

INFORMACIONA BEZBEDNOST I KRIPTOGRAFIJA

Sinkovski Stevan,dipl.inž. VP 1100 Beograd, ssinkovski@yahoo.com
mr Lučić Branislav,dipl.inž. Jugoimport SDPR, b_tempest@Eunet.yu

Apstrakt: U ponuđenom radu se razmatra odnos informacione bezbednosti i savremene kriptografije. Ključne reči: informaciona bezbednost, kriptografija, sistemi poverenja

INFORMATION SECUTITY AND CRYPTOGRAPHY

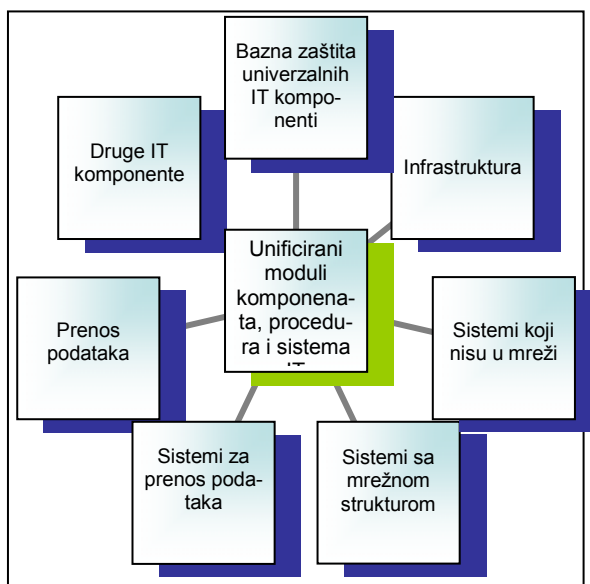
Abstact: In this paper observed the relacon of information security and modern criptogtaphy. Key words: information security, criptogtaphy , trust systems.

1. INFORMACIONA BEZBEDNOST

Informaciona bezbednost (IB) je, kao jedan od novijih pravaca istraživanja u sferi bezbednosti, posledica tehnološkog razvoja i odraz novog pogleda na svet. Ona se javlja ne samo kao jedan od vidova (oblika) bezbednosti, već i kao presek svih drugih vidova bezbednosti u kojima informacione tehnologije zauzimaju važno mesto. O značaju informacione bezbednosti govori i činjenica da je ona postala jedna od osnovnih komponenata nacionalne bezbednosti.

Informaciona bezbednost je definisana kao: ***zaštita informacionih sistema protiv neautorizovanog pristupa ili modifikacija informacija bilo u čuvanju, obradi ili prenosu i protiv lišavanja usluga autorizovanih korisnika, uključujući neophodne mere detekcije, dokumentovanja i otklanjanja takvih pretnji*** [1].

Informacionu bezbednost je moguće definisati i na drugačiji način, kao npr. *informaciona bezbednost je **zaštićenost** informacija i podržavajuće infrastrukture¹ od slučajnih ili namernih dejstava prirodnog ili veštačkog karaktera koja mogu naneti **neprihvatljive gubitke subjektima informacionih odnosa** pa, u tom smislu, i vlasniku i korisniku informacija kao i podržavajućoj infrastrukturi²* [2].



Slika 1: «Tipični» IT sistemi za koje se organizuju standarde mere zaštite (organizacione, kadrovske, infrastrukturne i tehničke) prema nemačkom standardu BSI

Kao što je moguće primetiti, koncept informacione bezbednosti je višedimenzionalan i kao takav podrazumeva različite aspekte (pravne, ekonomske, tehničke itd.). Različiti aspekti podrazumevaju različite metode.

Informaciona bezbednost je normativno definisana standardima (ISO/ICO 17799 i 15408, respektivno organizacioni i tehnički aspekt). Međutim, u realnom životu,

¹ Podržavajuća infrastruktura podrazumeva sisteme elektro-, vodo- i toplotnog snabdevanja, kondicionere, sredstva komunikacija i, konačno, osoblje.

² Definicija uvodi kategorije *informacionih odnosa* između različitih subjekata sa različitim interesima i *neprihvatljivih gubitaka*. Apsolutna zaštita ne postoji i zbog toga se uvodi upravljanje rizicima koje podrazumeva uvođenje praga prihvatljivosti gubitaka – obično materijalno izraženih. В.Галатенко, *Основы информационной безопасности*, Институт ИТ, Москва

od posebnog značaja su praktično orijentisani standardi kao što je npr. nemački standard BSI. Prema standardu BSI, standarde mere zaštite (organizacione, kadrovske, infrastrukturne i tehničke), se organizuju za rtv. «tipične»³ IT sisteme (slici 1) [3].

U okviru tehničkih metoda obezbeđenja informacione bezbednosti, posebno mesto pripada metodama zasnovanim na, posebno formulisanim, matematičkim disciplinama, odnosno metodama kompjuterske kriptografije. U ovom trenutku ne postoji nijedan, manje ili više složen, softversko-hardverski uređaj niti procedura rada računarskih mreža koji, u svom radu, ne koristi neke od metoda kriptografske zaštite informacija. Pri tome, navedeni kriptografski mehanizmi mogu biti usmereni za zaštitu podataka korisnika ili za zaštitu službenih podataka samog uređaja.

Metode kriptografske zaštite informacija obuhvataju, osim klasično shvaćene kriptografije, i duge vrste šenonovki shvaćenih „tajnih sistema“ kao što su steganografija, ali i potpuno nove oblasti kao što su kriptografski protokoli.

Navedene discipline i njima pripadajuće metode obrazuju tzv. kriptografske osnove bezbednosti. Neki od aspekata kriptografskih osnova bezbednosti su premet ovog rada.

2. KRIPTOGRAFSKE OSNOVE BEZBEDNOSTI

Sam pojam kriptografske osnove bezbednosti treba uslovno shvatiti kao oblast koja podrazumava kriptografske metode i neke druge srodne metode. Prirodu srodnosti je teško definisati jer je ona više intuitivna, kao što je recimo slučaj sa steganografijom. Naime, i kriptografija i steganografija, svaka na svoj način, se bave zaštitom informacija na prenosnom putu. Situacija je slična i kada je reč o kriptografskim protokolima koji, iako u nazivu sadrže reč kriptografija, za predmet rada imaju problematiku potpuno različitu od uvreženog shvatanja klasičnog pojma kriptografije.

Protokol je redosled radnji, koje preduzimaju dve ili više strana, namenjenih za rešavanje određenih zadataka. „Redosled radnji“ označava da se protokol izvršava u definisanom nizu od početka do kraja. Kriptografski protokol je protokol koji, pri rešavanju konkretnog zadatka npr. elektronskog plaćanja, upotrebljava kriptografske metode i tehnologije. On uključuje neke algoritme, ali, uopšteno govoreći, namena protokola prevazilazi granice jednostavne bezbednosti. Smisao upotrebe kriptografije u protokolima je sprečavanje ili otkrivanje prevara ili zloupotreba [4].

Ciljevi, odnosno objekti informacione bezbednosti, koji se realizuju pomoću kriptografskih metoda prikazani su u tabeli 1⁴.

Tabela 1: Neki od ciljeva informacione bezbednosti koji se realizuju kriptografskim metodama

Privatnost ili poverljivost	Podržava tajnost informacija koje su autorizovane i imaju svoga vlasnika
Integritet podataka	Onemogućava zamenu ili izmenu (falsifikat) podataka od strane neautorizovanih korisnika
Identifikacija i autentifikacija	Identifikacija i autentifikacija ovlašćenih korisnika (ličnosti, terminala, kreditnih kartica its.)
Autentifikacija poruka	Potvrda originalnosti izvornih poruka

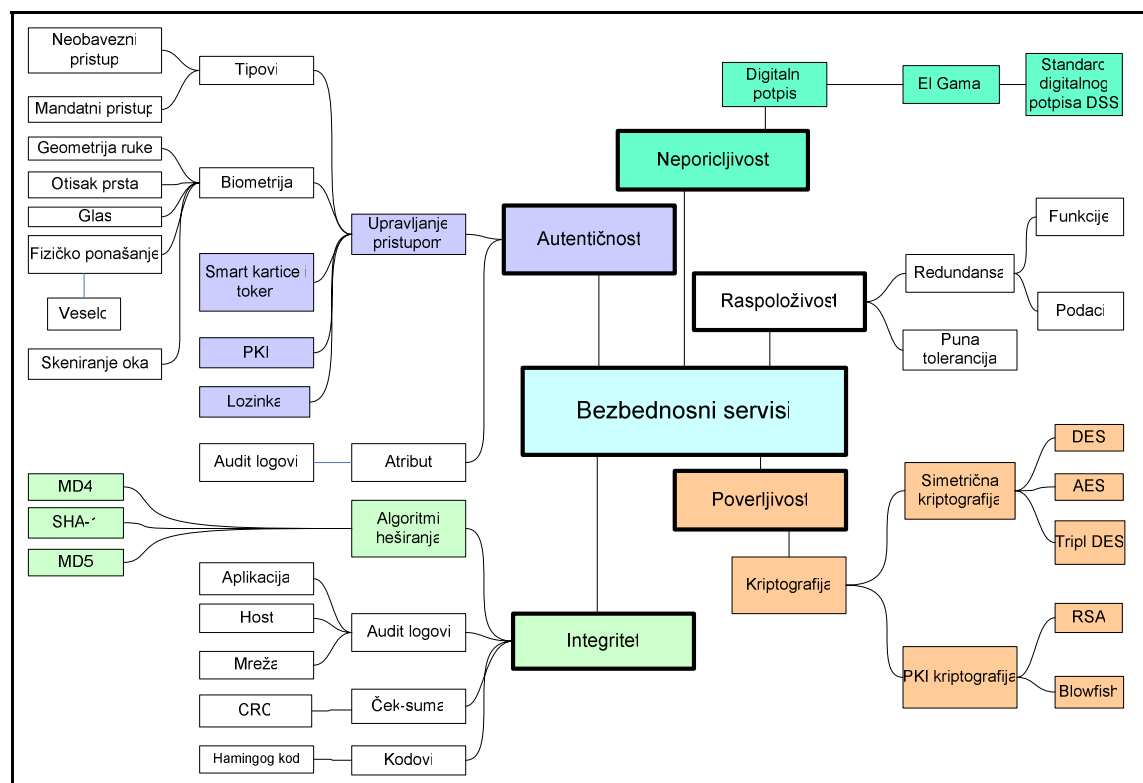
³ Pod «tipičnim» IT sistemima podrazumevaju se specifične grupe informacionih tehnologija – aktiva (*assets*) koje su tipične po rasprostranjenosti rešenja i imaju odlike vrste. «Tipični» IT sistemi su vrednost sa stanovišta organizacije i predstavljaju objekat zaštite. Oni obuhvataju opremu (fizički resursi), informacione resurse (baze podataka, datoteke i dokumentaciju), softver (sistemski, aplikativni, pomoćni), servise i odgovarajuću infrastrukturu (organizacijsku, kadrovsku, inženjersko-gradevinsku, elektronapajanje i klima uređaje).

⁴ A.Menezes, P.van Oorschot, S.Vanstone, *Handbook of Applied Cryptography*, CTC Press, 1996

Potpis	Način (sredstvo) povezivanja informacije i entiteta
Autorizacija	Prenošenje ovlašćenja izvršavanja određenih radnji i operacija
Validacija	Verifikovanje normama predviđenih ponašanja, operacija its.
Upravljanje pristupom	Restrikcija pristupa izvorima i dodela određenih ovlašćenja
Sertifikacija	Odobrenje i garancija poverenja
Neporicivost	Prevenција od mogućeg otkazivanja od akcije, potpisa its.
Anonimnost	Zadržavanje identiteta u tajnosti
Opoziv	Opoziv sertifikata ili autorizacije

Primena kriptotehnologija, u realizaciji servisa informacione bezbednosti, je znatno šira nego što to izgleda na prvi pogled. U cilju ilustracije ovog stava, na slici 2 je prikazana klasifikacija informacione bezbednosti (prema Ejba Ušera⁵) – osenčene mere i postupci su ili zasnovane ili koriste kriptografske metode.

Od pet bezbednosnih servisa IB, pomoću kriptotehnologija se mogu realizovati četiri: autentičnost, poverljivost, integritet i neporicivost. Autentičnost je obezbeđena upotrebom lozinki, smart kartica i infrastrukture javnog ključa PKI (*public key infrastructure*). Poverljivost (tajnost) informacija je realizovana pomoću simetrične i nesimetrične kriptografije. Integritet podataka je zagarantovan primenom heš funkcija i tzv. heširanjem poruka. Neporicivost obezbeđuje kriptotehnologija digitalnog potpisa.



Slika 2 : Kriptološke metode u realizaciji servisa bezbednosti

2.1. Kriptotehnologije

Kriptografski mehanizmi se realizuju u kriptosistemima. **Kriptosistem** čine: jedan ili više algoritama šifrovanja, jedan ili više ključeva, sistem upravljanja ključevima, tekst poruke koji se predaje, algoritmi randomizacije i pripreme teksta za rad sa algori-

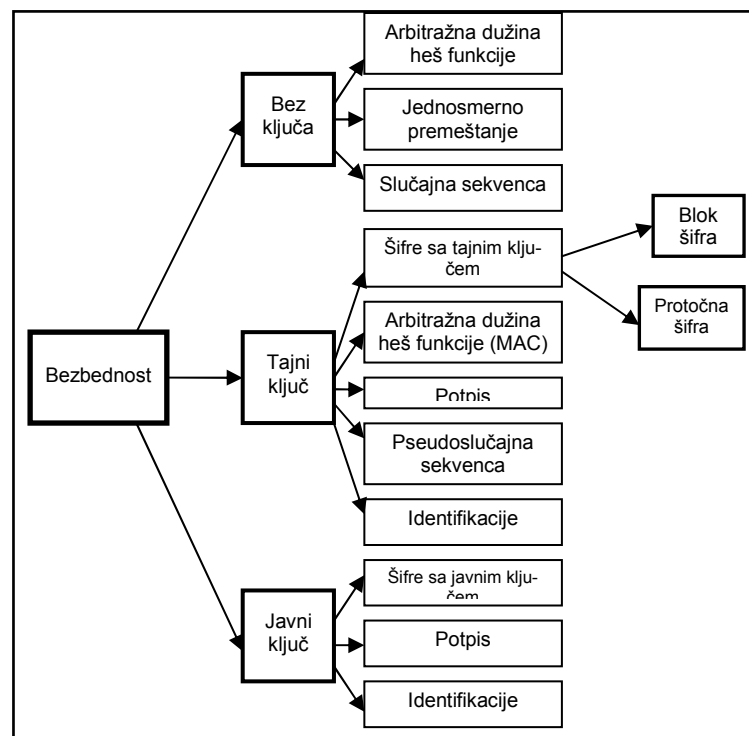
⁵ Abe Usher: Towards a Taxonomy of information assurance, sajt IW.

tmima šifrovanja i šifrovani tekst (kriptogram, šifrotekst). Kriptosistemi mogu biti realizovani hardverski, softverski i hardversko-softverski. Konkretna softverska realizacija kriptosistema se naziva kriptopaket.

Osnovna obeležja kriptosistema su:

- relativna **bezbednost** prenosa informacija (npr. šifrovanje i lozinka)
- postojanje nekakve **tajne** (poznata učesnicima, a nepoznata protivniku – npr. ključ) i
- u slučaju asimetričnih kriptosistema, bezbednost je osigurana postojanjem **treće poverljive strane** (TTP - *third trusted party*)

Kriptotehnologije su bazne metode transformacija informacija sa kojima raspolaže savremena kriptografija. U savremenoj kriptografiji razmatraniju se samo kriptotehnike koji se realizuju pomoću kompjutera⁶. Pomoću njih se grade postojeći kriptografski, odnosno informacioni sistema [5]. Ilustrativna klasifikacija osnovnih kriptografskih alata data je na slici 3⁷.



Slika 3:Klasifikacija kriptografskih alata

Osnovne kriptotehnologije, na osnovu kojih se formiraju kriptotalgoritmi i kriptografski protokoli (tzv. kriptografske šeme), su:

- algoritmi šifrovanja (simetrični i asimetrični),
- izračunavanje heš-funkcije,
- generisanje elektronskog-digitalnog potpisa i
- generisanje nizova pseudo-slučajnih brojeva [5]
-

⁶ Šifrovanje je mogući izvršiti pomoću šifroblankota ili specijalnih tehnika i uređaja. Zbog nedostatka javno dostupne literature o pomenutim tehnikama, ali i zbog činjenice da je njihova upotreba specijalizovana, a ne masovna, njih nećemo razmatrati.

⁷ Prema A.Menezes, P.van Oorschot, S.Vanstone, *Handbook of Applied Cryptography*, CTC Press, 1996

2.2. Primena kriptotehnologija u arhitekturi bezbednosti

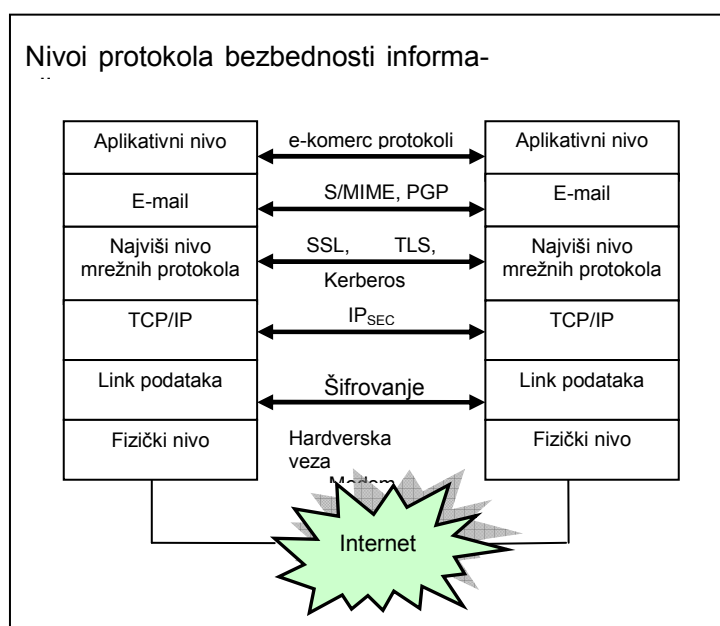
Savremena kriptografija, naročito u delu poznatom pod nazivom „građanska“, „javna“ ili „praktična“ kriptografija, je isključivo praktično orijentisana – njen smisao je da rešava konkretne probleme. Očigledan primer toga su računarske mreže i elektronska trgovina.

Prema ustaljenim shvatanjima, kriptografija se koristi za zaštitu informacija na prenosnom putu. Da je primena kriptografskih osnova bezbednosti mnogo šira, vidi se na primeru računarskih mreža (LAN mreže, globalna računarska mreža – Internet) kao i na primeru arhiviranja (čuvanje) podataka u sistemima obrade podataka.

Savremene računarske mreže se, uglavnom, zasnivaju na Internet tehnologijama⁸ i TCP/IP protokolima koji imaju, sa aspekta bezbednosti, brojne slabosti. Kao takve one su nazamislive bez podrške kriptotehnologija.

Arhitektura bezbednosti etalonskog TCP/IP modela je prikazana na slikama 4 i 5. Prikazani model operiše sa dva pojma: sa nivoima i sa protokolima. Protokoli su, standardima definisana, pravila uzajamnog delovanja različitih mreža. Oni su opisani u RFC dokumentima koji, praktično, predstavljaju standard Interneta. Svi protokoli odgovaraju određenim nivoima etalonskog modela ISO/OSI⁹ i podeljeni su na protokole gornjeg (7-5 nivo OSI) i protokole donjeg makronivoa (4-1 nivoa OSI).

Protokoli donjeg makronivoa upravljaju procesom predaje informacija po kanalima veze (razbijanje poruke na pakete – transportni nivo, maršrutizacija paketa – mrežni nivo, obrazovanje kadrova od paketa – kanalski nivo i podrška konekcije – fizički nivo). Protokoli gornjeg nivoa rešavaju zadatke korisnika (praktični nivo), predstavljanje informacija u jedinstvenoj formi (nivo predstavljanja) i organizuju seanse između različitih procesa (seansni nivo) [6].



Slika 4: Protokoli bezbednosni u ISO/OSI modelu

⁸ Internet je mreža sa komutacijom paketa u kojoj se relativno jednostavno pristupa informacijama koje se prenose a moguće je i ubacivanje poruka uz nemogućnost kasnijeg određivanja njihovog porekla i sadržaja.

⁹ ISO/OSI model je teoretski model koji se razlikuje od modela TCP/IP je realizovan u mreži Internet.

U skladu sa višeslojnom arhitekturom modela, u pojedine njegove nivoe (aplikativni, transportni i mrežni) su implementirani, u cilju unapređenja arhitekture bezbednosti, protokoli bazirani na kriptotehnologijama¹⁰.

Aplikacije		Aplikacije
		Bezbednost "sa kraja na kraj"
TCP		SSL
IP		TCP
		IPsec
IP		IP
NETWORK		NETWORK

Slika 5: Višeslojna implementacija protokola sa kriptotehnologijama

Najpoznati protokoli ovog tipa su: IPsec, SSL, TLS, SSH i protokoli e-trgovine. Njihove osnovne karakteristike, sa aspekta primenjenih kriptotehnologija koje se u njima koriste i arhitekture sistema zaštite informacija, date su u tabela 2.

Tabela 2: Primenjene kriptotehnologije u protokolima bezbednosti u mrežnom radu

¹⁰ Osnovni kriptografski aspekti savremenih računarskih TCP/IP mreža su: infrastruktura sistema sa javnim ključevima PKI (*Public key infrastructure*), tehnologija digitalnog potpisa bazirana na asimetričnim šifrosistemima i zaštita tajnosti podataka primenom simetričnih šifarskih sistema (M.Marković, *Infrastruktura sistema sa tajnim i javnim ključevima*, Institut za primenjenu matematiku i elektroniku)

Nivo modela	Arhitektura sistema zaštite	Kriptotehnologije
Mrežni nivo	Zaštita na mrežnom nivou obezbeđuje se između mrežnih čvorova pri čemu se vrši zaštita integriteta, tajnosti i autentifikacija IP paketa. Zaštita integriteta i autentifikacija IP paketa najčešće se realizuje primenom kriptografskih kompresionih funkcija sa upotrebom tajnog ključa, dok se zaštita tajnosti ostvaruje primenom simetričnih algoritama. Najpoznatiji protokol zaštite na mrežnom nivou jeste IPsec protokol.	IPsec protokol: 1. Šifrovanje: 3 DES, IDEA, Blowfish, Triple IDEA, RC5 2. Integritet podataka: MAC baziran na MD5 3. Distribucija ključeva: RSA 4. Sertifikat: X.509 5. Digitalni potpis: RSA 6. Heš-funkcija: MD5, SHA
Transportni nivo	Zaštita na transportnom nivou predstavlja zaštitu tajnosti podataka primenom simetričnih kriptografskih algoritama i uzajamne provere identiteta subjekata komunikacije. Najpoznatiji korišćeni protokoli su: SOCKS, SSH, SSL, TLS i WTLS.	SSL protokol: 1. Šifrovanje: RC4 sa 40 i 128-bitnim ključem, RC2 sa 128-bitnim ključem, IDEA sa 128-bitni ključem, DES sa 64(56)-bitnim ključem, tripl-DES sa 192 (168)-bitnim ključem 2. Integritet podataka: MAC baziran na MD5 3. Distribucija ključeva: RSA 4. Sertifikat: X.509 5. Digitalni potpis: RSA 6. Heš-funkcija: MD5
Aplikativni nivo	Zaštita na aplikativnom nivou zasniva se na primeni tehnologije digitalnog potpisa na bazi asimetričnih kriptografskih algoritama i zaštite tajnosti podataka primenom simetričnih kriptografskih algoritama. Najpoznatiji protokoli zaštite na aplikativnom nivou koji se primenjuju u mrežama Internet tipa su: S/MIME, Kerberos, SET, PGP i drugi.	S/MIME protokol: 1. Šifrovanje: RC2 sa 40-bitnim ključem u režimu CBC, DES i Triple-DES u režimu CBC 2. Distribucija ključa: RSA 3. Sertifikat: X.509 4. Digitalni potpis: RSA 5. Heš-funkcija: MD2, MD5 SET protocol: 1. Šifrovanje: novčane transakcije - DES sa 56-bitnim, naručivanje - DES sa 40-bitnim ključem u režimu CDMF (PKCS #7) 2. Asimetrično šifrovanje: RSA (PKCS #1) 3. Distribucija ključeva: RSA 4. Sertifikat: X.509 v3 5. Digitalni potpis: RSA 6. Heš-funkcija: SHA-1

Računarske mreže i, posebno, e-trgovina zahtevaju izgradnju mehanizama poverenja, koji garantuju poverljivost i integritet podataka i verodostojnost učesnika. Mehanizmi poverenja se, prema nekim autorima¹¹, nazivaju **modeli poverenja** (*trust models*). Neki od primera realizovanih modela poverenja su sistemi: PGP (*Pretty Good Privacy* – vrlo dobra privatnost), Kerberos i sistem sertifikata za algoritme sa javnim ključem.. U daljem tekstu koji sledi prikazani su sistem PGP i sistem autentifikacije Kerberos. U nastavku je dat osvrt na virtuelne privatne mreže VPN (virtuel privacy network) kao osnovu savremenog biznisa i jedan od servisa savremeno shvaćene informacione bezbednosti.

¹¹ G.Kessler, *An overview cryptography*, Handbook on Local Area Networks, September 1998

2.3. Modeli poverenja

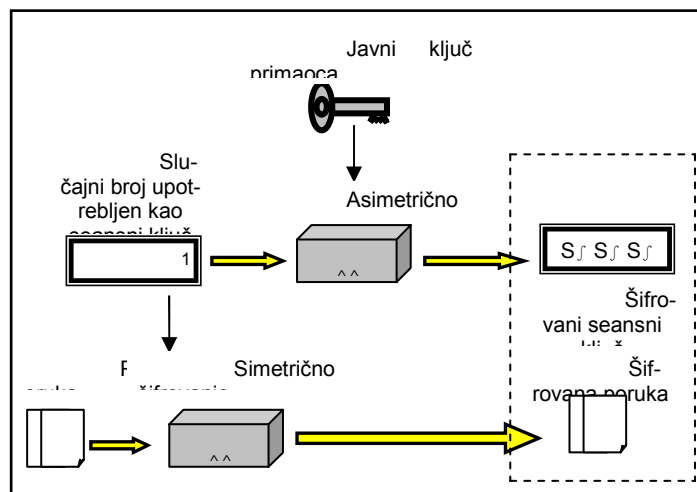
Tvorac **PGP** je Fil Cimerman - bivši agent američke agencije za nacionalnu bezbednost NSA. Prema rečima autora, PGP je nastao kao odgovor narušavanje personalne privatnosti usled razvoja informaciono-komunikacionih tehnologija i nastojanja vlade SAD da, u što je većoj mogućnosti, stavi pod kontrolu privatni život američkih građana¹².

PGP je zasnovan na temeljima „građanske“ kriptografije. Konceptcija bezbednosti bazira na konceptu kriptografije sa javnim ključem. Model poverenja je izgrađen na principu „prijatelj moga prijatelja je moj prijatelj“. Učesnici PGP po sopstvenom nahođenju razmenjuju javne ključeve. Ovako postavljen model poverenja ne ostavlja mogućnosti neovlašćenim licima (pa ni državi) da kontrolišu ili prisluškuju privatne razmene poruka [7].

PGP je hibridni sistem koji u sebe uključuje i algoritam sa javnim ključem, algoritam RSA, i algoritam sa tajnim ključem (algoritam IDEA) zbog čega ga karakteriše velika brzina, svojstvena simetričnim algoritmima, i komfornost, karakteristična za algoritme sa javnim ključem.

Algoritam RSA koristi aritmetiku modova - operaciju stepenovanja po modulu za šifrovanje i dešifrovanje poruka.

Proces šifrovanja fajlova i poruka u PGP je prikazan na slici 6.

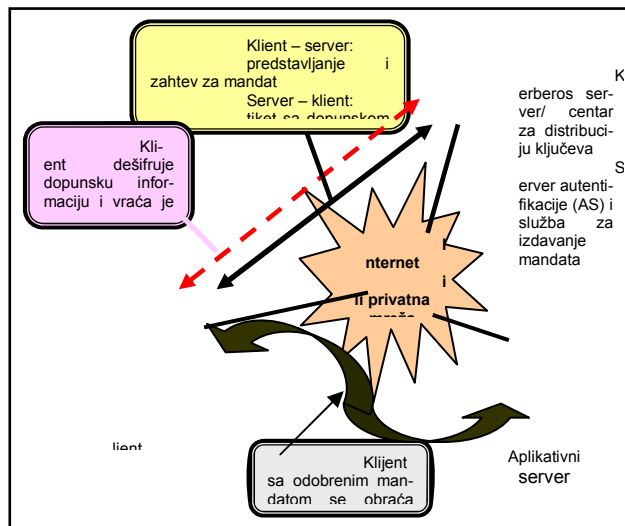


Slika 6: Proces šifrovanja u PGP

PGP omogućava i generisanje digitalnog potpisa za autentifikaciju poruka. Šifrovanjem sa tajnim ključem pošiljaoca poruke, formira se kriptootporna jednostrana heš funkcija koja ima svojstvo „potpisa“ koji garantuje verodostojnost pošiljaoca.

Originalnost javnog ključa u sistemu PGP se realizuje pomoću posrednika od poverenja (za razliku od infrastrukture javnog ključa gde postoji centar poverenja u liku sertifikacionog tela CA). Jedna od važnih prednosti PGP je što može funkcionisati i u centralizovanom okruženju (kakvo pruža sertifikaciono telo), tako i okruženju gde se individualno razmenjuju javni ključevi.

¹² „Tehnološke mogućnosti ne ostavljaju mogućnost zadržavanja status quo kada je reč o privatnosti. Ako ostanemo neaktivni, nove tehnologije će ostaviti takve mogućiti automatskog praćenja vladi o kojima ni Staljin nije maštao. Jedini način očuvanja privatnosti u informacionoj eri je otporna kriptografija“ (Fil Cimerman, Uputstvo korisniku PGP 5,0 za personalnu privatnost).



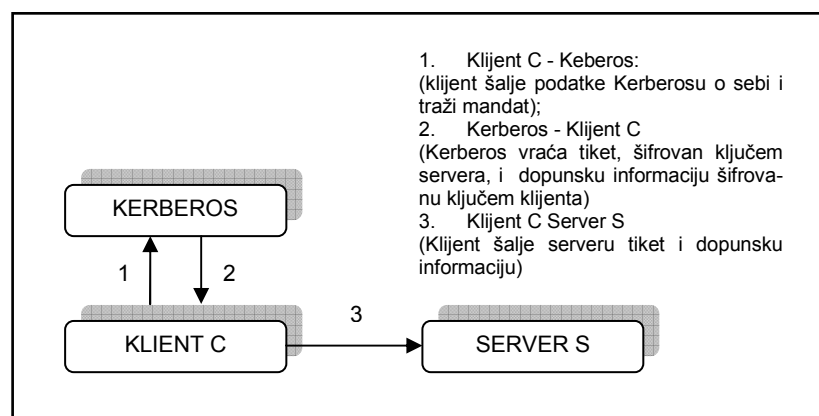
Slika 7: Arhitektura sistema Kerberos

Kerberos je softver koji je razrađen sredinom 80-ih godina u SAD i do današnjeg dana se njegov tzv. «klijenski deo» zadržao u većini operativnih sistema. Sistem Kerberos predstavlja, u procesu distribucije tajnih ključeva, poverljivu treću stranu koja raspolaže tajnim ključevima svih subjekata i koji im pomaže u uzajamnoj proveri identiteta (verodostojnosti). Arhitektura sistema Kerberos je data na slici 7 [8].

U čvorovima javne (nezaštićene) mreže nalaze se subjekti – korisnici i klijentski i serverski softverski sistemi. Svaki subjekt poseduje tajni ključ. Da bi subjekt C (klijent) dokazao svoju autentičnost subjektu S (server), on treba da se predstavi i da dokaže da zna tajni ključ. C ne može jednostavno da pošalje svoj tajni ključ serveru S, jer je mreža nezaštićena i može se aktivno ili pasivno prisluškivati a i, s druge strane, server S ne zna (a ne mora ni znati) tajni ključ klijenta C.

Princip rada sistema Kerberos je objašnjen na slikama 7 i 8 [2].

Klijent C šalje poruku serveru S u kojoj se predstavlja i navodi usluge koje od njega traži. U odgovoru, Kerberos vraća tiket, šifrovan tajnim ključem servera S, i kopiju dela tiketa šifrovanu tajnim ključem klijenta C. Klijent C dešifruje drugi deo poruke i vraća je zajedno sa tiketom serveru. Server S dešifruje tiket i upoređuje ga sa sadržajem dodatne informacije poslate od strane klijenta C. Poklapanje govori o tome da je klijent mogao da dešifruje drugi deo poslate poruke (sadržaj samog tiketa je dostupan samo serveru i Kerberosu) čime je demonstrirao da zna tajni ključ. Znači, klijent je taj za koga se izdaje. Primetimo da tajni ključ, u procesu provere verodostojnosti, nije prenošen nezaštićenom mrežom (čak ni u šifrovanoj formi) – on je samo korišćen za šifrovanje i dešifrovanje.



Slika 8: Provera identiteta klijenta C od strane servera S

Data šema je krajnje uprošćena verzija realne procedure provere verodostojnosti. Karakteristično za sistem Kerberos je ne samo da je otporan na mrežne napade, već i da podržava koncept „jednog ulaska u mrežu“ (pristup mreži samo na jednom mestu) koji mnogi stručnjaci smatraju jedino ispravnim [8].

Razvoj kompanijskih računarskih mreža (distribuiranih na širokom teritorijalnom području), ali i neki javni servisi su nezamislivi bez postojanja **virtuelnih privatnih mreža** VPN (*virtuel privaty network*). Proces formiranja VPN je rezultat integracije kriptografskih mehanizama i tuneliranja. Suština tuneliranja je „pakovanje“ porcije podataka zajedno sa službenim poljima u nove „konvertore“. Kombinacijom tuneliranja i kriptografskih servisa bezbednosti obezbeđuje se da udaljeni učesnik postane lokalni učesnik. VPN proširuje perimetar unutrašnje bezbednosti kompanije do udaljenog ofisa. Slom sistema zaštite tunela je ekvivalentan uništenju sistema zaštite unutrašnjeg perimetra, odnosno slomu zaštitnog zida (firewoall-a).

Bezbednost VPN je zasnovana na bezbednosti protokola autentifikacije i šifrovanja. Protokol PPTP (*point to point tunel protokol* – tunelni protokol tipa tačka-tačka) je namenjen za formiranje i upravljanje VPN po javno dostupnoj mreži TCP/IP sa upotrebom standardnog protokola PPP. U upotrebi je obično verzija ovog protokola za Windows NT.

Protokol PPTP omogućava tuneliranje PPP-konekcija po IP-mrežama putem formiranja VPN. Na taj način udaljeni kompjuter u mreži može imitirati priključenje sa unutrašnjim IP-adresom. Moguća su dva načina upotrebe protokola: po Internetu i po komutaciji spojeva [7].

3. ZAKLJUČAK

Osim algoritama šifrovanja, kriptografija podrazumeva ceo niz kriptografskih disciplina, ali i neka nekriptografskih sredstava (interfejsi, protokoli itd.).

Savremena „praktična“ kriptografija je okrenuta svakodnevnom životnim problemima i, kao takva je u sve većoj meri, postala deo opšteg interesovanja.

LITERATURA

1. Nacional Security Agency, Nacional Information Systems security Glossary, NSTISSI No 4009, Fort Meade, MD spt 2000
2. Галатенко А.В., Основы информационной безопасности, Университет ИТ – ИНТУИТ.ru, 2004
3. BSI, 2001
4. Schneier B., Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth), Publisher: John Wiley & Sons, Inc. 1996
5. Семенов Г., Не только шифрование, али обзор криптотехнологий, Jet Info 3, 2001
6. Олифер В., Олифер Н., Основы сетей передачи данных, Университет ИТ – ИНТУИТ.ru, 2004
7. Cimerman F., PGP 5.0, <http://www.pgpi.com>
8. Kessler G., An overview of cryptography, http://www.garykessler.net/kumquat_pubkey.html, 2006