VARNOST V RAČUNALNIŠKIH MREŽAH Z DODANO VREDNOSTJO

Borka Jerman-Blažič
Laboratorij za odprte sisteme in mreže, Institut Jožef Stefan
61111 Ljubljana, Jamova 39

Povzetek

Prispevek je pregled funkcij varnosti, ki se uporabljajo v računalniških mrežah z dodano vrednostjo (Value Added Network - VAN). Na kratko so opisane zahteve uporabnikov po varnih komunikacijah in najpreprostejše grožnje, ki so jim izpostavljeni komunikacijski sistemi. Predstavljeno je tudi ogrodje odprtega varnostnega modela (Open Secure Model - OSM), ki definira varnostne funkcije in servise, ki se uporabljajo v odprtih mrežah. Opisani so varnostni mehanizmi za zagotavljanje varnostnih servisov in funkcij.

Abstract

Article gives an overview of security functions, used in computer value added network systems. User demands for secure communications and the most simple threats, to which communication systems are exposed, are shortly described. Open Secure Model - OSM framework, defining security functions and services, used in open networks, is also presented, together with security mechanisms for ensuring security services and functions.

1. UVOD

Informacija pridobi na vrednosti takrat, ko se izmenja oziroma prevzame. Da pa bi se izmenjala ali prevzela, mora biti prenešena ali dostavljena. Potreba po učinkovitih in varnih načinih prenosa danes narašča hitreje kot narašča računalniška obdelava informacij in podatkov. Izmenjava informacij in podatkovne komunikacije so postali integralni del sodobnih informacijskih sistemov.

Izmenjava informacij je proces v okviru storitev, ki jih nudijo mreže z dodano vrednostjo. Te mreže navadno povezujejo uporabnike z različnimi informacijskimi servisi. Posamezne mreže se razlikujejo po strukturi in servisih, ki jih nudijo uporabnikom. Nekateri servisi so precej splošni, drugi pa so lahko zelo specializirani. Vsestranska mreža z dodano vrednostjo (VAN) mora imeti naslednje splošne komponente:

- osnovno prenosno infrastrukturo,
- splošne ali generične servise,
- obdelavo transakcij,
- uporabniške programske rešitve,
- podatkovno bazo,
- upravljanje mreže in pomoč uporabnikom.

Generični ali splošni servisi so servisi, ki jih uporablja širok krog odjemalcev. Zanje je značilno, da niso specifični za nobeno aplikacijo oziroma vejo industrije. Primer takšnih servisov so npr. elektronska pošta, masovni prenos podatkov, elektronska izmenjava podatkov (Electronic Data Interchange - EDI) in informacijski servisi, ki pomagajo vodstvenim ali strokovnim kadrom pri vodenju. VAN ne potrebuje geografsko obsežne infrastrukture (Wide Area Network - WAN), vendar jo navadno poseduje. V najbolj preprostem primeru VAN lahko zagotovi le preklapljanje paketov, v bolj dognanih sistemih pa nudi konverzijo protokolov za podporo široke palete različnih storitev in s tem zagotavlja popolno povezanost vseh naprav in sistemov, ki jih potrebujejo njihovi odjemalci.

S posebej dodanimi varnostnimi servisi je mogoče zgraditi odprto, popolnoma povezano mrežo na kateremkoli zahtevanem nivoju varnosti.

2. ODPRTE MREŽE IN GROŽNJE

Povezanost in varnost sta nasprotujoči si zahtevi. Vendar odprtost, kot jo razumemo danes, ne pomeni pomanjkanja varnosti, temveč medsebojno povezanost in sposobnost medsebojnega delovanja sistemov v različnih organizacijah in od različnih proizvajalcev.

Ko je odprt, distribuirani sistem zgrajen, postane zelo pomembno, da definiramo zahteve uporabnikov s stališča varnosti komunikacij. Glede na to, kateri servis komunikacijskega sistema uporabljajo, lahko uporabniki zahtevajo različne nivoje varnosti. Običajno se uporabniki zanimajo za naslednje vidike varnega komuniciranja:

- identiteta stranke, s katero komunicirajo,
- da nihče drug ne more prisluškovati seji med dvema računalniškima sistemoma,
- da nihče ne more neodkrito izbrisati, spremeniti ali dodati informacij, ki se izmenjujejo z drugo stranko,
- da se v primeru spora obveze, dogovorjene med sejo, lahko kasneje brez večjih dvomov zagotovijo z nepristransko sodbo.

Zaskrbljenost uporabnikov izhaja iz dejstva, da so komunikacijski sistemi in nanje priključeni viri pogosto tarča groženj. Grožnje se lahko nanašajo na samo komunikacijsko mrežo ali na neavtoriziran dostop do lokalnega sistema, kjer je komunikacijska mreža uporabljena le kot medij za dostop.

Definiramo lahko tri kategorije vrednosti, ki so lahko resno ogrožene znotraj globalno povezane mreže:

- viri v mreži,
- prenešene informacije,
- odnosi med strankami.

Lokalni sistemi in viri, ki so dostopni skozi komunikacijski kanal, morajo biti zaščiteni. Tudi komunikacijski sistem sam je tak vir in mora biti zaščiten. Uporabniki komunikacijskega sistema pričakujejo, da bodo komponente komunikacijskega sistema prisotne in da bodo vselej delovale. V tem smislu sta uporabnost in stabilnost servisov prav tako vrednosti komunikacijskega sistema in potrebujeta zaščito. Informacije so dejanska vsebina komunikacij. Neavtoriziran dostop do informacij z izgubo ali spremembo zapisanega lahko uniči vrednost informacije. Tej kategoriji pripadajo tudi informacije, ki se hranijo lokalno in so dostopne prek omrežja. Odnosi med strankami so naslednja osnovna vrednost komunikacij. Brez zaupanja v avtentičnost druge stranke so vse komunikacije z njo brez vrednosti. Zaupanja vredni odnosi s stranko pomenijo, da zaupamo v identiteto stranke in v delovanje komunikacij.

Vse te vrednosti komunikacijskega sistema so izpostavljene dvema v osnovi različnima vrstama groženj, namernim in nenamernim. Klasična teorija o varnostnem sistemu obravnava samo eno vrsto groženj; to so namerne grožnje, ki so ali vohunjenje ali pa sabotaža. Vohunjenje vključuje vse pasivne namerne grožnje kot so pridobivanje neavtoriziranega vedenja o zaupnih informacijah. Sabotaža vključuje vse aktivne namerne grožnje, to je vse vrste neavtoriziranega ravnanja s podatki, dostop do resorjev v komunikacijskem sistemu itd.

Druge možne nezgode, ki so prav tako pomembne za varnost komunikacijskih mrež, so naključne grožnje, npr.: slabo vzdrževanje vodi do prekinitve mrežnega servisa. S stališča uporabnikov je vseeno, če je to storjeno iz škodoželjnosti ali pa iz nesposobnosti administratorja oziroma operaterja.

Različne grožnje in napadi v odprtih okoljih so klasificirani v okvirnih dokumentih ISO. Dokument ISO-7498 PART 2 opredeljuje pet različnih napadov na odprt komunikacijski sistem:

- pretvarjanje,
- tajenje akcije ali servisa,
- zanikanje servisa,
- prestreženje podatkov,
- manipulacija s podatki.

V nadaljevanju podrobneje opisujemo vsako izmed teh dejanj:

a) Do pretvarjanja lahko pride pri medsebojnem overjanju oddajnikov in prejemnikov sporočila (Message Transfer Agent - MTA je procedura, ki prenese ali izmenja sporočila v servisu elektronske pošte) z zamenjavo MTA v tekstu. Nepoznan MTA se lahko (na primer v testni proceduri) poveže z nekim delujočim MTA, tako da pošlje enega od znanih imen. To je tipično pretvarjanje identitete z namenom kraje delovnih virov ali informacij. Pretvarjanje uporabnikove identitete je prav tako mogoče s spretno uporabo usmerjevalno orientiranih naslovov.

b) Tajenje akcije ali servisa. V primeru pogodb ali drugih poslovnih dokumentov je tajenje izvora, predlogov ali dostave zelo boleče. Kako zaupati ponudbi, sprejeti z EDI servisom, če ni zagotovljen dokaz o identiteti pošiljatelja?

c) Zanikanje servisa. Zanikanje servisa se lahko zgodi zaradi naključne prekinitve, ki jo povzročijo lokalne sistemske napake ali pa neprilagojene komponente v sodelujočih sistemih kot npr. napačen vnos pri usmerjanju naslovov ali tabelah preslikav. Namerne prekinitve so za vzdrževalne namene normalne.

d) Prestrezanje podatkov. Prekinitev zaupnosti je najobičajnejši napad v obstoječih mrežah. S pomočjo sistemskega administratorja ni mogoče uganiti števila namernih vohunjenj ali vdorov drugih nepooblaščenih oseb, ki so sposobne čitati podatke na svojih ali pa tujih sistemih. Podatki so lahko prav tako prestreženi nenamerno, npr. pri napačno usmerjenih sporočilih itd.

e) Manipulacija s podatki. Manipulacija s podatki je kakršnakoli sprememba podatkov, ki oskruni njihovo integriteto. Upravljanje z naslovi elektronske pošte je v nekem smislu prav tako oskrunitev integritete, ki je povzročena pomotoma zaradi slabega vzdrževanja. Jasen primer je tudi procesiranje v pretvor-

nikih (gateway), kjer se sporočilo odreže ali pa se iz sporočila izgubi del telesa. Taka vrsta ranljivosti komunikacijskega sistema vključuje tudi manipulacijo z vsebino sporočila v izvornem lokalnem pomnilniku po nezavrnjenem predlogu ali manipulacijo z vsebino sporočila v pomnilniku prejemnika po nezavrnjeni dostavi sporočila.

3. VARNOSTNE FUNKCIJE IN SERVISI

Varnostno ogrodje se ukvarja z uporabo varnostnih servisov v okoljih odprtih sistemov (Open System Environment), kjer izraz "odprti sistemi" vključuje področja kot so: podatkovne baze, distribuirane rešitve, obdelava pisarniške dokumentacije in komunikacijske mreže. To ogrodje definira načine, kako zagotoviti zaščito sistemom in objektom znotraj komunikacijskega sistema ter interakcijo med sistemi. Ukvarja se z informacijo in zaporedjem operacij, ki se uporabljajo za zagotovitev specifičnih varnostnih servisov. Ti varnostni servisi se lahko uporabljajo v komunikacijskih sistemih kakor tudi pri izmenjavi informacij med sistemi in pri lokalnih virih oziroma podatkovno manipulativnih sistemih. Izraz "varnost" je v ISO dokumentih definiran kot "način za minimiziranje ranljivosti sistema in njegovih virov". Varnost torej razumemo kot sistem, ki preprečuje napade in ščiti samo vrednost sistema pred grožnjami z varnostnimi servisi, ki se uporabljajo na različnih nivojih omrežja.

Varnostni servisi temeljijo na uporabi varnostnih mehanizmov. Nekateri mehanizmi ščitijo pred napadi, drugi napade odkrivajo, nekateri izmed njih pa kasneje obnovijo prvotno stanje. Ti mehanizmi so:

a) Overjanje. Mnoge uporabniške rešitve odprtih sistemov imajo varnostne zahteve, ki so odvisne od pravilnega identificiranja vključenih osebkov. Take zahteve lahko vsebujejo zaščito sistema in virov pred neavtoriziranim dostopom, za katerega mora biti uporabljen na identiteti osnovan mehanizem za kontrolo dostopa, oziroma za namene zaračunavanja/tarifiranja. Postopek potrjevanja identitete imenujemo overjanje.
b) Kontrola dostopa. Mnoge uporabniške rešitve v odprtih sistemih vsebujejo varnostne zahteve, da se viri sistema lahko uporabljajo le v soglasju z dogovorjeno varnostno politiko. Proces dovoljevanja uporabe virov posameznim osebam znotraj okolja odprtega sistema in posledično zaščito pred takšno uporabo imenujemo kontrola dostopa.
c) Preprečitev tajenja. Servis za preprečitev tajenja zagotavlja ustrezno zbirko informacij, ki so sestavljene iz podatkov o izvoru ali dostavi, z namenom, da zaščiti pošiljatelja pred neresničnim zanikanjem prejemnika, da je podatke sprejel, ali pa z namenom, da zaščiti prejemnika pred neresničnim zanikanjem pošiljatelja, da je podatke poslal. Servis te podatke hrani in vzdržuje.
d) Integriteta podatkov. Vrednost podatkov v komunikacijah je dejansko njihova integriteta oziroma zagotovljena nespremenljivost podatka pri komunikaciji. Mnogo uporabniških rešitev v odprtih sistemih postavlja varnostne zahteve, ki so odvisne od integritete informacij, s katerimi te aplikacije poslujejo. Take zahteve lahko vključujejo zaščito informacij, ki se uporabljajo kot podpora drugim varnostnim servisom kot so: overjanje, kontrola dostopa, zaupnost, preverjanje in preprečitev tajenja. Če napadalec spremeni te informacije, lahko omeji ali izniči učinkovitost omenjenih servisov.
e) Zaupnost podatkov. Pogosto se pojavljajo zahteve po tajnosti podatkov. Take zahteve lahko vključujejo zaščito informacij, ki se uporabljajo kot podpora drugim varnostnim servisom kot so overjanje, kontrola dostopa ali integriteta. Če napadalec pozna te informacije, lahko omeji ali izniči učinkovitost omenjenih servisov. Vzdrževanje tajnosti podatkov imenujemo zaupnost podatkov.
f) Preverjanje. Varnostno preverjanje je neodvisen pregled in preizkus sistemskih zapisov in aktivnosti. Namen varnostnega preverjanja je neodvisen pregled in preizkus sistemskih zapisov in aktivnosti. Varnostno preverjanje testira ustreznost sistemskega nadzora, potrjuje njegovo skladnost z varnostno politiko, svetuje spremembe v nadzoru, politiki in procedurah, pomaga pri analizi napadov na sisteme in priporoča procedure za nadzor škode. Varnostno preverjanje zahteva zbiranje in zapisovanje podatkov, ki se na poti varnostnega preverjanja nanašajo na varnost. Varnostno preverjanje samo pa vključuje analize in poročanje o informacijah, zbranih na poti varnostnega preverjanja.
g) Upravljanje s ključi. V komunikacijskih in informacijskih sistemih obstaja vse večja potreba po podatkih, ki bi bili zaščiteni pred neavtoriziranimi razkritji ali manipulacijami. Varnost in zanesljivost takih mehanizmov je direktno odvisna od zaščite, ki jo dosežemo z varnostnimi parametri, imenovanimi "ključ". Namen upravljanja ključev je zagotoviti procedure za upravljanje s kriptografskimi ključi, ki se uporabljajo v simetričnih ali nesimetričnih kriptografskih mehanizmih. Upravljanje ključev vključuje: generiranje, distribucijo, instalacijo ključev ter shranjevanje in uničevanje ključev. Osnovni problem upravljanja s ključi je pripraviti šifrirni material, čigar izvor, integriteto in, v primeru tajnih ključev, zaupnost lahko garantiramo.

Namestitev posamezne varnostne funkcije v odprti arhitekturi ni natančno določena. Varnostni servisi ali funkcije so lahko zagotovljeni na različnih nivojih in z različnimi

protokoli, odvisno od zahtev uporabnikov in programskih rešitev. Nekatere rešitve so bolj, druge manj ranljive. Njihova zaščita je prav tako odvisna od prevzete varnostne politike in od uporabljene tehnologije. Lahko rečemo, da univerzalen model ne obstaja ter da se namestitev posameznih funkcij izbira po definiranju značilnosti in zahtev dane rešitve v zvezi z varnostjo in po pragmatičnem razmisleku.

V primerih nepovezanih protokolov, kot je primer IP, se uporablja tehnika označevanja, znana kot IPSO (IP Security Option). Oznake kot so npr. "občutljivo", "nerazporejeno", "stroga tajnost" navadno spremljajo prikrite podatke. Če so podatki poslani zanesljivemu komunikacijskem sistemu (dostava podatkov avtoriziranemu lokalnemu sistemu je garantirana) so take oznake lahko zadovoljiva zaščita, v primeru nepreizkušenih mrež kot so npr. javne podatkovne mreže pa so paketi podatkov prekriti in taka zaščita ne zadostuje.

Namestitev funkcij overjanja, integritete in zaupnosti v višje nivoje ali direktno v proces (npr. elektronska pošta) je jasna in pragmatična rešitev, ni pa optimalna. Namestitev varnostnih funkcij za vsako aplikacijo posebej (npr. za virtualni terminal, prenos datotek, servise direktorija) zahteva veliko razvojnega dela in podvajanje funkcionalnosti. Tak pristop prav tako nasprotuje principu, po katerem naj bi bila varnost integralen del celotnega komunikacijskega sistema in servisov, ki jih ta zagotovlja. Praksa je pokazala, da je tak pristop dandanes uporabnejši le zaradi kompleksnosti medsebojno povezanih mrež in različnih varnostnih zahtev v različnih rešitvah globalnih mrež kot je Internet.

4. VARNOSTNI MEHANIZMI

Mehanizme in algoritme, ki zagotavljajo različne varnostne funkcije in servise, imenujemo varnostne mehanizme. Ti mehanizmi dejansko oblikujejo hierarhijo in so lahko:

- mehanizmi višjih nivojev, kot so varnostni protokoli in semantična vsebina sporočil,
- mehanizmi nižjih nivojev, kot so kripto sistemi za formiranje zgoraj omenjenih mehanizmov višjih nivojev,
- fizični mehanizmi, kot so integrirana vezja za kripto zaščito in deli programske kode, ki uporabljajo zgoraj omenjene mehanizme.

Uporaba teh mehanizmov je odvisna predvsem od zahtevanih varnostnih funkcij in celovitosti sistema, ki ga želimo zaščititi. Varnost lokalnih sistemov je lahko v večji meri zagotovljena s fizičnimi varnostnimi ukrepi. V odprtih globalnih mrežah pa je zagotovitev varnosti komunikacij v smislu fizične varnosti nemogoča, zato se najpogosteje uporabljajo kriptografske tehnike.

Kriptografija je že dolgo znan način, s katerim lahko obdržimo informacijo tajno. Dandanes so kriptografski mehanizmi posebej razviti in se uporabljajo za zaščito prenosa podatkov in informacij. Obstaja mnogo kriptografskih mehanizmov, omenili bomo le osnovne, ki se uporabljajo v globalno povezanih mrežah: šifriranje in tehnike za zagotavljanje integritete in overjanja sporočil. Za podrobnosti glej(8,9).

Šifrirni mehanizem se uporablja za pretvorbo čistih tekstovnih sporočil v šifrirana sporočila, kriptograme. Šifrirni mehanizem je osnovan na javno poznanih algoritmih in najmanj enem ključu, ki je naključno izbran iz velike množice možnih ključev.

Mehanizmi za integriteto podatkov zagotavljajo tehnike, ki omogočajo, da zaporedja sporočil ostanejo nedotaknjena. To pomeni, da nobeno sporočilo ne ostane neodkrito, prezrto ali podvojeno in je ostala ohranjena originalna razvrstitev sporočil. Integriteta podatkov zagotavlja odkrivanje sprememb na prenešenih podatkih, če do njih pride, lahko pa tudi odpravljanje sprememb oziroma generiranje sporočil, kadar odpravljanje sprememb ni mogoče.

Navadno se za odkrivanje sprememb v podatkovnem nizu uporablja tehnika preverjanje vsote (checksum), ali pa bolj zaželjeno preverjanje s ciklično redundanco (cyclic redundancy check).

Overjanje se dandanes izvaja z uporabo gesel (password). Ta metoda je zelo ranljiva, tako overjanje pa je znano kot šibko overjanje. Močno overjanje (strong authentication) je osnovano na simetrični ali javni kripto zaščiti. Procedura močnega overjanja in izmenjava ključev sta opisani v CCITT priporočilih X.509 ali pa v ISO 9594.

V simetričnih kriptosistemih je za močno overjanje med katerimkoli parom strank A in B uporabljen ustrezen varnostni kontekst, ki mu pripada paroma medsebojno usklajen ključ. V asimetričnih šifrirnih mehanizmih je ključ razdeljen na dva dela: šifrirni ključ in dešifrirni ključ. Prejemnik sporočila ima ključ, s katerim lahko dešifrira, pošiljatelj pa uporablja različne ključe za šifriranje. Sistem zagotavlja varno komunikacijo samo v eni smeri in je poznan kot asimetrični ali javni šifrirni mehanizem. Le-ta zagotavlja popolno zaupnost, ne pa tudi overjanja pošiljatelja; če uporabimo tehniko digitalnega podpisa, lahko zagotovimo tudi overjanje.

Javni mehanizmi za šifrirani podpis imajo za overjanje več prednosti pred simetričnimi kripto sistemi. Upravljanje s ključi zelo poenostavi dejstvo, da se delijo javne šifre samo v parih in da je za vsako stranko potreben samo en par ključev.

Hitro se razširja področje tako imenovanih tehnik ničelnega znanja (zero-knowledge technique). V teh tehnikah igra varnostno overjanje informacij vsake stranke zelo dobro enako vlogo kot varnostni ključ v javnih šifrirnih kriptografskih sistemih, vendar le-to ne sme biti uporabljeno za šifriranje podatkov, temveč le za over-

janje podatkov in morda digitalnega podpisa. Nekaj obstoječih tehnik ničelnega znanja nudi zelo preprosto upravljanje s ključi, ki v celoti odpravijo potrebo po od uporabnika odvisnih javnih ključev. Šibka lastnost teh tehnik pa je, da je za generiranje varnostnih ključev potrebna tretja stranka in da ne morejo biti uporabljene za zagotovitev zaupnosti.

5. VARNOSTNA POLITIKA

Varnostna politika je politika zagotovitve varnostnih storitev v mrežah. Je integralni del odprtega modela, ki ga za lastne potrebe izvaja določena organizacija. Varnostna politika je množica pravil, ki določa eno ali več množic varnostno pomembnih aktivnosti iz ene ali več znanih množic varnostnih elementov. Ni nujno, da se ta politika uporablja pri vseh aktivnostih in elementih komunikacijskega sistema. To pomeni, da mora njena specifikacija vključevati specifikacije aktivnosti in elementov, na katere se politika nanaša. Pravila za vsak varnostni servis so izpeljana iz varnostne politike.

Navadno delimo varnostno politiko na politiko, osnovano na identiteti (identity-based), in politiko, osnovano na pravilih (rule-based). Prva je osnovana na ugodnostih ali možnostih, ki so dane uporabnikom oziroma na sezname oseb za nadzorovanje dostopa do relevantnih podatkov ali drugih virov. Druga varnostna politika pa določa, kaj je avtorizirano obnašanje posameznika. V sistemih, ki so osnovani na identiteti, se uporabniki praviloma predstavijo sistemu s prepustno besedo (password).

Uveljavljanje sprejete varnostne politike navadno poteka z informacijami o nadzorovanju varnosti. Ena izmed njih je varnostna oznaka. Varnostna oznaka je množica varnostnih atributov, ki so povezani z elementom, komunikacijskim kanalom ali podatki. Varnostna oznaka prav tako eksplicitno ali implicitno označuje organ, ki je odgovoren za kreiranje povezave in za varnostno politiko, ki izvaja z uporabo oznak. Primeri varnostnih oznak so: naznačitev občutljivosti (npr. nerazvrščeno, zaupno, itd.), naznačitev zaščite, odredba in druge zahteve v zvezi z rokovanjem in delom z določenimi podatki ali informacijami.

Druga zelo pomembna varnostno nadzorna informacija (Security Control Information - SCI) je potrdilo. Potrdilo vsebuje SCI, ki se nanaša na enega ali več varnostnih servisov. Potrdilo izda organ za potrdila. Uporablja se za pošiljanje SCI od organa do teles, ki to informacijo zahtevajo, da bi izvršili varnostno funkcijo. V splošnem lahko potrdilo vsebuje SCI za vse varnostne funkcije. V zgornjem poglavju opisani varnostni mehanizem vključuje izmenjavo SCI in sicer ali med dvema komunicirajočima strankama ali pa med varnostnim organom in sodelujočima strankama.

V opisanih mehanizmih se uporabljata dve obliki zaščitenih varnostnih informacij. Prva se imenuje varnostni žeton in se uporablja za zaščito varnostnih informacij, ki se prenašajo med sodelujočima strankama. Druga se imenuje varnostno potrdilo, uporablja pa se za zaščito varnostnih informacij, ki jih pridobimo prek organa, za uporabo pri eni ali pa več sodelujočih strankah.

Varnostno ogrodje ne definira metod in postopkov za uvajanje varnostne politike in pripadajočih SCI. To je prepuščeno razvoju posameznih organizacij in sistemov.

6. ZAKLJUČEK

Varnost je ključnega pomena pri razvoju mrež z dodano vrednostjo. Varnostni servisi in funkcije so potrebni za zaščito infrastrukture komunikacijskih in lokalnih sistemov, kakor tudi za zagotovitev zaupanja bodočih uporabnikov in zagotavljanje varnega transporta občutljivih in pomembnih informacij. Na srečo današnji hitri napredek tehničnega razvoja rapidno izboljšuje varnost mrež, istočasno pa zagotavlja še njihovo odprtost in povezanost.

7. REFERENCE

1. R.Reardon (ed.) Future Networks, Blenheim Online, London 1989
2. Internet: Getting started, SRI International, Menlo Park, CA, 1992
3. ISO, Information Processing Systems, Open System Interconnection Reference Model, Part:1 Security Architecture, ISO 7498-2, Geneva 1988
4. R.Grimm, Security on Networks: Do WE Really Need it?, Comp.Networks and ISDN Systems, Vol.17, No 4&5, October 1989, p.315-321
5. A.T.Karila, Open System Security - an Architectural Framework, Espoo 1991, Helsinki
6. D.W.Davies and W.L.Price, Security for Computer Networks, Sc.ed.,J.Willey and Sons, Chichester, 1989
7. S.Muftic, (ed.) Security Mechanisms for Computer Networks, Ellis Horwood Ltd, Chichester, 1989
8. C.Shannon, Communication Theory of Secrecy Systems, Bell System Technical Journal, Vol.28, 1949, p.656-715
9. ISO, Information Technology, Security Techniques, A Data Integrity Mechanism, ISO DP 9797, Geneva 1990
10. S.Walker, Network security: The parts of the Sum, Proceedings of the 1989 IEEE Computer Society Symposium on Security and Privacy, Oakland 1989, p.2-9
11. The Directory - Overview of Concepts, Models and Services, CCITT Recommendation X.500, Melbourne 1988, and The Directory, Part 8: Authentication Framework, CCITT Recommendation X.509 (Melbourne 1989,)
12. ISO 9594, Information Processing Systems, OSI - The Directory, 9594 through parts 1 - 8, Geneva 1989
13. ISO 10181, Information Technology, OSI Security Model, Part 1 Security Framework, Part 2, Authentication framework A.Shamir, Identity-Based Cryptosystem and Signature Scheme, Advances in Cryptology: Proceedings of Crypto 84, Springer, Berlin, 1985, pp.47-53