:

- **Jedinstvenost** - opisuje koliko posmatrana biomerijska karakteristika jednoznačno identifikuje pojedinca,
- **Trajnost** - opisuje nepromenjivost biometrijske karakteristike s vremenom
- **Prikupljivost** - opisuje s kojom se lakoćom mogu dobiti uzorci od date navedene karakteristike,
- **Izvodljivost** - opisuje koliko su biometrijske metode primenljive u praksi
- **Prihvatljivost** - opisuje koliko je moguće primeniti ovu metodu bez narušavanja prava privatnosti

6.2.3.1. Biometrija zasnovana na fizičkim kakrakteristikama:

Na samim počecima primene ovih metoda fizičke karakteristike su imale primat u odnosu na drugo,na primer ponašanje. Mislilo se da su navedene karakteristike pouzdanije od onih koje su čisto biheviorističke. Na primer, lakše je lažirati rukopis nego otisak prsta ili snimak rožnjače. [6] Opisaćemo ukratko tipično fizičke karakteristike značajne za biometriju.

- **Otisak prsta** - Otisak prsta je jedinstveni za prst svake osobe. Mogu se digitalno predstaviti sa 7 - 22 tačke čiji raspored jedinstveno identifikuje osobu. Provera identiteta pomoću otisaka prstiju jedna je od najpoznatijih biometrijskih tehnologija. Postoje relativno jeftini uređaji za prepoznavanje otisaka prstiju za stone i prenosne računare. Ovakvi uređaji omogućavaju korisnicima da proveru identiteta lozinkom zamene efikasnom biometrijskom metodom. Karakteristike analize otiska prsta kao biometrijske metode su: osrednja prikupljivost i prihvatljivost i visoka jedinstvenost, trajnost i izvodljivost,
- **Rožnjača oka** - Skeniranje rožnjače oka obavlja se kamerom koja snima zapis o rožnjači. Dobijena slika se specijalnim programima predstavlja pomoću tačaka koje omogućavaju jednoznačno opisivanje uzoraka. Rožnjaču oka je moguće opisati sa 242 tačke. Ova tehnologija se često koristi za identifikaciju osoba koje ulaze u značajne prostorije.

Karakteristike ove metode su: visoka jedinstvenost i izvodljivost, osrednja trajnost i nizak nivo prikupljivosti i prihvatljivosti,

- **Geometrija šake** – Poslednjih dvadeset godina provera identita se radi i preko karakteristika šake. Biomerijski sistem meri fizičke karakteristike šake ili prstiju, kao što su dužina, širina, debljina prstiju i površina područja šake. Karakteristike ove metode su: visoka prikupljivost, osrednji nivo jedinstvenosti, trajnosti, izvodljivosti i prihvatljivosti,
- **Prepoznavanje lica** - Ova biometrijska tehnologija je jedna od najjeftinijih jer nije neophodna skupa specijalna oprema. Prepoznavanje lica može se obaviti na svakom računaru s kvalitetnijom video-kamerom, a za samo prepoznavanje zadužen je softver. Da bi prepoznavanje bilo uspešno, potrebno je prethodno na sistem staviti snimak lica osobe iz različitih uglova. Karakteristike ove metode su: visok nivo prikupljivosti i prihvatljivosti, osrednji nivo trajnosti i nizak nivo jedinstvenosti i izvodljivosti,
- **DNK** - Očitavanje i prepoznavanje jedinstvenog DNK osobe, relativno je nova grana biometrije. U kombinaciji s drugim biometrijskim tehnikama, analiza DNK obezbeđuje veoma visoku tačnost prepoznavanja. Ova tehnika se upotrebljava kako u civilne tako i u vojne svrhe. Verovatnoća je da će se biometrijski podaci čuvati u ličnim kartama.

6.2.3.2. Beometrija zasnovana na karakteristikama ponašanja:

Biometrija ponašanja je jedinstvena za bilo koju osobu(hod,boja glasa, pokreti ruku, način govora,..). Dobijeni uzroci se predstavljaju krivama na osnovu kojih je moguće identifikovati osobe.

- **Prepoznavanje glasa** - Upotrebljava se za proveru identiteta korisnika na osnovu jedinstvenih karakteristika glasa. Korisnik koji želi da se predstavi sistemu mora da izgovori reči prethodno unešene u bazu podataka. Ovu metodu provere identiteta treba primenjivati u kombinaciji s drugim metodama, jer postoji opasnost da neovlašćena osoba snimi ovlašćenog korisnika kako izgovara tu rečenicu i to kasnije reprodukuje. Prepoznavanje glasa se koristi i u druge svrhe, na primer, za prepoznavanje govora, tj. prevođenje glasa u tekstualni zapis. Karakteristike ove metode su: nizak nivo jedinstvenosti, trajnosti i izvodljivosti, osrednji nivo prikupljivosti i visok nivo prihvatljivosti,
- **Prepoznavanje rukopisa ili potpisa** - Ova biomerijska metoda je zasnovana na alalizi dinamike potpisa, tj. na merenju brzine, pritiska i ugla pri potpisivanju ili pisanju nekog teksta. Često se koristi u pravosuđu i tamo gde je pitpis prihvaćen kao metoda provere indentiteta. Karakteristike ove metode su: nizak nivo jedinstvenosti, tajnosti i izvodljivosti, visok nivo prikupljivosti i prihvatljivosti,
- **Dinamika kucanja** - Za ovu biomerijsku tehniku nisu potrebni dodatni uređaji za prikupljanje uzorka. Najznačajniji pokazatelj na kojoj se ova tehnika zasniva jesu različiti vremenski razmaci koje korisnik pravi između pritiskanja dva tastera. Karakteristike ove metode su: nizak nivo jedinstvenosti, tranosti i izvodljivosti, osrednji nivo prikupljivosti i prihvatljivosti. Tehnika je uvedena u Drugom svetskom ratu i primenu je našla u radio-telegrafiji, jer je primećeno da se brzina pritiskanja tastera razlikuje osobe koje šalju poruke.

6.2.3.3. Biometrija, fizička sigurnost i privatnost:

Razvoj biometrijske tehnologije uticao je na to da brojne kompanije i sistemi javnih usluga počnu da koriste biometrijske metode kao osnovne metode provere identiteta. Iako one metode donose izvesne prednosti, postoje aspekti koji u društvu stvaraju oprečna mišljenja o njihovoj primeni.

- **Fizički** - Ima mišljenja da biometrijske metode u nekim slučajevima mogu da izazovu povređivanje korisnika. U opštem slučaju, naoružani lopov će napasti vlasnika da bi mu oteo ključeve od automobila koji želi da ukrade (ukoliko vlasnik odbije da dobrovoljno preda ključeve). Ako je objekat koji lopov želi da ukrade biometrijski zaštićen, šteta nanesena vlasniku može biti nepovratna, a cena štete može biti veća od cene zaštićenog objekta. Na prime, 2005. godine kradljivci automobila u Maleziji odsekli su vlasniku prst pri pokušaju da ukradu automobil koji se pokretao po očitavanju otiska prsta. Osim toga, postoji velika verovatnoća da biometrijski uređaji mogu da budu nehigijenski. Na primer, skener koji snima rožnjaču ne mora da bude čist, što može prouzrokovati infekciju oka),
- **Privatnost** - Podaci prikupljeni pomoću biometrijskih uređaja mogu se kasnije upotrebiti bez korisnikovog znanja i odobrenja, prodati trećem licu i slično. Ovo narušava privatnost i može se iskoristiti za malverzacije, što pojedincu koji je predmet takve zloupotrebe može stvoriti velike neugodnosti. Primera radi, napomenućemo da su se u skorije vreme na Internetu pojavila uputstva za lažiranje otiska prsta, ukoliko se ima nečiji snimljen ili ostavljen otisak.

ZAKLJUČNA RAZMATRANJA

Zaštita mreže i njenih resursa sigurno je najveći izazov sa kojim se adminisrratori mreža sreću. Suština je sledeća: najpre proućite moguće pretnje po bezbednost mreže.Računarske mreže su srca firmi i poslovanja u današnjem svetu što dovodi do sve veće potrebe da se zaštite iste.

Svaka mreža treba da ima dobro isplaniranu zaštitu, koji predviđa moguće pretnje po bez-bednost mreže uključujući čak i fizičke upade u nekim slučajevima moguća fizička oštećenja i sadrži mere koje ćete sprovesti da biste otklonili te pretnje. U praksi postoji više težišta pri odbrani same mreže,da li je težište na unutrašnjem napadu ili spoljašnjem ce značajno uticati na izbor de uložiti većinu resursa kada se osigurava mreža. Ako mreža sadrži bitne i osetljive podatke,mora se računati da ce vaša mreža biće izložena napadima spolja i iznutra; poverljive podatke pokušaće iznutra da ukradu vaši službenici,radnici ili bilo koja osoba sa mogućnosti pristupa istim podacima , a spolja će napadati razbijači, lovci na vredne informacije.

Da bi mreža dobro funkcionisala trebaju se pripremiti više vrste odbrane protiv unutrašnjih i spoljašnjih napada kao i sigurnosne mere koje bi sprečile fizička oštećenja mreže,da samo odredjeni članovi imaju pristup odredjenim delovima opreme,dobre osigurane prostorije IT-a koje pružaju neophodnu zaštitu u slučaju havarija i osoblje obučeno da radi sa takvom opremom.

Nijedna mreža ne može biti sto posto sigurna što dokazuju godinama upadi u svetske mreže čak i u mrežama koje pripadaju državnim bezbednostima,ali je uvek potrebno izvući maksimum od dobijenih resursa,vremena i opreme sa kojom se radi koliko god ona bila dobrog ili loseg kvaliteta.U vecini slucajeva kod firmi koje se ne bave specifično IT opremom kod nas u državi se ulaže jako malo u taj sektor iako je veći deo posla obavljan i završavan brže baš zahvaljujući toj istoj opremi i ljudima koji je održavaju.

LITERATURA:

1. D. Pleskonjic, *„Modularni konvertor protokola“*, INFO Časopis za informatiku, računarstvo i telekomunikacije, br. 2/94,
2. D. Pleskonjić, N. Maček, B. Đorđević, M. Carić, *„Sigurnost računarskih sistema i mreža“*, Mikro knjiga, Beograd, 2007.god.,
3. D. Stinson, *„Cryptogrphy - Theory and Practice“*, CRC Press, Boca Raton, Florida, 1995.,
4. B. Schneier, *„Applied Cryptography“*, Second Edition, John Wiley and Sons, Inc, 1996.,
5. Wiliam Strallings, *„Cryptogrphy and Network security“*, Prentice Hall, 1997.,
6. Z. Petrović, S. Obradović, D. Jovanović, *„Jedan pristup uvođenju poslovanja s karticama“*, BELT 1999., Kopaonik, 1999.,
7. J. P. Arens, S. Obradović, Z. Petrović, *„Trgovanje putem interneta“*, BELT 1999., Lepenski vir, 1999.,
8. M. Živković, *„Algoritmi“*, Matematički fakultet, Beograd, 2000.,
9. S. Obradović, D. Pevac, *„Osnovnsa sredstva i motivi elektronskog placanja“*, YU-Info 2002., Žabljak, 2002.,
10. S. Obradović, *„Osnovi računarske tehnike i programiranja“*, četvrto izdanje, Viša elektrotehnička škola, 2003.,
11. B. Đorđević, D. Pleskonjić, N. Maček, *„Operativni sistemi: UNIX i Linux“*, Viča elektrotehnička škola, Beograd, 2004.,
12. V. Vasiljević, P. Gavrilović, B. Krneta, M. Krstanović, N. Maček, B. Bogojević, *„Priručnik za administraciju računarskih mreža“*, Viša elektrotehnička škola, Beograd, 2004.,
13. Greg S. Trucker, *„Voice Over Internet Protocol (VoIP) and Security“*, October, 2004.,

14. S. Obradović, A. Donchev, Ž. Vasić, B. Ilić, *„Faze realizacije projekta uvođenja poslovanja s karticama“*, IX Međunarodni simpozijum SYMORG 2004., Zlatibor, 2004.,

15. A. Whitaker, D. P. Newman, *„Penetration Testing and Network Defense“*, Cisco Press, 2005.,

16. B. Đorđević, D. Pleskonjić, N. Maček, *„Operativni sistemi: zbirka rešenih zadataka“*, Viša elektrotehnička škola, Beograd, 2005.,

17. S. Obradović, N. Vučinić, T. Pandurov, *„SQL: struktuirani upitni jezik“*, Viša elektrotehnička škola, Beograd, 2005.,

18. S. Mesarović, *„Infrastruktura javnih ključeva“*, Tehnički fakultet, „Mihajlo Pupin“, Zrenjanin, 2005.,

19. M. Bojović, *„Squid proksi server“*, Viša elektrotehnička škola, Beograd, 2005.,

20. V. Kovačević, *„SQL injection napad na baze podataka“*, Viša elektrotehnička škola, Beograd, 2006.

21. Mladen V., Aleksandar J., “Računarske mreže“, Univerzitet Singidunum, Beograd 2011. godine,