

UNIVERZITET SINGIDUNUM

**Departman za
poslediplomske studije**

**MASTER STUDIJE
STUDIJSKI PROGRAM:
SAVREMENE INFORMACIONE TEHNOLOGIJE**

MASTER RAD

**ZAŠTITA RAČUNARSKIH MREŽA
DEFINISANJE TEHNIČKIH ZAHTEVA ZA ZAŠTITU I
UPRAVLJANJE KRIPTOLOŠKIM KLJUČEVIMA**

**Mentor:
Prof. dr Mladen Veinović**

**Kandidat:
Milovan Simić**
br. indeksa:
410061/2013

Beograd, 2015.

KRATAK SADRŽAJ

Savremene računarske mreže se uglavnom baziraju na Internet tehnologijama i protokolima koji su podložni mogućim napadima koji narušavaju bezbednost podataka i identitet subjekata. U radu su obrađene metode napada, oblici ugrožavanja i vrste pretnji kojima su izložene računarske mreže, kao i moguće metode i tehnička rešenja za zaštitu mreža. Analizirani su efekti pretnji kojima mogu biti izložene računarske mreže i informacije koje se preko njih prenose. Opisana su određena tehnička rešenja koja obezbeđuju potreban nivo zaštite računarskih mreža, kao i mere za zaštitu informacija koje se preko njih prenose. Navedeni su standardi koji se odnose na metode i procedure kriptozastite informacija u računarskim mrežama. U radu je naveden primer zaštite jedne lokalne računarske mreže. Predstavljen je postupak upravljanja kriptološkim ključevima. Izvršena je analiza generisanja i distribucije ključeva i ukazano je na moguće napade koji se dešavaju u procesu distribucije. U radu su obrađeni Diffie-Hellman i Arithmetica sistemi za razmjenu ključeva i ukazano je na njihove prednosti i nedostatke. Predloženo je rešenje za postizanje većeg nivoa bezbednosti pri upravljanju kriptološkim ključevima.

KLJUČNE REČI : računarske mreže, ugrožavanje mreža, pretnje mreži, protivmere, zahtevi za zaštitu, tajnost informacija, autentičnost, integritet, autorizacija prava korisnika, tehničke mere zaštite, standardi metoda zaštite, algoritam, Arithmetica, generator ključeva, Diffie-Hellman, kriptološki sistem.

ABSTRACT

In this paper different methods of attacks, threats and different forms of dangers to the computer networks are described and presented the process of managing cryptographics keys. The possible models and technical solutions for networks protection are also given. The effects of threats directed to the computer networks and their information are analyzed certain technical solutions that provide necessary protection level of the computer networks as well as measures for information protection are also described. The standards for methods and security procedure for the information in computer networks are enlisted. There is also an example of protecting one local data network. The analysis of generation and distribution of keys was performed and is pointed to possible attacks that occur in the process of distribution. In the paper were processed Diffie-Hellman and Arithmetica systems for the exchange of keys and was indicates of their advantages and disadvantages. At the end of the paper was proposed solution for achieve a greater level of security when managing cryptographics keys.

KEY WORDS: computer networks, endanger of networks, network threats, countermeasures, protection demands, information confidentiality, authenticity, integrity, authorization of the user's rights, technical protection measures, standard methods of protection, algorithm, Arithmetica, key generator, Diffie-Hellman, cryptographics system.

SADRŽAJ

1. UVOD.....	4
1.1. UVODNE NAPOMENE I KONTEKST ISTRAŽIVANJA.....	4
1.2. METODOLOGIJA ISTRAŽIVAČKOG PROJEKTA	5
1.2.1. PREDMET ISTRAŽIVANJA.....	5
1.2.2. CILJ ISTRAŽIVANJA.....	5
1.2.3. ISTRAŽIVAČKE HIPOTEZE.....	6
1.2.4. METODI ISTRAŽIVANJA I TOK ISTRAŽIVAČKOG PROCESA.....	6
2. DEFINISANJE TEHNIČKIH ZAHTEVA KOJA OBEZBEĐUJU POTREBAN NIVO ZAŠTITE JEDNE LOKALNE RAČUNARSKJE MREŽE	7
2.1. POŽELJNE OSOBINE BEZBEDNE KOMUNIKACIJE	7
2.2. VRSTE I OBLICI PRETNJI I NAPADA NA RAČUNARSKJE MREŽE	7
2.2.1. Pretnje računarskim mrežama.....	7
2.2.2. Softverske metode za ugrožavanje računarskih mreža.....	9
2.2.2.1. Virusi (programi koji se mogu sami reprodukovati)	10
2.2.2.2. Crvi (računarski program koji kopiraju same sebe sa jednog računara na drugi).....	10
2.2.2.3. Trojanski konj (program koji se najčešće prenosi na ciljni računar).....	11
2.3. SUZBIJANJE PRETNJI - NAPADA NA RAČUNARSKU MREŽU	11
2.3.1. Protivmere (cauntermeasures) za suzbijanje pretnji ili napada	11
2.3.2. Standardi koji se odnose na zaštitu informacija	12
2.3.3. Organizaciono - tehnička rešenja zaštite računarskih mreža.....	14
2.3.4. Fizička i elektronska zaštita računarske mreže	15
2.3.5. Obezbeđenje pristupnih tačaka mreži i resursima mreže	15
2.3.6. Kriptozastita na prenosnim putevima.....	17
2.3.7. Integritet poruke	17
2.3.7.1. Kriptografske heš funkcije.....	17
2.3.7.2. Šifra autentifikacije poruke.....	18
2.3.7.3. <i>Digitalni potpis</i>	18
2.3.8. Autentifikacija krajnje tačke	18
2.3.9. Obezbeđivanje elektronske pošte	18
2.3.9.1. Bezbedna elektronska pošta.....	18
2.3.9.2. PGP (Pretty Good Privacy).....	19
2.3.10. Obezbeđivanje tcp konekcija : SSL.....	19
2.3.11. Bezbednost mrežnog sloja : IPSec	19
2.3.12. Obezbeđivanje bežičnih LAN-ova	20
2.3.13. Operaciona bezbednost : mrežne barijere i sistemi za otkrivanje uljeza.....	20
2.3.14. Zastita od nestanka napajanja i neadekvatnog napajanja iz javne distributivne mreže	20
2.4. PROJEKTOVANJE ZAŠTITE RAČUNARSKJE MREŽE	21
3. BEZBEDNO RUKOVANJE KRIPTOLOŠKIM KLJUČEVIMA	23
3.1. UPRAVLJANE KRIPTOLOŠKIM KLJUČEVIMA.....	23
3.2. GENERISANJE KRIPTOLOŠKIH KLJUČEVA	23
3.2.1. Pseudoslučajno generisanje bita PRBG	24
3.2.2. Pseudoslučajno generisanje bita CSPRBG.....	24
3.3. DISTRIBUCIJA KLJUČEVA U SIMETRIČNOJ KRIPTOGRAFIJI	24
3.4. DISTRIBUCIJA JAVNIH KLJUČEVA U ASIMETRIČNOJ KRIPTOGRAFIJI	26
3.4.1. Javno objavljivanje.....	26
3.4.2. Javno dostupan direktorijum	26

3.4.3.	Autoritet za javne ključeve (Public-Key Authority)	27
3.4.4.	Sertifikati	28
3.5.	DISTRIBUCIJA TAJNIH KLJUČEVA KORIŠTENJEM KRIPTOGRAFIJE SA JAVNIM KLJUČEM	29
3.5.1.	Jednostavna distribucija tajnog ključa.....	29
3.5.2.	Distribucija tajnih ključeva sa poverljivošću i verodostojnošću	30
3.6.	SISTEMI ZA RAZMENU KRIPTOLOŠKIH KLJUČEVA	30
3.6.1.	Diffie-Hellman algoritam za razmenu ključeva	30
3.6.2.	Arithmetika algoritam za razmjenu ključeva	31
3.7.	EVIDENCIJA KRIPTOLŠKIH KLJUČEVA.....	32
4.	ZAKLJUČAK	35
	Literatura:	36

1. UVOD

Današnja dešavanja na opštoj geopolitičkoj sceni kao i istorijski događaji u našem okruženju stvaraju potrebu za dubljim razmatranjem pojmova suvereniteta i nacionalne bezbednosti. Ovo izuzetno široko i važno pitanje, pored niza drugih elemenata, mora uzeti u obzir bezbednost informacija koje se koriste pri donošenju odluka bitnih za funkcionisanje sistema odbrane, sektora bezbednosti i diplomatije. Profesionalni sistemi kao što su vojska, policija i bezbednosne službe ne bi smele da se oslone na potpuno spoljna bezbednosna rešenja već je neminovno usmeravanje sredstava i resursa na interni razvoj kako bi se postigla kontrola nad svim parametrima koji čine sistem zaštite. Razvoj sistema zaštite, takođe predstavlja široko i važno pitanje čiji je segment u projektovanju računarskih mreža iznet u ovom radu.

1.1. UVODNE NAPOMENE I KONTEKST ISTRAŽIVANJA

Pri projektovanju računarskih mreža, najteži i najsloženiji problem predstavlja zaštita mreže i informacija koje se preko nje prenose. Iskustva pokazuju da problem predstavlja izbor tehničkih rešenja (softverska, hardverska) kojima se može obezbediti zahtevani nivo zaštite. Problemi često nastaju zbog toga što budući korisnik mreže u projektnom zadatku nije precizno definisao nivo i kvalitet zaštite. Takođe, problem predstavlja definisanje tehničkih zahteva za zaštitu, zbog toga što se oni moraju zasnivati na proceni (analiza, studija pretnji) realno mogućih pretnji i oblika ugrožavanja mreže i informacija, kao i proceni sigurnosti šifarskog sistema.

Značaj zaštite i bezbednosti informacija u telekomunikacijama rapidno se povećava, kako u vojnim tako i u javnim mrežama, među kojima su i računarske mreže.

Pri analizi metoda napada i zaštite računarske mreže važno je znati šta je to računarska mreža. Resursi telekomunikacionog sistema određenog kapaciteta, propusnog opsega, bitskog protoka i kvaliteta, angažovani za povezivanje i komunikaciju računara i terminala, čine računarsku mrežu. Drugim rečima, računarska mreža predstavlja telekomunikacionu mrežu koja zadovoljava posebne zahteve koji se odnose na prenos podataka, odnosno komunikaciju između povezanih računara i terminala. Računarska mreža formira se korišćenjem kanala prenosnih sistema (žičnih, optičkih, VF/VVF/UVF radio, radio-relejni i satelitskih sistema) i telekomunikacionih uređaja (opreme), kao što su: komutatori, modemi, multiplekseri, adapteri, mrežne kapije, ruteri (TCP/IP; X.25; ISDN; MPLS, ATM ili multiprotokolski ruteri), mostovi, repetitori, priključne kutije, uređaji za upravljanje multipoint vezama, itd. Funkcije računarske mreže obezbeđuju

mrežni operativni sistemi (na serverima i radnim stanicama), koji omogućavaju komunikaciju preko mreže korišćenjem određenih komunikacionih protokola.

Upravljanje kriptološkim ključevima je jedan od najbitnijih zadataka u savremenoj kriptografiji. Iako ovi algoritmi počivaju na obimnim akademskim istraživanjima sam process kreiranja sigurnih i kvalitetnih kriptoloških algoritama nije jednostavan. U suštini, generisanje ključeva i održavanje tajnosti ključeva je mnogo teže. Prilikom napada na simetrične i asimetrične sisteme kriptanalitičar će prije napasti sistem za upravljanje ključevima, nego što će pokušati da otkrije zakonitosti kriptografskog algoritma koji je primijenjen. Da bi se sigurno zaštitio jedan šifarski sistem cilj je da se što kvalitetnije izvrše: generisanje, distribucija i upravljanje kriptološkim ključevima. Apsolutnu slučajnost je teško definisati i njena mera se predstavlja entropijom. Izvore slučajnosti moguće je postići softverski. Međutim, treba uzeti u obzir da je softver deterministički sistem i da bi se slučajnost povećala u obzir treba uzeti eksterne slučajne događaje kao što su: kretanje miša, dinamika tastature, mrežna i procesorska aktivnost, termički šum elektronskih komponenti, procesi iz prirode i sl. Uzimanjem u obzir ovih parametara može se dobiti kvalitetan slučajan niz, ali ipak, količina ovakvih nizova ostaje ograničena. Posledica svega ovog navedenog je da korišćenje pseudo-slučajnih nizova u procesu generisanja tajnih vrednosti daje rezultat u pseudo-tajnosti. Kao dobri izvori "čiste" slučajnosti mogu se uzeti: detektori radioaktivnog raspada i termičkog šuma, uređaji u kojima je moguće ostvariti i detektovati optički kvantni efekat ili uređaji u kojima nastaju nepredvidive oscilacije frekvencije u fazno kontrolisanoj petlji i sl.

Imajući u vidu da podaci koji se prenose putem računarskih mreža danas mogu imati izuzetno veliku vrednost, u svim profesionalnim sistemima, donošenje odluka i uspeh u poslovanju uveliko zavise od sposobnosti sistema da osigura bezbednost tih podataka. S obzirom na obim korišćenja računarskih mreža i na tajnost kriptoloških ključeva kao jednog od osnovnih elemenata za zaštitu podataka koji se prenose preko komunikacionog spojnog puta, neophodno je razmatrati zaštitu informacija u ovom kontekstu.

1.2. METODOLOGIJA ISTRAŽIVAČKOG PROJEKTA

1.2.1. PREDMET ISTRAŽIVANJA

Težišno pitanje razmatrano u ovom radu jeste analiza mogućih pretnji i napada na računarsku mrežu, kao i tehničke mogućnosti zaštite mreža i informacija i analiza zaštite šifarskog sistema kroz sagledavanje načina i metoda generisanja, distribucije i upravljanja kriptološkim ključevima.

1.2.2. CILJ ISTRAŽIVANJA

Naučni cilj rada je sistematizacija znanja o zaštiti računarskih mreža, utvrđivanje problema pri projektovanju zaštite računarskih mreža i načina njihovog prevazilaženja i ukazivanje na prednosti i nedostatke primenjenih rešenja i mogućnost odabira konkretnog rešenja na bazi izvršenih analiza.

Društveni cilj rada je ukazivanje na ugrožavanje bezbednosti računarskih mreža.

Zadatak rada predstavlja dolazak do mogućeg rešavanja problema u definisanju tehničkih zahteva koja obezbeđuju potreban nivo zaštite jedne lokalne računarske mreže, definisanje mera za zaštitu informacija koje se preko nje prenose, odnosno dostizanje optimalnog rešenja prilikom projektovanja zaštite jedne lokalne računarske mreže, kao i dolazak do bezbednog upravljanja kriptološkim ključevima kao jednog od ključnih postupaka u zaštiti određenog šifarskog sistema.

1.2.3. ISTRAŽIVAČKE HIPOTEZE

Opšta hipoteza:

Bezbednost podataka pri prenosu kroz računarsku mrežu u profesionalnim sistemima je jedan od ključnih elemenata za uspešno poslovanje i donošenje odluka, pogotovo ako se radi o podacima značajnim za funkcionisanje državnih organa. Projektovanje zaštite računarskih mreža i zaštita podataka na prenosnom putu baziran na kriptografskim rešenjima predstavlja najvažniji segment te bezbednosti.

Posebna hipoteza:

Savremene računarske mreže se uglavnom baziraju na Internet tehnologijama i protokolima koji su podložni mogućim napadima koji narušavaju bezbednost podataka i identitet subjekata. Ključni problem leži u činjenici da podaci kruže i egzistiraju u elektronskom obliku koji nije neposredno vidljiv i zbog toga postaju izloženi novim vrstama napada, a osnovni razlozi za to leže u samim osnovnim karakteristikama arhitekture računarske mreže Internet/Intranet tipa:

- TCP/IP protokoli nisu projektovani da zadovolje zahteve za zaštitom informacija,
- Internet je mreža sa komutacijom paketa, u kojoj se jednostavno pristupa informacijama koje se prenose i moguće je ubacivanje poruka nepoznatog porekla i sadržaja.

1.2.4. METODI ISTRAŽIVANJA I TOK ISTRAŽIVAČKOG PROCESA

Kako bi se zadovoljila objektivnost, opštost i sistematičnost, a imajući u vidu specifičnost istraživanja, u radu su primenjene sledeće metode:

- Metoda deskripcije,
- Komparativna metoda,
- Metoda analize,
- Metoda sinteze,
- Metoda modelovanja.

Metoda deskripcije je postupak opisivanja činjenica, procesa i predmeta te njihovih empirijskih potvrđivanja odnosa i veza.

Komparativna metoda podrazumeva upoređivanje sličnih ili srodnih činjenica, pojava, procesa i odnosa, odnosno uvrđivanje njihove sličnosti u ponašanju i intenzitetu kao i razlika među njima.

Metoda analize je postupak naučnog istraživanja i objašnjavanja stvarnosti putem rasčlanjivanja složenih misaonih tvorevina na njihove jednostavne delove i elemente, kao i izračunavanje svakog dela za sebe i u odnosu na druge delove.

Metoda sinteze je suprotna od metode analize i podrazumeva spajanje jednostavnijih lako proverljivih misaonih tvorevina u složenije.

Modelovanje u ovom radu ima za cilj da se putem aproksimacije zamišljenog sistema lakše razumeju i objasne njegovi kompleksni delovi i prikaže predloženo rešenje problema.

Nakon metodoloških smernica, datih u uvodnom delu, drugi deo rada posvećen je realno mogućim pretnjama i oblicima ugrožavanja računarske mreže i definisanju tehničkih zahteva, prilikom projektovanja računarske mreže, koja obezbeđuju potreban nivo zaštite jedne lokalne računarske mreže.

Treći deo posvećen je bezbednosnom upravljanju kriptološkim ključevima kao jednom od ključnih postupaka u zaštiti određenog šifarskog sistema. Predstavljen je postupak upravljanja kriptološkim ključevima. Izvršena je analiza generisanja i distribucije ključeva i ukazano je na moguće napade koji se dešavaju u procesu distribucije.

U zaključnom delu sumirani su rezultati i dodatno naglašene prednosti i nedostaci primenjenih rešenja u vidu daljih pravaca razvoja.

2. DEFINISANJE TEHNIČKIH ZAHTEVA KOJA OBEZBEĐUJU POTREBAN NIVO ZAŠTITE JEDNE LOKALNE RAČUNARSKE MREŽE

2.1. POŽELJNE OSOBINE BEZBEDNE KOMUNIKACIJE

Poželjne osobine bezbedne komunikacije su :

- Poverljivost. Trebalo bi da samo pošiljalac i nameravani primalac razumeju sadržaj prenesene poruke. S obzirom na to da prislušivači mogu da presretnu poruku, to obavezno zahteva da ona bude nekako šifrovana, tako da presretnutu poruku prislušivač ne može da dešifruje.
- Integritet poruke. Čak i kad su pošiljalac i primalac u stanju da međusobno provere svoju autentičnost, oni takođe žele da obezbede da se sadržaj ne promeni, bilo zlonamerno, bilo nesrećnim slučajem tokom prenosa. Za obezbeđivanje takvog integriteta poruke mogu se koristiti proširenja tehnika kontrolnih zbirova.
- Provera autentičnosti krajnjih tačaka. I pošiljalac i primalac trebalo bi da mogu da se uvere u identitet druge strane u komunikaciji. U ljudskoj komunikaciji licem u lice taj problem se lako rešava vizuelnim prepoznavanjem, dok kod entiteta koji komuniciraju razmenjujući poruke preko medijuma, provera autentičnosti nije tako jednostavna.
- Operaciona bezbednost. Skoro sve organizacije danas imaju mreže koje su povezane sa javnim internetom. Te mreže potencijalno mogu postati meta napadača koji mrežama pristupaju preko javnog interneta. Napadači mogu da pokušaju da postave crve u računare te mreže, pribave korporacijske tajne, preslikaju internu konfiguraciju mreže i pokrenu napade odbijanja usluga (DoS).

2.2. VRSTE I OBLICI PRETNJI I NAPADA NA RAČUNARSKE MREŽE

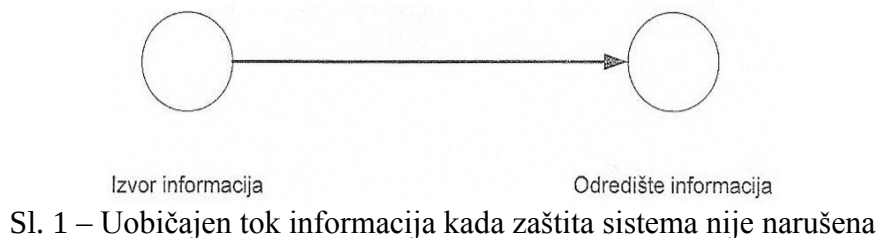
2.2.1. Pretnje računarskim mrežama

Savremene računarske mreže, kao i buduća generacija telekomunikacionih mreža, mogu biti izložene nizu ozbiljnih pretnji (threats) ili napada, koje uzimaju u obzir različite mrežne konfiguracije (arhitektura, topologija), komunikacione protokole i načine prenosa signala. To su, najčešće, sledeće pretnje:

- odbijanje usluge (denial of service). Ovim tipom napada elementi računarske mreže se blokiraju kontinualnim bombardovanjem podacima, tako da se zauzimaju svi mrežni resursi, pa mreža nije u stanju da korisnicima pruža usluge;
- prislušivanje (eavesdropping). Ovom pretnjom prikriveno ili potpuno tajno prislušuju se signali koji se preko mreže prenose između predajnika i prijemnika;
- maskiranje (masquerade). Izvršilac napada koristi maskiranje kako bi simulirao lažnu identifikaciju radi pristupa mreži;
- neautorizovani pristup (unauthorized access). Pristup ulazima u mrežu mora biti veoma restriktivan u skladu sa politikom zaštite. Ako napadač pokuša da realizuje neautorizovan pristup na bilo kom ulazu u mrežu, drugi različiti napadi mogu uporedo proći neprimećeni;
- modifikacije informacije (modification of information). U ovom slučaju podaci mogu biti izmenjeni, uništeni ili oštećeni korišćenjem deliberalizovane manipulacije porukama u datoj mreži;

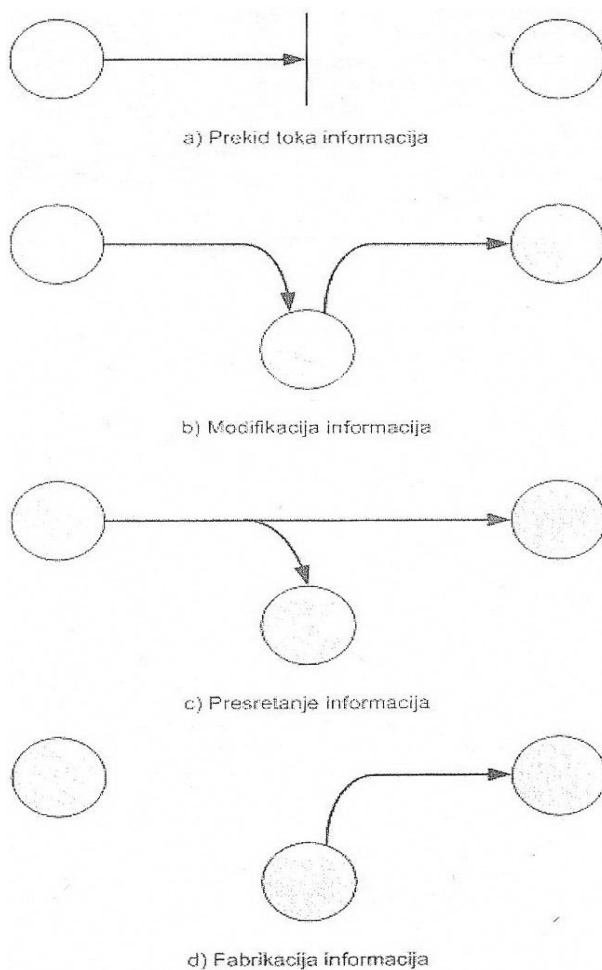
- odricanje (repudiation). Jedan ili više korisnika uključenih u komunikaciju može odbiti, u celini ili parcijalno, učešće u komunikacionom procesu sa drugim korisnicima ili serverima. Moguće metode napada uključuju odbijanje predaje podataka ili prijema podataka, pristup podacima ili modifikaciju podataka.

Uobičajen tok informacija kada zaštita sistema nije narušena je od izvora do odredišta kao na slici 1.



Kada je zaštita sistema narušena, tada postoje sljedeće mogućnosti:

- prekid toka informacija,
- modifikacija informacija,
- presretanje informacija,
- fabrikacija informacija (slika 2).



Sl. 2 – Tok informacija kada je zaštita sistema narušena

Napadi koji prouzrokuju prekid toka informacija se nazivaju napadi na raspoloživost sistema. Primeri takvih napada su: prekid komunikacione linije, uništenje neke hardverske komponente ili nedostupnost datog sistema za upravljanje datotekama. Napadi koji imaju za cilj modifikaciju informacija pripadaju klasi napada na integritet podataka. Primeri takvih napada su: modifikacija sadržaja elektronske pošte, modifikacija sadržaja date datoteke, modifikacija elektronskih dokumenata koji se prenose preko mreže. Treća vrsta napada su napadi na tajnost ili poverljivost podataka. Oni su prouzrokovani presretanjem informacija koje se prenose, tako što neautorizovani subjekt dobija pristup tim informacijama. Primeri takvih napada su: korišćenje sniffer programa, nedozvoljeno kopiranje datoteka ili programa koji se prenose. Četvrta vrsta napada su napadi na autentičnost, koji su prouzrokovani fabrikacijom informacija. Nastaju tako što neautorizovani subjekt generiše falsifikovane ili lažne informacije unutar datog sistema. Primeri napada na autentičnost su: dodavanje sadržaja unutar nekog elektronskog dokumenta, generisanje nepostojeće elektronske pošte ili ponovno slanje pošte poslatih u nekom prethodnom periodu.

Dakle, u zavisnosti od uticaja potencijalnog napadača na tok informacija sve napade na računarske mreže možemo podeliti u dve grupe:

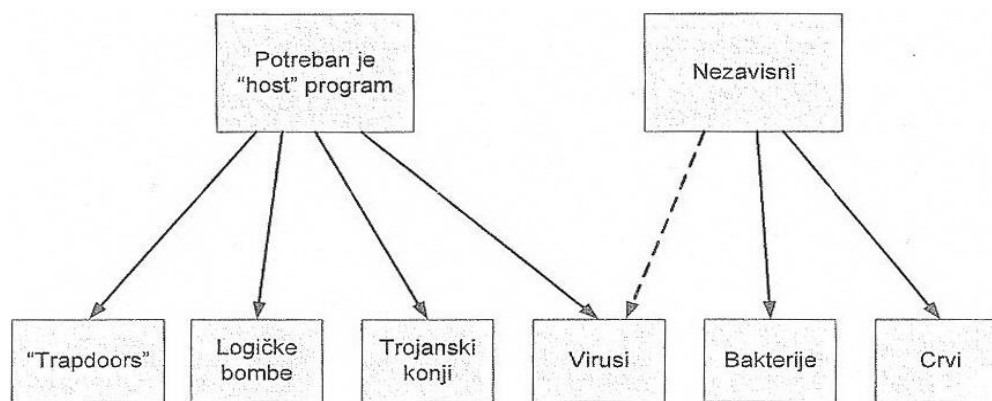
- Pasivni napadi (engl. passive attacks),
- Aktivni napadi (engl. active attacks).

Pasivni napadi se odnose na sve oblike prisluškivanja i nadgledanja toka informacija bez aktivnih izmena u samom toku. Na ovaj način napadač može doći do informacija koje se razmenjuju mrežom. Prisluškivanje koaksijalnih kablova je relativno lako izvodljivo uz pomoć elektromagnetnih senzora dok se prisluškivanje optičkih kablova ne može izvesti bez fizičkih intervencija na kablovima pri čemu dolazi do slabljenja signala koji se može detektovati i na taj način sprečiti eventualni pokušaj prisluškivanja. Pasivne napade je u zavisnosti od konfiguracije mreže teško ali ne i nemoguće primetiti i onemogućiti, a kao najčešći mehanizam odbrane primenjuje se šifrovanje informacionog toka odnosno mrežnih paketa koji se distribuiraju mrežom.

Aktivni napadi podrazumevaju promenu sadržaja informacija ili njihovog toka. Jasno je da su zbog ove činjenice aktivni napadi mnogo opasniji i raznovrsniji od pasivnih. Napadač mora da bude direktno priključen na mrežu da bi izvršio ovakav napad bilo na komunikacionom čvoru ili na jednom delu komunikacionog toka. U aktivne napade svrstavaju se i modifikacija mrežnih paketa, fabrikacija neautorizovanih mrežnih paketa i prekid informacionog toka od strane napadača.

2.2.2. Softverske metode za ugrožavanje računarskih mreža

Za ugrožavanje funkcionisanja Internet mreže i mreža koje su na njega povezane (IP mreže), najčešće se koriste zloćudni programi. Oni mogu postojati nezavisno od drugih programa, kao i programi koji se instaliraju i izvršavaju kao dodatni delovi nekih drugih programa. Logička bomba je zlonamjerna program koji se aktivira na neki događaj (npr. na neki datum). *Trapdoor* je nedokumentovani deo koda koji omogućava pristup neželjenim korisnicima. Bakterije su zlonamerni programi koji se replikuju sve dok ne napune ceo disk ili dok ne potroše sve procesorske resurse.



Slika 3. Klasifikacija zlonamernih programa

2.2.2.1. ***Virusi (programi koji se mogu sami reprodukovati)***

Računarski virus je program koji se može sam reprodukovati tako što dodaje sopstveni kod nekom drugom programu. Razultat izvršavanja virusa može biti ispisivanje neke poruke na ekranu, prikaz slike na ekranu, modifikovanje ili brisanje neke datoteke, poziv nekog telefonskog broja, itd. Drugim rečima, virus može uraditi sve što računarski program može uraditi.

Ciljevi autora virusa su:

- brzo širenje virusa,
- da se virus teško detektuje,
- da odbrana od virusa bude što komplikovanija.

Tipičan virus u toku svog životnog ciklusa prolazi kroz sledeće faze:

- faza spavanja,
- faza propagacije,
- faza trigerovanja,
- faza izvršavanja.

U fazi spavanja virus je besposlen. Iz ove faze virus se može aktivirati na neki događaj, kao što je datum, prisustvom nekog drugog programa ili datoteke, itd. Ova faza nije obavezna za sve viruse. U fazi propagacije se vrši kloniranje virusa. Identična kopija virusa se smješta unutar nekog programa ili datoteke i na taj način se vrši dalje inficiranje. U fazi trigerovanja dolazi do aktiviranja virusa i tada on započinje funkciju za koju je i namjenjen. Posljednja faza je faza izvršavanja u kojoj virus može samo ispisati neku poruku na ekranu ili izvršiti neku destruktivnu operaciju.

Najpoznatiji tipovi virusa su: paraziti, stalno prisutni u operativnoj memoriji, boot sektor, stealth i polimorfni. Paraziti se uvijek nalaze kao deo nekog izvršnog programa. Stalno prisutni virusi u memoriji su obično deo nekog sistemskog programa i inficiraju sve programe koji se izvršavaju. Boot sektor virusi inficiraju glavni boot slog (*master boot record*) i šire se nakon podizanja sistema sa diska. *Stealth* virusi su posebno projektovani da budu nevidljivi prilikom detekcije od strane antivirusnih softvera. Polimorfni virusi su virusi koji mutiraju prilikom svakog inficiranja, čime ostvaruju da detekcija na osnovu karakterističnog uzorka virusa nije moguća.

2.2.2.2. ***Crvi (računarski program koji kopiraju same sebe sa jednog računara na drugi)***

Crv je računarski program koji kopira samog sebe sa jednog računara na drugi. Crvi se mogu koristiti za prenošenje virusa ili za zamenu postojećih datoteka verzijama datoteka koje predstavljaju Trojanske konje. Obično se crvi prenose preko računarske mreže koristeći nedostatke

operativnih sistema u pogledu zaštite. Crvi se brzo replikuju i troše puno memorije na host računarima. Najčešće se prenose uz elektronsku poštu i uz dodatke elektronskoj pošti.

Između crva i virusa ne postoji baš uvek jasna granica. Crvi su dosta slični virusima, ali između njih postoji razlika. Za razliku od virusa, za aktiviranje crva nije potreban korisnik i oni skrivaju svoje širenje na druge računare. Propagacija crva može biti mnogo brža od propagacije virusa. Brzina propagacije je proporcionalna broju ranjivih računara.

2.2.2.3. *Trojanski konj (program koji se najčešće prenosi na ciljni računar)*

Trojanski konj je program koji se najčešće prenosi na ciljni računar kao nevidljivi dodatak uz neki drugi program, a zatim dolazi do njegovog aktiviranja. Mogu se preneti kopiranjem programa, skidanjem sa Interneta, kao i otvaranjem dodatka u elektronskoj pošti. Aktivnosti Trojanskih konja mogu biti veoma različite. Mogu da obrišu podatke, pošalju svoju kopiju na sve računare sa liste elektronske pošte i da omogući dodatne napade na dati računar. Obično ostvaruju povezivanje sa nekim udaljenim računarom i prenose informacije sa računara na kome su instalirani.

Trojanski konji koji se izvršavaju u okviru jezgra operativnog sistema su najopasniji. Tada ovi programi imaju potpunu kontrolu nad datim sistemom. To znači da programi kao što su, na primer, drajver uređaja, "screen saver" i bilo koji drugi programi koje operativni sistem izvršava predstavljaju potencijalni izvor napada.

Trojanski konji se najčešće prikazuju kao korisni programi, ali u suštini oni uvijek imaju neku neželjenu aktivnost po onoga ko ih koristi. Oni se koriste za indirektno izvršavanje funkcija koje neautorizvani korisnici ne bi mogli da ostvare direktno.

2.3. SUZBIJANJE PRETNJI - NAPADA NA RAČUNARSKU MREŽU

Apsolutna zaštita računarskih mreža se ne može ostvariti. Osnovni cilj je obezbediti visok nivo zaštite i zato pristup rešavanju problema zaštite mora biti sveobuhvatan sa stalnim razvijanjem novih mehanizama zaštite u skladu sa bezbednosnim problemima koji nastaju. Kod savremenih računarskih sistema primenjuje se sistem zaštite na više nivoa, tj. zaštita se primenjuje:

- na nivou mreže,
- na nivou operativnog sistema,
- na nivou aplikacije,
- na nivou baze podataka,
- kao proceduralna zaštita.

2.3.1. Protivmere (cauntermeasures) za suzbijanje pretnji ili napada

Suzbijanje pretnji, odnosno napada na računarsku mrežu, realizuje se protivmerama. Protivmere (cauntermeasures) za suzbijanje pretnji ili napada generalno se mogu okarakterisati kao preventivne ili detekcione. U te mere spadaju:

- autentifikacija (authentication) – komunikacioni proces koji omogućava, odnosno obezbeđuje pouzdanu informaciju o identifikaciji učesnika u vezi;
- autorizacija (authorization) – dozvola za uvid ili modifikaciju (promene) podataka ili obavljanje nekih drugih aktivnosti u računarskoj mreži;
- zaštita tajnosti informacija (cofidentiality) – zaštita sadržaja poruke od nedozvoljenog uvida i korišćenja;

- neporicanje (nonrepudation) – proces kojim se štite sistemi u komunikaciji tako što se osigurava predaja poruka, prijem poruka i obrada podataka;
- integritet (integrity) – procedure koje omogućavaju da informacija ne bude menjana u toku prenosa od izvora do odredišta;
- digitalni potpis (digital signature) – poruka koja potvrđuje identitet njenog pošiljaoca, kao i autentičnost i integritet poruke koja se prenosi. To znači da se digitalni potpis razmenjuje između učesnika u komunikaciji radi provere autentičnosti prenete informacije i identifikacije entiteta koji međusobno komuniciraju;
- kontrola pristupa (access control) – procedura kontrole kojom se utvrđuje pravo nekoj osobi da pristupi resursima računarskog sistema ili računarske mreže;
- virtuelna privatna mreža (Virtual Private Network – VPN) – metodama kriptozastite osigurana veza dva učesnika u IP računarskoj mreži;
- kriptozastita poruka (encryption) – algoritmi i metode (permutacija, supstitucija i sabiranje po modulu 2) kojima se obezbeđuje šifrovanje – dešifrovanje poruka u komunikaciji;
- otkrivanje napada (intrusion detection) – mere koje omogućavaju da se otkrije napad na računarsku mrežu i time spreči ugrožavanje;
- provera i presecanje pretnji (auditing and logging) – procedure kojima se proveravaju pristupni kanali veze ka mreži radi otkrivanja i sprečavanja pretnji.

2.3.2. Standardi koji se odnose na zaštitu informacija

Šifrovanje poruka, odnosno podataka, jedina je pouzdana metoda zaštite podataka pri prenosu preko računarske mreže. Na izvoru se podaci šifruju, a na odredištu dešifruju. Tajnost u prenosu postiže se korišćenjem šifarskih ključeva, kao i određenih algoritama i metoda transformacije podataka, odnosno poruka koje se prenose preko mreže.

Moderni šifarski sistemi se mogu klasifikovati u dve grupe:

- Simetrični šifarski sistemi (private key systems),
- Asimetrični šifarski sistemi (public key systems).

Kod simetrinih šifarskih sistema ključ za šifrovanje identičan je ključu za dešifrovanje. Zbog toga se ključ mora tajnim kanalima dostaviti strani koja treba da izvrši dešifrovanje, što ujedno predstavlja jedan od najvažnijih nedostataka ovakvih šifarskih sistema. Simetrični šifarski sistemi nazivaju se još i klasični šifarski sistemi. Simetrični šifarski sistemi karakterišu se relativno velikom brzinom rada i jednostavnom implementacijom. Mogu da obezbede kvalitetnu zaštitu komunikacionih kanala u računarskim mrežama pod uslovom da se tajni ključ za proces šifrovanja, odnosno dešifrovanja transportuje sigurnim kanalima i da je nepoznat potencijalnim napadačima.

Zahtevi za tajnošću i autentičnošću kod simetričnih šifarskih sistema zasnivaju se upravo na tajnosti ključa. Ukoliko napadač ne poseduje tajni ključ, on nije u mogućnosti da otkrije sadržaj poruke. Zbog ove činjenice najveći problem kod simetričnih šifarskih sistema je upravo obezbeđivanje sigurnih kanala za distribuciju tajnih ključeva.

Sedamdesetih godina prošloga veka dolazi do pojave i naglog razvoja asimetričnih šifarskih sistema, koji se još nazivaju i sistemi javnih ključeva (engl. public key systems) kod kojih se ključ za šifrovanje razlikuje od ključa za dešifrovanje i koji su ispravili postojeće nedostatke simetričnih šifarskih sistema.

Asimetrični šifarski sistemi rešili su dva velika problema simetričnih šifarskih sistema, a to problem distribucije tajnih ključeva i problem autentifikacije poruka. Kod asimetričnih sistema postoje dva ključa. Jedan za šifrovanje a drugi za dešifrovanje. Ključevi nisu isti ali su povezani jedan sa drugim određenim transformacijama. Poznavanje jednog ključa i algoritma transformacije ne omogućava dobijanje drugog ključa. Jedan od ključeva se označava za javni (eng. public key) i može se slobodno distribuirati, dok se drugi označava kao tajni i mora biti dostupan samo

njegovom vlasniku. Javni ključ se obično koristi za šifrovanje poruka koje se upućuju njegovom vlasniku. Ovakve poruke može dešifrovati samo vlasnik odgovarajućeg tajnog ključa. Na taj način moguće je izvršiti šifrovanje ali ne i dešifrovanje poruke. Pri distribuciji javnih ključeva treba voditi računa da može doći do zloupotrebe istih zbog neodgovarajuće autentifikacije. Naime, ukoliko korisnik A pošalje svoj javni ključ korisniku B, a korisnik C presretne tu komunikaciju i zameni javni ključ korisnika A svojim javnim ključem koji dalje prosledi korisniku B, tada će on biti u stanju da pročita svaku poruku korisnika B korisniku A. No, to nije sve. Korisnik C će dalje moći da dešifrovanu poruku šifruje uz pomoć originalnog javnog ključa korisnika A i predstavljajući se kao korisnik B pošalje šifrovanu poruku korisniku A.

Šifarski ključevi su tajni i nisu predmet standardizacije. Predmet standardizacije su metode i algoritmi za kriptozastitu koji se odnose na: simetrično šifrovanje, asimetrično šifrovanje i algoritme za transformaciju poruka.

Pregled najpoznatijih standarda za kriptozastitu podataka prikazan je u tabeli 1. Navedene su oznake i oblast primene standarda za kriptozastitu informacija.

Tabela 1: Pregled standardnih metoda i algoritama za kriptozastitu

Standardi metoda za kriptozastitu		Oznaka	Oblast primene
Simetrično šifrovanje	blok-šifra	DES IDEA CAST SKIPJACK RC2	tajnost poruka; digitalni potpis; provera autentičnosti.
	sekvencijalna šifra	RC4	
Asimetrično šifrovanje	standardni algoritmi	RSA PKCS DSS	tajnost poruka; ključevi za šifrovanje; digitalni potpis; provera autentičnosti.
	standardi za upravljanje ključevima	KERBEROS KEA	
Algoritmi za transformaciju poruka		MD2 MD4 MD5 SHA	ključevi za šifrovanje poruka; digitalni potpis; provera autentičnosti

U trećoj koloni tabele 1 date su skraćenice tj. oznake pomenutih standarda, koje imaju sledeće značenje:

- DES – Data Encryption Standard je standard za šifrovanje – dešifrovanje podataka, usvojen 1977. godine. Definisao ga je Nacionalni biro za standarde (NBS) SAD. Osnovni blokovi algoritma su permutacija, supstitucija i sabiranje po modulu 2. Za primene u kojima se DES smatra nedovoljno sigurnim sistemom (za tzv. blokovske šifre), primenjuje se varijanta DES-a – trostruki DES ili 3DES. DES ("Federal Data Encryption Standard") je jedan od najpoznatijih simetričnih sistema za šifrovanje. Iako je 1977. godine data preporuka od Američkog nacionalnog biroa za standarde za korišćenje ovog sistema, vlada SAD nikada nije koristila DES za zaštitu svojih poverljivih podataka zbog toga što je dužina ključa od 56 bita dovoljno kratka za pokušaje brute force napada.

- IDEA – U novije vreme od simetričnih sistema za šifrovanje izdvojio se tzv. IDEA International Data Encryption Algorithm kao međunarodni algoritam za šifrovanje podataka i predstavlja tzv. blok-šifru u kojoj se koristi šifarski ključ dužine 128 bita. Ovaj algoritam se smatra vrlo sigurnim. IDEA je evropski standard, razvijen je u Cirihu od strane James L. Massey i Xuejia Laia, a objavljen je 1990 godine. Do sada je IDEA algoritam bio otporan na različite pokušaje dekriptovanja, a najnoviji dokazi ukazuju na to da je IDEA algoritam otporniji od DES algoritma.
- CAST je američka blok šifra, koja koristi ključ dužine 128 bita.
- Skipjack-Capstone je šifra koju je razvila NASA, a koristi ključeve dužine 80 bita. Podržava algoritam digitalnog potpisa (Digital Signature Standard, DSS).
- RC 2 i RC 4 su šifre koje koriste šifarske ključeve promenljive dužine. Zamišljene su kao zamena za DES algoritam.
- RSA – Sigurno najpoznatiji asimetrični algoritam za šifrovanje je svakako RSA (Rivest-Shamir-Adelman). To je algoritam šifrovanja zasnovan na činjenici da je lako generisati dva velika prosta broja p i q , pomnožiti ih međusobno, ali je veoma teško izvršiti faktORIZACIJU rezultata množenja. Ovaj algoritam implementiran je u program za šifrovanje PGP (Pretty Good Privacy) autora Philipa Zimmermanna koji se najčešće koristi za ostvarivanje sigurnosti elektronske pošte (engl. e-mail) u računarskim mrežama.
- PKCS – Public Key Cryptography Standard je standard koji su predložili RSA i konzorcijumi koji čine Microsoft, Apple, Digital Equipment i drugi.
- DSS – Digital Signature Standard je šifra koju je kao standard prihvatila Vlada SAD. Dužina ključa može varirati od 512 do 1024 bita. Namenjen je za proizvodnju digitalnih potpisa i ne koristi se za zaštitu podataka.
- Kerberos je protokol koji je razvio Massachusetts Institute of Technology. Namenjen je za bezbedno čuvanje tajnih ključeva u bazi podataka. Do tajnog ključa može doći samo njegov vlasnik, koristeći Kerberos protokol.
- KES – Key Exchange Algorithm je algoritam za razmenu ključeva, ali se ne koristi za šifrovanje podataka.
- MD2, MD4 i MD5 su algoritmi za transformaciju poruka. Svaki od njih proizvodi tzv. Hash vrednost od 128 bita.

2.3.3. Organizaciono - tehnička rešenja zaštite računarskih mreža

Sa velikom sigurnošću može se tvrditi da potpuna, apsolutna zaštita računarskih mreža ne postoji. Postoji sigurna zaštita određene mreže samo za precizno definisane i procenjene pretnje, odnosno napade, pod uslovom da napadaču nije poznato kako je zaštita tehnički realizovana. Drugim rečima, korisnik ili imalac mreže mora proceniti kojim pretnjama ili napadima mreža može biti izložena, pa se za takve pretnje može realizovati sigurna zaštita. Mora se unapred proceniti šta konkretno može ugroziti mrežu, da bi se definisalo adekvatno tehničko rešenje za njenu zaštitu.

Zaštitu mreža i informacija čini skup pravila, procedura, algoritama, hardversko-softverskih komponenata, kao i skup organizacionih tehničkih mera kojima se obezbeđuju, odnosno štite, funkcije mreže pri izvršavanju mrežnih transakcija. Zaštitom računarske mreže obezbeđuje se: tajnost informacija, integritet i autentičnost informacija, autentifikacija i autorizacija korisnika mrežnih usluga i neporicanje.

Pod zaštitom informacija podrazumeva se zaštita od: neovlašćenog uvida i korišćenja informacija, nekontrolisanog oticanja informacija, slučajnog ili namernog oštećenja, izmene ili uništenja.

Zaštita računarske mreže i informacija izvodi se kroz realizaciju niza organizacionih tehničkih mera kao što su:

- mere kadrovske politike, zato što korisnik usluga mreže predstavlja nosioca informacija, ali i najveću potencijalnu opasnost po te informacije;

- organizaciono-administrativne mere, kojima se normativno regulišu prava, obaveze i odgovornosti, uključujući i sankcije korisnika informacionog sistema;
- tehničke mere fizičke, elektronske i protivpožarne zaštite;
- hardversko-softverske mere kojima se obezbeđuju pristupni putevi mreži i resursima mreže koji se štite;
- aplikativno-programske mere koje predstavljaju procedure koje se ugrađuju u aplikativni softver radi zaštite;
- mere kriptozastite radi zaštite podataka u memorijskim resursima u računarima i zaštite na prenosnim putevima.

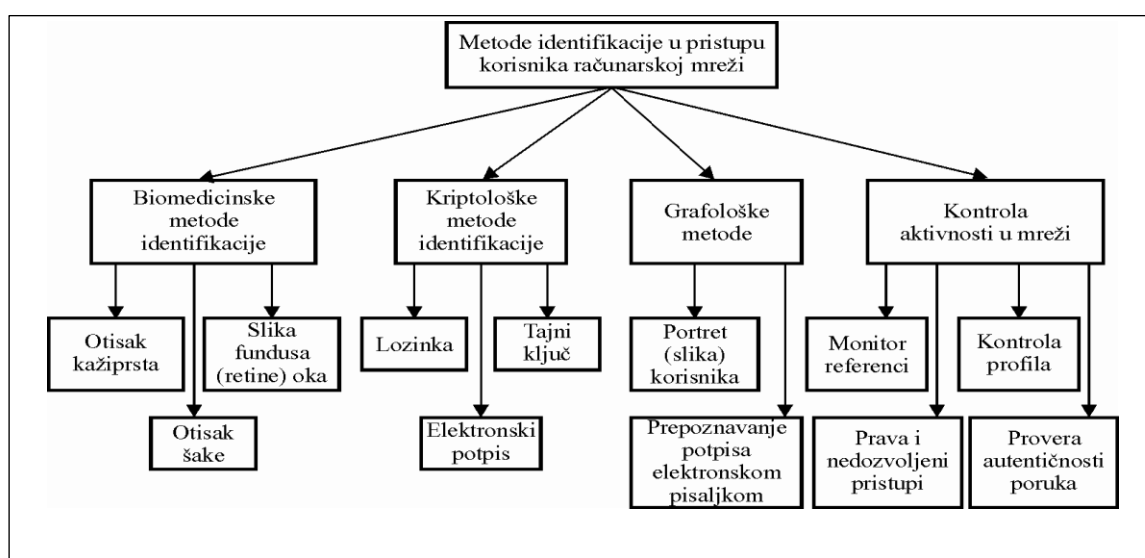
2.3.4. Fizička i elektronska zaštita računarske mreže

Fizičku zaštitu računarske mreže čini skup mera u koje spadaju: fizičko obezbeđenje, elektronska protivprovalna zaštita, protivpožarna zaštita i zaštita od nestanka i neadekvatnog napajanja električnom energijom.

Fizička i elektronska zaštita odnosi se na zaštitu: objekata, odnosno prostorija u kojima se nalazi računarska i telekomunikaciona oprema; računarske i telekomunikacione opreme; magnetnih i elektronskih nosilaca podataka, a predstavlja skup pravila i sredstava kojima se vrši kontrola i evidencija kretanja u objektima, kao i kontrola pristupa računarskoj opremi i magnetnim nosiocima podataka.

2.3.5. Obezbeđenje pristupnih tačaka mreži i resursima mreže

Obezbeđenje pristupnih tačaka mreži i pojedinim resursima mreže ostvaruje se nizom hardversko-softverskih mera. Te mere odnose se na identifikaciju korisnika i utvrđivanje prava i ovlašćenja koja su mu data u odnosu na resurse mreže kojima pristupa. Prepoznavanje korisnika, odnosno njegova identifikacija, sastoji se od fizičkog prepoznavanja – korišćenjem hardverskih uređaja i logičkog prepoznavanja – upotrebom određenih softverskih metoda (slika 4).



Sl. 4 – Metode identifikacije korisnika

Tradicionalani metod identifikacije u pristupu korisnika računarskoj mreži je sistem kod koga se koristi korisničko ime i lozinka kojim se verifikuje identitet korisnika i na taj način isključuje

moгуćnost rada neidentifikovanih korisnika. Tajnost lozinke je glavni deo sistema kojim se na ovaj naćin obezbjeđuje zaštita. Od naćina implemenatacije sistema lozinke najviše zavisi koliko će sistem biti zaštićen. Zato većina današnjih sistema ne omogućava korisnicima unos onih lozinke koje nisu dovoljno sigurne i koje se nazivaju slabe lozinke. Primeru slabih lozinke su ime i prezime, reć iz rećnika, ime ćlana porodice, itd. U cilju bolje zaštite, potrebno je da operativni sistem podrži jake lozinke, odnosno:

- kontroliše da lozinke budu reći koje se ne mogu naći u rećniku,
- kontroliše da lozinke budu reći najmanje 6 karaktera dućine,
- kontroliše da lozinke budu sastavljene i od slova i brojeva,
- obezbedi da lozinke imaju period vaćenja,
- ogranići broj pokućaja prijavljivanja na sistem sa pogrećnom lozinkom, tako što će nakon maksimalnog broja pokućaja automatski zabraniti korisnićki nalog.

Najvaćznija lozinka u datom sistemu je lozinka sistem administratora, jer ona ima kompletnu kontrolu nad sistemom. Upravo zbog toga najveći broj napada na sistem ima za cilj pronalaćenje lozinke sistem administratora. Sistem zaštite koji se zasniva na lozinkama se moće narućiti pogaćanjem lozinke. Drugi naćin je metodom grube sile gdje se koriććenjem današnjih raćunara veoma brzo moće pretraćiti kompletan skup mogućih lozinke ćija je maksimalna dućina unapred poznata. Narućavanje sistema zaštite koji se zasniva na lozinkama se moće narućiti kao rezultat vizuelnog ili elektronskog monitoringa. Vizuelni monitoring nastaje gledanjem u tastaturu prilikom unosa korisnićkog imena i lozinke. Elektronski monitoring se moće uraditi pomoću sniffing alata kojim se moće snimiti identitet korisnika i njegova lozinka.

Sistem lozinke koji se uglavnom primjenjuje nije potpuno siguran. Korisnici obićno biraju lozinke koje se lako pogaćaju ili biraju sloćenije, ali ih zapisuju i ostavljaju na vidljivim mjestima. Narućavanjem sistema lozinke dolazi se do neautorizovanog pristupa resursima datog sistema.

Veću bezbednost omogućavaju metode fizićkog prepoznavanja koje se zasnivaju na: prepoznavanju nekih identifikacionih sredstava koje korisnik poseduje, kao što su inteligentne (smart) kartice, magnetne i optićeke kartice, bećževi, žetoni i slićno, i prepoznavanju fizićkih, biometrijskih karakteristika korisnika, kao što su: otisak prsta, otisak i oblik šake, oblik uha ili glave, osobine glasa, slika mrećnjaće oka i dr.

Fizićeke metode prepoznavanja, odnosno identifikacije sredstava koju poseduje iskljućivo dati korisnik, ne zadovoljavaju u potpunosti zahteve za sigurnu identifikaciju. Razlog je u tome što postoji mogućnost: prenoćenja sredstava od jedne do druge osobe (sa ili bez znanja legitimne osobe), oštećenja ili gubitka naprave.

Fizićeke metode prepoznavanja, zasnovane na identifikaciji fizićkih biometrijskih karakteristika, obezbećuju pouzdanu i sigurnu tzv. „pozitivnu personalnu identifikaciju“. Prepoznavanje korisnika i provera njegovih ovlaćenja u korićenju resursa mreće korićenjem biometrijskih metoda moće se izvrćiti sa velikom sigurnošću. Meću metodama za biometrijsku identifikaciju korisnika najćećeće se koristi otisak prsta (fingerprint).

Prepoznavanje korisnika obavlja se putem njegovog otiska prsta, porećenjem sa ranije zapamćenim otiskom.

Metode logićekog prepoznavanja zasnovane su na informacijama koje korisnik u procesu identifikacije i autorizacije ovlaćenja daje sistemu. Te informacije moraju biti jednake informacijama kojima sistem raspolaće. Logićeke prepoznavanje obićeo se realizuje korićenjem ćetiri vrste softvera, a to su:

- kontrolni program komunikacionog servera;
- softver za upravljanje sistemskim resursima, realizovan kroz opcije mrećnog komunikacionog softvera, odnosno servera,
- softver za upravljanje bazama podataka, realizovan kroz server baze podataka;
- softver za upravljanje transakcijama, realizovan kroz server baze podataka.

Na bazi pozitivno identifikovanog korisnika ovaj softver omogućava da se za datog korisnika odredi vrsta i širina ovlašćenja pri radu u računarskoj mreži. Kao primer mogućeg rešenja logičke identifikacije može se koristiti operativni sistem AIX 5.2 i softver za upravljanje bazama podataka.

Na strani radnih stanica računarske mreže obično se primenjuje kombinovani sistem fizičkog i logičkog prepoznavanja korisnika, korišćenjem principa lokalne i mrežne identifikacije. Zatim sledi utvrđivanje vrste i širine ovlašćenja kojima korisnik raspolaže, upotrebom verifikacije otiska prsta i lozinke (fingerprint + password). Operativni sistem na radnim stanicama može, na primer, biti Windows XP, koji omogućava implementaciju softvera sistema zaštite na principu „fingerprint + password“. Ovaj operativni sistem omogućava postavljanje računara u režim automatskog izlaska iz mreže nakon određenog perioda neaktivnosti. Time se dodatno osigurava neovlašćeno korišćenje usluga mreže.

2.3.6. Kriptozaštita na prenosnim putevima

Komunikacione linije predstavljaju najosetljiviji deo računarske mreže zbog toga što se one ne mogu efikasno fizički kontrolisati. Svaki nekontrolisani deo komunikacionih linija predstavlja pristupnu tačku preko koje se mogu pratiti i prisluškivati signali koji se prenose kroz računarsku mrežu. Posebno su osetljivi oni delovi mreže koji se realizuju bežičnim prenosom, odnosno radio-vezama. Takve veze mogu se vrlo efikasno prisluškivati, ali i ometati. Ove pretnje mogu se najefikasnije eliminisati ili umanjiti primenom kriptozaštite signala na komunikacionim linijama, kao i paralelnim umrežavanjem. Za realizaciju kriptozaštite informacija potrebni su komunikacioni uređaji sa ugrađenim kriptomodulima. Ako se kriptomoduli ugrađuju i u radne stanice, obezbeđuje se zaštita informacija od izvora do odredišta. Jedno od rešenja kriptozaštite može se realizovati primenom IPSEC familije protokola sa 3DES algoritmom. Dodatni nivo zaštite na prenosnim putevima može se obezbediti primenom tzv. virtualnih privatnih „tunela“ VPN (Virtual Private Network), a ostvaruje se korišćenjem familije VPN protokola. Tim protokolima onemogućava se pristup informacijama, odnosno porukama u čvorovima mreže preko kojih se one prenose. Pomenute mogućnosti zaštite poseduju ruteri. Tako, na primer, ruteri Cisco System 1720 sa dodatnim VPN protokolima i IPSEC 3DES operativnim sistemom, mogu u potpunosti da zadovolje zahteve za kriptozaštitu podataka u računarskoj mreži. Podrazumeva se da korisnik mreže poseduje sopstvene šifarske ključeve, odnosno algoritme za njihovo generisanje.

2.3.7. Integritet poruke

Integritet poruke se ponekad naziva i proveravanje autentičnosti poruke. Kad su pošiljalac i primalac u stanju da međusobno provere svoju autentičnost, oni žele da obezbede da se sadržaj njihove komunikacije ne promeni. Da bi se proverila autentičnost poruke, potrebno je da se proverila da:

- Poruka zaista potice od lica koje je poslalo;
- Preneta poruka nije promenjena na putu do lica koje je predviđeno za primaoca.

2.3.7.1. Kriptografske heš funkcije

Heš funkcija uzima ulaz, i proračunava niz fiksne dužine koji se zove heš. Kontrolni zbirovi za internet i CRC - ovi zadovoljavaju ovu definiciju. Kriptografska heš funkcija mora da ima sledeće dodatno svojstvo, računarski je neizvodljivo pronaći bilo koje dve različite poruke x i y takve da je $H(x)=H(y)$. Nezvanično, ovo svojstvo znači da je uljezu računarski nedozvoljeno da poruku zaštićenu heš funkcijom zameni drugom porukom. Odnosno, ako su $(m,H(m))$ poruka i njen pripadajući heš koji je napravio pošiljalac, onda uljez ne može da podesi sadržaj druge poruke y , tako da ona ima istu vrednost heša kao originalna poruka.

2.3.7.2. Šifra autentifikacije poruke

Da bi se proverio integritet poruke, osim kriptografske heš funkcije pošiljaocu i primaocu je potrebna zajednička tajna s . Ta zajednička tajna, jedan niz bitova, naziva se **ključ autentifikacije**. Kada pošiljalac napravi poruku m , dodaje joj tajnu s i pravi $s+m$, a zatim izračunava heš $H(m+s)$. $H(m+s)$ se zove **šifra autentifikacije poruke (MAC – message authentication code)**.

2.3.7.3. Digitalni potpis

U digitalnom svetu, često želimo da ukažemo na vlasnika ili stvaraoca dokumenta, ili želimo da označimo nečiju saglasnost sa sadržajem dokumenta. Digitalni potpis je kriptografska tehnika za postizanje ovih ciljeva u digitalnom svetu. Baš kao i sa potpisima ljudi, digitalno potpisivanje bi trebalo da se izvrši na takav način da se digitalni potpisi mogu proveriti i da se ne mogu falsifikovati. Odnosno, mora biti moguće da se dokaže kako je dokument koji je neko potpisao zaista potpisala ta osoba i da je samo ta osoba mogla da potpiše dokument.

2.3.8. Autentifikacija krajnje tačke

Autentifikacija krajnje tačke je proces dokazivanja identiteta jedne osobe drugoj osobi. Kada izvršavaju autentifikaciju preko mreže, strane u komunikaciji ne mogu da se oslone na biometrijske informacije, kao što je vizuelna pojava ili uzorak glasa. Ovde autentifikacija mora da se uradi samo na osnovu poruka i podataka razmenjenih u okviru protokola autentifikacije. Protokol autentifikacije prvo ustanovljava identitet strana na obostrano zadovoljstvo; tek posle autentifikacije, strane mogu da pređu na posao koji ih očekuje. Postoji više vrsta **autentifikacionih protokola** :

- Autentifikacioni protokol *ap1.0*
- Autentifikacioni protokol *ap2.0*
- Autentifikacioni protokol *ap3.0*
- Autentifikacioni protokol *ap3.1*
- Autentifikacioni protokol *ap4.0*
- Autentifikacioni protokol *ap5.0*

2.3.9. Obezbeđivanje elektronske pošte

Usluge bezbednosti se mogu pružati na svakom od četiri gornja sloja internetovih protokola. Kada se bezbednost osigurava za konkretan protokol aplikacionog sloja, onda će aplikacija koja koristi taj protokol dobijati jednu ili više usluga bezbednosti, kao što je poverljivost, autentifikacija ili integritet. Kada se bezbednost osigurava za protokol transportnog sloja, onda sve aplikacije koje koriste taj protokol dobijaju usluge bezbednosti transportnog protokola. Kada se bezbednost pruža na mrežnom sloju, od računara do računara, onda svi segmenti transportnog sloja dobijaju usluge bezbednosti mrežnog sloja. Kada se bezbednost pruža u sloju veze podataka, onda podaci u svim okvirima koji putuju preko linka dobijaju ove bezbednosne usluge linka.

2.3.9.1. Bezbedna elektronska pošta

Projekat stvaranja sistema za bezbednost elektronske pošte je projekat visokog nivoa koji stvaramo na postupan način, tako što u svakoj fazi uvodimo nove usluge bezbednosti. Bezbednosne karakteristike koje su najpoželjnije :

- Poverljivost
- Autentifikacija pošiljaoca
- Autentifikacija primaoca
- Integritet poruke

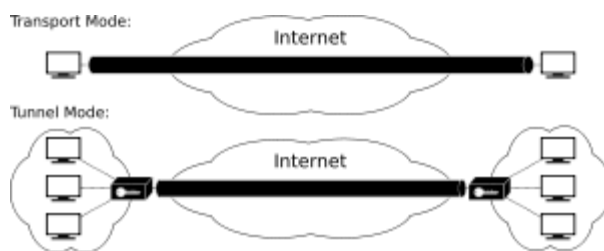
2.3.9.2. PGP (Pretty Good Privacy)

Pretty Good Privacy (PGP), koji je prvobitno napisao Fil Cimerman 1991. Godine, postao je *de facto* standardna šema za šifrovanje elektronske pošte. Njegova veb lokacija pruža više od milion stranica mesečno korisnicima u 166 različitih zemalja. Verzije PGP-a raspoložive su u javnom domenu (npr. PGP softver za vašu omiljenu platformu kao i mnogo zanimljivih tekstova za čitanje, mozete da pronađete na lokaciji International PGP Home Page). PGP se takođe može komercijalno nabaviti, a na raspolaganju je i kao dodatak agente korisnika elektronske pošte, uključujući Microsoftove Exchange i Outlook.

2.3.10. Obezbeđivanje tcp konekcija : SSL

SSL(Secure Sockets Layer) je sloj bezbednih soketa. Prvobitno je nastao u **Netscapeu**. Od samog početka, SSL je bio široko prihvaćen. SSL podržavaju svi popularni čitači veba i veb serveri, a koristi se praktično na svim komercijalnim lokacijama na internetu. SSL rešava probleme tako što unapređuje TCP uvođenjem poverljivosti, integriteta podataka, autentifikacije servera i autentifikacije klijenta. Međutim, pošto SSL obezbeđuje TCP, može ga koristiti svaka aplikacija koja se izvršava preko TCP-a. SSL nudi jednostavan API (Application Programmer Interface) sa sokaletima sličan i analogan API-ju koji nudi TCP.

2.3.11. Bezbednost mrežnog sloja : IPSec



Sl. 5 – IPSec-modes

IPSec (engl. *Protokol IP security*) jeste niz protokola koji pružaju bezbednost na mrežnom sloju. **IPSec** se nalazi u jezgri većine virtuelnih privatnih mreža. IPSec je vrlo složen. Mrežni sloj bi obezbedio poverljivost, ako bi svi podaci koje nose svi IP datagrami bili šifrovani. To znači da kad god neki računar želi da pošalje datagram, on bi šifrovao korisne podatke datagrama pre nego što ga isporuči mreži. Dva glavna protokola IPsec-a su :

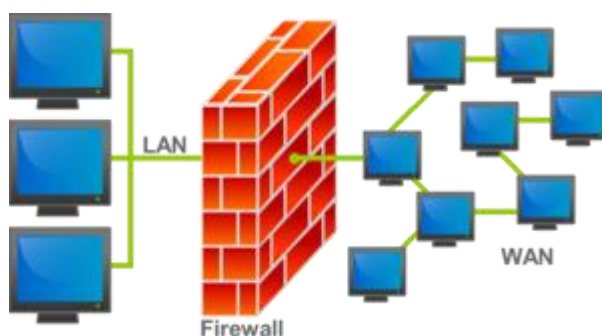
- **Protokol za autentifikaciju zaglavlja** (engl. *Authentication Header, AH*)
- **Protokol za bezbednosnu enkapsulaciju tereta** (engl. *Encapsulation Security Payload Protocol, ESP*)

Protokol za autentifikaciju zaglavlja, **AH**, obezbeđuje autentifikaciju izvornog računara i integritet podataka, ali ne i njihovu poverljivost. Protokol za bezbednosnu enkapsulaciju tereta, **ESP**, obezbeđuje poverljivost na mrežnom sloju, kao i autentifikaciju izvornog računara i integritet podataka.

2.3.12. Obezbeđivanje bežičnih LAN-ova

Bezbednost je posebno značajna u bežičnim mrežama, gde radio talasi koji nose okvire mogu da se prostiru daleko van zgrade u kojoj se nalaze osnovne bežične stanice i računari. Jedan od bezbednosnih mehanizama koji je u početku specifikaciji 802.11 je privatnost ekvivalentna ožičenju (*WEP*). Protokol *IEEE 802.11 WEP* obezbeđuje autentifikaciju i šifrovanje podataka između računara i bežične pristupne tačke, koristeći pristup simetričnog zajedničkog ključa. *WEP* ne određuje algoritam za upravljanje ključevima, pa se podrazumeva da su se računar i bežična pristupna tačka nekako sporazumeli o ključu, nekom metodom van opsega.

2.3.13. Operaciona bezbednost : mrežne barijere i sistemi za otkrivanje uljeza



Sl. 6 – Zaštitni zid

Mrežna barijera (*firewall*) jeste kombinacija hardvera i softvera koja izoluje unutrašnju mrežu organizacije od interneta, dozvoljavajući nekim paketima da prođu i blokirajući ostale. Mrežna barijera omogućava administratoru mreže da kontroliše pristup između spoljašnjeg sveta i resursa unutar *administrirane mreže*, tako što će upravljati tokom saobraćaja ka tim resursima i od njih.

Postoje tri vrste mrežnih barijera :

- Mrežne barijere sa običnim filtriranjem paketa
- Mrežne barijere sa stanjem filtera
- Mrežni prolazi aplikacionog nivoa

Sistem za otklanjanje uljeza (engl. *IDS, Intrusion Detection System*) je uređaj koji generiše upozorenja kada primeti potencijalno zlonamerni saobraćaj. **IDS** može da se koristi za otkrivanje široke lepeze napada, uključujući preslikavanje mreže, skeniranje portova, skeniranje *TCP steka*, *DoS* napade preplavlivanjem propusnog opsega, crve i viruse, napade na slabe tačke operativnog sistema i napade na slabe tačke aplikacija.

2.3.14. Zaštita od nestanka napajanja i neadekvatnog napajanja iz javne distributivne mreže

Napajanje aktivne telekomunikacione i računarske opreme u računarskoj mreži najčešće se obezbeđuje iz javne niskonaponske distributivne mreže 220 V, 50 Hz. U vezi s tim funkcionisanje računarske mreže može biti ugroženo:

- potpunim nestankom napona napajanja, kratkotrajnim i dugotrajnim prekidima u napajanju;
- pojavama prenapona i podnapona u slučaju kada napon napajanja varira izvan opsega zahtevanog za napajanje aktivne elektronske opreme;
- brzim električnim tranzijentima koji se javljaju u distributivnoj mreži;
- dejstvom jakih elektromagnetnih pražnjenja;

- delovanjem jakog elektromagnetnog polja.

Problemi u napajanju električnom energijom mogu se obezbediti upotrebom uređaja za neprekidno napajanje (UPS) koji moraju obezbediti planiranu autonomiju i imati potrebnu snagu za napajanje aktivne opreme računarske mreže. Da bi se mreža obezbedila od dugotrajnih prekida napajanja iz javne niskonaponske mreže, potrebno je obezbediti pomoćni izvor napajanja (agregat).

2.4. PROJEKTOVANJE ZAŠTITE RAČUNARSKE MREŽE

Problem zaštite mreža u praksi je prisutan pri projektovanju računarske mreže. Glavni, odnosno izvođački projekat računarske mreže, obavezno treba da sadrži tehničko rešenje za njenu zaštitu. Investitor, odnosno korisnik buduće mreže, u projektnom zadatku i tehničkim zahtevima, koji prethode izradi projekta, definiše projektante zahteve za zaštitu, kao i nivo kvaliteta zaštite mreže i informacija koje će se preko nje prenositi. Najteži zadatak je definisanje tehničkih zahteva za zaštitu, jer se oni moraju zasnivati na proceni (analiza, studija pretnji) realno mogućih pretnji i oblika napada na mrežu i informacije. Kvalitet tehničkog rešenja predloženog u projektu mreže treba da bude verifikovan u procesu revizije projekta mreže.

Pod verifikacijom se podrazumeva simulacija predloženog rešenja, uključujući simulaciju pretpostavljenih pretnji i oblika napada na mrežu i informacije. Tek nakon ovakve provere može se ići u realizaciju projekta mreže. Primer tehničkog rešenja zaštite jedne lokalne računarske mreže prikazan je u tabeli 2.

Gotovo svakodnevno pojavljuju se mnogi novi oblici pretnji. Za takve pretnje u relativno kratkom periodu nalazi se efikasna zaštita, obično primenom određenih softverski rešenja, tako da se relativno jednostavno mogu implementirati na postojeće mreže, odnosno umrežene računare. Ceo proces neprekidno se odvija, pretnje postaju sve ozbiljnije, a zaštita mreža sve teža i složenija. Problemi zaštite mreža i informacija posebno su izraženi u projektovanju i realizaciji multimedijalnih telekomunikacionih mreža.

Tabela 2: Primer tehničkog rešenja zaštite jedne LAN mreže

Red. broj	Pretnja mreži i informacijama	Zaštitna mera	Tehničko rešenje zaštite	Efikasnost zaštite
1.	Neovlašćeni pristup radnoj stanici ili računaru	Identifikacija osoba kontrolom pristupa proverom otiska prsta	Korišćenje uređaja za identifikaciju korisnika na bazi biometrijskih parametara (otisak prsta ili mrežnjače oka)	Izuzetno sigurna i pouzdana zaštita
2.	Nedozvoljeno korišćenje programa i pristup datotekama	Autorizacija prava korisnika proverom sadržaja inteligentne kartice	Korišćenje lozinke koja se unosi preko uređaja za identifikaciju korisnika sa inteligentnom karticom	Efikasna zaštita
3.	Neovlašćeni pristup centralnom komutatoru, serverima i dr.	Identifikacija osoba, kontrolom pristupa proverom otiska prsta; autorizacija prava inteligentnom karticom	Korišćenje specijalne brave na vratima prostorije ili na ulazu u objekat, koja se otvara identifikacijom otiska prsta ili retine oka korisnika	Izuzetno sigurna i pouzdana zaštita
4.	Ugrožavanje tajnosti podataka (informacija) elektronskim prisluškivanjem	Onemogućeno je prisluškivanje signala pri prenosu u mreži preko kablovske instalacije	Mrežna instalacija izvedena optičkim kablovima i bakarnim paricama, postavljena je u kanale pod zemljom. Nema zračenja signala	Signali pri prenosu nisu dostupni, a time ni informacija koju oni nose
5.	Narušavanje autentičnosti podataka (informacija)	Nedostupnost paketa koji bi se mogli „zameniti“ drugim paketom, tj. informacionim sadržajem	Nema memorisanja paketa u prenosu od izvora do odredišta	Sprečeno je narušavanje autentičnosti informacija
6.	Presretanje i promena integriteta poruke (podataka)	Pri prenosu komutatori ne memorišu pakete, pa je tehnički neizvodljivo presretanje	Ugradnja komutatora preko kojih se povezuju segmenti mreže	Sprečeno je presretanje poruka
7.	Mogućnost zabrane pristupa Internetu i pristupi mreži iz WAN mreža	LAN računarska mreža se uopšte ne povezuje sa Internetom	Za komunikaciju sa Internetom koristi se potpuno odvojena druga mreža	Mreža je potpuno zaštićena
8.	Ugrožavanje reemitovanjem paketa podataka iz drugih mreža	Nema komunikacije sa drugim WAN, odnosno LAN mrežama	Za komunikaciju sa drugim mrežama koristi se druga mreža	Mreža je potpuno zaštićena
9.	Zabrana neograničenog pristupa i prava korisnika iz drugih mreža	Nema komunikacije sa drugim WAN, odnosno LAN mrežama	Za komunikaciju sa drugim mrežama koristi se druga mreža	Mreža je potpuno zaštićena
10.	Naglo povećanje obima saobraćaja u mreži	Kontrola saobraćaja preko programa za nadzor i upravljanje mrežom	Operativni sistem sa programom SNMP i „monitorom referenci“	Permanently se kontrolišu tokovi saobraćaja

3. BEZBEDNO RUKOVANJE KRIPTOLOŠKIM KLJUČEVIMA

3.1. UPRAVLJANE KRIPTOLOŠKIM KLJUČEVIMA

Upravljanje kriptološkim ključevima se bavi sigurnim generisanjem, distribucijom i čuvanjem ključeva. Jedan od uslova za uspešnu primenu bezbednosnog modela predstavlja i njegova jednostavnost upotrebe. Osnovni zadatak dobro projektovanog rešenja jeste da krajnji korisnici u radu što manje osećaju prisustvo kriptografskog sistema. To podrazumijeva jednostavnost posla koji obavljaju, statičnost postojećih funkcija i minimum vremenskog perioda potrebnog za obavljanje konkretnog poslovnog zadatka. Model implementacije bezbednosnog rešenja komunikacionog kanala obezbeđuje odličan metod za zaštitu osetljivih podataka koji se prenose od predajne do prijemne strane. Usloznavanjem modela dovodi se do pada nivoa performansi kao i otežavanjem konkretne upotrebe predloženog sigurnosnog rešenja.

Sigurnost metoda upravljanja ključevima je od ekstremnog značaja. Kada je ključ jednom generisan on mora ostati tajan da bi se izbegle situacije kao što je impersonalizacija.

Kada je riječ o infrastrukturi sa javnim ključevima, u praksi se najviše napada dešava na nivou upravljanja ključevima, a vrlo retko napadi na same algoritme. Učesnici u PKI sistemima moraju biti sposobni da od treće strane od poverenja dobiju sertifikate koji im služe za generisanje ključeva. Takođe, moraju imati mogućnost da publikuju svoj javni ključ i da im budu dostupni javni ključevi ostalih korisnika u sistemu, za šta koriste sertifikate.

Ukoliko dođe do kompromitacije ili gubitka nečijeg privatnog ključa ostali učesnici moraju biti upozoreni. Korisnicima mora biti omogućeno da na siguran način čuvaju svoje ključeve i učine ih nedostupnim osim za legitimnu upotrebu. Napomenimo da ključeve možemo podeliti na: simetrične, javne i privatne ključeve. Simetrični i privatni ključevi su po svojoj prirodi tajni ključevi.

3.2. GENERISANJE KRIPTOLOŠKIH KLJUČEVA

U kriptologiji, velika pažnja se poklanja izboru samog generatora, odnosno, njegovim osobinama i potencijalnim slabostima koje se mogu upotrebiti pri kriptanalizi. Uz pomoć statističkih testova za određivanje osobine generisanog niza može se zaključiti da nijedan generator ne poseduje sigurno zadovoljavajuće parametre. Pošto ne postoji univerzalna kolekcija testova čiji prolaz garantuje da je dati generator potpuno pouzdan, generatori pseudoslučajnih brojeva se konstruišu na osnovu ozbiljne matematičke analize njihovih strukturalnih osobina.

Upotrebom pseudoslučajnih brojeva ne postiže se dovoljan nivo sigurnosti. Period generatora mora biti veoma velik. Ulaz u generator mora biti tako odabran da ga je praktično nemoguće otkriti nekom metodom pogađanja. Ovim se omogućava generisanje vrlo velikog broja niza slučajnih brojeva koje je nemoguće analizirati u realnom vremenu. Ovako dobijeni nizovi se mogu upotrebiti kao kriptološki ključevi. Ovakvi generatori slučajnih brojeva kod kojih je uz poznavanje algoritma i nepoznavanje početnih uslova nemoguće predvideti niz generisanih brojeva zovu se generatori kriptografskih sigurnih pseudoslučajnih brojeva. Algoritmi ovakvih generatora su veoma složeni ali i veoma spori. Ovo ne predstavlja problem za primenu u kriptografiji jer se ovakvi generatori ne koriste za generisanje velike količine slučajnih brojeva.

3.2.1. Pseudoslučajno generisanje bita PRBG

Pseudoslučajni biti se mogu generisati tako što se prvo generiše slučajna početna vrednost s , a zatim jednosmernu funkciju (npr. SHA-1 ili DSA) primenjena na sekvence $s, s+1, s+2, \dots$ čime se dobije izlazna sekvenca $f(s), f(s+1), f(s+2), \dots$. Da bi se izbegle moguće korelacije zbog uzastopnih vrednosti, uzimamo samo neke bite iz sekvenci $f(s+i)$. Ovakav metod nije kriptografski siguran ali zadovoljava većinu primena. U ovom radu će biti nabrojani samo neki, a to su:

- *ANSI X9.17 generator* - koristi se za pseudoslučajno generisanje ključeva k i inicijalnih vektora IV koji se koriste u DES algoritmu. X9.17 koristi trostruko šifrovanje sa dva ključa na sledeći način gdje je: $E(x) = EK_1(DK_2(EK_1(x)))$.
- *FIPS 186 generator* - je generator pseudoslučajnih brojeva koji se koriste kao privatni ključevi u DSA algoritmu. Algoritam koristi slučajno generisanu početnu vrijednost s i jednosmjernu funkciju zasnovanu na SHA-1 ili DES algoritmu

3.2.2. Pseudoslučajno generisanje bita CSPRBG

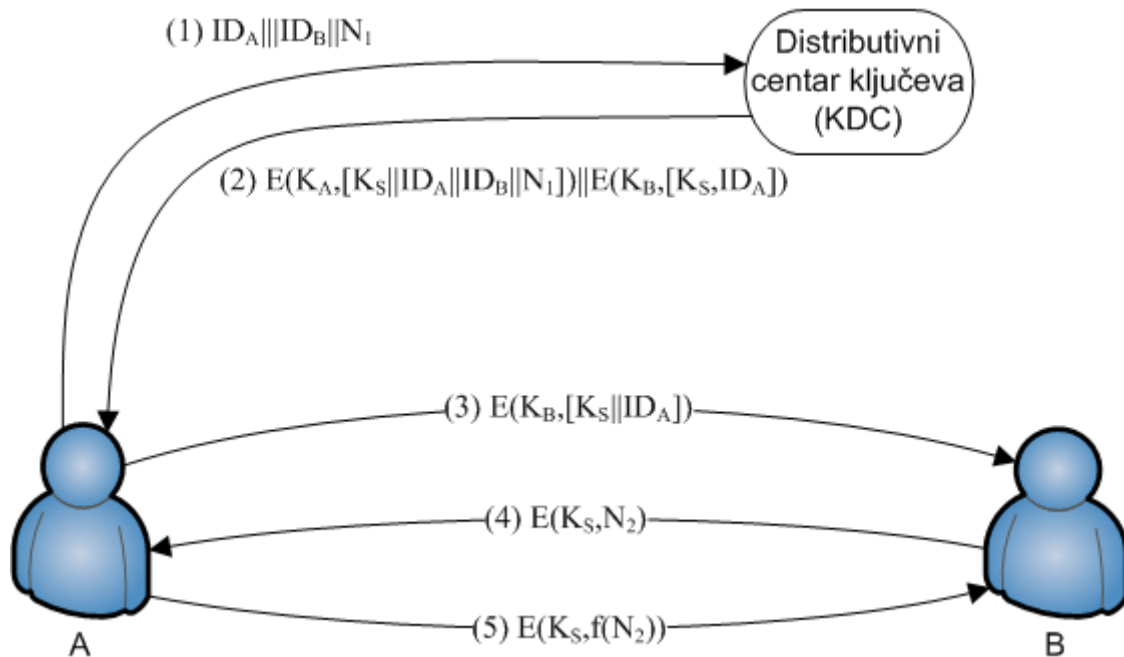
Zbog svog već pomenutog ograničenja generisanje pseudoslučajnih bita može biti od koristi ako se izvodi na uređaju koji već ima mogućnosti modularnog množenja, a neki od njih su:

- *RSA*,
- *Micali-Schnorr* ili
- *Blum Blum Shub generator*.

3.3. DISTRIBUCIJA KLJUČEVA U SIMETRIČNOJ KRIPTOGRAFIJI

Da bi simetrično šifrovanje i dešifrovanje sa druge strane funkcionisalo, obe strane moraju da poseduju isti ključ. Ovde se javlja problem distribucije ključeva. Da bi tajnost komunikacije između svaka dva korisnika u grupi od N korisnika bila zagarantovana, svaki učesnik mora da posjeduje $N-1$ ključ za komunikaciju sa ostalim korisnicima. To nas dovodi do ukupno $N(N-1)/2$ ključeva. Za grupu od npr. 1000 korisnika potrebno je približno 500000 ključeva, a svaki korisnik bi morao da posjeduje 999 ključeva. Ovakav sistem bi bio vrlo nepraktičan i težak za održavanje. Jedan od primera je distributivni centar koji podrazumijeva da svaka strana u komunikaciji deli jedinstveni ključ sa distributivim centrom.

A. Distributivni centar ključeva (Key Distribution Center - KDC)



sl. 7. Scenario distribucije ključeva

Pretpostavimo da A želi da komunicira sa B, ali nemaju zajednički ključ već samo imaju po jedan zajednički ključ sa distributivnim centrom. Komunikacija će se uspostaviti upravo posredstvom KDC distributivnog centra ključeva.

- Strana A generiše identifikator N_1 koji služi za jednokratnu upotrebu (može biti slučajna broj ili vremenska oznaka, a služi da bi sprečila maskiranje), i šalje ga zajedno sa svojim identifikatorom ID_A (npr. mrežna adresa od A) i identifikatorom ID_B , a sve to je šifrovano zajedničkim ključem korisnika A i KDC-a, K_A .
- KDC odgovara i šalje jednokratni ključ K_S , ID_A , ID_B , N_1 šifrovane ključem K_A i šalje podatke koje će A proslediti prema B a to su K_S , ID_A šifrovano ključem K_B . Sada i A i B poseduju sesijski ključ K_S , a B zna da je A inicirao komunikaciju.
- B šalje šifrovani identifikator N_2 šifrovan sesijskim ključem K_S i čeka odgovor od A, a to je $f(N_2)$ šifrovan sesijskim ključem K_S . Ovim se B obezbeđuje od mogućnosti falsifikovanja poruke u trećem koraku.

U daljnjem tekstu E predstavlja šifrovanje, a D dešifrovanje. Moguće je uspostaviti hijerarhiju KDC-ova pa korisnici iz različitih grupa mogu da komuniciraju tj. razmene sesijske ključeve. Da bi to bilo moguće KDC-ovi između sebe na prethodno opisan način ostvaruju komunikaciju i razmenjuju sesijske ključeve. Tokom komunikacije između dve strane poželjno je da se sesijski ključevi ne upotrebljavaju dugo i da se generišu novi.

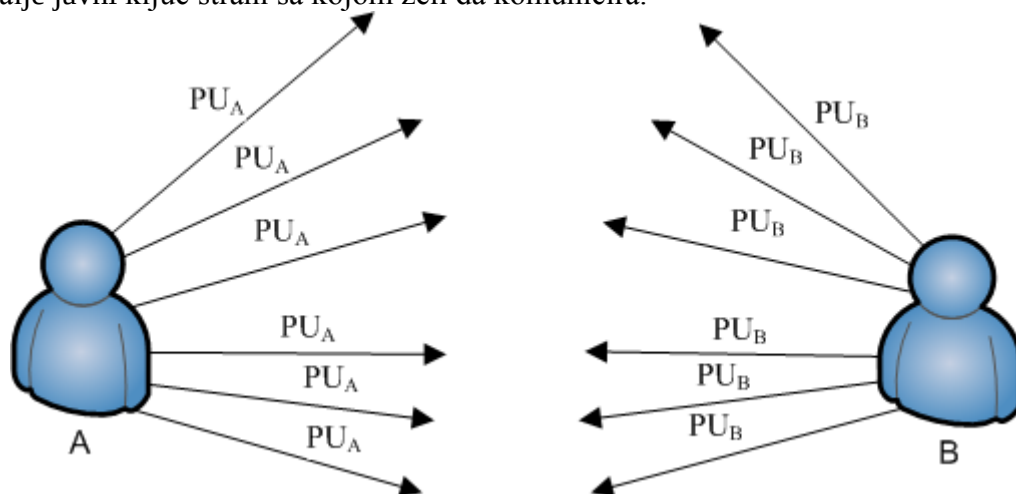
3.4. DISTRIBUCIJA JAVNIH KLJUČEVA U ASIMETRIČNOJ KRIPTOGRAFIJI

Postoji nekoliko tehnika za distribuciju javnih ključeva u asimetričnoj kriptografiji:

- javno objavljivanje
- javno dostupan direktorijum
- autoritet za javne ključeve
- sertifikati

3.4.1. Javno objavljivanje

Kao što im i samo ime govori javni ključevi trebaju biti javno dostupni-objavljeni, odnosno, svaki učesnik šalje javni ključ strani sa kojom želi da komunicira.



sl. 8. Nekontrolisana distribucija javnih ključeva

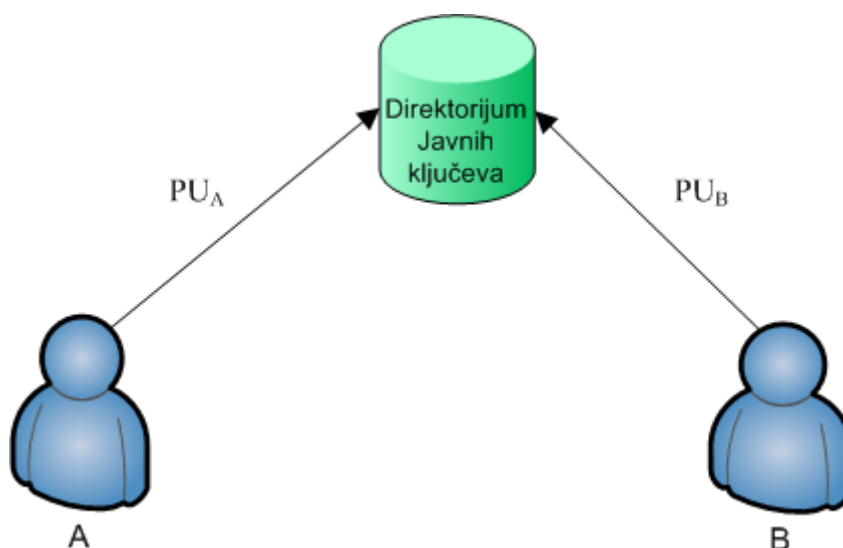
Dakle, ako postoji neki opšte prihvaćeni i široko rasprostranjeni asimetrični algoritam, kao što je RSA, dovoljno je da svaki učesnik pošalje javni ključ strani sa kojom želi da komunicira. Ovakav način razmjene ključeva je veoma jednostavan ali ima i nedostatke. Bilo ko može da se predstavi kao osoba A i pošalje svoj javni ključ, navodeći drugu stranu na pomisao da će šifrovane poruke razmjenjivati sa osobom A. Ovakav način razmjene ključeva ne obezbeđuje povezanost javnog ključa sa njegovim vlasnikom.

3.4.2. Javno dostupan direktorijum

Veći stepen sigurnosti u odnosu na javno objavljivanje postiže se korištenjem javno dostupnog direktorijuma. Održavanje i distribucija javnog direktorijuma je u nadležnosti nekog entiteta od poverenja ili neke organizacije.

Ovakva šema uključuje sledeće elemente:

- entitet održava direktorijum i unosi slogove sa sadržajem (ime, javni ključ) za svakog učesnika,
- svaki učesnik registruje javni ključ lično ili nekim sigurnim metodom autentifikacije,
- učesnik može zameniti javni ključ kada to odluči bilo da je razlog kompromitacija ili dugačak period upotrebe i
- učesnici mogu elektronskim putem pristupiti direktorijumu.

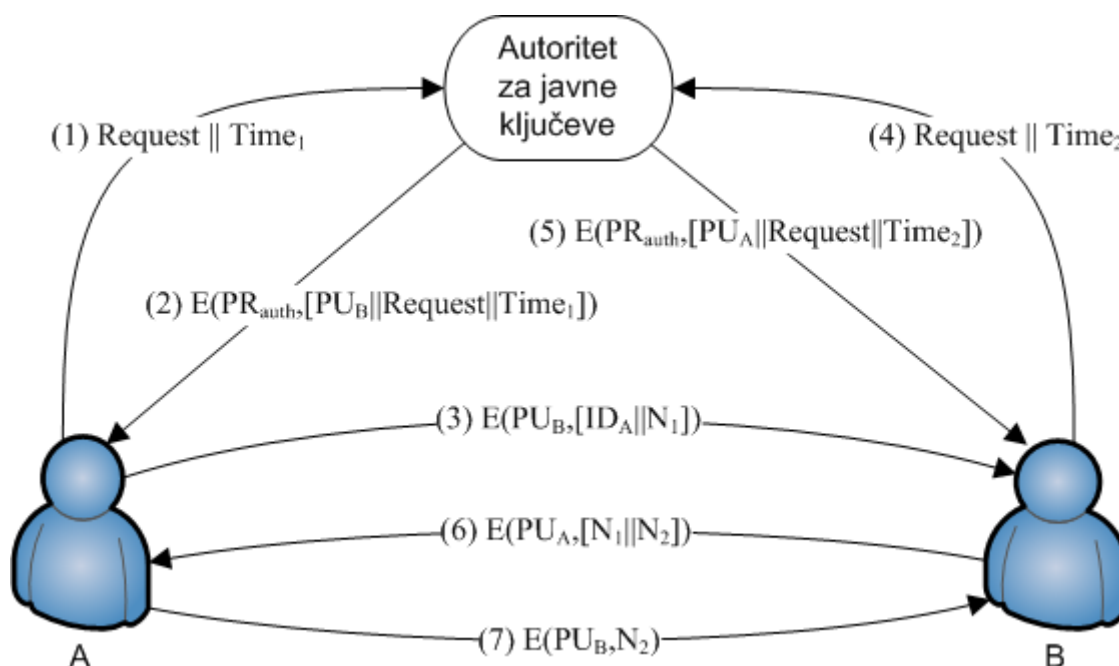


sl. 9. Publikovanje javnog ključa u direktorijum

Ovakav način distribucije je sigurniji od javnog objavljivanja, ali je još uvijek ranjiv. Nedostaci su što ako napadač uspe u nameri da pribavi ili rekonstruiše privatni ključ entiteta koji je u posedu direktorijuma, može doći do kompromitacije bilo kog učesnika u sistemu. Drugi problem koji se javlja je mogućnost krivotvorenja javnih ključeva u direktorijumu od strane napadača.

3.4.3. Autoritet za javne ključeve (Public-Key Authority)

Ovaj sistem je sličan prethodnom s tim što svaki učesnik poznaje javni ključ autoriteta, a privatni ključ autoriteta je dostupan isključivo njemu samom.



sl. 10. Scenario distribucije javnih ključeva

Razmena ključeva između dva učesnika se odvija na sledeći način:

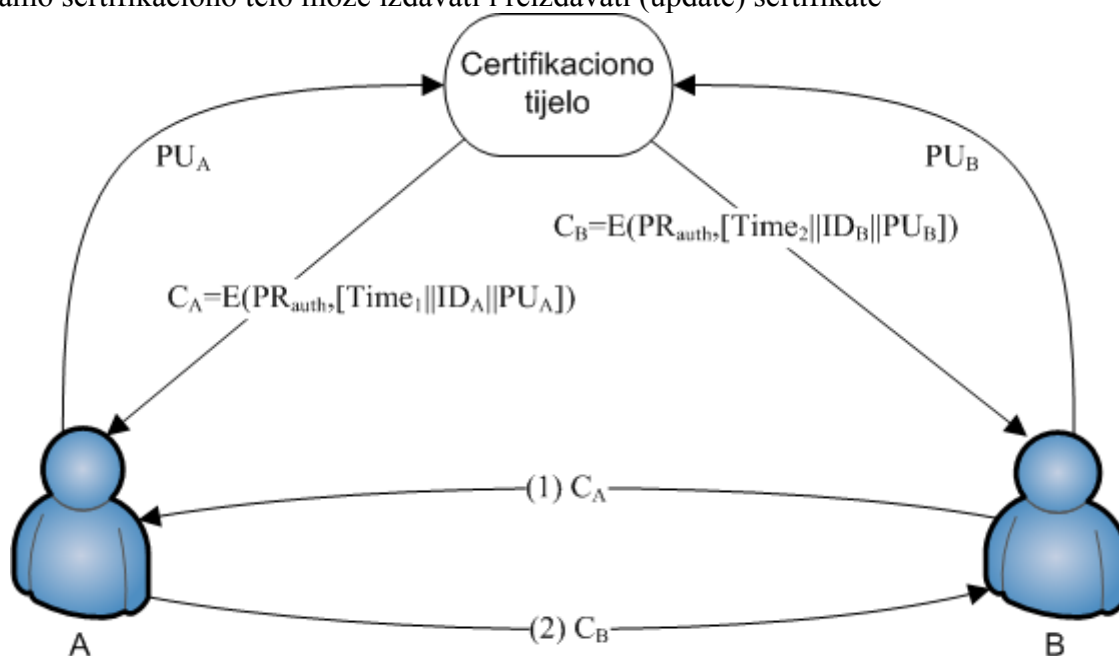
- A šalje vremenski označenu poruku autoritetu u kojoj se nalazi i zahtjev za javnim ključem od B
- autoritet odgovara šaljući javni ključ od B i originalan zahtjev, a sve je šifrovano privatnim ključem autoriteta PR_{auth}
- A šalje poruku prema B i šifrjuje je javnim ključem korisnika B PU_B , a u poruci se nalaze identitet učesnika A i jednokratna vrijednost N_1
- kao i u prvom koraku B šalje vremenski označenu poruku autoritetu u kojoj se nalazi i zahtjev za javnim ključem od A
- autoritet odgovara šaljući javni ključ od A PU_A
- B šalje poruku koja se sastoji od N_1 i N_2 , a šifrovana je upotrebom PU_A (N_2 je generisao B i samo njemu je poznata)
- A iz N_1 i N_2 uzvraća šaljući N_2 a šifrovano je upotrebom PU_B , pa je B siguran da je poruku primio baš od A

3.4.4. Sertifikati

Poboljšanje prethodnog metoda se postiže upotrebom sertifikata. Autoritet nekada može biti usko grlo u celom sistemu, jer se za svaki javni ključ mora podneti zahtev prema autoritetu. Alternativni pristup prethodnom rešenju je upotreba sertifikata. Korištenjem sertifikata nekom učesniku je moguće dostaviti vlastiti javni ključ na način kao da je to učinio autoritet. Sertifikat se sastoji od javnog ključa i identifikacije vlasnika tog ključa. Ovi podaci su potpisani od strane "treće strane", odnosno, sertifikacionog tela u koji svi učesnici u sistemu imaju poverenje. Korisnik na siguran način prezentuje svoj javni ključ autoritetu i nakon toga dobija sertifikat koji se može javno objaviti. Svako kome je potreban javni ključ ovog korisnika može preuzeti njegov sertifikat. Svi učesnici mogu proveriti da li je sertifikat kreiran od strane autoriteta.

Za ovakav način razmjene ključeva moraju biti ispunjeni sledeći zahtjevi:

- svaki učesnik može pročitati sertifikat da bi odredio javni ključ i ime vlasnika sertifikata
- svaki učesnik može utvrditi da je sertifikat izdat od strane sertifikacionog tela i da nije krivotvoren i
- samo sertifikaciono telo može izdavati i reizdavati (update) sertifikate



sl. 11. Razmena sertifikata

Izdavanje sertifikata započinje tako što svaki zainteresovani učesnik šalje svoj javni ključ i zahteva izdavanje sertifikata. Autentifikacija mora biti u ličnom kontaktu ili nekom drugim sigurnom metodom. Za nekog učesnika A autoritet izdaje sertifikat u obliku:

$$C_A = E(PR_{auth}, [T || ID_A || PU_A])$$

gdje su PR_{auth} privatni ključ autoriteta i T vremenska oznaka. A zatim može prosljediti sertifikat nekom drugom učesniku koji čita taj sertifikat i verifikuje sledeće:

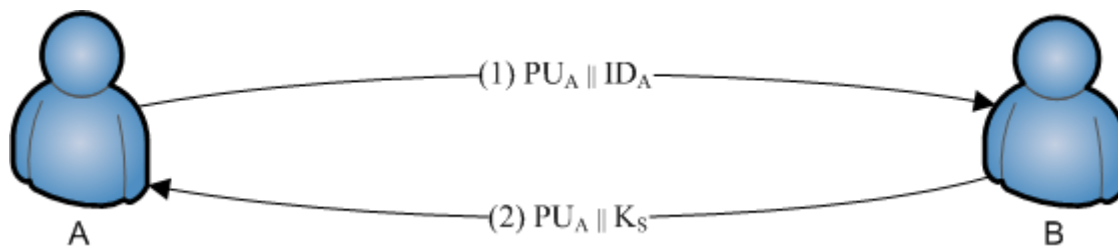
$$D(PU_{auth}, C_A) = D(PU_{auth}, E(PR_{auth}, [T || ID_A || PU_A])) = (T || ID_A || PU_A)$$

Sertifikat je moguće dešifrovati samo javnim ključem autoriteta, što garantuje da je baš taj autoritet izdao sertifikat. Ova šema je postala opšteprihvaćena i formalizovana je kroz standard X.509.

3.5. DISTRIBUCIJA TAJNIH KLJUČEVA KORIŠTENJEM KRIPTOGRAFIJE SA JAVNIM KLJUČEM

Kriptografija javnog ključa nije pogodna za razmenu poruka tj. šifrovanje i dešifrovanje veće količine podataka. Zato se pribegava tehnici razmene tajnih ključeva korištenjem kriptografije sa javnim ključevima.

3.5.1. Jednostavna distribucija tajnog ključa



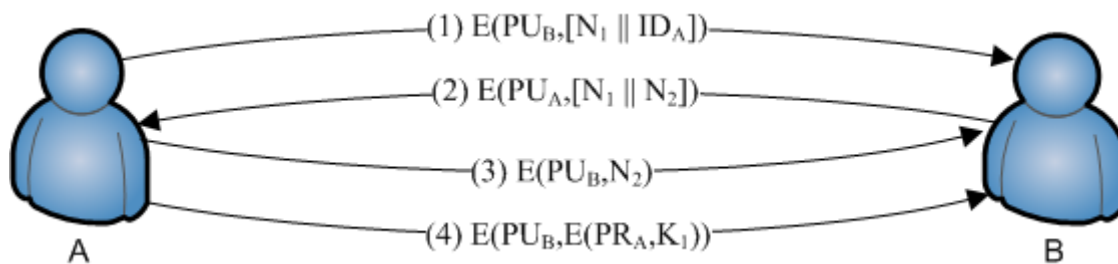
sl. 12. Jednostavna distribucija tajnog ključa

Distribucija se odvija na sledeći način:

- učesnik A generiše par ključeva $\{PU_A, PR_A\}$ i šalje poruku korisniku B koja se sastoji od PU_A i ID_A
- B generiše sesijski ključ K_S , šifrjuje ga javnim ključem PU_A i šalje ga učesniku A
- A dolazi do sesijskog ključa $K_S = D(PR_A, E(PU_A, K_S))$; sada samo A i B poznaju sesijski ključ K_S
- A uništava ključeve PU_A, PR_A , a B uništava ključ PU_A
- A i B mogu sigurno razmjenjivati šifrovane poruke upotrebom sesijskog ključa K_S
- po završetku komunikacije sesijski ključ se uništava

Ovakva razmena ključeva nije bezbedna zbog "man-in-the-middle" napada. Napadač C može da presretne prvi korak, generiše svoj par ključeva $\{PU_C, PR_C\}$ i komunikaciju A-B pretvori u A-C i C-B.

3.5.2. Distribucija tajnih ključeva sa poverljivošću i verodostojnošću



sl. 13. Distribucija tajnih ključeva sa poverljivošću i verodostojnošću

Distribucija se odvija na sledeći način:

- učesnik A koristi javni ključ učesnika B da bi poslao svoju identifikaciju ID_A i jednokratnu vrednost N_1
- učesnik B uzvraća i šalje poruku koja se sastoji od N_1 i N_2 , a šifrovana je sa PU_A
- A šalje poruku N_2 šifrovanu ključem PU_B
- sada su i A i B sigurni u identitet druge strane i A može generisati K_S i poslati ga učesniku B kao $M = E(PU_B, E(PR_A, K_S))$, a B do sesijskog ključa dolazi računajući $K_S = D(PU_A, D(PR_B, M))$

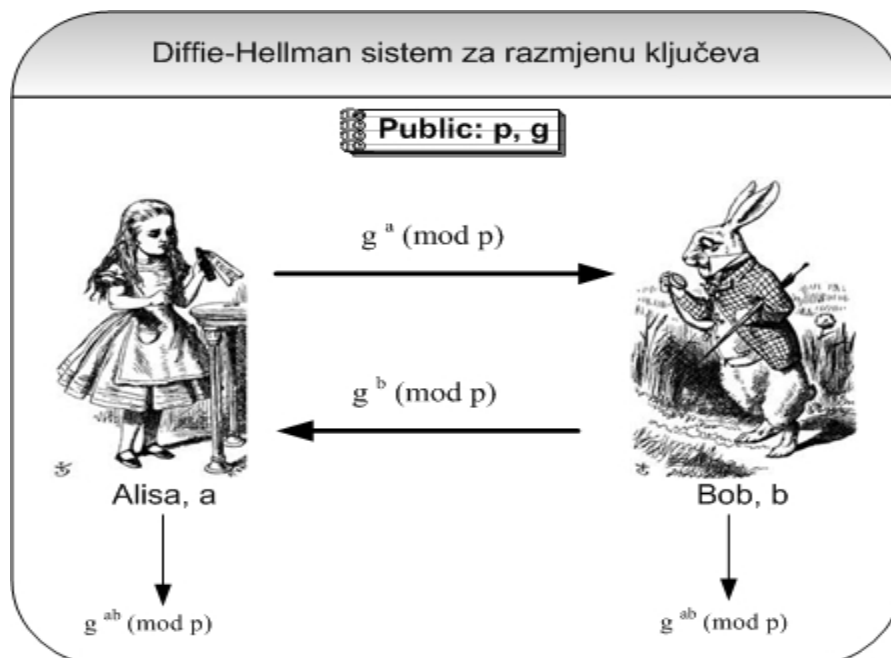
3.6. SISTEMI ZA RAZMENU KRIPTOLOŠKIH KLJUČEVA

U ovom radu analizirana su dva sistema za razmenu kriptoloških ključeva, a to su Diffie-Hellman i Arithmetika.

3.6.1. Diffie-Hellman algoritam za razmenu ključeva

U simetričnoj kriptografiji, obe strane koriste isti ključ za šifrovanje i dešifrovanje. Diffie-Hellman algoritam za razmenu ključeva omogućava bezbedno razmenjivanje ključeva između strana u komunikaciji preko javno dostupnog kanala. Diffie-Hellman algoritam se zasniva na činjenici da je teško izračunati broj α^{ab} ukoliko su poznati brojevi α^a i α^b . Postupak razmene ključeva se odvija na sledeći način:

- dva korisnika izaberu slučajan broj α
- korisnik A izabere slučajan broj a i izračuna α^a i pošalje ga korisniku B
- korisnik B izabere slučajan broj b i izračuna α^b i pošalje ga korisniku A
- zajednički tajni element je α^{ab} koji korisnik A dobije kao $(\alpha^b)^a$, a korisnik B izračunavanjem $(\alpha^a)^b$.



Slika 14. Diffie-Hellman sistem za razmjenu kriptoloških ključeva.

Ovaj algoritam nije otporan na "man-in-the-middle" napad. Napadač, Ted, može da presretne α^a i umjesto toga Bobu pošalje α^b i presretne α^b i umjesto toga Alisi pošalje α^a . Sada Ted i Alisa imaju zajednički element α^{ab} , a Ted i Bob zajednički element α^{ab} . Pošto Ted i dalje presreće komunikaciju, Alisa je uvjerena da komunicira sa Bobom, ali komunicira sa Tedom. I Bob je uvjeren da komunicira sa Alisom, ali komunicira sa Tedom.

Rešenja za ovaj problem mogu biti:

- šifrovanje DH razmene simetričnim ključem,
- šifrovanje DH razmjene javnim ključem,
- digitalno potpisivanje DH vrednosti privatnim ključem.

3.6.2. Arithmetika algoritam za razmjenu ključeva

Arithmetika je relativno nov sistem za razmenu kriptografskih ključeva. Njegov princip rada je drugačiji u odnosu na Diffie-Hellman algoritam za razmjenu ključeva. Arithmetika koristi složene matematičke formule. U Arithmetika sistemu za razmenu ključeva određena vrednost G sadrži sve varijacije ove vrednosti, kao što je prikazano:

$$\{1G, a, b, a-1, b-1\}$$

Tipični element G sadrži: $abaab-1b-1, bba-1 a1Gba, bbb, aba-1b-1, a, b-1, 1G$

Jedan od primera bi bila pretpostavka da Alisa i Bob žele koristiti simetrične ključeve. Prvi korak je da naprave podgrupu svojih javnih ključeva iz grupe javnih ključeva G , tako da vredi:

$$SA=(s_0, s_1, \dots, s_{n-1}) \text{ i } SB=(t_0, t_1, \dots, t_{m-1})$$

.

.

Alisa izračunava:

$$a-1(b-1ab)=(y-1)-1(x_2y)=yx_2y=x_2.$$

Slično tome Bob izračunava:

$$a-1ba = (yxy)^3=yxy*yxy*yxy = yxy_2xy_2xy=yx*1G*x*1G*xy = yx_3y=x.$$

U poslednjem koraku, Bob izračunava vrijednost od $a-1b-1a=(a-1b)-1=x-1$, koje koristi za dobijanje zajedničke tajne $(a-1b-1a) b=x-1*x3=x2$. Ostalo je još da Alisa i Bob izračunavaju zajednički simetrični ključ koji je baziran na zajedničkoj tajni.

3.7. EVIDENCIJA KRIPTOLŠKIH KLJUČEVA

Dobra organizacija zaštite informacionih sistema zasniva se na dobrom upravljanju zaštitom (Security management). Upravljanje ili menadžment predstavlja proces u kome se dolazi do nekog cilja korišćenjem određenog skupa resursa. Da bi proces informatičke bezbednosti postao efikasniji, neophodno je da se dobro razumeju osnovni principi upravljanja. Rukovodilac ili menadžer je neko ko radi sa ili preko drugih zaposlenih u organizaciji koordinirajući njihove radne aktivnosti u cilju postizanja što boljih rezultata organizacije. On ima mnoštvo uloga u organizaciji uključujući i sledeće:

- Uloga informisanja podrazumeva prikupljanje, obradu i korišćenje informacija koje mogu da ugroze ispunjenje planiranog cilja
- Interpersonalna uloga podrazumeva interakciju sa nadređenima, potčinjenima, spoljnim saradnicima i drugim činiocima koji su uključeni u izvršenje nekog zadatka
- Uloga u odlučivanju podrazumeva odabir između alternativnih pristupa, kao i razrešavanje konflikata, dilema ili izazova

Organizacija zaštite koja se kao što je rečeno zasniva na kvalitetnom upravljanju zaštitom podrazumeva neke od sledećih aktivnosti:

- Definisanje procesa zaštite
- Definisanje politika, standarda procedura i uputstava Upravljanje rizicima
- Kontrole
- Tehnologije
- Dokumentaciju
- IT kulturu
- Edukaciju

Zbog činjenice da je upravljanje zaštitom opterećeno preuzimanjem odgovornosti za specijalizovane programe određeni aspekti ove vrste menadžmenta imaju svoje osobenosti. Glavne karakteristike po kojima se odlikuje informatička bezbednost su poznate kao šest „P“.

- **Planiranje (Planning)** - Aktivnosti koje su uključene u model planiranja informatičke bezbednosti neophodne su da bi se obezbedio dizajn, kreiranje i implementacija strategije informatičke bezbednosti kao deo planiranja celokupnog informacionog sistema.
- **Polise (Policy)** - Skup organizacionih uputstava koja zahtevaju odgovorno ponašanje zaposlenih u nekoj organizaciji nazivaju se polise. U informatičkoj bezbednosti postoje tri kategorije polisa: generalne polise (polise na nivou preduzeća), polise koje se odnose na specifična problem i polise koje se odnose na specifične sisteme
- **Programi (Programs)** - Programi podrazumevaju definisanje naziva i opis radnih mesta zaposlenih koji se bave poslovima zaštite u nekoj organizaciji
- **Zaštita (Protection)** - Funkcije zaštite se odvijaju kroz dva odvojena procesa □ □ Risk menadžment koji uključuje procenu i kontrolu rizika i □ Mehanizme za zaštitu, tehnologije i alate
- **Ljudi (People)** – Podrazumeva obučeno ljudstvo. Postoje razni sertifikati koji se dobijaju u oblasti zaštite
- **Upravljanje projektom (Project Management)** - Ovaj proces podrazumeva identifikovanje i kontrolisanje sredstava koja se primenjuju na projektu, kao i merenje napretka projekta i prilagođavanje procesa kako bi se ostvario napredak u ispunjavanju cilja

Ovaj rad detaljno ne razmatra upravljanje zaštitom informacionionog sistema u celini. Dobro upravljanje zaštitom informacionionog sistema, podrazumeva i evidenciju kriptoloških ključeva (specijalnih dokumenata kriptozastite), koja su upotrebljena ili su u upotrebi.

Mogući obrazac za evidenciju kriptoloških ključeva predstavljen je na slici 15:

Редни број	ДОКУМЕНТ (Шифарски кључ)			ПРИМЉЕНО				ДОСТАВЉЕНО				Вратили примаоци	УНИШТЕНО		ВРАЋЕНО ПОШИЉАОЦУ		Примедба
	Врста	Број	Разрађен према организационој јединици	Од кога	Примерака	По спроводном документу	Потврда пријема	Коме	Евиденциони број	По спроводном документу	Потврда пријема		Датум	Потпис лица која су извршила уништење	По спроводном документу	Потврда пријема	

Slika 15. Sveska evidencije specijalnih dokumenata kriptozastite

4. ZAKLJUČAK

U ovom radu su prikazane osnovne karakteristike višeslojnog sistema zaštite savremenih računarskih mreža. Potencijalni napadi na mreže su širokog dijapazona. Razmatrani su mehanizmi zaštite na aplikativnom, transportnom i mrežnom nivou, a istaknut je i značaj kombinovane softversko-hardverske realizacije mehanizama zaštite. Na osnovu iznetog, može se zaključiti da je za realizaciju pouzdanog sistema zaštite date računarske mreže potrebno primeniti kombinovani višenivoski sistem zaštite, sa softverskim i hardverskim komponentama, koji se bazira na primeni asimetričnih i simetričnih šifarskih sistema, digitalnim certifikatima koje izdaje odgovarajuće certifikaciono telo i smart karticama za generisanje digitalnog potpisa i za bezbedno čuvanje kriptografskih ključeva.

Postojeće i buduće računarske mreže mogu biti izložene čitavom skupu raznovrsnih pretnji i oblika napada. Samo za poznate oblike pretnji ili napada na mrežu može se obezbediti efikasna zaštita računarske mreže i informacija koje se preko nje prenose. Pretnje se moraju unapred proceniti u projektnim zahtevima, odnosno u projektnom zadatku. Na osnovu toga u projektu mreže definiše se tehničko rešenje (softver, hardver) zaštite mreže i informacija.

Bezbednosno upravljanje kriptološkim ključevima je jedan od ključnih postupaka u kriptologiji. Nakon što se ključevi generišu, počinje njihov životni vijek. Posebno mesto u upravljanju ključevima ima distribucija ključeva.

Za simetrično šifrovanje i dešifrovanje predložen je "model distributivnih centara ključeva". Za veće mreže, umjesto jednog centra moguće je koristiti više distributivnih centara u hijerarhiji tako da svaki opslužuje manje domene ili mreže. Predložena metoda je centralizovanog karaktera.

U nastavku ovog rada razmotrena su dva osnovna aspekta kriptografije javnog ključa: distribucija javnih ključeva i upotreba kriptografije javnog ključa za distribuciju tajnih ključeva.

Najbolji rezultati u distribuciji sesijskih ključeva postižu se upotrebom hibridnog-troslojnog modela tj. upotrebom distributivnih centara ključeva koji sa svakim korisnikom dijele zajednički tajni master-ključ koji se upotrebljava za distribuciju sesijskih ključeva, i upotrebom asimetrične kriptografije za distribuciju zajedničkih master-ključeva. Na ovaj način se izbjegava degradacija performansi u sistemima u kojima se često mijenja sesijski ključ, a koja nastaje usljed činjenice da je šifrovanje/dešifrovanje sesijskog ključa asimetričnim alogiritmima sporo. Ovim se postiže da se spore operacije kao što su asimetrično šifrovanje sesijskog ključa zamijene sa dvije: simetričnim šifrovanjem sesijskog ključa upotrebom master-ključa i asimetričnim šifrovanjem master-ključa. Prva može biti i veoma frekventna ali je istovremeno i brza, a druga je spora ali i veoma rijetka.

Za distribuciju tajnih, privatnih i javnih ključeva treba primjenjivati novije metode, a posebno one kod kojih su uočeni nedostaci otklonjeni. Samo u tom slučaju korisnicima sistema kriptološke zaštite mogu se garantovati:

- autentičnost pošiljaoca poruke,
- zaštita integriteta podataka u poruci,
- neporecivost slanja poruke i tajnost.

Ako su osnovni kriterijumi za generisanje kriptografskih ključeva brzina, komercijala i sl. što nameće manji nivo sigurnosti, treba koristiti pseudoslučajne generatore.

Literatura:

- [1] Profesor dr Miloško Jevtović, Vojnotehnički glasnik 5/2005
- [2] http://sr.wikipedia.org/sr/Zaštita_racunarskih_mreza
- [3] http://www.znanje.org/abc/tutorials/operatingsystems/01/30_zastita_operativnih_sistema.htm
- [4] <http://www.scribd.com/nik0la/d/18284213/13-Zastita-radnih-stanica-i-servera>
- [5] http://issuu.com/jkp_put_ns/docs/zastita_podataka_u_mrezama
- [6] B.Schneier, *Applied Cryptography*, John Wiley & Sons, Inc., 1996.
- [7] R.Oppliger, *Internet and Intranet Security*, Artech House, 1998, ISBN 0-89006-829.
- [8] R.Oppliger, *Security Technologies for the World Wide Web*, Artech House, 2000, ISBN 1-58053-045-1.
- [9] W.Ford, M.S.Baum, *Secure Electronic Commerce*, Prentice Hall PTR, 2001.
- [10] S.Bosworth, M.E.Kabay, *Computer Security Handbook*, John Wiley & Sons, Inc., 2002.
- [11] E.Persson, "Digital Identity Service in Sweden," in Proc. of Information Security Solution Europe Conference, ISSE 2002, Paris, October 2-4, 2002.
- [12] T.Denny, "Secure Transactions over Open Networks," in Proc. of Information Security Solution Europe Conference, ISSE 2002, Paris, October 2-4, 2002.
- [13] P.VanEecke, "Legal status of non-qualified, qualified and enhanced electronic signatures in the Member States," EEMA Workshop "The Legal Impact of the Electronic Signature Directive on Business", November 29/30, 2001, Brussels, Belgium.
- [14] P.VanEecke, "The European Legal Framework on Electronic Signatures," in Proc. of Information Security Solution Europe Conference, ISSE 2002, Paris, October 2-4, 2002.
- [15] J.Dumortier, "The implementation of e-Signature Directive in the Member States," EEMA Workshop "Putting e-Signatures into Practice," November 25/26, 2002, Brussels, Belgium.
- [16] S.Upton, "Presentation of a voluntary accreditation scheme for certification service providers," EEMA Workshop "Putting e-Signatures into Practice," November 25/26, 2002, Brussels, Belgium.
- [17] C.Luyten, "A legally recognized platform for electronic invoicing," EEMA Workshop "Putting e-Signatures into Practice," November 25/26, 2002, Brussels, Belgium.
- [18] J.M.Eymeri, "The Electronic Identification of Citizens and Organizations in the European Union: State of Affairs," 37th Meeting of the Director-General of the Public Service of the Member States of the European Union, November 26/27, 2001, Bruges, Belgium.
- [19] B.Goetz, A.Kraft, "eGovernment – two success stories for G2E & G2C in Germany," in Proc. of Information Security Solution Europe Conference, ISSE 2002, Paris, October 2-4, 2002.
- [20] S.Klein, "Using electronic signatures for e-government services – the experiences of the city of Bremen," EEMA Workshop "Putting e-Signatures into Practice," November 25/26, 2002, Brussels, Belgium.
- [21] F.Wynants, "The Co-Sourced PKI Solution – the Belgian e-ID Project," EEMA Workshop "PKI – Making it Work," May 6/7, 2003, Stockholm, Sweden.

- [22] S.Kent, "A System Level Analyst of Biometric User Authentication," in Proc. of Information Security Solution Europe Conference, ISSE 2002, Paris, October 2-4, 2002.
- [23] R.Muller, "Biometrics and ISO standardisation," in Proc. of Information Security Solution Europe Conference, ISSE 2002, Paris, October 2-4, 2002.
- [24] Z.Savić, A.Nikolić, M.Marković, "Cryptographic Proxy Gateways in Securing TCP/IP Computer Networks," in Proc. of Information Security Solution Europe Conference, ISSE 2001, London, September 26-28, 2001.
- [25] Z.Savić, M.Marković, "Development of Secure WEB Financial Services in Serbia," accepted for Information Security Solution Europe Conference, ISSE 2003, Vienna, Austria, October 7-9, 2003.
- [26] William Stallings, "Cryptography and Network Security", Prentice Hall, 2005.
- [27] Mark Stamp, "Applied Cryptanalysis", John Wiley & Sons, 2007.
- [28] Mark Stamp. *Information security: principles and practice*. John Wiley & Sons, Inc, 2006.
- [29] ANSI X 9.17 (Revised), —American National Standard for Financial Institution Key Management (Wholesale), — American Bankers Association, 1985.
- [30] Bruce Schneier, "Applied Cryptography", John Wiley & Sons, 1996.
- [31] A.Menzes, P.van Oorschot, S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.
- [32] National Institute for Standards and Technology, — *Key Management Using X9.17*, — NIST FIPS PUB 171, U.S Department of Commerce, 1992.
- [33] National Institute for Standards and Technology, — *Secure Hash Standard*, — NIST FIPS PUB 180, U.S Department of Commerce, 1993.
- [34] National Institute for Standards and Technology, — *Digital Signature Standard*, — NIST FIPS PUB 186 U.S Department of Commerce, 1994.
- [35] Andrew Nash, William Duane, Celia Joseph, Derek Brink, "PKI Implementing and Managing E-Security", RSA Press, 2001.
- [36] Milan Milosavljević i Gojko Grubor, "Osnovi bezbednosti i zaštite informacionih sistema", Univerzitet Singidunum, 2006.
- [37] Carlisle Adams, Steve Lloyd, "Understanding PKI: Concepts, Standards and Deployment Considerations", Addison Wesley, 2002.
- [38] Steve Burnett, Stephen Paine, "RSA Security's Official Guide to Cryptography", RSA Press, 2001.