Profesor dr Milojko Jevtović,
dipl. inž.
Elektrotehnički fakultet,
Banja Luka

ZAŠTITA RAČUNARSKIH MREŽA

UDC: 004.738 : 65.012.8

Rezime:

U radu su obrađene metode napada, oblici ugrožavanja i vrste pretnji kojima su izložene računarske mreže, kao i moguće metode i tehnička rešenja za zaštitu mreža. Analizirani su efekti pretnji kojima mogu biti izložene računarske mreže i informacije koje se preko njih prenose. Opisana su određena tehnička rešenja koja obezbeđuju potreban nivo zaštite računarskih mreža, kao i mere za zaštitu informacija koje se preko njih prenose. Navedeni su standardi koji se odnose na metode i procedure kriptozaštite informacija u računarskim mrežama. U radu je naveden primer zaštite jedne lokalne računarske mreže.

Ključne reči: računarske mreže, ugrožavanje mreža, pretnje mreži, protivmere, zahtevi za zaštitu, tajnost informacija, autentičnost, integritet, autorizacija prava korisnika, tehničke mere zaštite, standardi metoda zaštite.

PROTECTION OF COMPUTER NETWORKS

Summary:

In this paper different methods of attacks, threats and different forms of dangers to the computer networks are described. The possible models and technical solutions for networks protection are also given. The effects of threats directed to the computer networks and their information are analyzed certain technical solutions that provide necessary protection level of the computer networks as well as measures for information protection are also described. The standards for methods and security procedure for the information in computer networks are enlisted. There is also an example of protecting one local data network (in this paper).

Key words: computer networks, endanger of networks, network threats, countermeasures, protection demands, information confidentiality, authenticity, integrity, authorization of the user's rights, technical protection measures, standard methods of protection.

Uvod

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

Značaj zaštite i bezbednosti informacija u telekomunikacijama rapidno se povećava, kako u vojnim tako i u javnim mrežama, među kojima su i računarske mreže. Evropska unija izdala je niz različitih direktiva koje se odnose na uputstva

za obezbeđenje tajnosti i zaštite informacija u javnim telekomunikacionim mrežama. Institut za evropske telekomunikacione standarde – ETSI (European Telecommunications Standards Institute) formirao je savetodavnu grupu za problematiku zaštite i bezbednosti mreža, a radi i na algoritmima za zaštitu informacija u javnim mrežama [1].

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

Zaštita predstavlja jedno od najznačajnijih pitanja u realizaciji buduće generacije mreža (Next Generation Networks – NGN), posebno onih koje za prenos budu koristile Internet protokol [2], odnosno njegov podsistem za multimedijalnu komunikaciju (Internet Multimedia Subsystem – IMS).

Težišno pitanje razmatrano u ovom radu jeste analiza mogućih pretnji i napada na računarsku mrežu, kao i tehničke mogućnosti zaštite mreža i informacija.

Vrste i oblici pretnji i napada na računarske mreže

Pretnje računarskim mrežama

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

– odbijanje usluge (denial of service). Ovim tipom napada elementi računarske mreže se blokiraju kontinualnim bombardovanjem podacima, tako da se zauzimaju svi mrežni resursi, pa mreža nije u stanju da korisnicima pruža usluge;

– prisluškivanje (eavesdopping). Ovom pretnjom prikriveno ili potpuno tajno prisluškuju se signali koji se preko mreže prenose između predajnika i prijemnika;

– maskiranje (masquerade). Izvršilac napada koristi maskiranje kako bi simulirao lažnu identifikaciju radi pristupa mreži;

– neautorizovani pristup (unauthorized access). Pristup ulazima u mrežu mora biti veoma restriktivan u skladu sa politikom zaštite. Ako napadač pokuša da realizuje neautorizovan pristup na bilo kom ulazu u mrežu, drugi različiti napadi mogu uporedo proći neprimećeni;

– modifikacije informacije (modification of information). U ovom slučaju podaci mogu biti izmenjeni, uništeni ili oštećeni korišćenjem deliberalizovane manipulacije porukama u datoj mreži;

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

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

– autentifikacija (authentication) – komunikacioni proces koji omogućava, odnosno obezbeđuje pouzdanu informaciju o identifikaciji učesnika u vezi;

– autorizacija (autorization) – dozvola za uvid ili modifikaciju (promene) podataka ili obavljanje nekih drugih aktivnosti u računarskoj mreži;

– zaštita tajnosti informacija (cofidentiality) – zaštita sadržaja poruke od nedozvoljenog uvida i korišćenja;

– neporicanje (non-repudation) – proces kojim se štite sistemi u komunikaciji tako što se osigurava predaja poruka, prijem poruka i obrada podataka;

– integritet (integrity) – procedure koje omogućavaju da informacija ne bude menjana u toku prenosa od izvora do odredišta;

– digitalni potpis (digital signature) – poruka koja potvrđuje identitet njenog pošiljaoca, kao i autentičnost i integritet poruke koja se prenosi. To znači da se digitalni potpis razmenjuje između učesnika u komunikaciji radi provere autentičnosti prenete informacije i identifikacije entiteta koji međusobno komuniciraju;

– kontrola pristupa (access control) – procedura kontrole kojom se utvrđuje pravo nekoj osobi da pristupi resursima računarskog sistema ili računarske mreže;

– virtuelna privatna mreža (Virtual Private Network – VPN) – metodama kriptozaštite osigurana veza dva učesnika u IP računarskoj mreži;

– kriptozaštita poruka (encryption) – algoritmi i metode (permutacija, supstitucija i sabiranje po modulu 2) kojima se obezbeđuje šifrovanje – dešifrovanje poruka u komunikaciji;

– otkrivanje napada (intrusion detection) – mere koje omogućavaju da se otkrije napad na računarsku mrežu i time spreči ugrožavanje;

– provera i presecanje pretnji (auditing and logging) – procedure kojima se proveravaju pristupni kanali veze ka mreži radi otkrivanja i sprečavanja pretnji.

Softverske metode za ugrožavanje računarskih mreža

Za ugrožavanje funkcionisanja Internet mreže i mreža koje su na njega povezane (IP mreže), najčešće se koriste zlođudni programi koji se klasifikuju kao: „virusi“, „trojanski konji“, „bakterije“, „crvi“, „bombe“ i slično. Oni se prenose preko piratskih aplikacionih programa, softverskih alata ili sa porukama elektronske pošte.

Virusi su programi koji „zaraze“ datoteku računara umetanjem svojih umnožaka (kopija), a obično se izvršavaju kada se učitavaju u memoriju računara. Na taj način se prenose i na ostale računare u mreži. Slanjem ogromne količine podataka virusi zagušuju ili sasvim isključuju mrežu. Njihovo delovanje je vrlo štetno, a ogleda se u oštećenju pojedinih delova računara, hard diska i zauzimanju memorijskog prostora operativne memorije računara. U računarskim mrežama u svetu kruži oko 200 hiljada virusa.

Trojanski konji su korisni ili prividno korisni programi koji, kada se uključe odnosno aktiviraju, obavljaju nepoželjne ili rušilačke aktivnosti u računaru. Mogu se koristiti sa ciljem da ispune neke zadatke koje neovlašćeni korisnik nije u stanju da realizuje. Da bi pristupio datotekama određenog računara, program trojanski konj, kada se izvršava, menja redosled ovlašćenja (privilegija, prava) za korišćenje datoteke. Takve datoteke, nakon njihovog delovanja omogućavaju da svako može da ih čita, odnosno ostaju bez zaštite.

Bakterije su programi koji izričito ne oštećuju datoteku, ali imaju ulogu da se intenzivno „razmnožavaju“ (po eksponencijalnom zakonu), zauzimajući, odnosno angažujući vreme procesora i memorijski prostor na disku ili u operativnoj memoriji. Time se onemogućava korišćenje umreženog računara.

Bombe – logičke bombe predstavljaju kodove koji se ubacuju u neki komercijalni program, a postavljeni su da „eksplodiraju“ kada se zadovolje određeni uslovi, kao, na primer, postojanje ili nepostojanje pojedinih datoteka, određeni dan u sedmici ili pri pojavi određenog korisnika. Kada se ti uslovi ispune nastupaju rušilačka dejstva čiji je efekat onesposobljavanje računara (operativnog sistema, aplikativnog softvera, memorijskog prostora i dr.).

Problem zaštite od ugrožavanja mreža korišćenjem navedenih softverskih metoda rešava se korišćenjem antivirusnog softvera, odnosno, softvera za otkrivanje prisustva zlćudnog programa. Čine se napori za realizaciju imunog sistemskog softvera za otkrivanje i uništavanje zlćudnih programa, a time programski obezbedi sprečavanje ugrožavanja računara, odnosno računarske mreže.

Standardi koji se odnose na zaštitu informacija

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

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

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

Tabela 1

Pregled standardnih metoda i algoritama za kriptozaštitu

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

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

DES – Data Encryption Standard je standard za šifrovanje – dešifrovanje podataka, usvojen 1977. godine. Definisao ga je Nacionalni biro za standarde (NBS) SAD. Osnovni blokovi algoritma su permutacija, supstitucija i sabiranje po modulu 2. Za primene u kojima se DES smatra nedovoljno sigurnim sistemom (za tzv. blokovske šifre), primenjuje se varijanta DES-a – trostruki DES ili 3DES.

IDEA – International Data Encryption Algorithm je međunarodni algoritam za šifrovanje podataka. To je tzv. blok-šifra u kojoj se koristi šifarski ključ dužine 128 bita. IDEA je evropski standard usvojen 1990. godine. Ovaj algoritam se smatra vrlo sigurnim. Uspešno konkuriše DES standardu po pitanju brzine i efikasnosti ključa.

CAST je američka blok šifra, koja koristi ključ dužine 128 bita.

Skipjack-Capstone je šifra koju je razvila NASA, a koristi ključeve dužine 80 bita. Podržava algoritam digitalnog potpisa (Digital Signature Standard, DSS).

RC 2 i RC 4 su šifre koje koriste šifarske ključeve promenljive dužine. Zamišljene su kao zamena za DES algoritam.

RSA – Riverst-Shamir-Adelman je algoritam šifrovanja zasnovan na činjenici da je lako generisati dva velika prosta broja p i q, pomnožiti ih međusobno, ali je veoma teško izvršiti faktorizaciju rezultata množenja.

PKCS – Public Key Criptography Standard je standard koji su predložili RSA i konzorcijumi koji čine Microsoft, Apple, Digital Equipment i drugi.

DSS – Digital Signature Standard je šifra koju je kao standard prihvatila Vlada SAD. Dužina ključa može varirati od 512 do 1024 bita. Namenjen je za proizvodnju digitalnih potpisa i ne koristi se za zaštitu podataka.

Kerberos je protokol koji je razvio Massachusetts Institute of Techhnology. Namenjen je za bezbedno čuvanje tajnih ključeva u bazi podataka. Do tajnog ključa može doći samo njegov vlasnik, koristeći Kerberos protokol.

KES – Key Exchange Algorithm je algoritam za razmenu ključeva, ali se ne koristi za šifrovanje podataka.

MD2, MD4 i MD5 su algoritmi za transformaciju poruka. Svaki od njih proizvodi tzv. Hash vrednost od 128 bita.

Tehnička rešenja zaštite računarskih mreža

Sa velikom sigurnošću može se tvrditi da potpuna, apsolutna zaštita računarskih mreža ne postoji. Postoji sigurna

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

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

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

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

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

– organizaciono-administrativne mere, kojima se normativno regulišu prava, obaveze i odgovornosti, uključujući i sankcije korisnika informacionog sistema;

– tehničke mere fizičke, elektronske i protivpožarne zaštite;

– hardversko-softverske mere kojima se obezbeđuju pristupni putevi mreži i resursima mreže koji se štite;

– aplikativno-programske mere koje predstavljaju procedure koje se ugrađuju u aplikativni softver radi zaštite;

– mere kriptozaštite radi zaštite podataka u memorijskim resursima u računarima i zaštite na prenosnim putevima.

Fizička i elektronska zaštita računarske mreže

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

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

Obezbeđenje pristupnih tačaka mreži i resursima mreže

Obezbeđenje pristupnih tačaka mreži i pojedinim resursima mreže ostvaruje se nizom hardversko-softverskih mera. Te mere odnose se na identifikaciju korisnika i utvrđivanje prava i ovlašćenja koja su mu data u odnosu na resurse mreže kojima pristupa. Prepoznavanje korisni-

ka, odnosno njegova identifikacija, sastoji se od fizičkog prepoznavanja – korišćenjem hardverskih uređaja i logičkog prepoznavanja – upotrebom određenih softverskih metoda (slika 1).

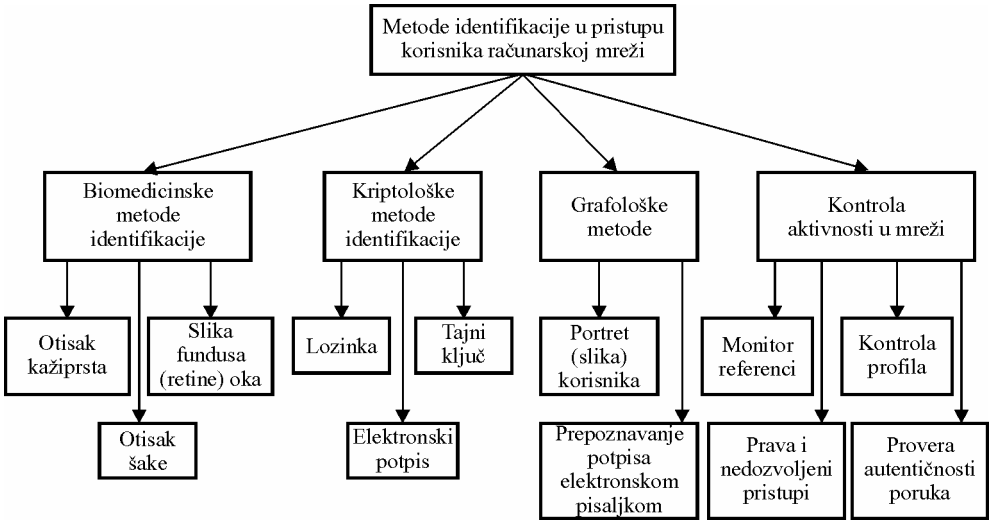
Metode fizičkog prepoznavanja zasnivaju se na: prepoznavanju nekih identifikacionih sredstava koje korisnik poseduje, kao što su inteligentne (smart) kartice, magnetne i optičke kartice, bedževi, žetoni i slično, i prepoznavanju fizičkih, biometrijskih karakteristika korisnika, kao što su: otisak prsta, otisak i oblik šake, oblik uha ili glave, osobine glasa, slika mrežnjače oka i dr.

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

Fizičke metode prepoznavanja, zasnovane na identifikaciji fizičkih biometrijskih karakteristika, obezbeđuju pouzdanu i sigurnu tzv. „pozitivnu personalnu identifikaciju“. Prepoznavanje korisnika i provera njegovih ovlašćenja u korišćenju resursa mreže korišćenjem biometrijskih metoda može se izvršiti sa velikom sigurnošću. Među metodama za biometrijsku identifikaciju korisnika najčešće se koristi otisak prsta (fingerprint). Prepoznavanje korisnika obavlja se putem njegovog otiska prsta, poređenjem sa ranije zapamćenim otiskom.

Metode logičkog prepoznavanja zasnovane su na informacijama koje korisnik u procesu identifikacije i autorizacije ovlašćenja daje sistemu. Te informacije moraju biti jednake informacijama kojima sistem raspolaže. Logičko prepoznavanje obično se realizuje korišćenjem četiri vrste softvera, a to su:

– kontrolni program komunikacionog servera;



Sl. 1 – Metode identifikacije korisnika

– softver za upravljanje sistemskim resursima, realizovan kroz opcije mrežnog komunikacionog softvera, odnosno servera,

– softver za upravljanje bazama podataka, realizovan kroz server baze podataka;

– softver za upravljanje transakcijama, realizovan kroz server baze podataka.

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

Na strani radnih stanica računarske mreže obično se primenjuje kombinovani sistem fizičkog i logičkog prepoznavanja korisnika, korišćenjem principa lokalne i mrežne identifikacije. Zatim sledi utvrđivanje vrste i širine ovlašćenja kojima korisnik raspolaže, upotrebom verifikacije otiska prsta i lozinke (fingerprint + password). Operativni sistem na radnim stanicama može, na primer, biti Windows 2000 Profesional, koji omogućava implementaciju softvera sistema zaštite na principu „fingerprint + password“. Ovaj operativni sistem omogućava postavljanje računara u režim automatskog izlaska iz mreže nakon određenog perioda neaktivnosti. Time se dodatno osigurava neovlašćeno korišćenje usluga mreže.

Usluga operativnog sistema u zaštiti

Operativni sistem koji se često primenjuje u računarskim mrežama svakako je operativni sistem Microsoft Windows NT Workstation ver. 4.0. Opredeljenje za ovo rešenje nastalo je kao rezultat objektivnih performansi, odlika i prednosti u odnosu na druge mrežne operativne sisteme (UNIX, LINUX, Windows 95, Windows 98, OS/2 i drugi). Osobine i prednosti OS Windows NT Workstation ver. 4.0 prikazane su u tabeli 2.

Tabela 2

Osobine OS Windows NT 4.0

Osobine	Prednosti
Desktop performanse	Podržava multitasking (višeprogramski rad) za sve aplikacije (16-bitske i 32-bitske) i rad sa više procesora za prave multitasking performanse
Hardverski profili	Mogućnost kreiranja liste različitih hardverskih konfiguracija da bi se zadovoljili različiti računarski zahtevi
Microsoft Internet Explorer	Poseduje brz i za upotrebu jednostavan Internet browser, kompatibilan sa svim postojećim standardima
Umrežavanje	Prijem i otprema E-mail poruka, uključujući datoteke i objekte kreirane u drugim aplikacijama
Bezbednost operativnog sistema	Omogućava bezbednost na lokalnom nivou za datoteke, direktorijume, štampače i druge resurse. Korisnika mora da autorizuje lokalni računar ili domen kontroler (server), da bi mu bilo omogućeno da pristupi nekom resursu na računaru, terminalu ili mreži
Stabilnost operativnog sistema	Svaka aplikacija izvršava se u sopstvenom memorijskom adresnom prostoru. Eventualni otkaz neke od aplikacija ne odražava se na ostale aplikacije ili funkcionisanje operativnog sistema

Pomenuti OS (operativni sistem) prošao je uspešnu bezbednosnu kontrolu. Američka vlada je decembra 1999. godine objavila da su Microsoft NT Server i Workstation ver. 4.0 uspešno prošli evaluaciju prema kriterijumima za klasu C2 u skladu sa dokumentom TCSEC (Trusted Computer System Evaluation Criteria). Kriterijumi za kvalitet zaštite OS

prikazani su u tabeli 3. Dokument TCSEC poznat je kao Orange Book i predstavlja najpoznatiju metodologiju vrednovanja od strane američke vlade. Klasa C2 predstavlja najviši stepen sigurnosti koji može dostići operativni sistem opšte namene.

Evaluacija operativnog sistema Windows NT 4.0 odnosila se na servere i radne stanice u šest različitih funkcija (uloga), kako u TCP/IP mrežnom okruženju, tako i u radu van mreže (stand-alone).

Bezbednosni sertifikat za Windows NT 4.0 potvrdila je i NSA – tajna američka agencija za nacionalnu bezbednost, kroz Trust Technology Assement Program.

Proces evaluacije prema TCSEC definisan je kao skup standardizovanih kriterijuma, u skladu sa formalnom metodologijom, poznatom kao Trusted Product Evaluation Process (TPEP), koja omogućava evaluaciju bezbednosnih osobina koje proizvod (operativni sistem) pruža i potvrdu da ih proizvod korektno i potpuno implementira.

Bezbednosne osobine koje se navode za klasu C2 su sledeće:

– sposobnost sistema da identifikuje autorizovane korisnike i samo njima dozvoli pristup resursima;

– mogućnost da korisnici zaštite sopstvene podatke u skladu sa potrebama;

– sposobnost sistema da detaljno prati i evidentira (beleži) sve akcije korisnika i samog sistema;

– sposobnost sistema da onemogući korisnicima pristup informacijama iz resursa koji su prethodno koristili drugi korisnici ili sistemi, memoriji koja je ispražnjena ili obrisanim fajlovima.

Tabela 3

Podela operativnih sistema po kriterijumu zaštite

Klasa	Osobina klase	Opis zaštite
D	Bez zaštite	Sistem bez zaštite ili sa minimalnim nivoom zaštite.
C1	Naglašena zaštita bezbednosti	Zaštita od neovlašćenog upisa po kritičnim delovima memorije (DOS nema tu zaštitu); zaštita sredstava sa nadzorom nad pristupom; provera autentičnosti korisnika sa lozinkama; zaštita lozinki.
C2	Zaštita sa precizno kontrolisanim pristupom	Nadzor nad pristupom za svakog korisnika i grupe korisnika; brisanje memorije posle prestanka njenog korišćenja; pregled funkcija-mogućnosti evidencije svih događaja značajnih za bezbednost; svi podaci o korisnicima su zaštićeni, čuvaju se za svakog korisnika posebno.
B1	Zaštita sa obaveznim označavanjem	Oznake za sve korisnike, procese i datoteke; čitanje informacija sa oznakom višeg nivoa je zabranjeno; sistem mora biti sposoban da raspoznaje oznake ili da radi samo sa jednom klasom oznaka; svi štampači pri štampanju moraju štampati i oznaku korisnika na svakoj strani.
B2	Strukturirana zaštita OS	Bezbednosno prepoznavanje; korisnikova autoidentifikacija operativnog sistema; izveštavanje o svim promenama bezbednosnih oznaka autorima tih informacija; gradnja sistema na osnovu zaštitnog jezgra; mogući skriveni kanali za oticanje informacija iz sistema moraju biti nađeni; strog nadzor nad promenama u bezbednosno osetljivim delovima operativnog sistema.
B3	Bezbednosna područja OS	Zabrana pristupa slučajnom korisniku; dozvoljen pristup slučajnom korisniku; dozvoljen pristup određenim korisnicima; pregled funkcija tokom rada – određeni događaji ili broj događaja moraju pružiti upozorenje nadzorniku sistema bezbednosti; bezbedni pad sistema – sistem mora obezbediti zaštitu pri padu sistema i ponovnom podizanju.
A1	Proveren razvoj operativnog sistema	Nivo B, ali sa proverenim razvojem operativnog sistema.

Kvalitativna kontrola po C2 kriterijumima obuhvata:

– ispitivanje izvornog koda,

– pregled detaljne projektne dokumentacije;

– ponovno testiranje kao potvrdu da su ispravljene greške primećene pri evaluaciji.

U prošlosti operativni sistem UNIX standardno je korišćen za bezbedne računarske mreže. U poređenju sa njim Windows NT je pouzdaniji, a ima i druge prednosti, kao što je jednostavnija obuka korisnika i efikasna rešenja za zaštitu.

Kriptozaštita na prenosnim putevima

Komunikacione linije predstavljaju najosetljiviji deo računarske mreže zbog toga što se one ne mogu efikasno fizički kontrolisati. Svaki nekontrolisani deo komunikacionih linija predstavlja pristupnu tačku preko koje se mogu pratiti i prisluškivati signali koji se prenose kroz računarsku mrežu. Posebno su osetljivi oni delovi mreže koji se realizuju bežičnim prenosom, odnosno radio-vezama. Takve veze mogu se vrlo efikasno prisluškivati, ali i ometati. Ove pretnje mogu se najefikasnije eliminisati ili umanjiti primenom kriptozaštite signala na komunikacionim linijama, kao i paralelnim umrežavanjem [6]. Za realizaciju kriptozaštite informacija potrebni su komunikacioni uređaji sa ugrađenim kriptomodulima. Ako se kriptomoduli ugrađuju i u radne stanice, obezbeđuje se zaštita informacija od izvora do odredišta. Jedno od rešenja kriptozaštite može se realizovati primenom IPSEC familije protokola sa 3DES algoritmom. Dodatni nivo zaštite na prenosnim putevima može se obezbediti primenom tzv. virtualnih privatnih „tunela“ VPN (Virtual Private Network), a ostvaruje se korišćenjem familije VPN protokola. Tim protokolima onemogućava se pristup informacijama, odnosno porukama u čvorovima mreže preko kojih se one prenose.

Pomenute mogućnosti zaštite poseduju ruteri. Tako, na primer, ruteri Cisco System 1720 sa dodatnim VPN protokolima i IPSEC 3DES operativnim sistemom, mogu u potpunosti da zadovolje zahteve za kriptozaštitu podataka u računarskoj mreži. Podrazumeva se da korisnik mreže poseduje sopstvene šifarske ključeve, odnosno algoritme za njihovo generisanje.

Zaštita od nestanka napajanja i neadekvatnog napajanja iz javne distributivne mreže

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

– potpunim nestankom napona napajanja, kratkotrajnim i dugotrajnim prekidima u napajanju;

– pojavama prenapona i podnapona u slučaju kada napon napajanja varira izvan opsega zahtevanog za napajanje aktivne elektronske opreme;

– brzim električnim tranzijentima koji se javljaju u distributivnoj mreži;

– dejstvom jakih elektromagnetnih pražnjenja;

– delovanjem jakog elektromagnetnog polja.

Tabela 4

Primer tehničkog rešenja zaštite jedne LAN mreže

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

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

Projektovanje zaštite računarske mreže

Problem zaštite mreža u praksi je prisutan pri projektovanju računarske mreže [6]. Glavni, odnosno izvođački projekat računarske mreže, obavezno treba da sadrži tehničko rešenje za njenu zaštitu. Investitor, odnosno korisnik buduće mreže, u projektnom zadatku i tehničkim

zahtevima, koji prethode izradi projekta, definiše projektantu zahteve za zaštitu, kao i nivo kvaliteta zaštite mreže i informacija koje će se preko nje prenositi. Najteži zadatak je definisanje tehničkih zahteva za zaštitu, jer se oni moraju zasnivati na proceni (analiza, studija pretnji) realno mogućih pretnji i oblika napada na mrežu i informacije. Kvalitet tehničkog rešenja predloženog u projektu mreže treba da bude verifikovan u procesu revizije projekta mreže.

Pod verifikacijom se podrazumeva simulacija predloženog rešenja, uključujući simulaciju pretpostavljenih pretnji i oblika napada na mrežu i informacije. Tek nakon ovakve provere može se ići u realizaciju projekta mreže. Primer tehničkog rešenja zaštite jedne lokalne računarske mreže prikazan je u tabeli 4.

Gotovo svakodnevno pojavljuju se mnogi novi oblici pretnji [7]. Za takve pretnje u relativno kratkom periodu nalazi se efikasna zaštita, obično primenom određenih softverski rešenja, tako da se relativno jednostavno mogu implementirati na postojeće mreže, odnosno umrežene računare. Ceo proces neprekidno se odvija, pretnje postaju sve ozbiljnije, a zaštita mreža sve teža i složenija. Problemi zaštite mreža i informacija posebno su izraženi u projektovanju i realizaciji multimedijalnih telekomunikacionih mreža [8].

Zaključak

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

Literatura:

[1] B. Gamm, B. Howard, O. Paridaes: Security features required in an NGN, Alcatel Telecommunications Review, 2-nd Quarter 2001, pp. 125–129.
[2] J. M. Robert, F. Cosquer: Protecting Data Network Availability, Telecommunications Review, 3-d Quarter 2002, pp. 199–203.
[3] D. I. Pipkin: Information Security, Prentice Hall, 2000.
[4] www.cert.org
[5] www.wired.com/news
[6] Jeftović, M.: Projektovanje računarskih mreža, I i II deo, skripta, Elektrotehnički fakultet, Banja Luka, 2000.
[7] www.microsoft.com/homepage/ms.htm
[8] Jeftović, M.: Multimedijalne telekomunikacije; ISBN 86-903281-6-4; izdavač Grafo-Žig, Beograd; 2004.