



UNIVERZITET SINGIDUNUM

-MASTER STUDIJSKI PROGRAM-

SAVREMENE INFORMACIONE TEHNOLOGIJE

Zaštita računarskih mreža

- Master rad -

Mentor:

Prof. dr Mladen Veinović

Student:

Damjan Begović

Br. indeksa:410706/2013.



Beograd, 2014.

Sažetak

U ovom radu opisana je organizacija zaštite kompjuterskih sistema pomoću više tehnika i praktična primena u zaštiti kompjuterskih sistema. U radu su prikazani mogući propusti i različite tehnike zaštita. U radu je opisana i kriptografija, odnosno šifrovanje podataka i sistema. Savremene tehnike šifrovanja puštaju osobi koja šalje da preriši informacije na način da napadač nema mogućnost da dobije nikakve nikakve informacije iz presretnih podataka. Potrebno je da osoba koja ih prima bude u mogućnosti da vrati prvobitne informacije iz prerišenih podataka.

Ključne reči: zaštita kompjuterskih sistema, šifrovanje, komunikacija, računarske mreže

Abstract

In this paper describes the organization of the security of computer systems using multiple techniques and practical application of the protection of computer systems. The paper presents various possible omissions and various techniques of protection. The paper that described and kriptografija or encryption of data and systems. Modern techniques of encryption allows the sender to mask data so that an intruder can not get any information from any presusretnih data. The recipient must be able to extract the original data from the masked data.

Keywords: Cryptographic protection of computer networks, encryption, communication, data masking.

SADRŽAJ

SADRŽAJ	3
1. Uvod	5
2. Metodologija naučnog istraživanja	6
2.1. Uvodne napomene i obrazloženja rada	6
2.2. Predmet istraživanja	6
2.3. Ciljevi i zadaci istraživanja	6
2.4. Istraživačke hipoteze	6
2.5. Metode istraživanja i tok istraživačkog procesa	7
3. Kriptografija	8
3.1. Osnovni pojmovi	8
3.2. Simetrična kriptografija	8
3.3. Asimetrični šifro sistemi	11
3.4. Tehnika digitalnog potpisa	13
3.5. Upravljanje ključevima	13
4. Zlonamerni softveri	14
5. Zaštita računara	15
5.1. Antivirusni programi	15
6. Hakerski upadi	16
6.1. Hakerski alati	16
6.2. Sigurnosne metode	17
7. Firewall	18
7.1. Zaštita lokalne mreže od štetnog delovanja "napadača"	19
7.2. Zaštita od štetnog delovanja lokalnih korisnika	20
8. Spyware	21
8.1. "Adware" i praćenje	21
8.2. Dobijanje spyware-a	21
8.3. Efekti, posledice i ponašanje	22

<i>Zaključak</i>	<i>23</i>
<i>Literatura.....</i>	<i>24</i>

1. Uvod

Zaštita računarskih mreža u ovom veku kao i njihovo nadgledanje i praćenje su od veoma velikog značaja za normalno funkcionisanje i rad jedne IT infrastrukture. Imamo mogućnost da instaliramo protekciju na različitim nivoima.

Ubrzani napredak računarskih sistema uz čiju pomoć se vrši digitalna komunikacija dovodi do promena i pri takvom napretku proizvođača dolazi do nedostatka vremena za temeljno isprobavanje robe. U tom nedostatku vreme dolazi dogrešaka koji mogu da budu početak potencijalnim napadačima. Oni pronalaze svoje načine da bi došli do „važnih“ podataka. Zaštita podataka je postala toliko bitna da je danas jedna od komponenti na koje se najviše obraća pažnja kod državnih administracija, banaka, nacionalne bezbednosti zemalja, i drugih bitnih kompanija. Takođe, danas velike kompanije poklanjaju sve više pažnje i mere bezbednosti svojih informacionih sistema. Kao najpopularniji način za digitalnu komunikaciju koriste se računarske mreže. Samim tim, računarske mreže su najveći izvor polju sigurnosti informacijama koje se preko računarskih mreža transportuju. Zbog toga, dosta se misli i ulaže u zaštitu podataka i njihov transport preko računarskih mreža.

Načini i alati za pravljenje sigurnosnih sistema su Anti-spyware, Firewall, Anti-virusni softver, sigurne šifre, Backup, sigurnosne zakrpe, preventive, dobra sigurnosna praksa i ostale vrste zaštite kao što su kontrola pristupa, enkripcija i uočavanje upada.

Kroz razvoj informacionih sistema vidi se da je značajno povećanje rizika sigurnosti računarskih sistema prouzrokovalo pojava umreženih računarskih sistema odnosno pojava Interneta.

Sve dok su kompjuterski sistemi bili „izolovani“ od drugih kompjutera osnovna mera zaštite je bila autentikacija tj. osiguravanje da kompjuteru a time i podacima imaju pristup samo određene ličnosti. Što je više osoba koristilo računarski sistem to je i njegova zaštita postala kompleksnija a sigurnost je opadala. Autentikacija se uglavnom ostvarivala šiframa i drugim sigurnosnim informacijama. Savremeni sistemi pored toga sve češće koriste i biometrijske informacije za autentikaciju, kao što je otisak palca, skeniranje irisa oka, prepoznavanje glasa i druge inovativne metode.

2. Metodologija naučnog istraživanja

2.1. Uvodne napomene i obrazloženja rada

Projektni zadatak ima cilj da definiše pojmove koji se koriste u zaštiti u kompjuterskim mrežama. Sa razvojem tehnologije sve je teže obezbediti kvalitetnu zaštitu podataka.

Mnoge organizacije koje se suoče sa napadima i izgube podatke nikada se više ne oporave od tog gubitka. Stoga se ovaj rad bazira na zaštiti računarskih mreža.

Projektni zadatak je izrađen korišćenjem teoretskih i praktičnih znanja iz domena zaštite računarskih mreža, a poseban akcenat dat je na kriptografiji.

2.2. Predmet istraživanja

Predmet istraživanje je zaštita računarskih mreža koja je sa svojom aktuelnošću sve više i više zastupljena u istraživanjima kada su u pitanju moderne tehnologije. Uz zaštitu čiji osnov predstavlja kriptografija posebno mesto zauzimaju ključevi i upravljanje ključevima.

Tokom rada postavljala su se pitanja na koje rad daje odgovor:

- Šta je kriptografija?
- Kako se upravlja zaštitom računarskih mreža i sistema?
- Kako se zaštititi od zlonamernih softvera?

2.3. Ciljevi i zadaci istraživanja

Cilj istraživanja je da se pokaže neophodnost primene kriptografske i antivirusne zaštite računara i podataka koji se nalaze u računaru, pri tom vodeći računa o efikasnosti i efektivnosti procesa zaštite u cilju povećanja sigurnosti podataka a samim tim i sigurnosti informacionog sistema .

2.4. Istraživačke hipoteze

Opšta hipoteza:

- ❖ Kriptografska zaštita računara i podataka je jedna od najefikasnijih zaštita koja uz korišćenje ključeva predstavlja najbolji vid zaštite

Posebne hipoteze:

- ❖ Sigurnosni sistemi TCP/IP su jedni od najefikasnijih sistema sigurnosti

- ❖ Kriptografsku zaštitu računara i podataka najbolje je koristiti uz korišćenje ključeva
- ❖ Ključevima je potrebno upravljati, a najpre je potrebno kreirati, zapisati i distribuirati.

2.5. Metode istraživanja i tok istraživačkog procesa

U ovom istraživanju korišćene su sledeće metode istraživanja:

- ❖ Opšte analitičke metode pri prikupljanju i proučavanju dostupne literature;
- ❖ Hipotetičko – deduktivne;
- ❖ Statističke.

Pri izradi rada korišćene su referentne web adrese koje su pružale dodatne informacije vezano za zaštitu podataka.

3. Kriptografija

3.1. Osnovni pojmovi

Plaintext je izvorni tekst koji se može pročitati bez upotrebe određenih alata i metoda. Da bismo takav tekst preneli od tačke A do tačke B kao poruku možemo birati da li će tekst biti svima razumljiv ili kao nerazumljiv skup koji je šifrovan tj. kriptovan.

Metod uz čiju se pomoć izvorni tekst menja u šifrovan tekst zove se šifrovanje. Šifrovanjem postizemo to da niko ne može da pročita tekst poruke osim onaj kome je namenjena. Šifrovanje se izvršava uz pomoć kriptografskog algoritma a on sadrži izvorni tekst i ključ i kao rezultat daje šifrovan tekst. Inverznom metodom se izvršava dešifrovanje.

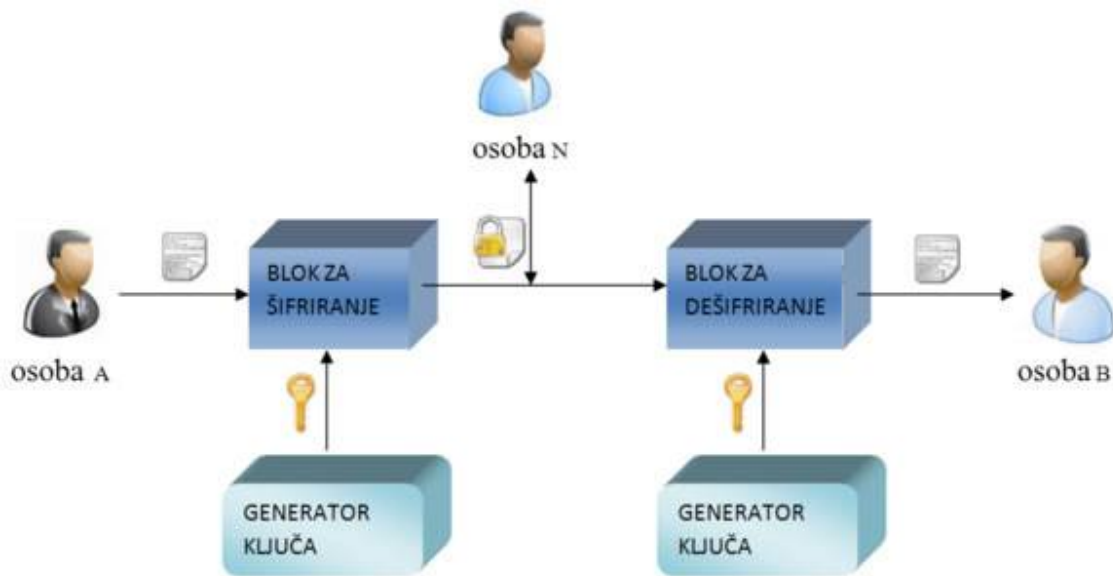
Kriptografija je nauka koja uz pomoć matematike obezbeđuje siguran transfer podataka preko mreža tj bavi se zaštitom podataka, dok je Kriptoanaliza nauka o dešifrovanju poruka. Ove dve naučne discipline zajedno čine Kriptologiju.

Blok šifrovanje se upotrebljava za kraće poruke (lozinke, potpise, ključeve), i u ovom principu šifrovanja, izvorni tekst se razdvaja u blokove, a zatim se oni nezavisno šifruju. Za blok šifrovanje je karakteristično da se svaki blok kriptuje na istom metodom, bez obzira na poziciju koju zauzima kao i činjenica da nema potrebe za dešifrovanjem od početka već može bilo koji blok.

3.2. Simetrična kriptografija

Glavna osobina simetričnih šifarskih sistemaolikuje se u tome da se kodšifrovanja, odnosno dešifrovanjaporuka,upotrebljava jedan ključ.

Slika3.1, u vidu blokova, pokazuje način rada simetričnog šifro sistema. ObjekatA ima želi da pošalje porukuMobjektuB putemkanala za komunikacijukoji nije zaštićen.ObjekatA prvo pravi poruku M (izvorni tekst) i onaprosleđuje u šifrarskiblok E gde se izvodi šifrovanje poruke M , upotrebomključa K koji je dobijen pomoću generatora ključa. Tako se dobija šifrovana poruka C . Zatim se taporuka komunikacionim kanalom prosleđuje do osobe B .



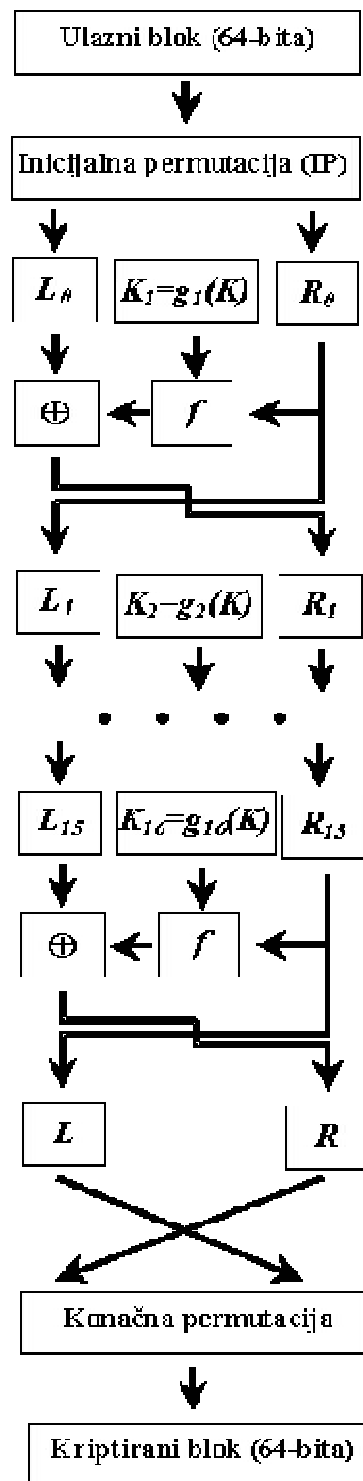
sl. 3.1 Simetrični šifarski sistem

Obrnutim postupkom od šifrovanja dolazi do dešifrovanja u bloku D . Dešifrovanje poruke C izvodi se istim ključem K upotrebljavanim tokom šifrovanja. Posle dešifrovanja rezultat je izvorni tekst M .

U slučaju da na kanalu za prenos osoba N (napadač) poseduje ključ, on onda može da pročitati ili zloupotребiti izvornu poruku. Zbog toga je neophodno da obe strane drže ključ u tajnosti. U odnosu na ključ, šifrovana poruka ima mogućnost slanja po kanalu koji nije zaštićen.

Najpopularniji algoritmi simetričnih šifarskih sistema danas u upotrebi su: „DES, 3DES, DES-CBC, IDEA, RC5, RC6, AES” i drugi.

Šifrovanje DES algoritma odvija se u više faza. Najpre se bitovi ulaznog bloka dužine 64 bita permutuju startnom permutacijom. To je permutacija koja izvršava promenu mesta bitova. Permutovan ulazni blok razdvaja se na po 32 bita, levi $L0$ i desni $R0$ deo. Nad desnim delom bloka vrši se funkcija $f(R0, K1)$, pri čemu je $R0$ desnih 32 bita, a $K1$ je 48-bitni ključ. Ta funkcija donosi 32-bitni proizvod. Nadstečenim rezultatom funkcije f i $L0$ izvršava se operacija XOR. Rešenjem XOR operacije dobija se nova 32-bitna vrednost $R1$ i ona se posle upotrebljava u operaciji. Kao levi deo $L1$ upotrebljava se vrednost $R0$ iz malopredložene iteracije. Posle ponavljanja 16 istih faza, blokovi između sebe menjaju mesta da bi se na kraju spojili. Poslednje se vrši konačna permutacija, suprotna početnoj. Rezultat, 64-bitna vrednost je deo šifrovanog bloka podataka.[4]



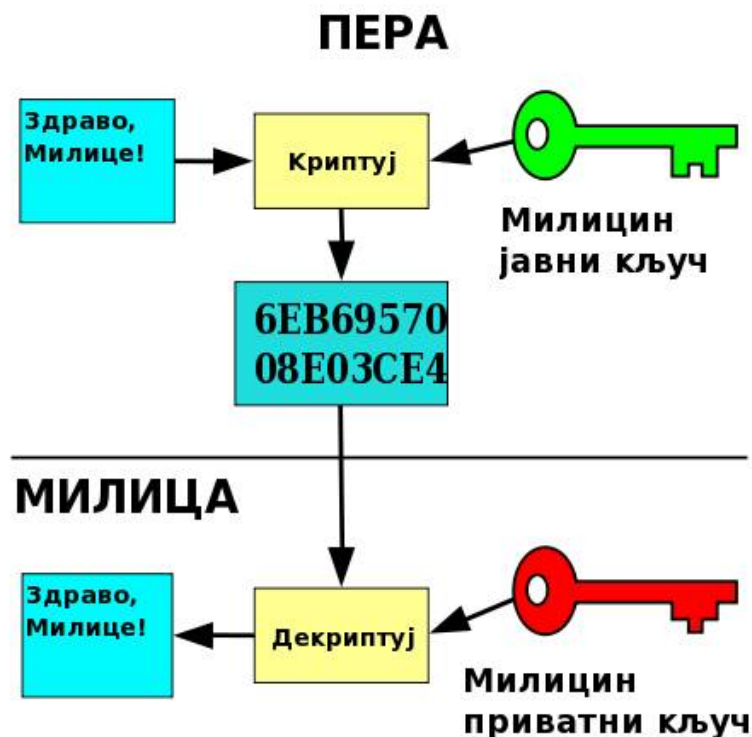
sl. 3.2 Izgled DES algoritma za šifrovanje

Prednost simetričnog šifrovanja je efikasnost zahvaljujući kratkim ključevima pa se s toga koristi kod obimnijih poruka. Glavni nedostatak je što je neophodno da obe osobe imaju jedinstveni ključ pa se pojavljuje problem distribucije istih jer sem fizičkog sretanja ne postoji bezbedan način razmene ključeva.

3.3. Asimetrični šifrosistemi

Princip asimetrične kriptografije se zasniva na postojanju dva ključa, privatni i javni i u tome se ogleda najveća razlika u odnosu na simetričnu kriptografiju. Informacije se šifruju javnim ključem ali se mogu dešifrovati isključivo privatnim ključem. Ključevi su povezani jednosmernom funkcijom što onemogućava računanje privatnog ključa iz javnog.

Algoritmi asimetričnih šifrosistema se baziraju na principima brojeva. U toku šifrovanja izvorni tekst se posmatra u obliku niza prirodnih brojeva čijom selektovanom funkcijom šifrovanja, ključem K_{pub} pretvara u šifrovani niz. Neophodno je da funkcija šifrovanja iz šifrovanog teksta nije u mogućnosti da odredi izvorni tekst, bez obzira na to da li se zna ključ za šifrovanje. Ali, ako je poznat ključ za dešifrovanje K_{priv} nije teško izračunavanje izvornog teksta. Ovakva vrsta šifrovanja je veoma kompleksan način zaštite. Da bi se realizovao, svi objekti koji komuniciraju moraju da imaju oba ključa (javni i tajni). Pored toga što su drugačiji, ključevi su i konektovani transformacijama. Slika 3.3 pokazuje primer asimetričnog šifrovanja. [15]



sl. 3.3 Asimetrično šifrovanje

Sigurnost sadržaja poruke direktno zavisi od toga kakose čuva privatni ključ. Najzastupljeniji asimetrični princip šifrovanja podataka je 'RSA' algoritam.

Osnovna prednost asimetričnog šifrovanja je da nema ograničenja u smilu mogućnosti komunikacije sa trećom osobom bez odobrenja osobe B zbog toga što svako ima svoja dva ključa i može da bira sa kim će da vrši komunikaciju. Jedna od prednosti je i dosta manji broj ukupno potrebnih ključeva u odnosu na simetrično šifrovanje. Npr. u sistemu gde komunikaciju vrši hiljadu korisnika neophodno je 2 hiljade ključeva dok bi kod simetričnog bilo potrebno 500 miliona ključeva. Kao glavni nedostatak asimetričnog šifrovanja izdvaja se kompleksnost algoritama tj operacije sa velikim brojevima I zato su asimetrični algoritmi pogodni samo za rad sa kraćim porukama.

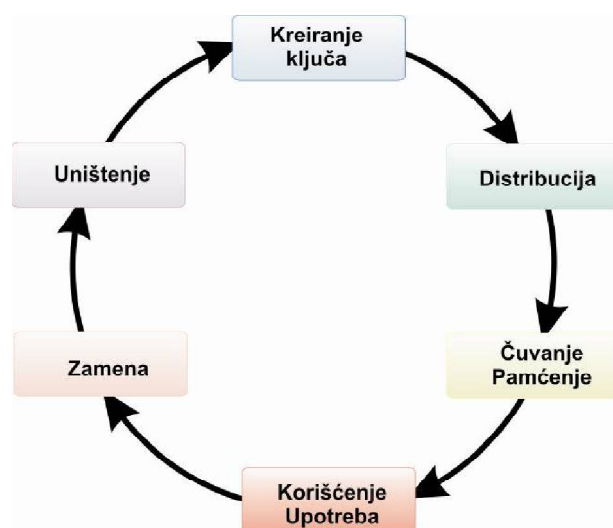
3.4. Tehnika digitalnog potpisa

Princip digitalnog potpisa je sličan potpisivanju dokumenata i upotrebljava se za identifikaciju osobe, organizacije ili računara pri slanju dokumenata elektronskim putem. Ova vrsta potpisa se ne može falsifikovati, a zasniva se na matematičkoj funkciji i dva ključa, tajnom i javnom ključu što je slično rešenju koje se primenjuje asimetričnim šifro sistemima. Digitalni potpisi se upotrebljavaju u elektronskoj trgovini i za razne finansijske transakcije.

3.5. Upravljanje ključevima

Ključevi su najvažnije informacije u kriptografiji pa je i upravljanje njima podjednake važnosti u šifro sistemima.

Na Slici 3.4 je prikazan životni ciklus ključa. Ciklus započinje kreiranjem samog ključa a zatim sledi distribucija do svog korisnika i čuvanje do upotrebe. Cilj upravljanja ključevima je da uvek osigura tajnost i integritet ključeva.



sl. 6.1 prikaz životni vek ključa

Korisnik najčešće formira ključ odabirom lozinke koja se uz pomoć algoritma pretvara u ključ. Vrlo je bitna dužina ključa. Uvek je bolje kada korisnik bira dužinu ključa dok je kod npr DES algoritma dužina fiksna. Za prenos ključeva je vrlo bitno koristiti sigurne linije, npr preko pošte. Svaki kriptografski system ima opciju zamene ključa a razlozi za to mogu biti redovna obnavljanja ili sumnja u korišćeni ključ.

4. Zlonamerni softveri

Osnovne vrste zlonamernog softvera (malware) su virusi, crvi, trojanski konji, rootkit, spyware i adware. Oni prave štetu kompjuteru i podacima, remete konekciju s Internetom i upotrebljavaju kompjuter da bi se širili po drugim kompjuterima. Predostrožnosti zdravo razmišljanje može da spreči da se postane žrtva ovakvih pretnji. U nastavku će biti reči o definicijama, metodama saznanja da li je kompjuter napadnut, rešenjima uz čiju pomoć se može podići nivo bezbednosti kompjutera.

Virus je program ili kod koji se sam replicira u drugim datotekama s kojima dolazi u kontakt. *Virus* nikodje kreirana definisanim ciljem sopstvenog razmnožavanja. On se trudi da se raširi na kompjutere upadanjem na host program. Oštećuje hardver, softver i podatke.

Računarski virus čini kod koji se sam kopira, i on pruža umnožavanje virusa i upotrebljivih informacija bez obzira da li su bezopasne ili opasne.

Kompjuterski crvi su kompjuterski programi koji upotrebljavaju računarske mreže za samokopiranje po ostalim računarima, uglavnom bez odluke korisnika. Nije obavezno da se i ostali programi inficiraju kao u slučaju virusa. Stiču oblik priloga elektronske pošte a ulazak na kompjuter im dozvoljavaju nedostaci u aplikacijama i operativnim sistemima. Crvi dosta remete funkcionisanje mreže, štete podacima i kompromituju sigurnost kompjutera.

Trojanski konj je štetni računarski program. On je prerusen tako da deluje kao ostali korisnički programi ali pri pokretanju otkriva svoje namere. On se ne umnožava.

Zlonamerni kod zvani dialer se dobija na sličan način kao trojanski konji a rezultat je prekid veze sa internetom i biranje telefonskog broja u stranoj državi sa ciljem dobijanja profita autora kroz velike cene poziva. Ukoliko se na telefonskom računu pojave nepoznati međunarodni brojevi velika je šansa da korisnik poseduje dialer na kompjuteru.

5. Zaštita računara

Prvi vid odbrane od virusa je zaštita kompjutera. Radi se o veoma kompleksnoj aktivnosti kojom primena određenih programa zahteva i oprezno rukovanje.

Protekcija kompjutera sprečava napade virusa uz pomoć antivirusnih programa. Oni konstantno vrše proveru podataka koji ulaze u kompjuter i prepoznaju štetne zapise a zatim upozoravaju korisnika na taj virus. Postoji više stepeni zaštite a najpreporučljiviji je najviši stepen, koji ima stalne provere ali zahteva veće resurse.

5.1. Antivirusni programi

To su programi koji mogu da detektuju, izdvoje i unište viruse. Sastoje se iz dva dela, "Monitor" koji je u memoriji i garantuje zaštitu od virusa, i "Scan" koji skenira ceo sistem. Antivirusi su danas nezaobilazni deo softvera svakog korisnika. Kompanije koje prave i razvijaju ove programe su Panda, Sophos, Symantec, Kaspersky... Najpopularniji programi : "NORTON ANTIVIRUS, SOPHOS ANTI-VIRUS, NOD32, PANDA ANTIVIRUS TITANIJUM, AVG ANTI-VIRUS, MCAFFEE"...

Osnovni koraci u antivirusnoj zaštiti:

1. Instalacija nekog antivirusnog alata!
2. Podesiti na automatsko skeniranje svih datoteka
3. Automatsko ažuriranje i skidanje antivirusne definicije.
4. Skeniranje hard disk nakon instalacije softvera
5. Provera svih datoteka koje dolaze sa Interneta.
6. Skeniranje celog diska

6. Hakerski upadi

Iako reč se haker u javnosti gleda u negativnom kontekstu, u programerskom svetu ta reč označava vrstu poštovanja između dva programera. Slavni programerski leksikon poznat kao „The Jargon File“ definiše reč „haker“ kao:

1. Osoba koja uživa istraživati detalje računarskih programa i traži način da poveća performanse sistema, za razliku od ostalih korisnika koji uče i koriste samo osnove programa.
2. Osoba koja programira s posebnim entuzijazmom ili čiji je užitek pre programiranje nego diskutovanje o njemu
3. Čovek koji ceni vrednosti pravog „hacka“
4. Osoba koja brzo programira
5. Stručnjak za neki korisnički program tj. osoba sa mnogo iskustva u korišćenju istog.

White hat hackers koriste svoje umeće u dobre svrhe tako što „razbijaju“ računarske sisteme da bi postali zaštićeniji i sigurniji. Sarađuju s proizvođačima programa i nalaze mane programima.

Gray hat hackers izdokolice prave probleme u računarsom sistemu nekog neutralnog korisnika.

Black hat hackers su najveća pretnja i oni prave viruse, upadaju u kompjutere, brišu podatke, obaraju sajtove...

Hakeri pronalaze načine za pristup tuđim kompjuterima i time testiraju svoje znanje ili koriste za ilegalne postupke. Glavni motivi su radoznalost, dosada, osveta zabava...

Načini napada su različiti a mogu se i klasifikovati:

- 1) **Presecanje**- sprečava se pružanje neke usluge ili rad sistema.
- 2) **Presretanje**- udar na poverljivost kroz prisluškivanje i uvid u osetljive informacije. S obzirom da je pasivan napad otežano se otkriva jer se podaci ne menjaju
- 3) **Izmena**- udar na integritet kroz aktivan napad koji menja podatke, rad sistema i programa. Uglavnom je i on neprimećen zbog vrhunskih tehnika napada.
- 4) **Proizvodnja**- udarna autentičnost kroz predstavljanje lažnih podataka, prometa, davanja neovlašćenih naredbi...

6.1. Hakerski alati

Hakeri upotrebljavaju različite alate za napade i svaki od njih ima svoje sposobnosti:

1) Skener portova (port scanners) je alat koji se najviše upotrebljava za pretraživanje na Internetu. On pretražuje velike IP prostore i izveštavaju o sistemu koji je napadnut, priključnim tačkama koje su slobodne i ostalim informacijama, kao što je tip operativnog sistema. Najpopularniji skener portova je Network Mapper (NMap) koji ubrzano pretražuje velike mreže.

2) Skeneri koji traže slabosti traže specifičnu slabu tačku u sistemu. Nessus kao jedan od najboljih skenera danas, daljinski proverava mrežu i predviđa potencijalno probijanje u nju.

3) Alati za dobijanje administratorskih prava na sistemu (rootkit) čine skup ispisa i izvršnih paketa koji omogućuju hakerima da prikriju dokaze da su dobili pristup u sistem. Ovi alati:

- Menjaju sistem dnevnika datoteka kako bi uništili tragove o hakerskim aktivnostima
- Menjaju alate sistema da bi se otežalo otkrivanje
- Prave skrivene ulazne tačke sistema
- Koriste sistem kao polaznu tačku napada na druge umrežene sisteme

4) Alati za „njuškanje“ (sniffer)

Solarisov „snoop“ služi za hvatanje i prikazivanje svog mrežnog prometa koji trenutno vidi. Može se reći da je primitivan ali ima mogućnost da prikupi ID adrese. Kad dobije pristup sistemu, haker instalira program za uvid u promet na mreži da bi dobio korisnički ID i informacije uz čiju pomoć dolazi do saznanja koji način je mreža građena i za šta se koristi.

6.2. Sigurnosne metode

Po mišljenju nekih autora, postoje četiri grupe načina zaštite: programske, organizacijske, kriptografske i fizičke metode.

Mnogi ovakvu grupaciju smatraju zastarelom i sve više se koristi šema koju je napravila organizacija (ISC)2.

Aspekti zaštite se uglavnom definišu prema položaju mehanizma zaštite u računarskom i informacionom sistemu. Postoje različiti nivoi:

- Zaštita na nivou aplikacije,
- Zaštita na nivou mrežne infrastructure,
- Zaštita na nivou operativnog sistema.[5]

7. Firewall

Firewall je sigurnosni alat koji se nalazi između javne i lokalne mreže, napravljen s ciljem da sačuva poverljive, korisničke podatke od korisnika kojima nije dozvoljen pristup. Nije obavezno da svaki objekat LAN-u ima ista prava pristupa Internetu. Instaliranjem Firewalla između dvaju više delova mreže moguće je upravljati pravima pristupa korisnika određenim mrežnim delovima. Tada je Firewall postavljen da odobrava pravo pristupa željenim zahtevima, a odbija one koji ga nemaju. Firewall je istovremeno odlično rešenje za pravljenje virtualne privatne mreže zbog toga što kreiranjem virtualnog tunela preko kog se prenose šifrovani podaci omogućuje bezbednu razmenu delikatnih podataka između dislociranih korisnika.

Firewall čine firewall uređaj i Policy (pravilnika o zaštiti) i provlači kroz filter korisnika različitih tipova mrežnog saobraćaja s zadatkom da podigne nivo bezbednosti i pruži visok nivo zaštite od probijanja u sistem. Firewall-a služi da ne dođe do nedozvoljenog pristupa mreže na mrežu što znači zaštitu unutrašnje mreže od Internet-a. Temelj rada Firewall sistema sadrži od provere IP paketa koji se razmenjuju između objekata i servera i time se dobija nadzor nad tokom informacija u oba smera za sve servise po IP adresi i portu.

Firewall ima odgovornost za više stvari:

1. Postavlja politiku sigurnosti.
2. Notira sumnjive događaje.
3. Firewall alarmira administratora pri pokušajima proboja i kršenja politike sigurnosti.
4. Često Firewall obezbeđuje statistiku korišćenja.

Firewall može biti softverski ili hardverski:

Softverski pruža zaštitu jednog kompjutera sem kada je taj kompjuter predviđen za protekciju cele mreže.

Hardverski firewall pruža zaštitu cele mreže ili određenog broja kompjutera.

Da bi firewall-a pravilno funkcionisao, neophodno je koncizno definisati pravila o tome kojije mrežni saobraćaj dozvoljen.

7.1. Zaštita lokalne mreže od štetnog delovanja “napadača“

Firewall bez stroge politike prema paketima koje prima može da doživi različite vrste napada. Ako firewall nema opciju upravljanje virtualnih privatnih mreža, a system pokušava omogućiti ulazna lokalne mreže sa nekih IP adresa, postoji opcija konfigurisanja da firewall prima podatke sa unapred definisane izvorišne IP adrese. Taj princip konfigurisanja ima mane. Npr. moguće je da onaj ko želi da napadne dođe do paketa ilogičke adrese uz čiju pomoć je moguć pristup lokalnoj mreži. Posle, napadač ima mogućnost da pravi pakete koji će imati za izvornu adresu logičku adresu kompjutera koji ima potvrdu za spajanje i tako uz pomoć posebno konfigurisanih paketa da nanese štetu lokalnoj mreži. Firewall se mora podesiti na način kojim će sprečavati sve moguće napade. Danas, veliki broj proizvođača firewalla sa ponosom naglašava vrste ataka gde su njihovi firewall rezistentni, dok se novije vrste napada, sve komplikovanije, svaki dan prave.

Međutim, svi firewall bi morali da budu rezistentni na pokušaje kao što su :

1. Address Spoofing- pruža mogućnost slanja paketa sa neznane adrese na neki od unutrašnjih kompjutera ako napadač kao izvornu adresu postavi određenu adresu iz lokalne mreže. Tada je on podesen da dozvoli protok paketa i željeni kompjuterski da primi specijalno izmenjeni paket. Kako bi se ovakav napad sprečio neophodno je sprečiti prosleđivanje paketa čija je izvorna adresa jedna od lokalnih, dok je ulazno okruženje konektovano na Internet.
2. Smurf ima zadatak da spreči rad servera i kompjutera odnosno to je DoS napad. Napadač prosleđuje ICMP echo request paket na broadcast adresu lokalne mreže i tako adresira sve kompjutere u lokalnoj mreži. Kao destinaciju stavlja željeni kompjutera on se poremeti pretrpavanjem odgovorima. Za odbijanje ovakvog napada potrebno je u sprečiti broadcast paket.
3. Syn-Flood- bazira se na prosleđivanju prvobitnih TCP paketa koji sadrže instaliranu SYN zastavicu, i zanemarivanjem TCP odgovora sa postavljenim SYN i ACK zastavicama. Tako je željeni kompjuter preokupiran slanjem odgovora. Odbijanje ovakvog napada se vrši ograničavanjem broja pristiglih TCP paketa.
4. Port-Scanner- bazira se na prepoznavanju slobodnih TCP i UDP portova tako što se šalje SYN ili FIN paket portovima, nakon čega se čeka RST odgovor. Neophodno je podesiti količinu prozivljanja.
5. Ping-of-Death- izaziva kolaps operativnog sistema kada je na kompjuter preusmeren preveliki broj ICMP-echo zahteva. Način odbijanja napada je sprečavanje echo request paketa.[1]

7.2. Zaštita od štetnog delovanja lokalnih korisnika

Tokom podešavanja firewalla najviše se gleda na obrađivanju dolaznih paketa. Oni su podešeni tako da ne pružaju mogućnost korišćenja materijaa lokalnim korisnicima. Između ostalog web stranice za skidanje raznih video i audio zapisa, web stranice koje propagiraju mržnju, porno web stranice itd. Uzimajući u obzir to da se one konstantno kreiraju neophodno je ažurirati podešavanja firewall-a. Kod ograničavanja neophodno je ne otići daleko sa restrikcijama, jer može doći do kontraefekta. Korisnik bi imao nemogućen pristup materijalima koji olakšavaju rad, a taj odnos bi izazvao pasivni odbijanje rada. Tokom podešavanja firewall-a mogu se upotrebiti određena pravila onemogućavanja konektovanja lokalnih korisnika sa Internetom. Osnovni princip je ravnopravan odnos ka svakom korisniku lokalne mreže. Takođe postoji mogućnost da se lokalne kompjuteri klasifikuju zavisno po njihovim IP adresama. Tako se može jedino nekom sektoru u organizaciji pružiti neometana konekcija sa Internetom, dok bi drugima bio ograničena ili nepostojeća. Firewall se može podesiti tako da prima sve pakete sa paketa poslatih kompjuterima sa specifičnim IP adresama u Internetu.

8. Spyware

Spyware je deo štetnog softvera čiji je cilj da presretne ili preuzme delimično kontrolu kompjutera bez svesti i odobrenja korisnika.

Spyware se izdvaja od virusa i crvaja jer se ne reprodukuje. Spyware je napravljen da koristi maliciozne kompjutere za komercijalnu dobit. Klasični principi su iskakanje neželjenih popup oglasa; zloupotreba personalnih informacija (finansijske, PIN kreditne kartice i lozinke); uvid u surfovanje internetom zarad marketinga; ili usmeravanje HTTP zahteva na reklame. U mnogim slučajevima spyware se upotrebljava za potvrdu i održavanje uslova licence za korišćenje programa. Sa 2005-om spyware je problem karakterističan samo za kompjutere sa Microsoft Windows operativnim sistemima.

8.1. "Adware" i praćenje

Adware je program koji pruža reklame, ne uzimajući u obzir da li ima dozvolu korisnika ili ne. Dobar deo programa smatranih kao spyware rade kao adware ali je njihova glavna odlika iskakanje reklama. Claria Corporation Gator Software može biti primer takvog programa. Neke stranice umeju tajno da instaliraju Gator na kompjuter korisnika, i preusmeravaju dobit na njihovu stranicu. To se može primetiti kada kompjuter bez naznake izbací ogromnu količinu popup reklama.

Ostale spyware prakse, npr. beleženje poseta korisnika stranici, uglavnom postoje u prikazu reklama. Svrha beleženja aktivnosti je kreiranje marketinškog profila korisnika zbog naknadnog davanja "ciljane" reklamne kampanje. Postojanje spywarea šteti i ostalim programima koji prate aktivnost na internetu, tako i za potrebe statistike i istraživanja. Mnogi imaju Alexa Toolbar, Internet Explorer plug-in koji je kreirao Amazon.com, kao spyware iako korisnici sami donose odluku o instalaciji.

8.2. Dobijanje spyware-a

Spyware se instalira na sistem putem manje korisnika upotrebom propusta u ostalim programima. Najjednostavniji način primanja spyware na kompjuter se događa u situaciji kada ga primalac instalira jer je predstavljen kao željeni program, ili nezavisnom instalacijom bez svesti primaoca.

Spyware može stići uz shareware ili ostale programe. Primalac npr. skine program za gledanje filmova zatim ga instalira, a instalacijom uz to instalira i spyware. I pored toga što željeni

program nije zlonameran, spyware koji ide uz njega jeste. Postoje slučajevi gde kreatori spyware-a plaćaju kreatoru shareware-a da aktivira spyware u sklopu njegovog softvera, npr. Gator spyware.

Još jedan princip širenja spyware je zloupotreba mana delova programa kojima je zadatak da zastave instalaciju štetnog programa. Dizajn Internet Explorer Web browser-a sprečava instalaciju nepotvrđenih programa sa web stranica na kompjuter.

8.3. Efekti, posledice i ponašanje

Kompjuteri koji koriste Windows mogu dobiti mnogo spyware programa za malo vreme. Korisnici onda primete čudne aktivnosti ili gubitak performansi. Spyware izaziva ipopriličnu opterećenost CPU aktivnosti, korišćenje diska, i mrežnu komunikaciju -- remeteći korisnu upotrebu računarskih resursa. Veći problemi, kolaps aplikacija i sistema, su isto uobičajene posledice. Spyware izaziva poteškoće povezivanja na Internet. Problem sa spyware-om je jedan od najvećih uzroka zbog kojih je korisnicima potrebna tehnička podrška - od proizvođača kompjutera, ili ostalih izvora. Najčešće primalac nije ni svestan da poseduje spyware i misli da su sa performansama, stabilnošću i konekcijom uzrokovani hardware-om, instalacijom Windowsa ili virusima. Mnogi su voljni da kupe i nov kompjuter jer je trenutni isuviše spor. Računarima koji su preterano zaraženi često je preostalo rešenje reinstalacija sistema—zahtevna procedura i iskusnim korisnicima.

Neuobičajeno je da kompjuter bude zaražen jednim jedinim štetnim softverom. Studija AOL-a iz 2004. je došla do zaključka da ako kompjuter sadrži spyware, velike su šanse da ima više štetnih programa.. Takođe se dešava da spyware gasi firewall i anti-virus programe, te eliminiše sigurnosne postavke korisnika, postavljajući sistem pogodan za nove viruse.

Zaključak

Ubrzani razvoj tehnologije računarskih sistema i mreža, dovodi do velikih razmena podataka svakog dana. Tako je postala neophodna zaštita istih od krađe i zloupotrebljavanja, iz čega se izrodio novi pravac usferi bezbednosti podataka. Napredak tehnologije doneo je bolje performanse metoda u toj sferi. Ali, ubrzani razvoj je doprineo i efikasnijem pronalaženju mana i pospešio moguće zloupotrebe. Vremenom su principi protekcije podataka bivalo kompleksnije.

Osnovne mere za stvaranje sigurnih sistema jesu kriptografija, jaka autentikacija, provereni softver i dr. Kriptografija je nauka koja se koristi za zaštitu podataka transportovanih s kompjutera na kompjuter. Provereni softver mora biti proveren i ispitan sa sigurnosti da nema zaražen kod.

Kroz izloženo može se primetiti da se anti-virusni softver i druge sigurnosne aplikacije najčešće reaktivno prilagođavaju novim štetnim pojavama. Naime, programeri ne mogu unapred znati na koji način će njihov softver biti napadnut, ali pokušavaju u što većoj meri otežati rad virusim, crvima, hackerima i dr. Programeri Anti-virusnih programa, Firewall-a i sl. aplikacija u toku eksploatacije istih „krpe“ sigurnosne rube uzrokovane novim virusima, crvima i td. pa je prema tome izuzetno važno vršiti redovno aktualiziranje sigurnosnog softvera putem Interneta.

Cilj rada je da skrene pažnju ka tome koliko je bitno zaštititi podatke, kao i da definiše neke od mehanizama uz čiju pomoć se štite.

Literatura

- [1] "Zaštita u računarskim mrežama"- Aleksandar Jevremović, Mladen Veinović, Marko Šarac, Goran Šimić,
- [2] Narcis Behlilović , Pamela Begović, Saša Mrdović- Različiti aspekti zaštite pristupa digitalizovanoj kulturnoj baštini, Elektrotehnički fakultet u Sarajevu,
- [3] S. Sinkovski, B. Lučić, "Informaciona bezbednost i kriptografija", *Jugoimport SDPR Beograd*,
- [4] Behrouz A. Forouzan, "Data Communications and Networking", *Book Mc Graw Hill*, ISBN 9780072967753, 4th edition, 2007.
- [5] Marin Perko- HAKERI, GOSPODARI INTERNETA -diplomski rad, Sveučilište u Zagrebu, 2008 god.
- [6] Vladimir Kovačević- Zaštita podataka primenom kriptografskih metoda- seminarski rad, Univerzitet u Nišu, 2010.god.
- [7] Zaštita podataka u računarskim mrežama, *MTVU lekcije*
- [8] Dejan Simić, "Tehnike zaštite u računarskim mrežama", Fakultet Organizacionih Nauka Beograd, PPT Prezentacija, Beograd, Jun 2002.
- [9] Dragan Spasić, "Kriptozaštita podataka u računarskim mrežama primenom simetričnih i asimetričnih šifarski sistema", Direkcija za poštanski saobraćaj,
- [10] Dokumenti sa Microsoftova konferencija o sigurnosti informacijskih sustava – "Microsoft Security Days 2008." ,
- [11] www.wikipedia.com
- [12] <http://bs.wikipedia.org/wiki/Spyware>
- [13] <http://es.elfak.ni.ac.rs/Papers/Zastita%20podataka.pdf>
- [14] www.budimo-sigurni.hr
- [15] Z. Ž. Avramović, Dražen Petrović, "Kriptografija simetrični i asimetrični algoritmi", *Seminarski rad Fakultet poslovne informatike*, Banja Luka, maj 2008.