Mr. Antun Brumnić

Fakultet organizacije i informatike
V a r a ž d i n

UDK:681.324
Stručni rad

SIGURNOST RAČUNARSKIH KOMUNIKACIJA

Opisuje se ugroženost računarskih komunikacija od neovlaštenih korisnika i tipovi mogućih napada na njih. Navode se načini zaštite i sigurnosni mehanizmi kojima se postiže sigurnost komunikacija, posebno postupci šifriranja.

Sigurnost računarskih sistema; podatkovne komunikacije; kriptografija.

Razvoj računarskih mreža i njihov značaj te ranjivost zahtijevaju posvećivanje posebne pažnje njihovoj sigurnosti.
Poznati su primjeri zloupotrebe računarskih komunikacija zbog njihove nedovoljne zaštite, a time su izazvane velike materijalne štete napadnutim sistemima.

Ugroženost sistema

Ugrožavanje sistema može biti **slučajno** (kvarovi opreme i pogreške u programima) ili **namjerno**, odnosno **aktivno** (promjena informacija i/ili promjena rada sistema) ili **pasivno** (nema promjena, npr. prisluškivanje komunikacijskog voda radi neovlaštenog dobivanja informacija).
Sistem s računarskim komunikacijama ugrožen je zbog mogućnosti

- uništenja podataka i informacija i/ili drugih resursa (npr. programa),
- iskrivljenja ili promjene informacija,
- krađe, uklanjanja ili gubitka podataka i informacija,
- neovlaštenog korištenja usluga (odn. resursa),
- odavanja informacija i
- ometanja usluga.

Ciljevi zaštite jesu da se to otkrije i onemogući, ili bar otkrije.
Sistemi su najviše ugroženi **napadima**. Napad je namjerno realizirana prijetnja. **Tipovi napada**, koji posebno prijete sistemima koji obrađuju podatke i njima komuniciraju jesu :

- **maskiranje**,
- **ponavljanje**,
- **promjena poruke**,
- **sprečavanje ili ometanje usluge**,
- **unutrašnji napad**,

- **napad izvana**,
- **ulaz na mala vrata**,
- **trojanski konj**.

Maskiranje je postupak kojim netko nastoji preuzeti tuđu ulogu kako bi time neovlašteno stekao tuđa prava. Obično se koristi u kombinaciji s drugim tipovima aktivnih napada.

Ponavljanje je reproduciranje poruke ili dijela poruke da bi se ostvarila lažna autorizacija. Napadač na sistem ponavlja npr. poruku ili dio poruke koja sadrži informacije za provjeru autentičnosti da bi se predstavio sistemu kao netko drugi (maskiranje) i time stekao prava tog drugog.

Promjena poruke je napad kojim se mijenja sadržaj poslane poruke da bi se neovlašteno postigao neki cilj.

Sprečavanje usluge se događa kada netko ne izvršava svoje funkcije kako treba ili kada sprečava druge da izvršavaju svoje funkcije na ispravan način.

Unutrašnji napad se događa kada legitimni korisnik upotrebljava sistem na nedozvoljen način. Ovo je jedan od najopasnijih napada na sistem. Sprečava ga se

- rigoroznom provjerom osoblja,
- praćenjem korištenja sistema da bi se otkrili pokušaji napada na nj i
- pomnom provjerom uređaja, programa, sigurnosne politike i konfiguracije sistema
- da se osigura njihov ispravan rad (pouzdana funkcionalnost).

Vanjski napad poduzima netko izvan sistema. Najčešće korišteni načini ovog tipa napada jesu:

- **upad u vod** (aktivni i pasivni),
- **hvatanje ili sprečavanje odašiljanja**,
- **maskiranje u autoriziranog korisnika** ili **u komponentu sistema**,
- **zaobilaženje postupaka provjere autentičnosti ili kontrole pristupa**.

Ulaz na mala vrata je napad u kojem se neka cjelina sistema mijenja tako da dozvoljava napadaču neautorizirano djelovanje na naredbu ili na određeni događaj ili niz događaja. Npr. ovim napadom može se tako promijeniti provjeravanje šifre da mehanizam provjeravanja prihvati šifru napadača, koji tako neovlašteno uđe u sistem (kroz pokrajnji ulaz).

Trojanski konj ima dvije vrste funkcija: autorizirane i neautorizirane. Autorizirane mu omogućuju pristup do resursa sistema, koji onda napada neautoriziranim funkcijama.

Ciljevi zaštite podataka, informacija i računarskih resursa od zloupotrebe, oštećenja ili uništenja (namjernog i slučajnog) u računarskim komunikacijama su **očuvanje**

- **tajnosti podataka i informacija**,
- **integriteta podataka i informacija**,
- **raspoloživosti podataka i informacija**,
- **raspoloživosti usluga (servisa)**

sistema koji se štiti.

Očuvanje tajnosti podataka i informacija je sprečavanje neovlaštenog upoznavanja njihovog sadržaja ili drugih osobina (npr. frekvencije korištenja određenih podataka i informacija).

Očuvanje integriteta podataka i informacija je sprečavanje njihovih neovlaštenih promjena i slučajnog ili namjernog oštećenja ili uništenja.

Očuvanje raspoloživosti podataka i informacija, odnosno **usluga sistema** je sprečavanje aktivnosti (namjernih ili slučajnih) koje onemogućuju privremeno ili trajno korištenje podataka i informacija, odnosno usluga.

Štite se:

- **informacije i podaci** (uključivo programi i pasivni podaci koji se odnose na sigurnosne mjere kao što su lozinke,
- **komunikacije i usluge obrade podataka** i
- **oprema i sredstva**.

Načini zaštite

Korisnici sistema u pravilu su osobe ili programi. Oni mogu biti autorizirani za pristup podacima i informacijama, i/ili za njihovu promjenu i/ili korištenje usluga sistema. Pravo korištenja podataka, informacija i drugih resursa imaju samo autorizirani korisnici. Autorizacija može biti bez ograničenja, ili može biti selektivna - ograničena samo na pravo pristupa do određenih podataka i informacija, ili mijenjanja samo nekih podataka, ili korištenja dijela resursa.
Prijetnje sistemu potječu od neautoriziranih, ali i autoriziranih korisnika.
Ovisno o prirodi autorizacije koja se koristi sigurnosne politike (politike zaštite) mogu se svrstati u dvije skupine:

- politike temeljene na **pravilima** i
- politike temeljene na **identitetu**.

Politika temeljena na pravilima zasniva se na manjem broju propisanih općih atributa. U zaštićenom sistemu podaci i resursi označuju se sigurnosnim oznakama (labelama). Njihova pravila i atributi mogu biti pohranjeni u informacijsku bazu specijaliziranu za sigurnost (zaštitu) /SMIB - Security Management Information Base/. Sigurnosnom politikom određen je način upotrebe oznaka i atributa koje one sadrže u cilju zaštite sistema. Ponekad je potrebna suradnja i dogovaranje između cjelina koje komuniciraju da se ustanovi sigurnosno značenje atributa u oznakama.

Politika temeljena na identitetu koristi kriterije autorizacije temeljene na specifičnim individualnim atributima. Cilj ove politike je ograničavanje pristupa podacima i/ili resursima. Ostvaruje se na dva načina:

- informaciju o pravu pristupa nosi onaj tko pristupa podacima ili resursima,
- informacija o pravu pristupa je sadržana u podacima kojima se pristupa.

Mjere za zaštitu podataka i informacija, i računarskih resursa, mogu se svrstati u tri kategorije:

- sprečavanje neovlaštenog pristupa,
- evidentiranje pristupa i
- selektivno ograničavanje pristupa

podacima, informacijama i resursima.

Za sigurnost sistema nisu dovoljne samo mjere zaštite komunikacija. Informacije koje se razmjenjuju između sistema mogu biti zaštićene, ali ako ne postoji fizička zaštita pristupa sistemima, ova zaštita će biti uzaludna. Zato je za sigurnost komunikacija potrebno, uz mjere njihove zaštite, poduzeti i druge mjere zaštite sistema.

Sigurnosni mehanizmi

Sigurnosna politika se ostvaruje raznim sigurnosnim mehanizmima.
Postoje tri klase mehanizama kojima se postiže sigurnost. To su:

- **sprečavanje**,
- **otkrivanje**,
- **oporavak**.

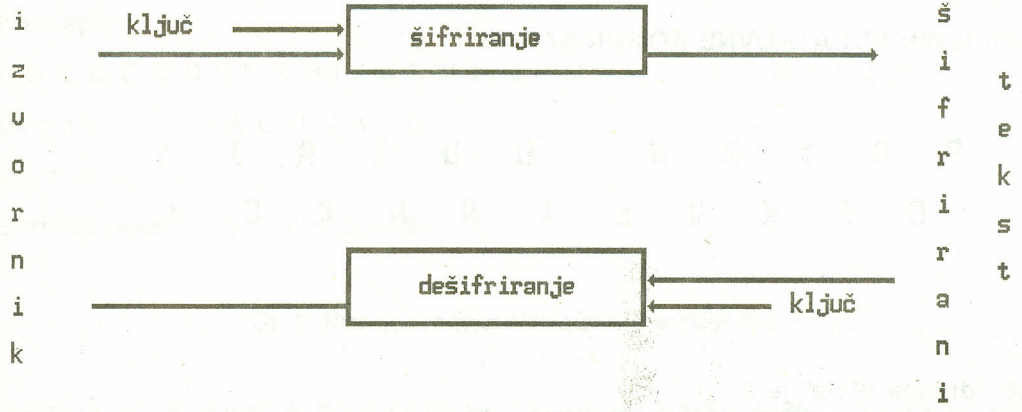
Mehanizmi kojima se ostvaruju postupci osiguranja podataka jesu:

- **šifriranje**,
- **digitalni potpis**,
- **kontrola pristupa**,
- **cjelovitost podataka**,
- **provjera autentičnosti**,
- **promet bez sadržaja**,
- **kontrola puta**,
- **ovjeravanje** (notarizacija),
- **fizička sigurnost i sigurnost osoblja**,
- **pouzdana sklopovska oprema (hardware) i programi**

Kriptografske tehnike i šifriranje

Kriptografija je temelj mnogim mehanizmima za postizanje sigurnosti. Kriptografske funkcije koriste se u šifriranju, dešifriranju, očuvanju cjelovitosti podataka, provjeri autentičnosti, pohranjivanju i provjeravanju lozinki, ostvarenju vjerodostojnosti i drugim.
Kriptografija je skup postupaka kojima se mijenja način predstavljanja informacija s ciljem da se one zaštite.
Suprotnu funkciju ima kriptoanaliza koja predstavlja skup postupaka za neovlašteno otkrivanje sadržaja šifriranog teksta ili postupaka šifriranja.
Kriptografija i kriptoanaliza su područja kriptologije, znanosti o tajnosti informacija.

Pretvaranje izvornog teksta (izvornika) u šifrirani (kriptogram) naziva se **šifriranje** (encipherment) ili enkripcija, a vraćanje šifriranog teksta u izvorni **dešifriranje** (decipherment) ili dekripcija. Šifrira se i dešifrira uz upotrebu jednog **ključa** ili više njih.
Rezultat dešifriranja je izvorni tekst (čitav ili djelomičan). Dešifriranje je ponekad ireverzibilno (npr. dio podataka se gubi, pa se ne dobiva čitav izvorni tekst) kada je nepoželjno da se dobije originalni izvorni tekst, kao što su npr. lozinke. (Npr. dešifriranjem se dobije samo dio poruke u kojem nema lozinke.)
Kriptografske funkcije djeluju na polja, jedinice podataka, i/ili nizove podatkovnih jedinica. One koriste kriptovarijable. Glavna kriptovarijabla je **ključ** koji upućuje na specifične transformacije.
Kriptografski protokoli se oblikuju da budu otporni na napade na kriptosistem kojima se mijenja sadržaj poruka, a često i na analizu prometa kojom se pokušava probiti



Sl. 1 Zaštita sadržaja

kriptosistem. Specifična protumjera za analizu prometa, tajnost prometnog toka, nastoji sakriti prisustvo ili odsustvo podataka i njihove karakteristike. Ako se šifrirani tekst prespaja (komutira, npr. kod komutacije paketa), adresa mora ostati izvorna u skretištima i prolazima (gateway). Ako se podaci šifriraju samo na svakoj vezi, a dešifriraju (i tako postaju ranjivi) u skretištima i prolazima, onda je to šifriranje od veze do veze. Ako su u skretištima ili prolazima u izvornom obliku samo adresa i kontrolni podaci, onda je to šifriranje s-kraja-na-kraj. Šifriranje s-kraja-na-kraj je poželjnije sa sigurnosne točke gledišta, ali je znatno kompleksnije. Šifriranje od-veze -do- veze i s-kraja-na-kraj može se kombinirati da se ostvare višestruki sigurnosni ciljevi.

Kriptografske tehnike mogu osigurati ili pomoći osiguranju protiv:

- promatranja i/ili promjene niza poruka,
- analize prometa,
- oporecivosti (poslanih poruka),
- krivotvorenja,
- neautoriziranog spajanja i
- promjene poruka.

Postoje dva osnovna postupka šifriranja:
- transpozicija i
- supstitucija,

koji se koriste samostalno ili u kombinaciji.

Transpozicija mijenja međusobni položaj jedinica kojima se predstavljaju informacije (npr. znakovi ili bitovi). Primjer transpozicije znakova putem ključa "dubina plota" prikazan je na sl. 2.

Izvorni tekst: PODATKOVNE KOMUNIKACIJE

P D T O N O U I A I E
O A K V E K M N K C J

Ključ: "dubina plota" je 2
Šifrirani tekst: PDTON OUIAIEOAKVEKMNKCJ

a)

P O O A
O K V K M K C
D T N U I I E
A E N J

Ključ: "dubina plota" je 4
Šifrirani tekst: POOAOKVKMKCDTN UIIEAENJ

b)

Sl. 2 Primjer dobivanja šifriranog teksta transpozicijom

Supstitucija zamjenjuje bitove, znakove ili skupine bitova ili znakova supstitutima. Najjednostavniji oblik je **linearna supstitucija**. Kod nje se svaki znak (skupina znakova ili riječ) izvornika zamjenjuje uvijek istim znakom ili skupinom znakova. Npr. slovo A uvijek se u šifriranom tekstu predstavlja slovom Ć. Primjer zamjene slovnih znakova linearnom supstitucijom prikazan je na sl. 3. Ključ je tri, što znači da se svako slovo izvornika zamjenjuje slovom koje ga slijedi s udaljenošću tri. Npr. slovo A zamjenjuje se slovom Ć, slovo B slovom D, itd. Budući da se koristi jedna abeceda ili alfabet, linearna supstitucija u primjeru je monoalfabetska (jednoabecedna). (Iza posljednjeg znaka abecede ona se ponavlja, tj. iza slova Ž slijedi slovo A.)

Abeceda:

A B C Č Ć D Đ E F G H I J K L M N O P Q R S Š T U V W X Y Z Ž

Izvornik: R A Č U N A L O

Ključ = 3

Šifrirani tekst: U Ć E Y R Ć P S

Sl. 3 Primjer monoalfabetske supstitucije

Poseban slučaj linearne supstitucije predstavlja **kodiranje**. Kod kodiranja se kao ključ koristi **kodna knjiga**. Ona sadrži riječi i izraze izvornika i njihove substitute šifriranog teksta. Na sl. 4 ilustrirano je kodiranje jednostavnim primjerom. Svakoj riječi (skupina slova) pridružen je kod (skupina znamenki).

Riječ	Kod
AVION	1420
ELEKTRONIČKO	2643
INŽENJER	5839
RAČUNALO	7561

ELEKTRONIČKO RAČUNALO = 2643 7561

Sl. 4 Primjer kodiranja

Kod **nelinearne supstitucije** svakom znaku izvornika, kada se više puta javlja u tekstu, u pravilu se pridružuje drugi šifrirani znak (ili skupina znakova). Ako se pritom koristi više abeceda, supstitucija se naziva polialfabetska (višeabecedna). Većina polialfabetskih šifri su šifre s periodičkom supstitucijom, baziranom na periodu d. (Kada je d = 1, šifriranje je monoalfabetsko.) Za ilustraciju se navodi Vigenerovo šifriranje, bazirano na pomaknutim abecedama. Na sl. 5 prikazana je Vigenerova tabela s osnovnom abecedom koja je proširena znakovima engleske abecede, a iz nje su radi jednostavnosti grafičkog prikazivanja izostavljena naša slova koja se predstavljaju s više nego jednim znakom ("dž", "lj" i "nj"). Koristi se ključ koji se sastoji od **d** slova:

$$K = k1\ k2\ \ldots\ kd,$$

a svako slovo ki određuje pomak u i-toj abecedi. Primjer takvog šifriranja prikazan je na sl. 6.

Korisnici kriptografskog sistema - pošiljalac i primalac -moraju poznavati dva bitna elementa:

- algoritam i
- ključ.

Kada se isti ključ koristi za šifriranje i dešifriranje, šifriranje je **simetrično**, a ako se koriste različiti ključevi za šifriranje i dešifriranje, šifriranje je **asimetrično**.

Kod simetričnog šifriranja algoritam je često javan, a ključ ili ključevi su tajni. Sigurnost zavisi o sigurnosti ključeva. Najpoznatije simetrično šifriranje je "Data Encryption Standard" (DES) koji je usvojen u SAD kao standard, a u postupku je njegovo usvajanje kao međunarodnog standarda. Razvila ga je kompanija IBM. Njegov algoritam šifriranja je javno publiciran.
Podaci koji se šifriraju prema DES-u podijele se u blokove od 64 bita (8 bajtova). Svaki blok se permutira, a zatim 16 puta transformira transpozicijom i polialfabetskom supstitucijom, koje ovise o ključevima. Ključevi su 64-bitni, a generiraju se iz tzv. glavnog ključa. Budući da sigurnost sistema ovisi o zaštićenosti ključeva, posebnu pažnju treba posvetiti njihovoj zaštiti i baratanju njima.

Kod asimetričnog šifriranja ključ je javan, pa se sistemi s takvim šifriranjem nazivaju i sistemi s javnim ključem.

		izvornik																											
		A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž
	A	A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž
	B	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž	A
	C	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž	A	B
	Č	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž	A	B	C
	Ć	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž	A	B	C	Č
	D	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć
	Đ	Đ	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D
	E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ
	F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E
	G	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F
	H	H	I	J	K	L	M	N	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G
	I	I	J	K	L	M	N	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H
	J	J	K	L	M	N	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H	I
k	K	K	L	M	N	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J
	L	L	M	N	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K
lj	M	M	N	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L
	N	N	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M
u	O	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N
	P	P	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O
č	Q	Q	R	S	Š	T	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P
	R	R	S	Š	T	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S	S	Š	T	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	Š	Š	T	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	T	T	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š
	U	U	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	T
	V	V	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	T	U
	W	W	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	T	U	V
	Z	X	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	T	U	V	W
	Y	Y	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	T	U	V	W	X
	Z	Z	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	T	U	V	W	X	Y
	Ž	Ž	A	B	C	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	T	U	V	W	X	Y	Z

Sl. 5 Vigenerova tabela

Izvornik: PODATKOVNEKOMUNIKACIJE
Kljuc: TERMINAL

PODATKOV NEKOMUNI KACIJE
TERMINAL TERMINAL TERMIN

Sifrirani tekst: HUVMCZOY FLCBWGNV DESWST

Sl. 6 Primjer polialfabetske supstitucije

Najpoznatiji takav sistem je RAS (naziv potječe od inicijala prezimena njegovih tvoraca: Rivest, Shamir, Adelman). Temelji se na upotrebi velikih prim brojeva. Do sada je ostao neprobojan. Zbog dugog vremena potrebnog za šifriranje i dešifriranje koristi se samo za specijalne svrhe (npr. distribuciju ključeva DES-a).

Mehanizmi digitalnog potpisa

Digitalni potpis je šifrirani identifikator pošiljaoca koji se koristi u uslugama osiguranja, npr. uslugama provjere autentičnosti i neporecivosti. Podatkovna jedinica s potpisom može se generirati samo uz upotrebu privatnog ključa, što znači da je može generirati samo posjednik tog ključa i nitko drugi (npr. primalac podataka). Na taj način može se uvijek jednoznačno odrediti pošiljaoc potpisanih podataka. Ako naknadno dođe do nesporazuma između primaoca i pošiljaoca, pouzdana treća strana (sudac) može prosuditi autentičnost potpisane podatkovne jedinice. Ako primalac želi biti siguran u cjelovitost primljenih podataka i autentičnost pošiljaoca, može isto tako koristiti usluge pouzdane treće strane (posrednika ili arbitra) koja mu to potvrđuje, pa pošiljalac ne može poreći poslane podatke.

Mehanizmi kontrole pristupa

Kontrola pristupa je ograničavanje pristupa resursima sistema na samo ovlaštene (autorizirane) korisnike, programe ili procese. Mehanizmi kontrole pristupa ostvaruju se tehnikama popisa ovlaštenih korisnika, matrica s podacima o ovlaštenim korisnicima i kontroliranim resursima, lozinkama i oznakama kojima se mogu dokazati prava pristupa.

Mehanizmi cjelovitosti podataka

Cjelovitost (integritet) podataka je stanje kada su podaci preuzeti u računarske resurse jednaki (identični) onima na izvornim dokumentima, odnosno u komunikacijama kada su primljeni podaci identični poslanima. Mehanizmi cjelovitosti podataka koji se prenose čuvaju cjelovitost pojedinačnih podatkovnih jedinica ili čitavog niza podatkovnih jedinica u nekom podatkovnom toku koji se ostvaruje podatkovnom vezom.
Za otkrivanje iskrivljenja (promjene) sadržaja poruke mogu se koristiti tehnike koje se upotrebljavaju za zaštitu od pogrešaka. Ako zaglavlje poruke (odnosno bloka koji se prenosi) ili njezin završni dio nije zaštićeno mehanizmima cjelovitosti, uljez koji poznaje postupak zaštite od pogrešaka može zaobići provjere i promijeniti sadržaj poruke.
Promjena sadržaja poruke ne može se spriječiti, ali se može otkriti.

Mehanizam provjere autentičnosti

Za provjeru autentičnosti koriste se lozinke. Ako postoji opasnost ponavljanja dijela poruke (od strane napadača) u kojem se nalazi lozinka, lozinka se može šifrirati. Autentičnost se provjerava i digitalnim potpisom.

Mehanizmi prometa bez sadržaja

Sprečavanje analize prometa postiže se slanjem poruka koje ne sadrže informacije, već služe samo za zavaravanje onoga koji neovlašteno analizira podatkovni promet. Taj lažni promet mora svojim karakteristikama što više odgovarati stvarnom, a podaci o njemu, na temelju kojih bi se mogla otkriti njegova lažnost (npr. iz zaglavlja poruka) šifrirani ili maskirani.

Mehanizam kontrole puta

Sigurnost podataka u prijenosu može se povećati ako se za sve podatke ili za one posebno osjetljive odredi specifičan put prijenosa koji je fizički zaštićen.

Mehanizam ovjeravanja

Mehanizam ovjeravanja koristi pouzdanog trećeg učesnika ("bilježnika", notara) koji za račun strana koje komuniciraju ovjerava autentičnost pošiljaoca, integritet podataka, vrijeme u koje su podaci poslani ili primljeni ili neka druga svojstva ili činjenice.

Fizička sigurnost i sigurnost osoblja

Fizička zaštita (postizanje fizičke sigurnosti) je skupo i nastoji se smanjiti potreba za njom korištenjem drugih, jeftinijih načina.
Radne postupke treba definirati da bi se osigurali odgovarajući postupci i da se odredi odgovornost osoblja.

Pouzdanost sklopovske opreme (hardware) i programa

Pouzdani uređaji i programi bitan su uvjet postizanja sigurnosti u sistemima s telekomunikacijama, kao i u onima bez njih.
Treba obratiti pažnju da pojedine cjeline nisu promijenjene slučajno ili namjerno, u smislu smanjenja pouzdanosti rada ili zaštite sistema, npr. za vrijeme dogradnje ili održavanja.
Za postizanje sigurnosti sistema neke cjeline u njemu moraju djelovati pouzdano.

ZAKLJUČAK

Sigurnost podataka, informacije i računarskih resursa može biti ugrožena namjernim akcijama čiji je cilj zloupotreba i/ili uništenje podataka, informacija ili drugih resursa, ali i slučajnim nezgodama. Masovno korištenje telekomunikacijskih mreža za pristup udaljenim računarskim resursima znatno povećava ranjivost sistema. Zato treba posebnu pažnju posvetiti zaštiti sistema od zloupotreba i nezgoda kojima su podložne računarske komunikacije.

Potpunu sigurnost (100 %) nekog komunikacijskog sistema nemoguće je ostvariti, no uz dobru sigurnosnu politiku i primjenu razvijenih mehanizama zaštite, moguće je postići vrlo visok stupanj zaštite i sigurnosti. Pri određivanju potrebnog stupnja sigurnosti treba imati u vidu rizik i štete koje mogu nastati zbog slabe zaštite, ali i troškove zaštite koji rastu sa stupnjem sigurnosti.

Literatura

1. Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture, ISO (1989)

2. D.E.Denning, Cryptography and data security, Addison-Wesley Publishing Co. (1983)

3. J.M.Carrol, Computer security, 2nd ed.,Butterworths, (1987)

4. F.Piper, Cryptografic Uses of Large Numbers, Mathematical Spectrum 21 (1988), The University of Sheffield

Primljeno: 1989-07-15.

Brumnić A. Computer communication security

Summary

The paper deals with the security of computer communications. The threats of unauthorised users and the types of attacs to data communication facilities, as well as to the computer resources which are accessible by data communication are described. Protection methods and security mechanisms are presented. A special attention is paid to the encryption/decryption techniques.