

DEPARTMAN ZA POSTDIPLOMSKE STUDIJE
SAVREMENE INFORMACIONE TEHNOLOGIJE

BEZBEDNOSNI RIZICI NA INTERNETU I REŠENJA
ZAŠTITE PODATAKA

-MASTER RAD-

Mentor:

prof. dr Mladen Veinović

Student:

Banjari Nikola
410325/2011



Beograd, 2013

BEZBEDNOSNI RIZICI NA INTERNETU I REŠENJA ZAŠTITE PODATAKA

Abstrakt

U radu su predstavljeni sajber napadi i rešenja koja se bave problemom sigurnosti informacionih sistema u oblasti komunikacije i zaštite saobraćaja preko postojeće telekomunikacione infrastrukture. Rešenje je predstavljeno preko hardversko-softverskih modula i predstavljene su njihove funkcije.

Ključne reči: zaštita podataka, vrste napada preko interneta, zaštitni hardver, zaštitni softver

Abstract

This study presents the cyber attacks and solutions to deal with the problem of security of information systems in the field of communications and protection of telecommunications traffic over the existing infrastructure. The solution was introduced through the hardware and software modules and their functions are presented.

Keywords: data protection, types of attacks across the internet, protection hardware, security software

Sadržaj

Abstrakt.....	2
Abstract.....	2
1. Teorijsko metodološke osnove.....	5
1.1. Uvodne napomene i obrazloženje rada	5
1.2. Predmet istraživanja i ciljevi rada	5
1.3. Hipotetički okvir istraživačkog rada	6
1.4. Metode istraživanja i tok istraživačkog procesa	6
2. Istorija i pojava modernih komunikacija	7
3. Internet.....	7
3.1 Upotreba interneta	8
4 Bezbednost na internetu	10
4.1 Protokoli i standardi	11
4.2 Slojevitost	12
5 IT Security	15
6 Zlonamerni softver (malware).....	17
6.1 Ostali zlonamerni softveri	27
7 Bezbednosni rizici u prenosu podataka.....	31
8 Kriptografija.....	32
8.1 Simetrična kriptografija.....	35
8.2 Asimetrična kriptografija.....	36
8.3 Sekvencijalni šifarski sistemi	37
8.4 Blok šifra	38
9 Network Security	39
9.1 Primeri veza.....	40
9.2 Rasprostranjene tehnologije / protokoli.....	41
10 Crypto AG	45
11 Mils Electronic	47
12 Generisanje i distribucija kriptoloških ključeva	49

13	Rešenja višeslojne zaštite	53
13.1	Zaštita na aplikativnom nivou	54
13.2	Zaštita na transportnom nivou.....	57
13.3	Zaštita na mrežnom nivou.....	58
14	Zaključak	58
15	Literatura	60
16	Sadržaj slika	62

1. Teorijsko metodološke osnove

1.1. Uvodne napomene i obrazloženje rada

Pojava Interneta, kao i sve veća, globalno rasprostranjena upotreba informacionih i telekomunikacionih tehnologija, uticalo je na porast ilegalnih aktivnosti u ovom prostoru. Upotreba računarskih servera koji pružaju opcije anonimnog korišćenja Interneta, mogućnost otvaranja Web elektronske pošte i korišćenja lažnih elektronskih adresa, postavljanje lažnih internet sajtova, danas su osnovno oruđe u rukama sajber-kriminalaca za izvršenje prevara pomoću savremenih informacionih tehnologija.

Kada se govori o sajber napadima, oni često počinju diverzijom. Slabo zaštićeni računarski sistemi su polazna tačka za uspešan napad. Motivi napada mogu biti različite prirode i mogu dovesti do trajnog oštećenja poslovanja neke kompanije, banke, ambasade, vojne ustanove itd.

Ovaj rad se bavi opisivanjem sajber napada na informacione sisteme kao i analizom rešenja sa aspekta protivmera od napada u domenu zaštite računarskih sistema i sistema telekomunikacija. Rad je nastao ispitivanjem teoretskih, praktičnih znanja i analizom softversko-hardverskog rešenja koji se opisuje.

1.2. Predmet istraživanja i ciljevi rada

Predmet istraživanja rada je opisivanje sajber napada, hardvera i softvera koji deluju u domenu rešenja zaštite informacionih sistema putem postojeće telekomunikacione infrastrukture, a za cilj ima definisanje moguće pretnje i protivmere.

1.3. Hipotetički okvir istraživačkog rada

Opšta hipoteza

Računarske tehnologije kakve danas poznajemo se razvijaju ubrzanim korakom i podložne su raznim napadima i kriminalnim aktivnostima. Napadi na privredna društva, preduzeća, banke, ambasade postaju vrlo učestali i pojedini trpe velike gubitke u poslovanju ili obavljanju definisano normalnih aktivnosti.

Posebna hipoteza

Upotrebom posebno razvijenih sistema može se smanjiti broj ostvarenih napada i bezbednost u oblasti zaštite podataka.

1.4. Metode istraživanja i tok istraživačkog procesa

Metoda naučnog istraživanja je sistematski i ponovljiv proces sticanja novih znanja neophodnih za određivanje i rešavanje naučnog problema. U naučnom istraživanju glavni principi su :

- *sistematičnost* – dobra uređenost istraživanja i obezbeđivanje prirodnog i logičkog toka procesa,
- *kontrolisanost* – sprovođenje istraživanja u što je moguće boljim i nadzornim uslovima kako bi se isključila alternativna rešenja i
- *kritičnos t*– sve važne tvrdnje o pojavama, procesima, odnosima i svojstvima moraju se ozbiljno, iskreno i strogo procenjivati, proveravati i obrazložiti.

Tok istraživačkog procesa

- Prikupljanje literature koja se tiče najčešćih sajber napada.
- Iščitavanje i sortiranje literature izlaganje najučestalijih napada iz oblasti zaštite informacionih sistema
- Prikazivanje rešenja.
- Izlaganje sopstvenog mišljenja i preporuka.

2. Istorija i pojava modernih komunikacija

Kada se govori o komunikacijama zapaža se da je komunikacija i razmena podataka i informacija staro koliko i svet. Raniji oblici komuniciranja su se svodili na razne oblike vizuelno-audio načine kao što su dimni signali, razne vrste duvačkih instrumenata pa čak i korišćenje prenosa poruka preko glasnika, golubova pismoša i raznih drugih metoda.

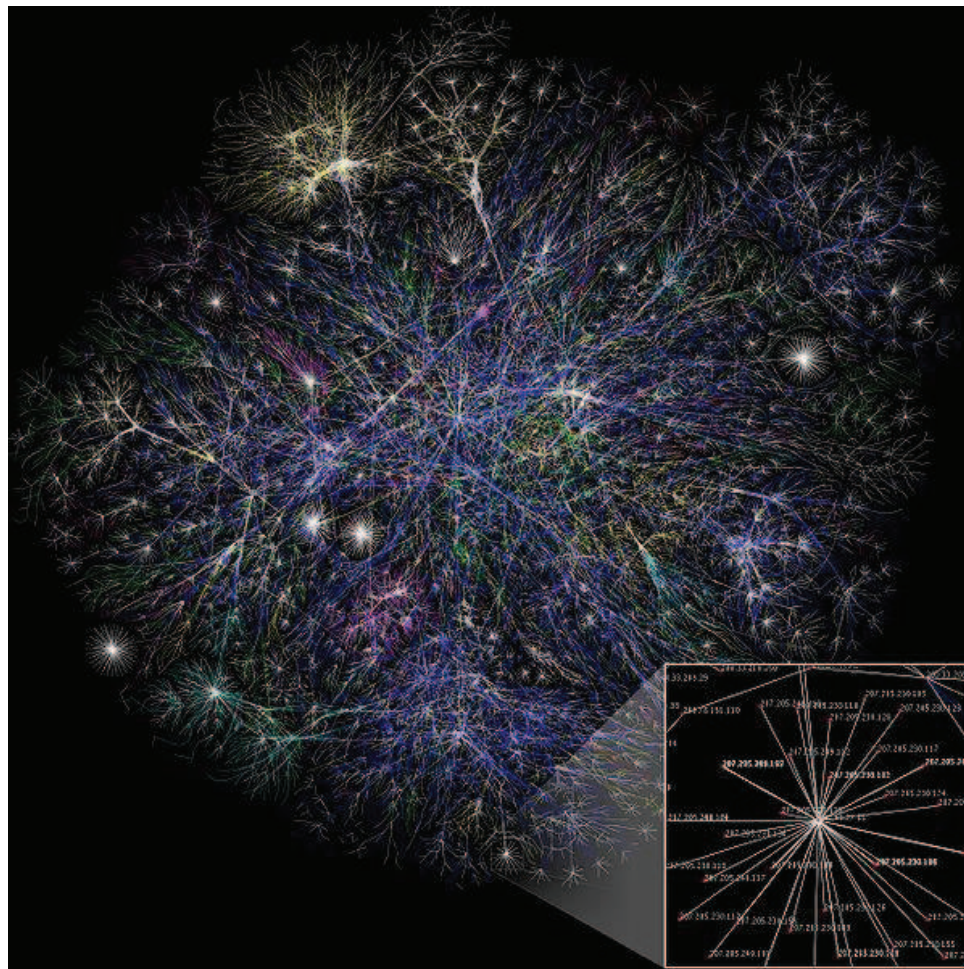
- 1851. godine postavljen je prvi telegrafski kabl između Engleske i Francuske
- 1876 i 1878 godine pojavljuje se telefonija kao sredstvo komunikacije
- 1934. godine u Londonu je demonstriran prenos slike tj. televizija
- 1956. godine postavljen je telefonski kabl između Amerike i Engleske
- 1965. godine ostvaren je eksperimentalan prenos slike u boji između Pariza i Moskve
- 1969. godine počinju počeci Interneta koji se vezuju za stvaranje ARPANET
- Početkom 70-tih pojavljuju se softveri za upravljenje biznis procesima
- Početkom 80-tih dolazi do ubrzanog razvoja optičkih kablova
- Sredinom 90-tih definiše se arhitektura OSS i razvoj mobilne telefonije
- U toku je razvoj mreža nove generacije

Kao što se primećuje razvoj telekomunikacija je išao progresivnim tokom. A današnje komunikacije se dobrim delom obavljaju preko Interneta.

3. Internet

Internet je svetski sistem umreženih računarskih mreža koji je transformisao način na koji funkcionišu komunikacioni sistemi. Počeci Interneta se vežu za stvaranje ARPANET-a, 1969. godine, mreže računara pod kontrolom Ministarstva odbrane SAD. Danas, internet povezuje milijarde računara širom sveta na jedan nehijerarhijski način. Internet je proizvod spoja medija, računara i telekomunikacija. Međutim, internet nije samo proizvod tehnološkog napretka, nego takođe društvenih i političkih procesa, uključujući naučnu zajednicu, politiku i vojsku.

Pojam Internet znači mreža unutar mreže, ili internakonekcija između više računara. Strukturno postoje male mreže koje se međusobno vezuju, i time čine ovu strukturu. Internet se sve više naziva globalnom mrežom informacija (velika internacionalna-globalna baza podataka). Broj računara na Internetu se trenutno



Slika 1 : Vizuelizacija puteva interneta

3.1 Upotreba interneta

Svi razlozi zbog kojih ljudi koriste internet mogu se iskoristiti i kao ideja u kreiranju sopstvenog web sajta putem kojeg ćete zarađivati, pomaže u komunikaciji i povezivanje među ljudima, postavlja korisne informacije bitne za unapređenje znanja.

Možete vaš proizvod ili uslugu diferencirati u odnosu na konkurente, predstavljajući alternativna rešenja za vaše kupce ili unaprediti postojeće usluge uspešnih online kompanija i tako privući pažnju tržišta.

Komunikacija i socijalizacija

Jedan od razloga su komunikacija i socijalizacija. Ovo je jedna od osnovnih ljudskih potreba. Ljudi vole da se sreću i razgovaraju sa drugim ljudima na Internetu. Na taj način održavaju postojeće veze sa ljudima ili stvaraju nove. Razmenjuju ideje, pričaju o njima, pridružuju se online mrežama onih koji imaju slično mišljenje njihovom.

Pronalaženje informacija, učenje, zabava

Drugi razlog je pronalaženje informacija, učenje novih stvari i zabava. Internet je ogromna arhiva novih i starih informacija. Takođe je i izvor zabave, pružajući trenutno zadovoljstvo u formi slika, zvukova, interaktivnosti. Kao edukativno sredstvo, web je suštinski bitan za ljude koji su u potrazi za novim znanjima. Ljudi jednostavno vole da pronalaze stvari online.

Pokretanje online biznisa i generisanje profita

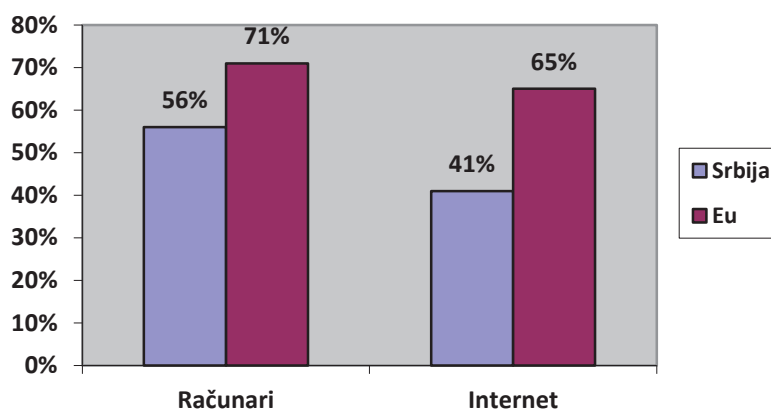
Treći razlog je pokretanje biznisa i generisanje profita. Mnogi koriste Internet da bi od njega zarađivali za život. Suštinski je za mnoge poslovne ljude koji žele da unaprede svoj biznis i profitiraju. Da bi uspeali na Internetu nije potrebno da budete programer. Potrebno je da imate originalnu ideju, da znate kako da je realizujete i povežete se sa pravim ljudima.

Elektronska trgovina

Tu je naravno, i elektronska trgovina koja podrazumeva kupovinu i prodaju proizvoda i usluga online. Aukcijski portali su naročito popularni jer omogućavaju nadmetanje u cenama i povoljniju kupovinu odnosno prodaju.

Zastupljenost Interneta

U Srbiji 50,4% domaćinstava ima računar i 39% domaćinstava ima Internet priključak. Broj računara je povećan u odnosu na predhodnu godinu za 3,6%, a broj Internet priključaka za 2,3%. U Evropskoj uniji u proseku 71% domaćinstava koristi računare, a 65% koristi Internet.(Podatak iz 2011.)



Slika 2 : Grafički prikaz upotrebe računara i interneta

4 Bezbednost na internetu

Bezbednost na Internetu postaje sve učestalija tema i među običnim korisnicima, zbog toga jer Internet nudi mnogobrojne servise za obavljanje različitih delatnosti kao što su on-line banking, kupovina i prodaja, razmena poverljivih informacija, elektronsko poslovanje..itd.

Računarska bezbednost je proces zaštite računara i računarskih sistema od neželjene upotrebe, ugrožavanja sistema i uljeza. Pod ugrožavanjem se smatra vid upotrebe računara u cilju nanošenja štete podacima, programima ili računarskim procesima. Nedostaci u računarskoj bezbednosti se javljaju zbog ranjivosti ili slabosti računarskog sistema, ali češće zbog ljudskih faktora, odnosno ljudske greške u podešavanju sistema. Agent koji ima nameru da ugrozi neki računarski sistem, bilo da se radi o osobi, događaju, ili određenim okolnostima, iskorištava te slabosti. Računarska bezbednost obuhvata zaštitu od nedostupnosti računarskog sistema (takođe: uskraćivanje usluga, engl. denial of service - DoS), zaštitu integriteta podataka i programa i poverljivosti i privatnosti podataka i informacija.

Da bi smo bolje razumeli slabosti sistema i preventivno zaštitili moderne informacione sisteme potrebno je poznavati i samu arhitekturu kao i protokole.

4.1 Protokoli i standardi

Prenos podataka kroz mrežu se obavlja po protokolima, utvrđenim pravilima koja su poznata svim učesnicima u komunikaciji. Protokol predstavlja standard za ostvarivanje i kontrolu veze i prenosa podataka između dve krajnje tačke. Komunikacioni protokol predstavlja set standardizovanih pravila za predstavljanje podataka, signalizaciju, proveru autentičnosti i kontrolu grešaka, neophodnih da bi se informacija prenela komunikacionim kanalom.

Razmena podataka u računarskoj mreži je složena. Sa povećanjem broja umreženih računara koji komuniciraju i sa povećanjem zahteva za sve savršenijim uslugama neophodno je usavršavanje protokola. Koraci protokola moraju da se sprovedu u skladu sa redosledom koji je isti za svaki računar u mreži.

Osnovni principi u dizajnu protokola su efikasnost, pouzdanost, robusnost i prilagodljivost. Potrebno je da oba računara, predajni i prijemni, svaki korak izvedu na isti način kako bi prijemni podaci imali istu strukturu kakvu su imali pre slanja. U mreži više protokola radi zajedno. Njihov zajednički rad obezbeđuje ispravnu pripremu podataka, prenos do željenog odredišta, prijem i izvršenje. Rad više protokola mora da bude usaglašen kako se ne bi dogodili konflikti ili nekompletne operacije, odnosno nekompletan prenos informacija. Rezultat tog usaglašavanja je slojevitost.

Osnovni razlog za postavljanje standarda jeste omogućavanje korišćenja komponenti različitih proizvođača i njihove međusobne kompatibilnost u kompleksnim sistemima.

Protokol HTTP (HyperText Transfer Protocol) se koristi za prenos stranica između dva računara. Sesiju pokreće klijent slanjem zahteva za resursom (HTTP request). Server odgovara slanjem traženog resursa (npr. Web stranice) i okončava sesiju.

Protokoli za slanje pošte serveru SMTP (Simple Mail Transfer Protocol) i za pregled i preuzimanje pošte sa servera POP (Post Office Protocol) predstavljaju standarde za slanje i prijem elektronske pošte. Nešto savremeniji protokol IMAP (Internet Message Access Protocol) omogućava pretraživanje, organizovanje i filtriranje pošte pre preuzimanja, na samom serveru elektronske pošte.

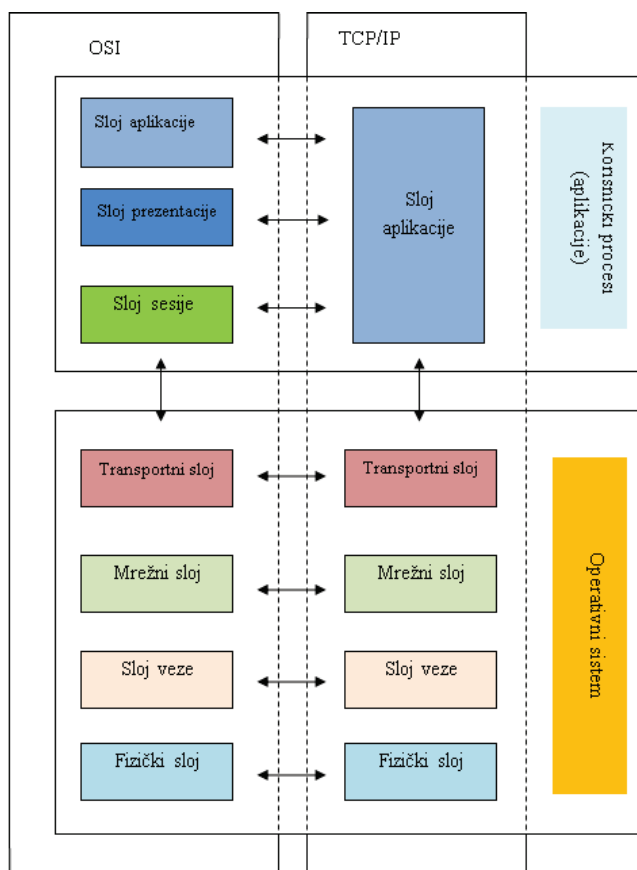
Protokol FTP (File Transfer Protocol) je efikasan namenski Internet servis za prenos programa i čitavih baza podataka jednim zahtevom. Koristi se za prenos velikih

fajlova, većih od Web stranica i poruka elektronske pošte. Protokol aplikativnog sloja Telnet koristi se za prijavu klijentskog računara na udaljeni računar putem računarske mreže, radi pokretanja programa ili pristupa fajlovima sa udaljene lokacije.

Poseban protokol za zaštitu podataka koji se prenose između klijenta i servera je SSL (Secure Socket Layer), koji šifruje i digitalno potpisuje sadržaj poruka.

4.2 Slojevitost

Krajem 70-ih godina Internacionalna Organizacija za Standardizaciju (ISO) razvila je model za komunikaciju između srodnih sistema. Model je objavljen 1984, godine i nazvan je *Open System Interconnection Basic Reference Model* ili OSI model. Ovaj model je ponudio fazno prevođenje formata podataka kroz sedam slojeva.



Slika 3 : OSI i TCP/IP modeli

Jedna od glavnih mana OSI modela je nepotrebno zalaženje u interne delove računarskih sistema i definisanje komponenti koje nisu direktno zadužene za međusistemsku komunikaciju. Kao posledica toga javio se veći broj korisničkih aplikacija koje nisu poštovale u potpunosti OSI standard. Ovakva tendencija je rezultovala pojavljivanjem jednostavnijeg Internet modela TCP/IP (Transmission Control Protocol TCP Internet Protocol IP) koji daje veću slobodu pri izboru arhitekture aplikativnog softvera.

- **Fizički sloj**

Definiše električna i fizička svojstva mrežnih uređaja (mrežnih adaptera - engleski termin u širokoj upotrebi je NIC (eng. Network Interface Card) . Definišu se naponski nivoi, broj pinova na konektorima (odnosno parica u kablovima), ili debljina opleta koaksijalnog kabla. Mrežne kartice (integrisane na matičnoj ploči ili samo utaknute u sabirnicu na matičnoj ploči), hub-ovi i repeater-i su primeri uređaja na fizičkom sloju OSI modela.

- **Sloj veze**

Brine se za razmenu podataka između mrežnih uređaja, i za detekciju, korekciju mogućih grešaka u fizičkom sloju. Uređaji komuniciraju pomoću "hard-kodiranih" adresa (MAC adrese kod ethernet mrežnih uređaja), i komunikacija na ovome nivou je moguća samo unutar lokalnih mreža. Komutatori (Switchevi) su uređaji koji "rade" na sloju podataka, jer oni čuvaju u memoriji MAC adrese svih mrežnih uređaja koji su spojeni na njih, i kad do njih dođe paket, oni pročitaju adresu polaznog i odredišnog uređaja iz zaglavlja, te ostvaruju električnu vezu između ta dva uređaja.

- **Sloj mreže**

Na internetu je ogroman broj računara, a mi ih raspoznavamo po njihovim imenima u obliku ime.domen.vršni_domen (npr. sr.wikipedia.org) Naravno, taj sistem je napravljen radi ljudi, i takozvani DNS serveri pretvaraju takve upite veb pregledača u IP adrese, po trenutno važećem IPv4 standardu u adresu tipa a.b.c.d, gde su a,b,c i d brojevi od 0 do 255 (veličina reči 1 bajt). Ali kao što znamo, mrežne kartice u računarima nemaju IP adrese, nego MAC adrese. To znači da je potreban još jedan sloj, koji će pretvoriti IP adrese u MAC adrese. Kad bi svaki računar na internetu imao tablicu pretvaranja IP adresa u MAC adrese, to bi bilo vrlo nepraktično, iz više razloga, kao što su veličina tablice, onda dodavanje novih adresa, pa je smišljeno drugo rešenje. Na svakom segmentu mreže (subnetu) postoji ruter, koji poseduje tabelu usmeravanja.

Pakete koji dođu do njega, a cilj im nije na lokalnom mrežnom segmentu on prosleđuje dalje, a pakete koji su namenjeni lokalnoj mreži, prosleđuju se na lokalnu mrežu. To se izvodi tako što dok ostali uređaji na mreži imaju jedan mrežni adapter (NIC), ruter ima dva. Jedan je povezan na lokalnu mrežu, a drugi na spoljašnju, pa ruter pakete koje dobije na lokalnoj mreži, a koji su namenjeni svetu upućuje napolje, a pakete iz spoljašnjeg sveta upućene lokalnoj mreži upućuje unutra.

- **Transportni sloj**

Ovaj sloj vodi računa o paketima koji putuju između dva računara. Primeri protokola na transportnom sloju su TCP i UDP. Ako se neki paket "izgubi" na putu, TCP će tražiti da se ponovo pošalje, pa je stoga pogodan za razmjenu podataka za koje je integritet podatak na višem nivou od brzine prenosa. S druge UDP nema kontrolu da li se poneki paket zagubio, pa je zgodan za multimedijalne aplikacije, gde nije toliko bitno da li se zagubi poneki paket, nego je bitna brzina komunikacije.

- **Sloj sesije**

Bavi se uspostavljanjem veze između krajnjih korisnika, i sinhronizacijom iste. Najlakše ga je objasniti kod videa preko interneta, gde ne želimo imati ton bez slike, ili sliku bez tona, ili oboje ali bez sinhronizacije. Za to se brine ovaj sloj.

- **Sloj prezentacije**

Podaci koji se koriste na raznim računarima se kodiraju na razne načine (little-endian, big-endian); txt datoteke na Mac-u, juniksu i Windows-ima na različite načine označavaju prelazak u novi red. Sve takve konverzije se izvode (ukoliko su implementirane) na prezentacionom sloju.

- **Sloj aplikacije**

Na ovom sloju programer koristi API-je kojima ostvaruje mrežnu komunikaciju s određenom svrhom, a da pritom ne mora voditi računa o nižim slojevima, za koje se brine operativni sistem. Primeri protokola na ovom sloju su HTTP, FTP, telnet, SMTP, NNTP i mnogi drugi.

5 IT Security

Aplikacije bazirane TCP/IP predstavljaju sve veći udeo u globalnom umrežavanju. Međutim, globalno umrežavanje znači da su sve vrste informacija izložene riziku od prisluškivanja, menjanja sadržaja i ostalim napadima.

IT radne stanice mogu da se nalaze u najrazličitijim okruženjima. Pri obradi osetljivih informacija, sigurnosni sistemi moraju da ispune visoko specijalizovane zahteve i potrebe pod određenim okolnostima.

Danas, vlada i administrativne agencije su međusobno povezane. Bez standardne infrastrukture, saradnja i rezultati su nezamislivi u okviru savremenih država. Vlada, ministri, diplomate i politički donosioci odluka su svi integrisani u jednoj grupi komunikacije i trebalo bi da razmenjuju informacije lako, bezbedno i brzo. Još uvek ima prostora za poboljšanje, međutim, tendencija u budućnosti vlade će biti da sa što manje ljudi obrade sve složenije zadatke. Ključ će biti moderna IKT infrastruktura koja dosledno uzima u obzir organizacionu strukturu, metode i procese poslovanja.

Odbrambene organizacije su radili godinama na umrežavanju vojske, flote i vazdušnih snaga, kao deo opšte transformacije oružanih snaga. Informaciona superiornost se postiže kada su relevantne informacije dostupne u pravo vreme i na pravom mestu. To znači da i tokovi podataka moraju da se prenose hiljadama kilometara u milisekundama. Veoma je važno da ne dođe do zagušenja saobraćaja podataka, posebno u kritičnim situacijama. Elektronska infrastruktura mora biti u stanju da obradi maksimalne količine podataka – nema lak zadatak s obzirom da konstantno raste potražnja za propusni opseg. Komunikacione mreže su kičma države. Njihov neuspeh može ugroziti suverenitet.

Trenutni trend u svetu će nastaviti umrežavanje u budućnosti, u velikoj meri zahvaljujući InternetProtokol-u (IP). IP omogućava konvergenciju glasa, podataka i videa na jednom standardnom organizovanom protokolu, pružajući korisnicima ogroman potencijal za izgradnju jednostavne i ekonomične IKT strukture. Vlade, uprave i industrija mogu da usvoje "sve više IP" strategija za stvaranje end-to-end mreža sa hiljadama kanala štedeći troškove, kao i logističke i kadrovske resurse. Tipični IP rizici moraju biti eliminisani pouzdano.

Uprkos mnogim prednostima, javne IP mreže, podrazumevaju sve bezbednosne rizike uprkos savremenoj IP tehnologiji. Ti rizici uključuju prisluškivanje, viruse, trojanske konje i broj drugih (manje poznatih) opasnosti. Apsolutno je neophodno da se

održi poverljivost, integritet i autentičnost u prenošenju podataka političkih strategija, vojne komande, ličnih podataka, kao i rezultate istraživanja iz obaveštajnih službi ili tokom finansijske transakcije. Sveobuhvatna kriptografska zaštita je jedino pouzdano rešenje za obezbeđivanje bezbednosti informacija iz svih vidova napada.

Pojam bezbednost računara (IT Security) može se interpretirati na više načina u zavisnosti od razdoblja u kojem se taj pojam koristio. Pojavom i korišćenjem Interneta ovaj pojam poprima šire značenje koje podrazumeva zaštitu od kradljivaca podataka (Data Thieves) i mrežnih napadača (Network Attackers), koji se danas popularno nazivaju hakeri (Hackers).

Budući da je Internet poslednjih godina doživeo veliku ekspanziju omogućivši brzu komunikaciju među korisnicima na udaljenim destinacijama, stvorila se potreba da se znatno ozbiljnije pristupi problemu bezbednosti na Internetu. Međutim, brzi razvoj i globalizacija otežavaju uspostavljanje valjane pravne regulative koja bi sankcionisala sve veći broj zloupotreba koje nastaju na Internetu. Zbog ogromnog broja korisnika Interneta u gotovo svim državama sveta, skoro je nemoguće učinioca prekršaja pronaći i kazniti. Mnoge vlade su donele zakone koji važe samo u njihovim zemljama, međutim još uvek postoji veliki broj država koje nisu dovoljno svesne negativnih strana Interneta. Pri tom donošenje ovakvih zakona i pravila nije nimalo lak zadatak. Upravo je nedostatak adekvatnih zakona jedan od osnovnih razloga pojave velikog broja zlonamernih softvera koji narušavaju bezbednost korisnika Interneta.

Korisnike Interneta bi zato veoma trebalo da zanima šta sami mogu da učine u cilju zaštite od ovakvih pojava, pogotovo kada se radi o poslovnom okruženju gde se nameću i dodatni zahtevi, vezani za osiguranje kontinuiteta poslovanja i sprečavanje krađe, oštećenja i uništenja podataka. Prvi korak je svakako elementarna edukacija o bezbednosti na Internetu.

Najčešći oblici i načini narušavanja bezbednosti računara na Internetu su:

- skidanje elektronske pošte (*e-maila*) zaražene zlonamernim softverom koji se obično nalazi u prilogu (*attachmentu*),
- otvoreni računarski portovi (kao posledica aktiviranja zlonamernog softvera) preko kojih je moguće preuzeti kontrolu nad napadnutim računarom – *Distributed Denial-on-Service* (DDoS),
- poseta sumnjivim sajtovima (koji su obično postavljeni na besplatnim serverima) koji preko Java ili ActiveX apleta ubacuju zlonamerni softver na računar,
- instalacija i startovanje "sumnjivih" programa koji su zaraženi zlonamernim softverom,

- bezbedonosni propusti u programima koji se inače koriste na računaru (operativni sistem, Internet pretraživači, e-mail klijenti i dr.) zbog kojih je neophodno svakodnevno ažuriranje ("skidanje") sigurnosnih dodataka (*update-ova*),
- korišćenje "zakpra" (*crack-ova*) koji omogućavaju nelegalno korišćenje softvera,
- mrežna krađa identiteta (Phising) koja predstavlja prikupljanje personalnih podataka (korisničko ime, lozinka, broj platne kartice, broj telefona i dr.) od lakovernog korisnika na lažnim web sajtovima,
- preusmeravanje na "lažni" web sajt (Pharming) modifikacijom lokalnog DNS servera na računaru koji je prethodno zaražen zlonamernim sofverom,
- neoprezno korišćenje servisa društvenih (socijalnih) mreža – Facebook, Twitter, My Space,...

6 Zlonamerni softver (malware)

Malware je složenica od engleskih reči **malicious** i **software**. Doslovno prevedeno to bi značilo maliciozni ili zlonamerni softver. Definicija prema organizaciji NIST (National Institute of Standards & Technology) glasi: "pojam **malware** se odnosi na program koji je, najčešće tajno, ubačen u sistem sa namerom kompromitovanja poverljivosti, integriteta ili dostupnosti žrtvinih podataka, aplikacija ili operativnog sistema, ili na neki drugi način pokušava ometati žrtvu".

Svrha ovog softvera je da se bez znanja i pristanka korisnika pristupi resursima računara. Ovaj softver je napravljen tako da se neprimetno ubaci u softver računara i načini neku vrstu štete. Rezultati zloupotrebe ovakvog softvera mogu da variraju počev od krađe lozinki, bankovnih računa, identiteta na Internetu do korišćenja zaraženog računara za DDoS (Distributed Denial-of-Service) napade, slanje hiljada nepoženjih poruka (Spam) ili za "anonimno" surfovanje Internetom (zaraženi računar se koristi za izvršavanje nelegalnih radnji na Internetu). U ovu kategoriju spada bilo koji softver koji remeti normalan rad računarskog sistema ili računarske mreže. Klasična podela ovakvog softvera je izvršena na sledeće podkategorije:

- računarski virus,
- crv (engl. worms),
- Trojanski konj ili Trojanac (engl. trojan horse),
- Rootkit,

- Backdoor,
- Spyware,
- Adware,
- Phishing,
- Pharming i
- ostali.

Naravno da postoje zlonamerni softveri koji mogu da imaju osobine i ponašaju se kao tipovi nekoliko podkategorija, tako da granice ove podele nisu precizne. Takav softver je samo mnogo destruktivniji i teže se otklanja sa računarskog sistema.

- **Računarski virus**

Računarski virus je programski kod koji se ugrađuje u pojedine fajlove aplikativnog ili sistemskog softvera. Obično se sastoji iz dva dela od kojih je prvi samokopirajući kod koji omogućava razmnožavanje virusa, a drugi deo, glavni kod ili payload, može biti škodljivog ili neškodljivog sadržaja.

Nakon pokretanja, računarski virus može da izazove replikaciju unutar ugroženog operativnog sistema inficiranjem drugih fajlova ili foldera na istom računaru ili mreži, brisanje ili oštećivanje podataka ili fajlova i trošenje drugih računarskih resursa sa ili bez oštećivanja fajlova. Životni ciklus računarskog virusa se sastoji od ulaska u računarski softver, njegove aktivacije, traganja za softverskim resursima koji se podložni infekciji, pripremi za kopiranje virusa i konačno inficiranju softverskih resursa.

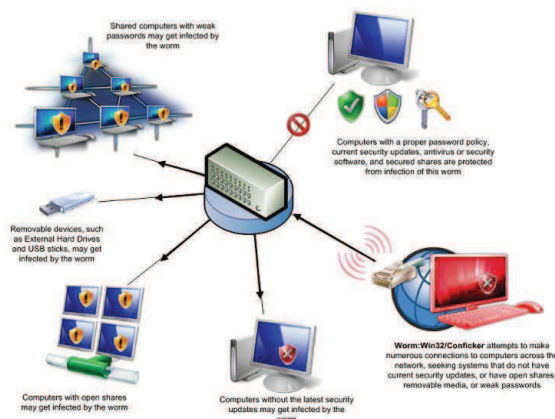
Termin "virus" se svakodnevno koristi i za druge vrste zlonamernog softvera (Adware, Spyware) koji nemaju reproduktivne sposobnosti. Pravi virus se može prenositi sa jednog računara na drugi (u nekim oblicima izvršnih fajlova). Na primer, može se desiti da ga korisnik pošalje preko mreže ili Interneta, ili ga jednostavno prekopira na neki od prenosnih uređaja kao što su disketa, CD, DVD ili USB fleš. Virusi mogu povećati svoju šansu za širenje na druge računare inficirajući fajl unutar mreže ili neki sistemski fajl kome drugi računar unutar mreže može pristupiti. Među računarskim virusima postoje oni koji su samo mala smetnja pri radu do onih koji su potpuno destruktivni. Ipak, pravi virus se ne širi bez ljudskih postupaka koji bi ga pokretali, kao što su deljenje fajlova ili foldera ili slanje elektronske pošte.

Postoje različite tehnike preživljavanja virusa kao što su enkripcija (šifrovanje), metamorfizam (preobražavanje) i razmnožavanje, od kojih prve dve tehnike služe za prikrivanje virusa kako ga antivirusni programi ne bi prepoznali. Kombinacijom navedenih tehnika moguće je razlikovati sledeće tipove virusa kao što su: šifrovani, metamorfni i polimorfni virusi.

Polimorfni virusi menjaju svoj kod svaki put kada se repliciraju kako bi izbegli šansu da budu otkriveni od strane antivirusnih softvera. Šifrovanje je najčešći način da sakriju svoj kod. Sa šifrovanjem, telo glavnog koda (payload) se šifrira, a zatim kopira u više primeraka. Kada se kod izvršne funkcije pokrene, pokreće se i ovaj virus, koji se izvlači iz šifre i prelazi u svoju originalnu funkciju. Ovo ih čini dosta prilagodljivim na bilo koju sredinu unutar računara.

- **Crv**

Virusi inficiraju domaćine, dok crvi napadaju sisteme. Crv predstavlja potklasu računarskog virusa i on je, kao i virus, napravljen tako da se kopira sa jednog računara na drugi, samo što on to radi automatski, preuzimanjem kontrole nad funkcijama računara koje omogućavaju prenos fajlova i foldera. Kada crv dospe u sistem, on se nadalje samostalno replicira u izvornoj ili izmenjenoj varijanti. Velika opasnost jeste i njihova sposobnost da se umnožavaju u ogromnim količinama. Na primer, crv bi mogao da pošalje kopije samog sebe svim kontaktima iz adresara e-mail klijenta, a zatim bi zaraženi računari uradili to isto, čime se izaziva domino efekat zagušenja u mrežnom saobraćaju što usporava poslovne mreže i Internet u celini. Kada se oslobode, novi crvi se šire veoma brzo, zagušujući mreže, što može da znači da će svi zaraženi korisnici računara morati da čekaju duplo duže da se otvore web stranice na Internetu ili će računar biti toliko zagušen da će prestati da reaguje. Osim opasnosti ubrzanog razmnožavanja, crvi omogućavaju udaljenom korisniku i preuzimanje kontrole nad zaraženim računarom.



Slika 4 : Širenje Worm-a

Danas se susrećemo sa veoma naprednim crvima koji se distribuiraju putem USB fleš memorija, preko MSN-a, peer-to-peer aplikacija, pa čak i preko sajtova za društveno umrežavanje kao što je Facebook. Šteta koja može da bude naneta sistemu se uglavnom bazira na bespotrebnom zauzimanju resursa sistema (CPU, RAM, hard disk) do veoma maštovitih radnji kao što su otvaranje i zatvaranje CD/DVD-ROM-a, pomeranje rasporeda tastera na tastaturi, itd... Takođe postoje i oni čiji je glavni cilj samo download nekog drugog malware-a i dalje širenje putem propusta u operativnom sistemu.

Najnovijim verzijama crva pridružene su funkcije ostalih podkategorija zlonamernog softvera, što ih čini mnogo opasnijima od onih prvobitnih, čak toliko opasnim da je neretko jedini način njihovog uklanjanja sa računara formatiranje hard diska i ponovna instalacija operativnog sistema. Na taj način dolazi do potpunog brisanja svih podataka sa hard diska što je veliki problem ukoliko ne postoje sačuvane rezervne kopije.

- **Trojanski konj**

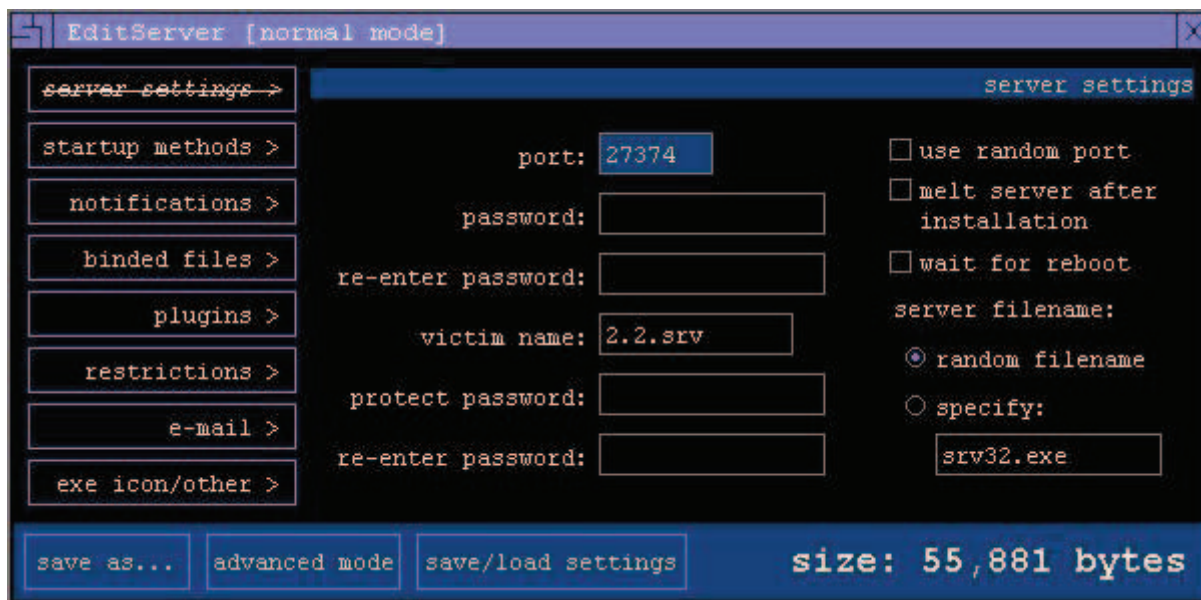
Savremeni trojanski konji su računarski programi koji deluju kao koristan softver, a zapravo ugrožavaju bezbednost računara i izazivaju puno štete. Trojanski konji se šire tako što navode korisnike da otvaraju programe misleći da oni potiču iz legitimnih izvora, a u pozadini onemogućavaju rad antivirusnih programa i zaštitnog zida i, samim tim, omogućavaju neovlašćeni pristup računarskom sistemu korisnika. Mogu se nalaziti i u besplatnom softveru. Najbolji način zaštite od njih podrazumeva izbegavanje preuzimanja softvera iz nepoznatog i nepouzdanog izvora. Glavna karakteristika koja ih deli od ostalih kategorija zlonamernog softvera je ta da se Trojanci se ne šire sami od

sebe već zahtevaju uputstva od strane hakera za to, kao i za ostale stvari koje rade na zaraženom računaru.

Trojanci obično vrše neželjene akcije na računaru potpuno sakriveni u pozadini tako što presreću programe tokom razmene informacija ili podataka, ili jednostavno čitaju fajlove i šalju sve sakupljene podatke svom kreatoru.

Trojanci su dizajnirani tako da omogućavaju hakeru pristup drugom računarskom sistemu preko Interneta. Kad se Trojanac instalira na željeni računar on ima mogućnost da izvršava određene operacije na tom računaru, koje zavise od njegovog dizajna i namene. Najčešće operacije koje haker može da izvršava na računaru zaraženom Trojancem su:

- prikupljanje i krađa poverljivih informacija – lozinki, bankarskih računa i dr.,
- instalacija softvera (uključujući i druge oblike zlonamernog softvera),
- download, upload, brisanje, kreiranje i modifikacija fajlova,
- pregled radne površine korisnika,
- dodavanje računara u BotNet mrežu (DDoS napad),
- prikupljanje i preuzimanje teksta koji je unet sa tastature (Keylogging) i
- zauzimanje resursa računarskog sistema i njegovo usporavanje.



Slika 5 : Sub7 trojan horse

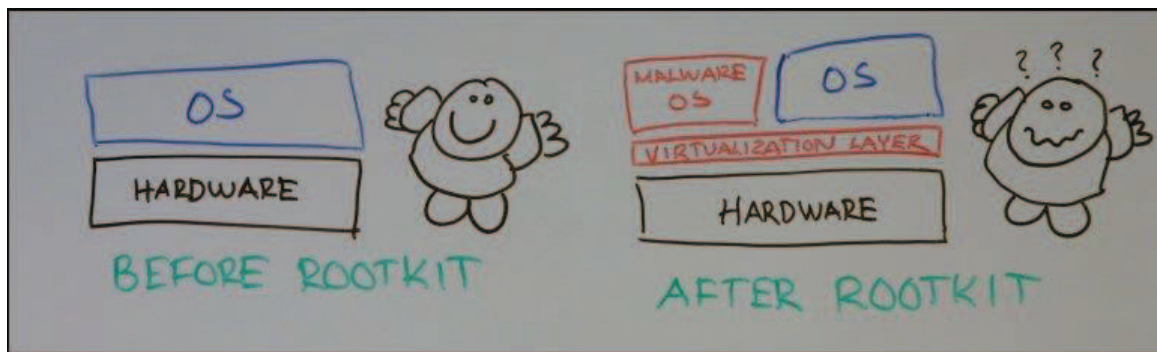
Ovo je samo deo onoga što može da uradi jedan Trojanac, dok kompletna lista operacija zavisi od znanja i umeća hakera koji ga je kreirao. Trenutno su Trojanci najbrojnija vrsta zlonamernog softvera sa preko 50% zastupljenosti. Najveću opasnost

predstavlja Zeus koji vrši krađu on-line bankovnih računa iz preko 700 centara od kojih svaki kontroliše oko 40.000 zaraženih računara (oko 60% u Brazilu i SAD-u).

- **Rootkit**

Rootkit (od *root* – "administrator" i *kit* – oprema, alat) je zlonamerni softver koji se može sastojati od više programa čiji je glavni cilj da prikriju činjenicu da je sistem kompromitovan. Rootkit predstavlja jednu ili skup više programskih alatki, dizajniranih u cilju prikrivenog preuzimanja kontrole nad operativnim sistemom zbog sakrivanja drugih zlonamernih aktivnosti.

U početku, Rootkit programi pojavili su se na Unix operativnim sistemima (uključujući i Linux), u vidu jedne ili skupa više alatki koje su napadaču omogućavale kontrolu rada određenog korisnika računarskog sistema sa najvišim privilegijama, tj. administratora (na Unix sistemima se taj korisnik naziva *root*, pa odatle i potiče ime ove vrste zlonamernog softvera). Na Windows računarskim sistemima, naziv Rootkit najčešće se vezuje za alatke korišćene u cilju sakrivanja određenog programa ili procesa od korisnika. Posle instalacije, Rootkit u Windows sistemu koristi funkcije operativnog sistema da bi se prikrio, odnosno da ne bi mogao biti otkriven. Često se koristi u cilju prikrivanja nekog drugog zlonamernog programa (npr. Keylogger programa). Korišćenje Rootkit programa ne mora biti zlonamerno, ali se pojam Rootkit sve više dovodi u vezu sa neželjenim ponašanjem operativnog sistema i zlonamernim programima.



Slika 6 : Rootkit šema

Suprotno onome što njegov naziv može da podrazumeva, Rootkit ne dodeljuje administratorske privilegije korisniku, već omogućava pristup, pokretanje i modifikovanje sistemskih fajlova i procesa. Napadač može da koristi Rootkit za zamenu

(modifikaciju) vitalnih procesa sistema, koji tada mogu da se koriste za sakrivanje procesa i fajlova koje je napadač instalirao, kao i za sakrivanje samog Rootkit-a.

- **Backdoor**

Backdoor (stražnji ulaz) je program koji instaliraju virusi, crvi ili Trojanci (bez ikakvog znanja korisnika računara) i koji služi za zaobilaženje uobičajene autentifikacije (procesa provere korisnikovih ličnih podataka u toku pokušaja prijavljivanja ili konektovanja) da bi omogućio nesmetan i neovlašćen pristup vlasnika korisnikovom sistemu. Backdoor koristi slabosti i propuste u operativnim sistemima, zaštitnim zidovima i antivirusnim programima. Backdoor trojanci otvaraju "stražnji ulaz" napadnutog računara i dopuštaju neovlašćeno korišćenje hardverskih i softverskih resursa napadnutog računara aplikacijama koje ih koriste. Po trenutnoj zastupljenosti, nalaze se odmah iza Trojanaca sa 20%.

- **Spyware**

Spyware (od spy – špijun i ware – programski paket) je široko rasprostranjena kategorija zlonamernog softvera sa ciljem da prisluškuje ili delimično preuzima kontrolu nad računarom bez korisnikovog znanja i dozvole. Razlikuje se od virusa i crva, jer ne može da se replicira. Spyware je dizajniran da iskoristi zaraženi računar u komercijalne svrhe. Spyware je tip zlonamernog softvera koji sakuplja podatke o korisnicima bez njihovog znanja. Postojanje Spyware-a je sakriveno od korisnika sistema i uglavnom je instaliran tajno, mada se može desiti da je instaliran na nekom deljenom računaru od strane administratora za tajni monitoring ostalih korisnika. Funkcije Spyware-a takođe mogu prevazići uobičajeno tajno "nagledanje" korisnika. U tom slučaju mogu da prikupljaju veoma širok spektar informacija (istoriju Internet surfovanja, sliku celokupnog desktopa, zapamćene šifre na računaru, kucana slova sa tastature, itd.). Imaju mogućnost da instaliraju i drugi zlonamerni softver koji može da uradi redirekciju Internet pretraživača na neku drugu adresu bez obzira na adresu koju je korisnik želeo da poseti. Spyware je poznat i po tome što menja kompjuterska podešavanja, koja za rezultat imaju veoma spore brzine pristupa Internetu, nefunkcionalnost programa koji koriste Internet, itd.



Slika 7 : Spyware instalacija

- **Adware**

Adware (od ad – reklamiranje, oglas i ware – programski paket) je bilo koji softverski paket, deo zlonamernog softvera, koji automatski pokreće, prikazuje ili skida reklame na računar posle instalacije ili dok se program koristi.

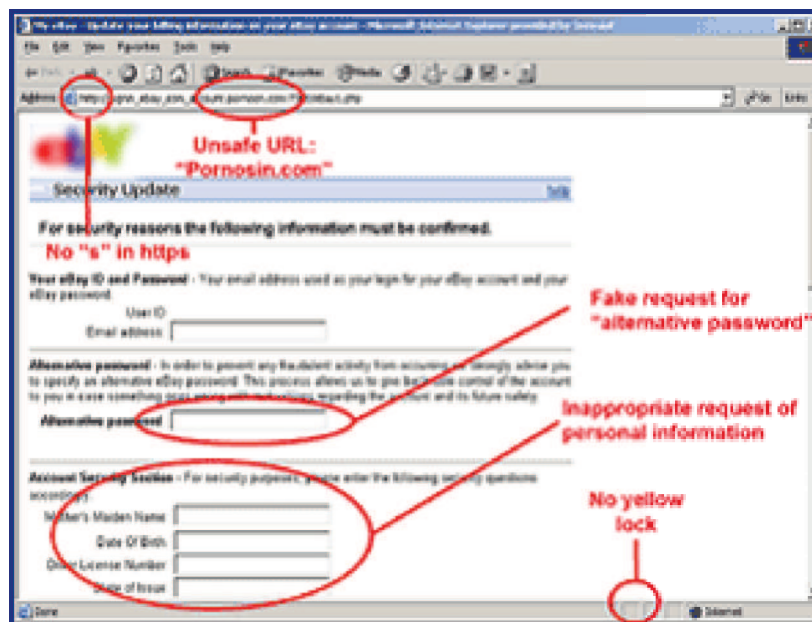
Odličan odziv ovih reklama kod korisnika, može motivisati programera da nastavi sa unapređivanjem i razvijanjem svog softvera. U suprotnom, ove reklame kod nekih korisnika mogu dovesti do negodovanja pošto posle nekog vremena postaju zamorne. Neke vrste Adware-a su deo Spyware-a jer ugrožavaju privatnost na Internetu. Funkcije reklamiranja su integrisane ili su u vidu paketa pridružene softveru. Dizajniran je obično tako da ima za cilj prikupljanje Internet sajtova koje korisnik posećuje i pokazuje reklame koje su veoma slične sadržaju posećene Internet strane. Adware često šire sami programeri softvera da bi smanjili razvojne troškove, i ponekad dozvoljavaju da se program koristi besplatno ili sa plaćenjem manje cene. Po svojoj prirodi i svrsi Adware zna da bude voema iritantan i da skreće pažnju korisnika od posla koji radi za računarom.

- **Phishing (“pecanje” personalnih podataka)**

Phishing je slično pecanju na jezeru, ali umesto da pokušaja da se ulovi riba, phisher-i pokušavaju da ukradu personalne podatke. Oni šalju e-mail-ove tako da izgledaju da su došli sa nekog legitimnog Web sajta kao što su eBay, PayPal, ili neke

druge bankarske institucije. U e-mail-u se tvrdi da vaše informacije treba da se ažuriraju ili proveriti i traži se od vas da unesete svoje korisničko ime i lozinku, nakon što ste kliknuli na link koji se nalazi u e-mail-u. Neki e-mail-ovi će tražiti da unesete još više informacija, kao što su puno ime, adresa, broj telefona, broj socijalnog osiguranja ili broj kreditne kartice. Naravno, dovoljno je i samo to što ste posetili lažni websajt i uneli svoje korisničko ime i lozinku, pa da phisher može da dobije pristup do više informacija logujući se vašim računom (account-om).

Phishing je prevara koju čine kriminalci da bi prikupili personalne podatke od nesumnjivih korisnika. Lažni e-mailovi česo izgledaju začuđujuće legitimno, čak i Web stranice gde se od vas traži da unesete vaše informacije mogu izgledati realno. Naravno, URL adresa u adresnom polju može vam reći da li je stranica na koju ste upućeni valjana ili ne. Na primer, ako posećujete Web stranicu na eBay, poslednji deo imena domena bi trebalo da bude završen sa "ebay.com." Stoga su <http://www.ebay.com> i <http://cgi3.ebay.com> valjane Web adrese, ali <http://www.ebay.validate-info.com> i " <http://ebay.login123.com> " su lažne adrese, koje se možda koriste od phishera. Ako URL sadrži neku IP adresu, kao što je 12.30.229.107, umesto imena domena možete poprilično biti sigurni da neko pokušava da ulovi (phish) vaše lične podatke.



Slika 8 : Phising web sajt

- **Pharming**

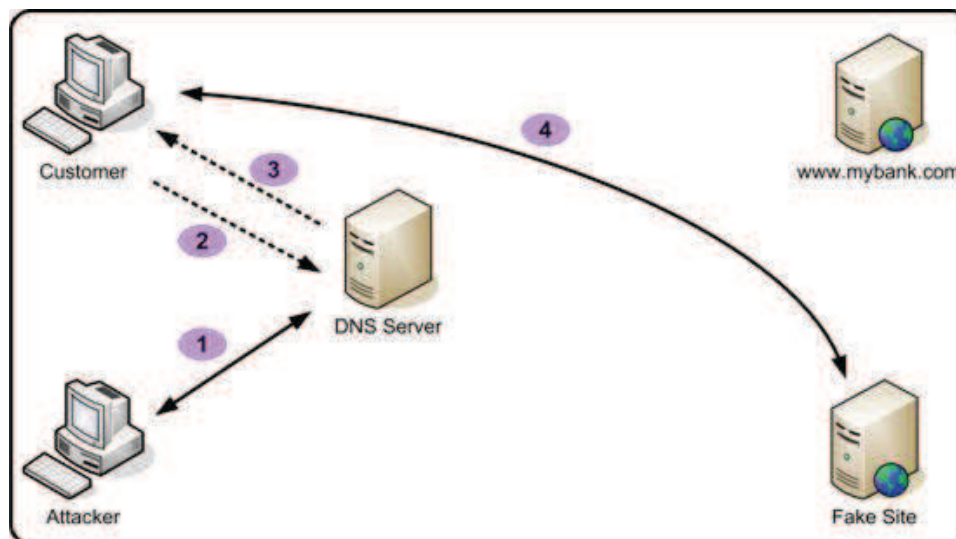
Pharming je još jedan način kojim hakeri pokušavaju da manipulišu korisnicima na Internetu. Dok phishing uzima lične podatke od korisnika upućujući ga na lažni Web sajt, pharming preusmerava korisnika na lažni Web sajt a da on toga i nije svestan.

Web sajtovi obično koriste imena domena za svoje adrese, dok je njihova stvarna lokacija određena IP adresom. Kad korisnik otkuca ime domena u svom Web pretraživaču i pritisne Enter, ime domena se prevodi u neku IP adresu preko DNS servera. Web pretraživač se tada povezuje na server sa tom IP adresom i preuzima podatke sa Web strane. Nakon što korisnik poseti željeni web sajt, DNS ulaz za taj sajt se često pamti u korisnikovom računaru DNS kešu. Na taj način, računar ne mora da pristupi DNS serveru svaki put kad korisnik želi da poseti web sajt.

Jedan od načina da se javi pharming je preko e-maila zarezanog virusom koji otruje korisnički lokalni DNS keš. To se čini tako što se modifikuju DNS ulazi, ili host fajlovi. Na primer umesto IP adrese 17.254.3.183 koja vodi na to www.apple.com, ona može biti promenjena tako da ukazuje na neki drugi web sajt koji je odredio haker. Pharms-i mogu da „otruju“ i neke DNS servere, što znači da će bilo koji korisnik koji koristi taj server biti preusmeren na pogrešan web sajt. Obično većina DNS servera ima mere zaštite kojima se štite od takvih napada. To ne znači da su oni 100% imuni, jer hakeri nastavljaju da nalaze načine da im pristupe.

Pharming može da utiče na više ljudi odjednom. To je pogotovo tačno ako je neki veliki DNS server modifikovan. Ako posetite neki sigurni web sajt i čini vam se da se značajno razlikuje od onog što očekujete, možda ste žrtava pharminga.

Kako računarski kriminal pokriva veoma širok opseg kriminalnih aktivnosti, gornji primeri su samo neki od više hiljada kriminalnih aktivnosti koje spadaju pod računarski kriminal. Kako računari i Internet čine naše živote lakšim na više načina, razumljivo je da ljudi koriste te tehnologije. Zbog toga je pametno zaštititi sebe krišćenjem antivirusnog i softvera za blokadu špijunaže (spyware) i biti pažljiv kod davanja (unosa) svojih ličnih podataka.



Slika 9 : Pharming

Jedan od najpoznatijih oblika računarskog kriminala je krađa identiteta, gde kriminalci koriste Internet da bi ukrali personalne podatke od nekog drugog korisnika Interneta. Dva najpoznatija načina da se to učini su Phishing i Pharming. Obe metode varaju korisnike lažnim web sajtovima (kao da su pravi), tako što se od korisnika traži da unesu personalne podatke. To uključuje informacije kao što su korisničko ime i lozinka, telefonski brojevi, adrese, brojevi platnih kartica, brojevi bankovnih računa i druge informacije koje kriminalci mogu da koriste da bi ukrali identitet neke osobe. Iz tog razloga je pametno uvek proveriti URL ili web adresu sajta, da bi bili sigurni da je taj sajt legitiman, pre nego što se unesu lični podaci.

6.1 Ostali zlonamerni softveri

Scareware (od scare – zaplašiti i ware – programski paket) je lažni bezbedonosni softver, tj. softver koji bi trebalo da bude namenjen u bezbedonosne svrhe, a u praksi korisniku ne nudi ni najmanju bezbednost. Zlonamerni softveri ovog tipa generišu lažne greške i inficirane fajlove, ili pokušavaju da ubede korisnika da kupi njihov proizvod radi "veće" bezbednosti, koja je lažna i netačna. Naziv Scareware se može dodeliti i nekim aplikativnim virusima koji stvaraju paniku kod korisnika zbog otvaranja velikog broja običnih ili pop-up prozora.

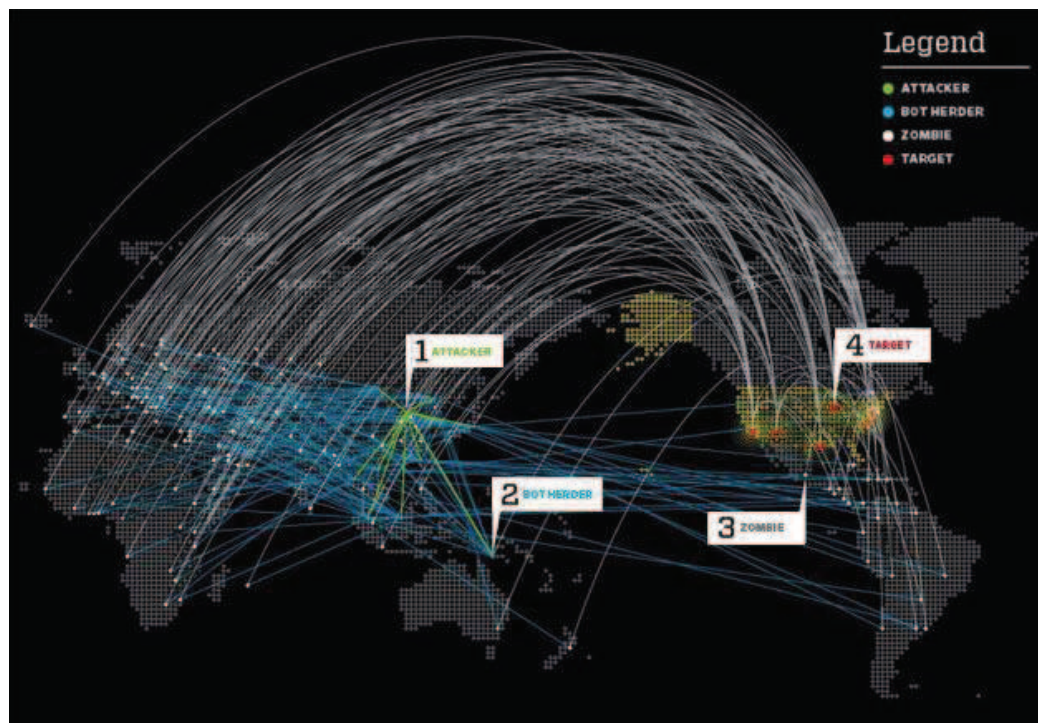
Dialer (komunikator, birač brojeva) je softver koji poziva komercijalne telefonske brojeve sa visokom cenom poziva i nakon toga ostavlja liniju otvorenom, što za posledicu ima veliku potrošnju telefonskih impulsa i samim tim veliki telefonski račun inficiranog korisnika. Samo korisnici sa modemskim pristupom Internetu su izloženi riziku od ovog oblika zlonamernog softvera.

DDoS (*Distributed Denial-of-Service* – distribuirano odbijanje servisa) je sinhronizovani napad sa više računara koji pokušava da ostavi napadnuti računar bez dostupnih resursa zauzimajući mu Internet protok. DDoS napada web sajtove i servise banaka ili kanale za plaćanje preko platnih kartica kombinacijom od nekoliko uzastopnih napada na isti ili različit način. Veliki broj poruka kojima se napadnuti računar zatrpava dovodi do njegovog gašenja i na taj način odbijanja zahteva za servisima svim ostalim legitimnim korisnicima sistema.

Zombi je kompjuter sa pristupom Internetu koji je ugrožen od strane hakera, računarskog virusa ili Trojanca. Ugrožena mašina je samo jedna od mnogih u BotNetu koja se koristi se za obavljanje zlonamernih zadataka jedne ili druge vrste sa udaljene mašine. Mnogi korisnici Zombi računara nemaju saznanje da se njihov računar koristi u ovakve svrhe. Zbog toga što korisnici nisu svesni šta se upozadini dešava, ova vrsta virusa se metaforički naziva Zombi.

- **BotNet**

Jedna od najefikasnijih i najpoželjnijih hakerskih alatki na Internetu jesu BotNet mreže. U pitanju je veći broj računara pod kontrolom botmastera – hakera koji je kreirao i koji kontroliše veliku grupu botova, tj. kompromitovanih PC sistema. Računar korisnika se pretvara u bot, najčešće pomoću trojanca downloadera, koji instalira na sistem poseban softver da bi omogućio botmasteru da sa inficiranim računarom radi šta želi: pokreće DoS (Denial of Service) napade, šalje spam poruke, širi botnet mrežu itd. Mnogi korisnici nisu ni svesni da je njihov računar deo ovakve mreže, a prvi znakovi koji ih alarmiraju obično su usporena Internet konekcija ili bezrazložna opterećenost procesora.



Slika 10 : BotNet

Exploit ("iskorišćavanje") je parče softvera, komad podatka ili niz komandi za iskorišćavanje grešaka, bagova i drugih propusta u cilju da izazovu nepredviđeno i neplanirano ponašanje kompjuterskog softvera, hardvera ili neke manje elektronske naprave. Često mu je namena nasilno sticanje kontrole nad računarskim sistemom ili kreiranje sigurnosnih propusta kako bi zaraženi računar mogao da se uništi DDoS napadima. Mnogi Exploit softveri su dizajnirani tako da omogućavaju nelegalan pristup računarskom sistemu. Međutim, moguće je koristiti više Exploit softvera u nizu, tako da prvi otvori pristup sistemu, a sledeći da polako sve više podrivaju sistem zaobilazeći odbrambene mehanizme sa ciljem da na kraju potpuno preuzmu kontrolu nad sistemom.

Keylogging (od key – taster i logging – logovanje, registrovanje događaja) je prikriveno i nelegalno praćenje tastera koje je korisnik pritisnuo na tastaturi, tako da osoba koja koristi tastaturu nije ni svesna da se njene akcije nadgledaju. Postoje brojne metode koje Keyloggeri koriste, od hardvera i softvera do elektromagnetne i akustičke analize. Isto kao i bilo koji drugi zlonamerni softveri, može da se prenosi kao Trojanac ili kao deo nekog posebnog virusa. Jedan od najbitnijih oblika Spyware-a su Keylogger-i. Oni "sakupljaju" sve što se unosi sa tastature, gde se unosi, preko koje aplikacije, koji

su sve sajтови posećeni, kako izgleda radna površina i sve prikupljene informacije šalju napadaču. To znači da čak iako ne postoje sačuvane razne šifre u obliku fajlova na hard disku, postoji mogućnost da ih napadač preuzme.

Boot virus je virus koji inficira zapise na sektoru koji uobičajeno sadrži zapise koji iniciraju učitavanje operativnog sistema nakon uključivanja računara (boot sector) na floppy disketi ili hard disku i on može samostalno da se replicira sa jednog diska na drugi. Obično se pojavljuje u okviru Boot.ini fajla. Lako se prepoznaje time što računar neće hteti da se uključi ili će antivirusni program stalno prijavljivati da je Boot.ini fajl zaražen.

Hoax (obmana, podvala) je poruka upozorenja za korisnika o pretnji nepostojećeg kompjuterskog virusa. Poruka obično stiže preko cirkularnih elektronskih poruka i sugerise primaocu da prosledi poruku dalje svima koje zna. Većina Hoax virusa su senzacionalistički i lako prepoznatljivi zbog činjenice da oni uvek ukazuju da će virus uraditi skoro nemoguće stvari, kao što su na primer da će sistem eksplodirati i da će se računar zapaliti, ili manje senzacionalni, da će nestati sve sa korisnikovog računara. Hoax virus nije ništa opasniji od neke preteće poruke i sve što treba uraditi je brisanje dobijene poruke.

Scam (prevara) je zavera u pokušaju da se prevari jedna osoba ili grupa osoba sticanjem njihovog poverenja. Žrtva je poznata kao "meta", a varalica ili prevarant je poznat kao "čovek od poverenja". Prevarant iskorišćava ljudske osobine kao što su pohlepa i nepoštenje, ili neka individualna dešavanja u žrtvinom životu. Postoji više vrsta Scam-ova kao što su poruke o dobijanju nagrade na lutriji, donacijama humanitarnim organizacijama i dr.

Macro virusi imaju sposobnost da se sami kopiraju, brišu ili menjaju dokumente na inficiranom računaru. Neke aplikacije dopuštaju makro programima da se prikaže u njihov dokument, tako da bi se program pokrenuo automatski odmah po pokretanju određenog dokumenta, što predstavlja mehanizam kojim se virusi mogu širiti.

Malware dropper (malver "pipeta") je program koji je dizajniran da instalira neku vrstu zlonamernog softvera na određeni računar. Zlonamerni kod može biti ugrađen u dropper na takav način da ga je nemoguće otkriti od strane antivirusnih programa.

Kako računarski kriminal pokriva veoma širok opseg kriminalnih aktivnosti, gornji primeri su samo neki od više hiljada kriminalnih aktivnosti koje spadaju pod narušavanje bezbednosti na Internetu. Kako računari i Internet čine živote ljudi lakšim na više načina, razumljivo je da ljudi koriste te tehnologije. Zbog toga je razumljivo zaštititi se korišćenjem zaštitnog zida (*firewall-a*), antivirusnog i softvera za blokadu špijunaže (*Antispyware*) i biti pažljiv kod davanja (unos) ličnih podataka.

7 Bezbednosni rizici u prenosu podataka

Biznis, društvo i politika u današnjem svetu su toliko isprepleteni jedni sa drugima putem raznih komunikacionih kanala da je lako za potencijalne napadače da načine štetu koju prouzrokuju kroz špijunažu. Problem sa isprepletanim komunikacionim kanalima je složenost koja nastaje pošto su različiti sistemi integrisani jedni sa drugima. Da stvar bude gora, ovi sistemi su više usmereni na performanse a manje na obezbeđivanje zaštite podataka.

Optički kablovi su dobar primer. Vrsta ne-destruktivnih tehnika napada se može koristiti da se protok informacija preko optičkih vlakana prisluškuje bez da iko primeti. U stvari, svaki laptop povezan na mrežu je takođe potencijalna kapija za uljeza, baš kao i svaki razgovor koji se obavlja preko mobilnog telefona može da bude presretnuta. To je čak i lakše da se špijunira na bežičnim mrežama - elektromagnetno polje nosi informacije koje mogu lako da se presretnu. Podjednako je jednostavno da se prisluškuje telefon i faks veze. Sve što je potrebno je kačenje na nezaštićeni komunikacioni kanal ili razvodnu kutiju. To nas dovodi do najvažnijeg nalaza o elektronskom prisluškivanju napada: Ako protivnik dobija fizički pristup u špijunske napade, on je osvojio pola bitke. Ali, postoji i dobra vest. Prave fizičke špijuniranje je teže izvesti, jer je napadač prvo mora da pronađe pravu granu veze. Isto važi i za Internet, to nije tako lako da fizički pristupe kao ljudi često pretpostavljaju. Optički kablovi su često pod zemljom ili ispod vodenih površina.

Bezbednosna rešenja su bazirana na više linija odbrana. Najvažnije kriptografske linije odbrane su:

- **Simetrična enkripcija** proces obezbeđuje punu poverljivost primenjenih algoritama i efikasno blokira čak brute force napade.

- **Individualni algoritmi** kreirani od strane kompanije nepoznate bilo kojem drugom kupcu.
- **Autonomno profilisanje algoritama**, algoritam je poznat samo kupcu (čak Crypto AG kao isporučilac više nema korisne informacije o tome).
- **Hardversko šifrovanje** je preduslov za maksimalnu kriptografsku varijabilnost za šifrovanje. To takođe obezbeđuje kriptografsko odvajanje procesa šifrovanja iz mreže i ne zahteva «poznat» operativni sistem (otporan na viruse).
- **Kripto bezbednosna arhitektura** omogućava pun potencijal kriptografije da podrži svoju bezbednosnu politiku.
- **Fleksibilni sistem za upravljanje** bezbednošću je alat za pojednostavljenje upotrebe celokupnog sistema. To olakšava bezbedan, pouzdan monitoring i promenu svih kriptografskih parametara ili direktno povezivanje opreme preko mreže.

Da bi razumeli metode kriptografske zaštite potrebno je poznavati i njene elemente.

8 Kriptografija

Kriptografija je nauka koja se bavi metodima očuvanja tajnosti informacija. Kada se lične, finansijske, vojne ili informacije državne bezbednosti prenose sa mesta na mesto, one postaju ranjive na prisluškivačke taktike. Ovakvi problemi se mogu izbeći kriptovanjem (šifrovanjem) informacija koje ih čini nedostupnim neželjenoj strani.

Šifra i digitalni potpis su kriptografske tehnike koje se koriste da bi se implementirali bezbednosni servisi. Osnovni element koji se koristi naziva se šifarski sistem ili algoritam šifrovanja. Svaki šifarski sistem obuhvata par transformacija podataka, koje se nazivaju šifrovanje i dešifrovanje. Šifrovanje je procedura koja transformiše originalnu informaciju (otvoreni tekst) u šifrovane podatke (šifrat).

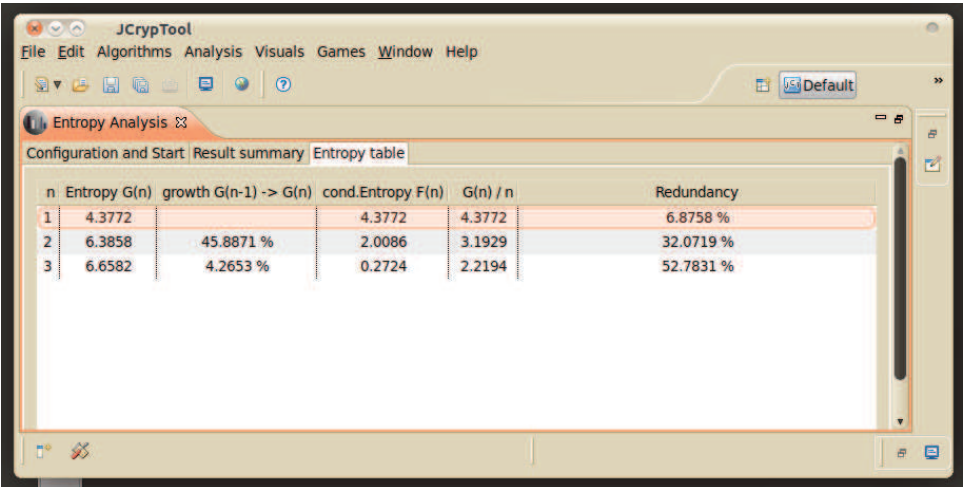
Obrnut proces, dešifrovanje, rekonstruiše otvoreni tekst na osnovu šifrata. Prilikom šifrovanja, pored otvorenog teksta, koristi se jedna nezavisna vrednost koja se naziva ključ šifrovanja. Slično, transformacija za dešifrovanje koristi ključ dešifrovanja.

Broj simbola koji predstavljaju ključ (dužina ključa) zavisi od šifarskog sistema i predstavlja jedan od parametara sigurnosti tog sistema.



Slika 11 : Enigma u saobraćajnom muzeju u Lucernu, Švajcarska

Kriptoanaliza je nauka koja se bavi razbijanjem šifri, odnosno otkrivanjem sadržaja otvorenog teksta na osnovu šifrata, a bez poznavanja ključa. U širem smislu, kriptoanaliza obuhvata i proučavanje slabosti kriptografskih elemenata, kao što su, na primer, heš funkcije ili protokoli autentifikacije. Različite tehnike kriptoanalize nazivaju se napadi.



The screenshot shows the 'Entropy Analysis' window of JCryptTool. It displays a table with the following data:

n	Entropy G(n)	growth G(n-1) -> G(n)	cond.Entropy F(n)	G(n) / n	Redundancy
1	4.3772		4.3772	4.3772	6.8758 %
2	6.3858	45.8871 %	2.0086	3.1929	32.0719 %
3	6.6582	4.2653 %	0.2724	2.2194	52.7831 %

Slika 12: Kriptoanaliza

Prilikom šifrovanja, pored otvorenog teksta, koristi se jedna nezavisna vrednost koja se naziva ključ šifrovanja. Slično, transformacija za dešifrovanje koristi ključ dešifrovanja. Broj simbola koji predstavljaju ključ (dužina ključa) zavisi od šifarskog sistema i predstavlja jedan od parametara sigurnosti tog sistema.

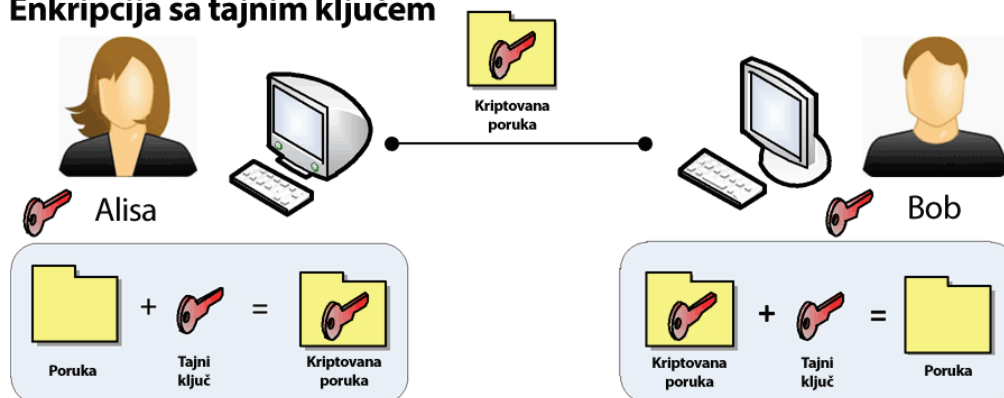
Kriptografija mora da obezbedi sledeće:

- Integritet ili verodostojnost informacija koje se šifruju (engl. Data integrity) se brine o tome da ne dođe do neovlašćene promene informacija, kao što su menjanje informacije, brisanje informacije i zamena informacije. Da bi se osigurala verodostojnost, mora postojati način provere da li je informacija promenjena od strane neovlašćene osobe.
- Tajnost (engl. Confidentiality) informacija osigurava da je sadržaj informacije dostupan samo ovlašćenim osobama odnosno samo onim koji poseduju ključ. Postoje brojni načini zaštite tajnosti, počev od fizičke zaštite do matematičkih algoritama koji skrivaju podatke.
- Provera identiteta (engl. Autentification) korisnici koji počinju komunikaciju se trebaju prvo predstaviti jedan drugome pa tek onda počinju sa razmenom informacija.
- Nemogućnost izbegavanja odgovornosti (engl: Non-repudiation) je vrlo važna stavka, pogotovo u novije vreme kada se veliki deo novčanih transakcija obavlja putem interneta.

8.1 Simetrična kriptografija

Kod simetričnog šifrovanja koristi se isti ključ i za šifrovanje i za dešifrovanje. Baš zbog toga i sigurnost algoritama ovakvog šifrovanja je velika. Bitan faktor je i brzina - simetrično šifrovanje je veoma brzo. Pored svih prednosti koje ima na polju sigurnosti i brzine algoritma, postoji i jedan veliki nedostatak. Kako preneti tajni ključ? Problem je u tome, što ako se tajni ključ presretne, poruka se može pročitati. Zato se ovaj tip šifrovanja se najčešće koristi prilikom zaštite podataka koje ne delimo sa drugima (šifru znate samo vi i nju nije potrebno slati drugome).

Enkripcija sa tajnim ključem



Slika 13 : Razmena podataka simetričnim ključem

Klod Šenon je definisao uslove savršene tajnosti, polazeći od sledećih osnovnih pretpostavki:

- Tajni ključ se koristi samo jednom.
- Kriptoanalitičar ima pristup samo kriptogramu.

Šifarski sistem ispunjava uslove savršene tajnosti ako je otvoreni tekst X statistički nezavisan od kriptograma Y , što se može matematički izraziti na sledeći način:

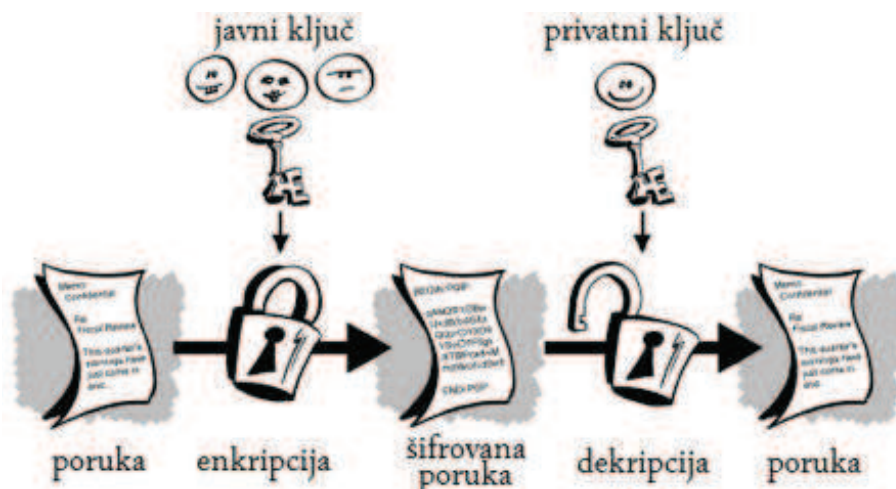
$$P(X=x|Y=y) = P(X=x)$$

Za sve moguće otvorene tekstove $x=(x_1, x_2, \dots, x_m)$ i sve moguće kriptograme $y=(y_1, y_2, \dots, y_n)$; drugim rečima, verovatnoća da slučajna promenljiva X ima vrednost x jednaka je sa ili bez poznavanja vrednosti slučajne promenljive Y . Zbog toga kriptanalitičar ne može bolje proceniti vrednost X poznavajući vrednost Y od procene bez njenog poznavanja, nezavisno od raspoloživog vremena i računarskih resursa kojima raspolaže. Koristeći pojam entropije iz teorije informacija, Šenon je odredio minimalnu veličinu ključa potrebnu da bi bili ispunjeni uslovi savršene tajnosti. dužina ključa K mora biti najmanje jednaka dužini otvorenog teksta M :

$$K \geq M$$

8.2 Asimetrična kriptografija

Za razliku od simetrične kriptografije, asimetrična koristi dva ključa — javni i privatni. Princip je sledeći: u isto vreme se prave privatni i odgovarajući javni ključ. Javni ključ se daje osobama koje šalju šifrovane podatke. Pomoću njega te osobe šifruju poruku koju žele da pošalju. Kada primalac dobije šifrat, dešifruje ga pomoću svog privatnog ključa. Na taj način svaki primalac ima svoj privatni ključ a javni se može dati bilo kome, pošto se on koristi samo za šifrovanje, a ne i dešifrovanje.



Slika 14 : Razmena fajla asimetričnim ključevima

Prednost ovog načina šifrovanja je u tome što ne mora da se brine o slučaju da neko presretne javni ključ, jer pomoću njega može samo da šifruje podatke. Takođe, programi sa ovakvim načinom šifrovanja imaju opciju da potpisuju elektronske dokumente.

8.3 Sekvencijalni šifarski sistemi

Kao najosnovnijim simetričnim algoritmima, dovoljno je samo reći da se oni zasnivaju na svojstvu logičke operacije xor (engl. exclusive or — ekskluzivno ili) za koju vazi:

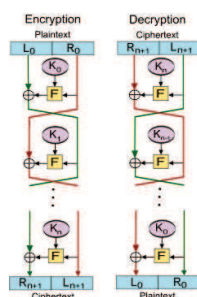
$$(X \text{ xor } Y) \text{ xor } Y = X, X, Y \in (0,1)$$

Naime, možemo zamisliti da nam je X jedan bit originalne poruke a Y bit ključa. Tada $(X \text{ xor } Y)=Z$ predstavlja jedan bit šifrata koji putuje javnim kanalima i koji neko može prisluškivati, dok je $Z \text{ xor } Y$ originalni bit X koji se dobija xor-ovanjem bita kodirane poruke sa bitom ključa. Definišimo još operaciju xor za proizvoljnu dužinu bita tj. bajtova i tada X , odnosno Y možemo smatrati bajtom, rečju odnosno porukom U praksi se često koriste generatori pseudo slučajnih nizova (engl. PRNG – Pseudo Random Number Generator), koji predstavljaju determinističke algoritme za šifrovanje, ali nizovi simbola koje oni generišu imaju osobine slične slučajnim nizovima. Generatori pseudoslučajnih nizova koriste kratke ključeve radi započinjanja procesa generisanja. Ovi ključevi moraju biti prisutni na obe strane pre početka komuniciranja. Izlazni niz iz generatora se sabira po modulu 2 sa nizom otvorenog teksta i na taj način se dobija niz šifrata. Na prijemnoj strani se sabira primljeni niz šifrata sa pseudoslučajnim nizom generisanim pomoću istog ključa, počevši od istog početnog simbola kao i na predajnoj strani. Na taj način je prijemnik u stanju da rekonstruiše otvoreni tekst. Jasno je da dokle god se slučajni nizovi dobijaju pomoću bilo kog algoritma oni mogu biti samo pseudoslučajni i kao takvi postaju mamac za sve one koji se bave razbijanjem šifri. Pseudoslučajni nizovi su periodični u širem smislu (što znači da mogu imati aperiodični početak), ali ako su periodi takvih nizova mnogo veći od dužina nizova otvorenog teksta, sistem će se ponašati na sličan način kao i Vernamova šifra. Osnovna ideja koja

stoji iza sekvencijalnih šifara je da se generiše duga i nepredvidljiva sekvenca simbola iz nekog alfabeta (npr. binarnog) na osnovu kratkog ključa izabranog na slučajan način. Sekvencijalna šifra sa generatorom pseudoslučajnog niza je aproksimacija Vernamove šifre, i utoliko je bolja ukoliko je pseudoslučajni niz bliži po karakteristikama pravom slučajnom nizu.

8.4 Blok šifra

Blok šifrom se nazivaju oni algoritmi kod kojih se originalna poruka šifrue po grupama (blokovima) od dva i više elemenata. Najpoznatiji algoritmi blok šifara su: LUCIFER, DES, FEAL, IDEA, RC5, SKIPJACK, BLOWFISH, TWOFISH, AES (RIJNDAEL) i drugi.



Slika 15 : AES

Danas se najčeće koristi AES.

AES (engl. Advanced Encryption Standard, napredni standard za šifrovanje) je specifikacija za šifrovanje elektronskih podataka. Usvojen je od strane Vlade SAD i koristi se širom sveta. AES je zamenio prethodno korišćeni standard DES. AES je algoritam simetričnog ključa, što znači da se isti ključ koristi i za enkripciju i za dekripciju podataka.

U Sjedinjenim Državama, AES je najavio Nacionalni institut za standarde i tehnologiju (NIST) kao Savezni standard za obradu informacija (engl. FIPS) PUB 197 (FIPS 197) 26. novembra, 2001. nakon petogodišnjeg procesa standardizacije tokom koga je petnaest konkurentskih nacrtā ocenjivano i odabran je najprimereniji. Stupio je na snagu kao standard Savezne vlade SAD 26. maja, 2002. nakon odobrenja od strane Komesara za trgovinu. Dostupan je u mnogim različitim paketima enkripcije. AES je

prva javno dostupna i otvorena šifra koju je Državna bezbednosna agencija (NSA) odobrila za zaštitu tajnih podataka.

Prvobitno nazvanu Rijndael, šifru su razvila dva belgijska kriptografa, Joan Dajmen i Vinsent Rejmen, i oni su je predali u postupak izbora za AES. Ime Rijndael je igra reči bazirana na imenima izumitelja.

9 Network Security

Sve industrije zavise od sposobnosti prenosa i prijema podataka pouzdanim kanalima sve većim brzinama. Lak brz pristup informacijama glavni je kriterijum performansi u današnjim komunikacijama. Data autoputevi čine kičmu svih komunikacija. Hiljadama novih širokopojasnih priključaka širom sveta tržište raste svaki dan. Na primer, svaki laptop ili PDA uređaj sada mogu komunicirati preko širokopojasnih mreža. Prenos poslovnih video konferencija, prenos radarskih slika ili e-government sistema je svakim danom u upotrebi. Sve ove aplikacije generišu ogromnu količinu podataka kojina kraju moraju da se prenose preko mreže. Podaci se transportuju kroz nezaštićene mreže (Wide Area Network -WAN), jer kapacitet prenosa i brzina su glavni prioriteti u toj mreži.

Bezbednost informacija utiče na celokupno društvo. Umrežavanje raste skoro eksplozivnim tempom u javnosti, vlasti i u poslovnom svetu. Glavna briga je kako osigurati zaštitu infrastrukturu jer ona je često izložena tehničkim napadima. Pored toga, sav prenos informacija tehnologijama, uključujući i optičke linkove, su laki za napde. Postoji takođe i rizik od nepravilnog rukovanja, nepravilnog korišćenja a i nemar.

Informacije koje cirkulišu mrežama predsedničkih kancelarija, vladinih ministarstava, odbrane i policijske organizacije ili velikih preduzeća su veoma osetljive. Bezbednost informacija koje koriste širokopojasne komunikacije je egzistencijalno važno. Informacije preko širokopojasne mreže treba da budu zaštićene od neovlašćenog pristupa. Postoji samo jedan pouzdan način da to urade, naime šifrovanje svih podataka koje se prenose.

9.1 Primeri veza

Mrežni operateri nude izbor nekoliko transportnih protokola promenljivih performansi u cilju da zadovolji veoma individualne potrebe korisnika. Svaka tehnologija ima svoje prednosti i zadovoljava različite potrebe. Širokopojasna komunikacija se zasniva na transportnom mediju optičkih vlakana, mikrotalasnima, bakarnim i satelitskim vezama.

- **Bakarni kabl (ADSL, iznajmljena linija)**

Bakar je klasičan medij za prenos glasa podataka i informacija. Bakarni kablovi takođe povezuju korisnike koji su daleko geografski. Uspostavljaju fiksne veze praktično preko javnog provajdera mreže. Bakar je testirani medij srednje transmisije, lak za postavljanje, pouzdan i ekonomičan u funkciji.

- **Optički kabl**

Optičko vlakno prenosi signale, optički koherentnu svetlost. Drugim rečima, električni signali moraju biti konvertovani u optičke signale pre prenosa. Svako vlakno može postići ogroman propusni opseg za prenos svetlosti, istovremeno koristeći različite talasne dužine. Optički kabl je imun na elektromagnetne impulse.

- **Mikrotalasni prenos**

Mikrotalasni linkovi su posebno pogodni za komunikaciju na teškom terenu (planine, pustinje). Kao medijne zahtevaju pravi put nad zemljištem i minimalno je održavanje. Mikrotalasni prenos je brzo dostupan i nudi relativno veliki propusni opseg. Mikrotalasne stanice se lako transportuju i mogu brzo biti puštene u rad na otvorenom terenu ili na zgradama, na primer, lokalnih događaja (konferencije, upravljanje krizama, itd) ili taktičke misije koje sprovede oružane snage.

- **Satelitska veza (SatCom)**

Satelitska veza može biti uspostavljena sa jednom ili više sekvencijalnim vezama bilo koje udaljenosti. To je efikasno rešenje bilo za stacionarne primene (npr. preko teško dostupnog terena) ili privremenog raspoređivanja na vojnih snaga bez odgovarajuće infrastrukture. Sateliti su danas postigli praktično kompletnu geografsku pokrivenost i veoma visoku tehničku dostupnost.

9.2 Rasprostranjene tehnologije / protokoli

- **Ethernet**

Ethernet je prvobitno napravljen za lokalne mreže, ovaj protokol je dalje razvijan i danas se koristi u globalnim mrežama za razmenu podataka. Ethernet standard igra ključnu ulogu u end-to-end umrežavanju. Ethernet je čest izbor protokola bez obzira da li se podaci transportuju u lokalnoj mreži (LAN), preko optičkih vlakana u gradskoj mreži (MAN) ili na velikim udaljenostima u širokom prostoru. Ovaj vid umrežavanja evidentno danas ima široke primene.

- **SONET / SDH**

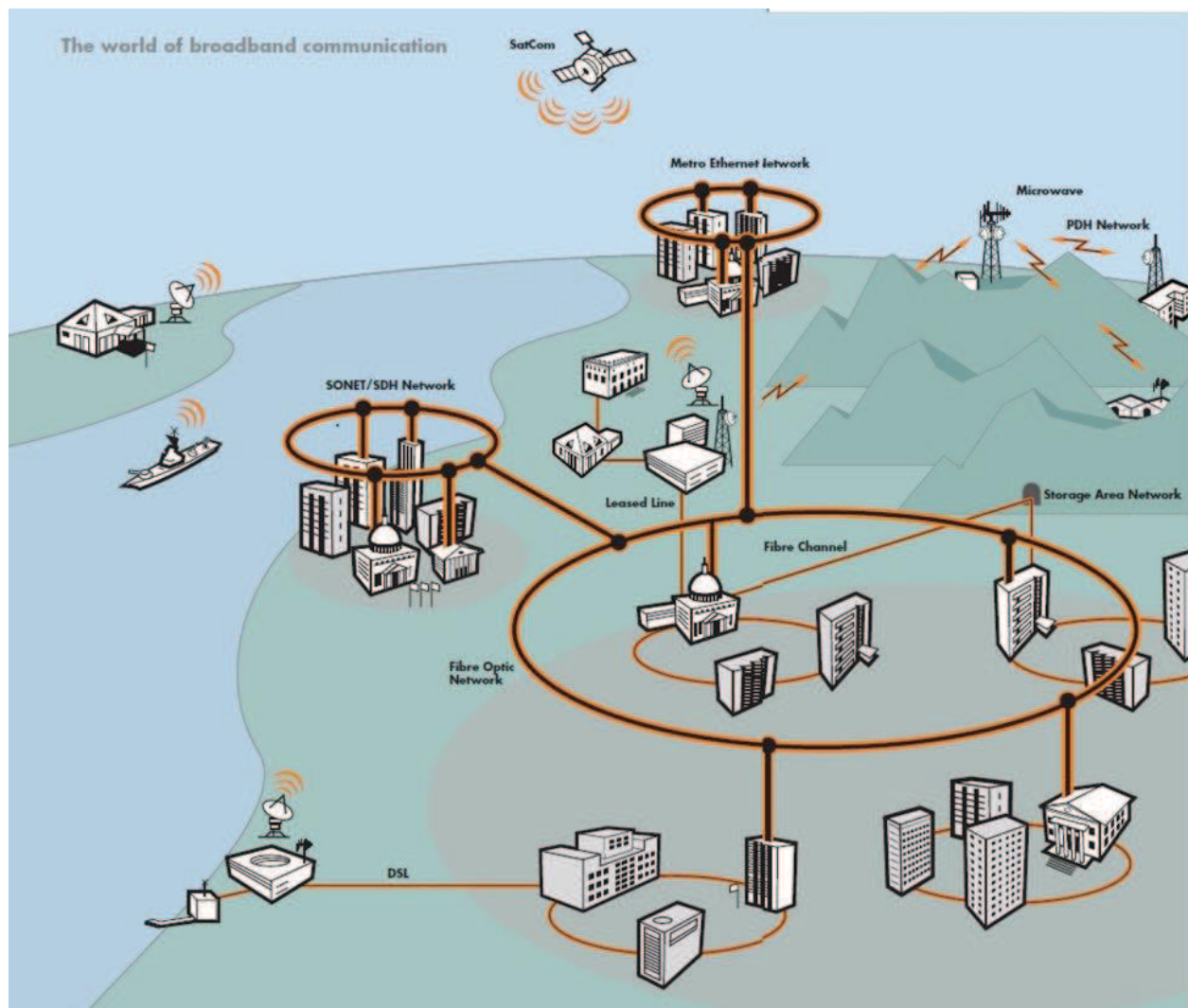
SDH ("Synchronous Digital Hierarchy") je idealna je za velike brzine transporta velikih količina podataka, obično preko optičkih vlakana. Visoka stopa sinhronizacije prenosa čini jednostavnim za upravljanje tokova podataka i visok kvalitet usluga. Logički linkovi se postavljaju između mreže pretplatnika. SONET / SDH mreža se sastoji od čvorova. Prenos podataka je standardizovan, olakšavajući transport najraznovrsnijih tipova podataka (glas, podaci i video) preko centralne i end-to-end mreže, SONET / SDH mreže takođe imaju mnoge prednosti što se tiče otkrivanja grešaka i izveštavanja. Mreža za upravljanje je jednostavna, centralizovana i polu-automatska (prema zadatim kriterijumima). To znači da kvalitet usluga (QoS) može biti usmeren na potrebe korisnika. Ako mrežni čvor ili optičko vlakno ne uspeju da uspostave vezu, SONET / SDH mrežne komponente mogu automatski preusmeriti tokove podataka u nekoliko milisekundi do paralelnog puta bez ugrožavanja funkcionalnosti aplikacije.

- **PDH**

PDH ("Plesiochronous Digital Hierarchy") je godinama pokušavan da se koristi za transport protokola srednje distance. PDH ("Plesiochronous Digital Hierarchy") je, standardizovana tehnika za prenos i multipleksiranje podataka. PDH može da se koristi u vezi sa tehnologijama, npr bakarne linije, mikrotalasne linkove ili satelitske veze. Crypto AG ima PDH rešenja nastavi će da razvijaju ovu tehnologiju u budućnosti.

- **Fibre Channel**

FC je moderan transportni protokol razvijen posebno za mreže za skladištenje podataka (SAN) sposoban da obezbedi visoke performance veze od tačke do tačke. Ovi linkovi obično povezuju računarski centar sa disaster-recovery centrom.



Slika 16 : Prikaz mreža i tehnologija

Da bi se ostvarila sveukupna zaštita u komunikaciji potrebno je sagledati telekomunikacione resurse koji se koriste i na taj način isprojektovati i primeniti zaštitne mehanizme od raznih vrsta napada i prisluškivanja saobraćaja. Da bi se postigao najviši sepen zaštite potrebno je koristiti sve dostupne tehnologije, ali samo tehnologija neće rešiti problem. Organizaciona politika i pravilne procedure su veoma bitne kako tehnologija ne bi bila zloupotrebljena. Da bi se ostvarila zaštita podataka koji se prenose koriste se različiti mehanizmi kao što su poverljivost, integritet, dostupnost, zaštita od neovlašćenog korišćenja.

U komunikacionim procesima i razmeni poverljivih podataka sagledavanje mogućih pretnji i napada su veoma bitan faktor planiranja, a najčešće pretnje mogu biti: infiltracija u sistem, prekoračenje ovlašćenja, suplantacija, prisluškivanje, promena podataka u komunikacionoj liniji, odbijanje servisa, poricanje transakcije i mnogi drugi.

Sagledavši sve elemente u poslovanju, razmeni podataka i komunikacionim kanalima postoje kompanije kao što su Crypto AG i Mils Electronic koje su osmislile rešenja koje se ogledavaju u korišćenju specijalizovanih uređaja i softvera koje omogućavaju da se problem zaštite podataka dovede na nivo najviše sigurnosti. Pored hardveskih modula koji su otporni na parazitna zračenja postoje i jaki sistemi autentifikacije i šifrovanja. U procesu šifrovanja se mogu koristiti standardni algoritmi kao i posebno napravljeni i prilagođeni za upotrebu koja situacija nalaže.



Slika 17: Crypto AG i Mils Electronic

10 Crypto AG

Inženjer i pionir kriptologije Boris Hegelin osnovao je Crypto AG u Zugu u 1952. Napustio je svoju rodnu Švedsku i krenuo put neutralne Švajcarske da izgradi preduzeće za proizvodnju i prodaju šifrarskih sistema. C-52 je bila prva mašina u potpunosti proizvedena u Švajcarskoj i uživala veliki uspeh na tržištu. To je napredak u odnosu na C-36, koji je Boris Hegelin već prodao pre drugog svetskog rata mnogim državama, američkoj vojsci, a pod licencom (tip M-209).

Bezbednosna rešenja iz Crypto AG su bazirana na više linija odbrane. Crypto AG garantuje sigurnost od napada najjačim mogućim merama bezbednosti.

Crypto AG u svom proizvodnom programu nudi rešenja različitih kategorija po vrsti namene:

IT Security

- ✓ Crypto IP VPN

Office Security

- ✓ Voice
- ✓ Fax
- ✓ File & Messaging
- ✓ Platforms
- ✓ Remote AccessOn the move

Network Security

- ✓ Storage Security
- ✓ Ethernet
- ✓ SONET/SDH
- ✓ PDH

Radio Security

- ✓ MultiCom

- ✓ Mcom Messenger

- ✓ Mid Rate Coder

- ✓ RC Unit

- ✓ RC Software

- ✓ EPM/SECOS

- ✓ Line of sight

Satellite Security

- ✓ VSAT

- ✓ Inmarsat

- ✓ Deployable SAT

Security Management

- ✓ IP VPN

- ✓ Brodband

- ✓ MultiCom Radio

Portfolio CRYPTO AG rešenja pokrivaju sve uobičajene medije, mrežne tehnologije i transport protokola. Oni u pogledu performansi variraju, tako da odabrana verzija može biti korišćena za određenu specifičnu upotrebu. Uz kupovinu sistema, svaki kupac dobija svoj tajni algoritam koje korisnik može menjati u bilo koje vreme i na taj način ga personalizovati. Šifrovanje je sprovedeno u zaštićenom hardverskom modulu i potpunosti je zaštićen od javne mreže. Kao rezultat toga, bezbednosni podaci nikada nisu podložni napadu. Moderan, robustan dizajn je veoma pouzdan u radu čak i pod ekstremnim klimatskim uslovima. Posebna znanja za instalaciju nisu neophodna. Šifrovanje se sprovodi upozadini potpuno automatski.

Security management je centralni element pouzdane politike poslovanja i razmena podataka. To omogućava kupcu da definiše algoritme, ključeve, lozinke i druga sigurnosna podešavanja u skladu sa svojom politikom bezbednosti i daprte njihovu efikasnost. Redovna promena kriptografskih ključeva treba da bude jednostavna za

konfigurisanje kao i da postoji opcija pokretanja u automatski režim dok su jedinice za šifrovanje u funkciji. Crypto AG omogućava sve ovo sa svojim SMC-1100 Security Management centrom. SMC-1100 je izuzetno jednostavna platforma za rad i nudi visok stepen bezbednosti za definisanje, upravljanje i distribuciju bezbednosnih podataka. Intuitivno Windows grafičko okruženje čini posao menadžera bezbednosne politike jednostavnijim. Omogućava da prikaže šifrovanje sistema jednostavno i jasno tako da sva podešavanja iza sve jedinice može da konfigurišena jednom mestu. Poruke menadžmenta se distribuiraju u jedinice u šifrovanom obliku online preko Ethernet veze ili putem smart kartica. Online distribucija je pod kontrolom tako da se operacije mogu sprovesti bez prisustva osoblja.

11 Mils Electronic

Kompanija „Mils electronic“ je osnovana 1946. godine u Trieru u Nemačkoj. Na samom početku zadatak je bio razvoj šifrarskog sistema koji bio pružio najviši stepen zaštite. 6723 rupičasti perforator hartije za generisanje ključeva je bio prvi uređaj spreman za tržište 1946.godine

Mils electronic je jedan od vodećih kompanija na polju telekomunikacija i zaštiti informacija. Više od 60 godina tehnološka rešenja pružaju besprekorne rezultate u zaštiti telekomunikacionih kanala. Tokom godina tehnološka rešenja su napredovala i prilagođavala se uslovima i tehnologijama telekomunikacija. Danas javne agencije, vojne ustanove, komercijalne ustanove i kompanije u preko 50 zemalja širom sveta su izabrale i koriste tehnološka rešenja kompanije „Mils electronic“. Oblasti delovanja u polju sigurnosti su:

- Sigurna razmena fajlova
- E-mail zaštita
- Virtuelne privatne mreže (VPN)
- Oprema za generisanje i distribuciju ključeva

Kao vrhunac neprobojnosti ključeva, u sistem je integrisan One Time pad metod generisanja i razmene kriptografskih ključeva.

Reputacija „Mils elecotronic“ kompanije se zasniva na sledećim principima:

- Optimalna rešenja
- ISO 9001 standard
- Najviši nivo zaštite
- Custom rešenja za korisnika
- Tehička podrška
- Vrhunska stručnost osoblja

Mils electronic pruža „state of art“ tehnološka rešenja i softvere, a to su:

- Secure messaging
- Secure file exchange
- E-mail security
- VPN security
- Key factory



Slika 18 : Lista proizvoda Mils electronic

12 Generisanje i distribucija kriptoloških ključeva

Upravljanje kriptološkim ključevima je jedan od najbitnijih zadataka u savremenoj kriptografiji. Iako ovi algoritmi počivaju na obimnim akademskim istraživanjima sam proces 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 pre 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.

Jedan od uslova za uspešnu primenu bezbednosnog modela predstavlja i njegova jednostavnost upotrebe. Model implementacije bezbednosnog rešenja komunikacionog kanala obezbeđuje odličan metod za zaštitu osjetljivih podataka koji se prenose od predajne do prijemne strane. Uslozňjavanjem modela dovodi se do pada nivoa performansi kao i otežavanjem konkretne upotrebe predloženog sigurnosnog rešenja.

Upravljanje ključevima se bavi sigurnim generisanjem, distribucijom i čuvanjem ključeva. 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 reč 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.

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. Kako su algoritmi javno dostupni, način izbora početnih uslova mora ostati tajna. 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.

U ovom radu analiziran je sistema za razmenu kriptoloških ključeva, a to je Diffie-Hellman metoda.

Šemu je prvi put objavio Whitfield Diffie i Martin Hellman u 1976. Godine. Difi-Helman metoda je specifičan način razmene ključeva. Difi-Helman razmena ključeva omogućuje da dve stranke koje nemaju prethodno znanje jedni od drugima uspostave zajednički tajni ključ preko nesigurnog komunikacijskog kanala. Ova metoda se onda može koristiti za šifrovanje naknadne komunikacije korištenjem simetričnog ključa.

Primer:

Alice i Bob pristaju na korištenje prostog broja $p = 23$ i baza $g = 5$.

Alisa odabire tajni celi broj $a = 6$, a zatim šalje Bobu $A = g^a \bmod p$

$$A = 5^6 \bmod 23$$

$$A = 15625 \bmod 23$$

$$A = 8$$

Bob odabire tajni celi broj $B = 15$, a zatim šalje Alisi $B = g^b \bmod p$

$$B = 5^{15} \bmod 23$$

$$B = 30517578125 \bmod 23$$

$$B = 19$$

Alisa računa $s = B^a \bmod p$

$$s = 19^6 \bmod 23$$

$$s = 47045881 \bmod 23$$

$$s = 2$$

Bob računa $s = A^b \bmod p$

$$s = 8^{15} \bmod 23$$

$$s = 35184372088832 \bmod 23$$

$$s = 2$$

Alisa i Bob sada dele tajnu $s = 2$. Ovo je zato što je $6 \cdot 15$ isto koliko i $15 \cdot 6$. Dakle, neko ko je poznavao oba privatna tajna broja može da izračuna s na sledeći način:

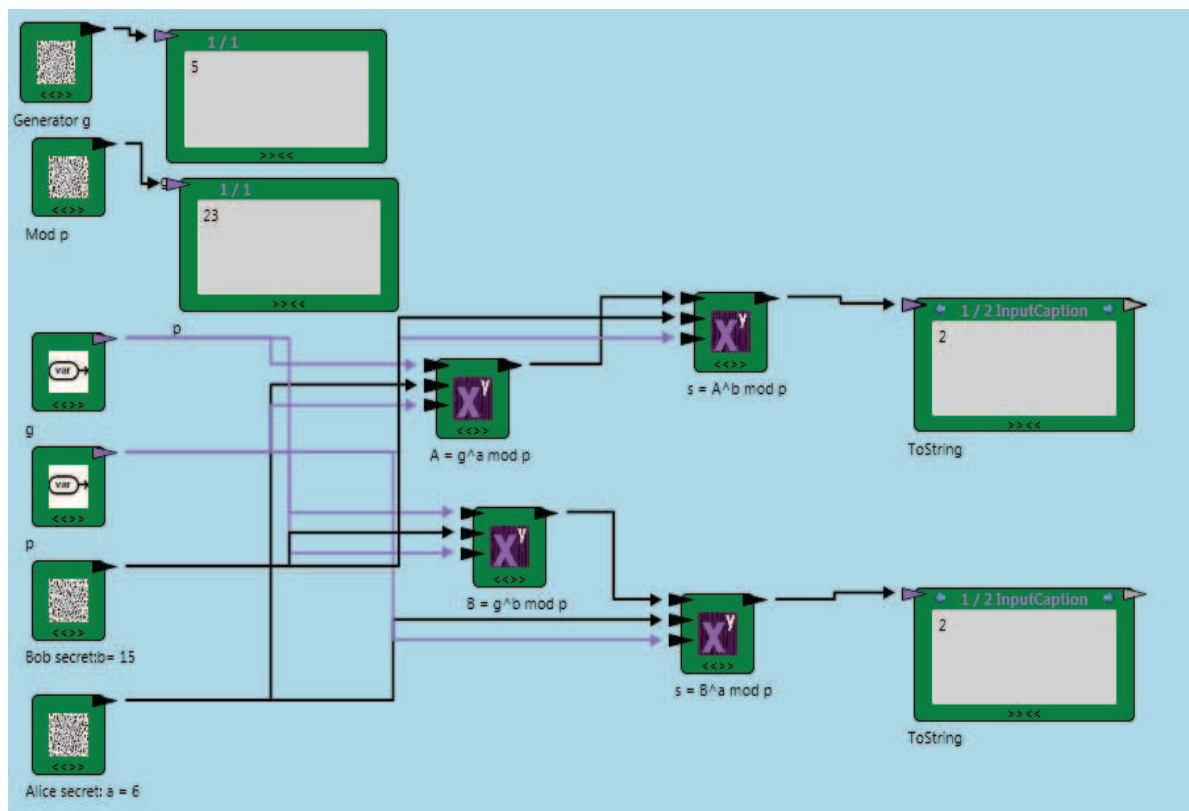
$$s = 5^{6 \cdot 15} \bmod 23$$

$$s = 5^{15 \cdot 6} \bmod 23$$

$$s = 5^{90} \bmod 23$$

$$s = 807.783.566.946.316.088.741.610.050.849.573.099.185.363.389.551.639.556.884.765.625 \bmod 23$$

$$s = 2$$



Slika 19: Simulacija izračunavanja ključeva u crpyto tool-u

13 Rešenja višeslojne zaštite

U cilju optimalne odbrane informacionih sistema i savremenih računarskih mreža od potencijalnih opasnosti i raznovrsnih napada kojima se ugrožavaju različiti servisi i resursi, predlaže se arhitektura sistema zaštite koja se sastoji od mehanizama zaštite primenjenih na tri nezavisna bezbednosna nivoa koji su namenjeni za odbranu odrazličitih tipova napada. Ovi nivoi su projektovani da minimizuju i ograniče moguću štetu tako što eventualno ugrožavanje jednog nivoa ne može kompromitovati ostale bezbednosne nivoe arhitekture sistema zaštite. U tom smislu, mehanizmi zaštite informacionog sistema mogu da se sastoje od primenjenih mehanizama na sledeća tri nivoa:

- Zaštita "s kraja na kraj" (end-to-end security) na aplikativnom nivou koja se zasniva na primeni tehnologije digitalnog potpisa na bazi asimetričnih kriptografskih algoritama i zaštite tajnosti podataka primenom simetričnih kriptografskih algoritama. Primenom ovog nivoa zaštite globalno se obezbeđuje:
 - ✓ provera autentičnosti korisnika servisa kako u smislu komunikacije (end-user authentication) tako i (opciono) u smislu kontrole pristupa mreži (access control),
 - ✓ zaštita integriteta podataka koji se prenose,
 - ✓ zaštita od mogućnosti naknadnog poricanja odgovornosti za poslate podatke i
 - ✓ zaštita tajnosti podataka
- Zaštita na transportnom nivou predstavlja zaštitu tajnosti podataka primenom simetričnih kriptografskih algoritama i autentikacije čvorova komunikacionog segmenta mreže na transportnom nivou. Ovaj nivo štiti mrežu od eksternih napada primenom kriptografskih tunela (zaštićenih sesija) između čvorišta komunikacionog segmenta mreže na transportnom nivou na bazi simetričnih kriptografskih sistema i primenom procedure jake autentikacije između čvorišta mreže čime se obezbeđuje provera autentičnosti strana u komunikaciji.
- Zaštita na mrežnom IP nivou obezbeđuje kriptografsku i logičku zaštitu na nivou IP paketa koji se razmenjuju između mrežnih čvorova i štiti čitavu mrežu od eksternih napada korišćenjem zaštitnih mehanizama koje pruža standardna komunikaciona oprema. Ova zaštita se bazira na ostvarivanju kriptografskih tunela na IP nivou na bazi IPSec protokola zaštite putem koga se ostvaruju Virtuelne Privatne Mreže (VPN – Virtual Private Network)

Sušтина predloga primene višeslojne arhitekture zaštite je u preporuci korišćenja kombinovanih mehanizama zaštite na više različitih nivoa ISO/OSI modela. Dakle, ukoliko nije moguće koristiti mehanizme na svim nivoima, kao minimalna arhitektura, predlaže se primena kombinacije mehanizama na dva nivoa, i to:

- Zaštita na aplikativnom nivou (kao obavezna) i
- Dodatna zaštita na transportnom ili mrežnom nivou.

Na taj način, sistem se brani kako od internih (aplikativna zaštita) tako i od eksternih napada (transportna ili mrežna zaštita).

13.1 Zaštita na aplikativnom nivou

U cilju realizacije mehanizama zaštite na aplikativnom nivou u okviru informacionog sistema, predlaže se primena digitalnog potpisa i digitalne envelope, na bazi smart kartica za korisnike. Za realizaciju zaštite na aplikativnom nivou, neophodno je primeniti odgovarajuću kriptografsku biblioteku kako na klijentu, u okviru odgovarajuće klijentske aplikacije(standalone) ili Internet browser programa, tako i za primenu na odgovarajućem web ili aplikativnom serveru. Ove kriptografske biblioteke na klijentu i serveru su u potpunosti odgovorne za realizaciju kriptografskih funkcija na aplikativnom nivou. Naime, klijentska offline aplikacija (standalone) sa ugrađenom kriptografskom bibliotekom (ili odgovarajućom ActiveX kontrolom) ili web pretraživački program izkoga se poziva odgovarajuća ActiveX kontrola (ili JAVA aplet u non-Windows baziranim aplikativnim sistemima), treba da ima sledeće kriptografske karakteristike:

- Primena mehanizmima zaštite na aplikativnom nivou kojima se obezbeđuju sledeće funkcije:
 - ✓ Autentičnost potpisnika (asimetrični kriptografski algoritam i tehnologijadigitalnog potpisa),
 - ✓ Zaštita integriteta fajlova (asimetrični kriptografski algoritam i tehnologija digitalnog potpisa),

- ✓ Obezbeđenje neporecivosti (asimetrični kriptografski algoritam i generisanje ključeva na samim smart karticama i tehnologija digitalnog potpisa),
 - ✓ Zaštita tajnosti podataka (simetrični kriptografski algoritam i tehnologija digitalne envelope).
-
- Koriste se tehnologije digitalnog potpisa i digitalne envelope.
 - Univerzalnost u odnosu na smart kartice i čitače smart kartice. Ugrađena ActiveX kontrola na klijentu, kao i kriptografske biblioteke ugrađene na serveru, koristi odgovarajući middleware (koji se sastoji od: CSP(Cryptographic Service Provider), PKCS#11 biblioteke i token menadžera za administraciju smart kartice) za pristup smart karticama. Na ovaj način, klijentska i serverska aplikacija su nezavisne od konkretne smart kartice koja će biti korišćena a i prelaz na drugi tip kartice je u potpunosti direktan.
 - Klijentska aplikacija (bilo standalone bilo da se koristi web pretraživački program) sa ugrađenom krypto kontrolom mora da obezbedi funkciju provere autentičnosti korisnika na bazi njegove smart kartice i odgovarajućeg PIN-a pre nego što se omogući korišćenje same aplikacije, tj. aplikacija ne može da se startuje bez korišćenja odgovarajuće smart kartice ovlašćenog korisnika. Pri tome, provera nije samo da li se određena kartica nalazi u čitaču kartica već se mora proveriti i sertifikat korisnika (proverom validnosti, da li je izdat od CA kome se veruje i provera statusa povučenosti).
 - Bazira se na kriptografskim operacijama koje se izvršavaju na samoj smart kartici: digitalni potpis (tj. RSA private key encryption) i dešifrovanje simetričnog ključa kod digitalne envelope (digital envelope retrieval). Ostale kriptografske operacije (šifrovanje/ dešifrovanje simetričnim algoritmima, kreiranje hash vrednosti podataka koji se digitalno potpisuju, verifikacija digitalnog potpisa) se izvršavaju u klijentskom i serverskom softveru (softverski deo krypto komponenti na klijentu i serveru).
 - Bazira se na PKCS de facto standardima za zaštitu, i to:
 - ✓ PKCS#1 za digitalni potpis i digitalnu envelopu,
 - ✓ PKCS#7 za format zaštićenih podataka,
 - ✓ PKCS#11 standardni interfejs za pristup smart karticama.
 - Aplikacija treba da bude standardna u smislu formata digitalno potpisanih i šifrovanih podataka. U tom smislu, treba primeniti standarde: PKCS#7 (ili
 - noviji Cades) ili XML DIGSIG standard (ili noviji Xades) za format zaštićenih fajlova.

- Aplikacija pri realizaciji bezbednosnih mehanizama treba da koristi standardne načine pristupa smart karticama: CSP (Cryptographic Service Provider) i PKCS#11 biblioteka, i stoga je nezavisna od konkretne smart kartice koja će biti korišćena tako da je prelaz na drugi tip kartice u potpunosti direktan.
- Klijentska standalone aplikacija, ili odgovarajuće stranice web aplikacije, trebada omogućće:
 - ✓ Izbor sertifikata potpisnika (koji stoje u Personal Store-u) ukoliko nadatnoj radnoj stanici postoji veći broj korisničkih sertifikata.
 - ✓ Izbor sertifikata (koji stoje u Other PeopleStore-u) namenjenog primalaca šifrovanog fajla, tj. lice/korisnik za koga se šifrue taj fajlna kon digitalnog potpisivanja. To može biti i sam server ukoliko se radio šifrovanoj dostavi podataka do servera.
 - ✓ Prikaz informacija o podacima koji se digitalno potpisuju pre samog potpisivanja,
 - ✓ Prikaz informacija o rezultatima digitalnog potpisivanja i/ili šifrovanja datih podataka,
 - ✓ Prikaz informacija o rezultatima uspešne ili neuspešne verifikacije digitalnog potpisa i/ili uspešnog ili neuspešnog dešifrovanja datih podataka.
- Klijentska i serverska krypto komponenta treba da u ovom trenutku podrži sledeće kriptografske algoritme i pridružene dužine ključeva:
 - ✓ Asimetrični algoritmi – RSA algoritam (koji se izvršava na smart kartici)sa dužinom asimetričnog ključa od 2048 bita.
 - ✓ Hash algoritmi – SHA-1, SHA-224, SHA-256, SHA-384 ili SHA-512.
 - ✓ Simetrični algoritmi – 3DES algoritam sa dužinom ključa od 168 bita ili AES algoritam sa dužinama ključa od 128, 192 ili 256 bita.
- Aplikacija treba da bude otvorena za stalnu dogradnju kako novih algoritama tako i za zamenu onih algoritama za koje je utvrđeno da su kriptografski slabi za korišćenje. Takođe, aplikacija treba da obezbedi promenu dužina odgovarajućih kriptografskih ključeva ukoliko se ukaže potreba za tim.
- Aplikacija treba da bude otvorena za eventualnu ugradnju privatnih simetričnih algoritama kreiranih i verifikovanih od strane nadležne institucije za poslove kriptozastite u zemlji, ukoliko postoje zahtevi za to.
- U okviru aplikacije (klijentske i serverske) treba obezbediti funkciju verifikacije digitalnog potpisa odgovarajućih podataka (koji se razmenjuju između korisnika i

sistema ili podataka/dokumenata koji su arhivirani i pregledaju se u okviru sistema) koji se sastoji od sledeća dva koraka (tim redom):

- ✓ Provera digitalnog potpisa podataka na osnovu javnog ključa iz digitalnog sertifikata potpisnika (koji je došao uz digitalno potpisane podatke u samoj formatiranoj poruci),
- ✓ Provera samog digitalnog sertifikata. Ova provera se izvršava na sledeći način:
 - proverava se da li je dati sertifikat istekao,
 - proverava se da li je sertifikat izdat od CA (certification Authority) kome se veruje i
 - proverava se da li je sertifikat povučen, tj. da li se nalazi navažećoj CRL listi koje izdaje dato CA

U okviru mehanizama zaštite na aplikativnom nivou mogla bi se integrisati i odgovarajuća challenge-response procedura jake autentikacije korisnika na aplikativnom nivou. Alternativa tome je da se za te potrebe iskoristi standardna procedura klijentske i serverske autentikacije u okviru SSL protokola zaštite na transportnom nivou.

13.2 Zaštita na transportnom nivou

U vezi realizacije transportnih mehanizama zaštite, predlaže se primena standardnog SSL (Secure Sockets Layer) protokola (novija verzija je TLS (Transport Layer Security) protokol) između korisnika i web servera (ili web servisa).

- ✓ SSL protokol sa serverskom autentikacijom – neophodan je SSL serverski sertifikat izdat za dati web server i
- ✓ SSL protokol sa klijentskom i serverskom autentikacijom na bazi digitalnih sertifikata i smart kartica korisnika. U ovom slučaju je takođe neophodno da web server (ili odgovarajući web servis) ima SSL serverski sertifikat.

Naime, za potrebe autentikacije korisnika informacionog sistema Organizacije, predlaže se primena zaštite na transportnom nivou i jake autentikacije korisnika nabazi SSL protokola sa klijentskom i serverskom autentikacijom.

13.3 Zaštita na mrežnom nivou

Umesto SSL protokola na transportnom nivou, ili dodatno njemu, mogu se koristiti i kriptografski mehanizmi zaštite na mrežnom nivou koji se najčešće baziraju na IPSec protokolu zaštite i uspostavi virtuelnih privatnih mreža (VPN – Virtual PrivateNetwork). U zavisnosti od načina komunikacije kao i protokolima koji se koriste za komunikaciju, kriptografske VPN mreže se najčešće baziraju na čistom IPSec protokolu zaštite ili na kombinacijama PPTP/IPSec ili L2TP/IPSec. U okviru informacionog sistema generalno se predlaže primena IPSec protokola na bazi digitalnih sertifikata čvorova u računarskoj mreži (ili između klijentai VPN servera). U tom smislu, VPN mreža, koja se bazira na IPSec protokolu, može se uspostaviti između dva rutera ili rutera i firewall-a, ili između VPN klijenta i VPN koncentratora (ruter ili firewall uređaj) – opet na bazi digitalnih sertifikata. Sa druge strane, neophodno je primeniti firewall uređaje u cilju podizanja sveukupne zaštite i kontrole pristupa sistemu. Jedan primer moguće primene firewall uređaja dat je na slici.

Takođe, potrebno je razmotriti i primenu drugih „nekriptografskih“ mehanizama zaštite i to: antivirusne zaštite, patch management, web content filtriranja, Intrusion Prevention Sistema (IPS), end-point security mehanizama, itd.

14 Zaključak

Danas kada je upotreba računara, informacionih sistema i Interneta gotovo neizbežna u poslovanju, učenju, pronalaženju informacija itd. neophodno je koristiti zaštitu od raznih malicioznih softvera, napadača na korporativne i privatne podatke, koja se ogleda primenom kriptografskih i nekriptografskih mehanizama u više slojeva arhitekture informacionih sistema. Vrlo je bitno definisanje zaštitnih polisa kako u poslovnom tako i u privatnim segmentima korišćenja i upotrebe mrežnih servisa i Interneta.

Postoje razni softveri i hardverska oprema koja omogućuje pouzdanu zaštitu podataka, ali se među njima izdvajaju Mils Electronic i Crypto AG zbog kompletnih profesionalnih rešenja koja su spremna za implementaciju bez menjanja postojeće infrastrukture.

Kvantna i DNK kriptografija će možda u nekoj skorijoj budućnosti predstavljati osnov za zaštitu poverljivih dokumenata. Kvantna kriptografija nastala je kao posledica otkrića u oblasti kvantnog računarstva. Ona se zasniva na jednom od osnovnih principa kvantne fizike: Hajzenbergovom principu neodređenosti.

Postojeći komercijalni sistemi su uglavnom orijentisani na zvanične insitucije i korporacije sa visokim sigurnosnim potrebama. Distribucija ključeva preko kurira se uglavnom koristi gde tradicionalna distribucija ključa ne pruža zadovoljavajuću sigurnost. Ovo ima prednost jer nema razdaljinsko ograničenje, i bez obzira na dugo vreme putovanja stopa transfera je visoka zbog postojeće infrastrukture koja nudi velike kapacitete uređaja za čuvanje podataka. Najveća odlika kvantne kriptografije je mogućnost da se otkrije bilo kakvo presretanje sigurnosnih ključeva, dok kod kurira sigurnost ključa nije dokazana. Sistemi za kvantnu distribuciju ključa imaju i prednost što su automatski, imaju veću pouzdanost i manju cenu.

Faktori koji sprečavaju širu primenu kvantne kriptografije van visoko bezbednosnih oblasti su cena neophodne opreme, kao i činjenica da još uvek nije dokazano da postoji pretnja postojećim protokolima za razmenu ključeva. Ipak, mreže sa optičkim kablovima već postoje u nekim zemljama, tako da to daje nagoveštaj da će doći do šire primene.

Kada se govori o zaštiti i bezbednosnim rizicima mora se imati u vidu da je to neprestana borba između ljudi koji osmišljavaju zaštitne sisteme i napadača. Ono što je danas aktuelno kao metod napada u bliskoj budućnosti može biti modifikovana ili skroz zamenjena novom metodom koja zaobilazi postojeće sisteme zaštite. Stoga zaštita informacionih sistema ima i jako bitan zadatak praćenja svih novih metoda koje se koriste i koje bi mogle da se koriste od strane napadača.

15 Literatura

- [1] Milan Milosavljević i Gojko Grubor, "Osnovi bezbednosti i zaštite informacionih sistema", *Univerzitet Singidunum*, 2006.
- [2] Mladen Veinović, Aleksandar Jevremović „Uvod u računarske mreže”
Beograd 2008
- [3] William Stallings, "*Cryptography and Network Security*", Prentice Hall, 2005.
- [4] Mark Stamp, "Applied Cryptanalysis", John Wiley & Sons, 2007.
- [5] ANSI X 9.17 (Revised), —American National Standard for Financial Institution Key Management (Wholesale), || American Bankers Association, 1985.
- [6] Bruce Schneier, "Applied Cryptography", *John Wiley & Sons*, 1996.
- [7] A.Menzes, P.van Oorschot, S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.
- [8] National Institute for Standards and Technology, —*Key Management Using X9.17*, || NIST FIPS PUB 171, U.S Department of Commerce, 1992.
- [9] National Institute for Standards and Technology, —*Secure Hash Standard*, || NIST FIPS PUB 180, U.S Department of Commerce, 1993.
- [10] National Institute for Standards and Technology, —*Digital Signature Standard*, || NIST FIPS PUB 186 U.S Department of Commerce, 1994.
- [11] Andrew Nash, William Duane, Celia Joseph, Derek Brink, "PKI Implementing and Managing E-Security", RSA Press, 2001.

Web sajтови

[1]www.wikipedia.com

[2]<http://www.crypto.ch/>

[4]<http://www.mils.com/>

[5]<http://www.crypto.ch/>

[5]<http://www.singipedia.com/>

16 Sadržaj slika

- Slika 1: Vizuelizacija puteva interneta
- Slika 2 : Grafički prikaz upotrebe računara i interneta
- Slika 3 : OSI i TCP/IP modeli
- Slika 4 : Širenje Worm-a
- Slika 5 : Sub7 trojan horse
- Slika 6 : Rootkit šema
- Slika 7 : Spyware instalacija
- Slika 8 : Phising web sajt
- Slika 9 : Pharming
- Slika 10 : BotNet
- Slika 11 : Enigma u saobraćajnom muzeju u Lucernu, Švajcarska
- Slika 12 : Kriptoanaliza
- Slika 13 : Razmena podataka simetričnim ključem
- Slika 14 : Razmena fajla asimetričnim ključevima
- Slika 15 : AES
- Slika 16 : Prikaz mreža i tehnologija
- Slika 17 : Crypto AG i Mils Electronic
- Slika 18 : Lista proizvoda Mils electronic
- Slika 19 : Simulacija izračunavanja ključeva u crpypto tool-u