

# Sigurnost

- **Problem sigurnosti**
- **Autentifikacija**
- **Programske pretnje**
- **Sistemske pretnje**
- **Sigurnosni sistemi**
- **Detekcija provaljivanja-upada**
- **Šifrovanje**
- **Windows NT**

# Problem Sigurnosti

- Pod **sigurnošću** moramo smatrati **spoljašnju okolinu** sistema,
- i **zaštititi sistem** od:
  - ☞ **neautorizovanog pristupa**
  - ☞ **zlonamernih modifikacija ili uništenja**
  - ☞ **slučajnih nedoslednosti**
  - ☞ **zabrana usluga (DoS)**
- **Lakše je zaštititi se od**
  - ☞ **slučajnih**
  - ☞ **nego**
  - ☞ **od zlonamernih zloupotreba**

# Nivoi Sigurnosti

- **Apsolutna sigurnost ne postoji, ali se uvek primenjuje**
- **i to na 4 nivoa:**
- **1. Fizički nivo**
  - ☞ Računari i mrežna oprema moraju biti fizički obezbeđeni
  - ☞ od vatre, vode, provalnika itd
- **2. Ljudski faktor**
  - ☞ Poverljivi i ozbiljni ljudi moraju da se izaberu da rade sa sistemom.
- **3. Mrežni nivo**
  - ☞ Računari danas intenzivno koriste mreže pa imaju dva problema po mreži,
    - 📄 da ne dozvole pristup svakome
    - 📄 da ne dozvole modifikaciju svojih podataka
    - 📄 ulazak virusa ili drugih zlonamernih podataka i programa u svoj sistem.
- **4. Nivo operativnog sistema**
  - ☞ Operativni sistem mora zaštititi samog sebe
  - ☞ od slučajnog ili namernog oštećenja

# Autentičnost

- **Glavi problem sigurnosti za operativne sisteme je**
  - ☞ **korisnička autentičnost**
  - ☞ odnosno da se zna
  - ☞ da li je to **pravi ovlašćeni korisnik** ili nije
- **Svaki korisnik prilikom dolaska na sistem**
  - ☞ mora
  - ☞ sebe da identifikuje
- **Generalno, autentifikacija se bazira na 3 načina:**
  - ☞ **1. hardverskim komponentama** kao što je ključ ili ID kartica
  - ☞ **2. poznavanjem poverljivih informacija** kao što je lozinka
  - ☞ **3. korisničkim atributima** kao što je otisak prsta, otisak sa mrežnjače oka, potpis

# Autentičnost Kroz Password-e(lozinke)

- **Korisnički identitet je najčešće ostvaren:**
  - ☞ uz pomoć **password**-a(lozinke)
  - ☞ mogu biti ostvareni ili neke specialne vrste ključeva
- **Lozinke moraju biti čuvane u tajnosti:**
  - ☞ Česta promena lozinke
  - ☞ Korišćenje lozinke koje se **ne pogađaju lako**
  - ☞ **Registrowanje svih neuspelih pokušaja.**
- **Lozinke takođe mogu biti:**
  - ☞ **šifrovane**
  - ☞ **ili**
  - ☞ **se smeju koristiti samo jednom**

# Programske Pretnje

- Kada je program napisao jedan korisnik,
  - ☞ a njime se služe drugi korisnici,
  - ☞ moguće je zlonamerno korišćenje
- **Trojan Horse(trojanski konj)**
  - ☞ segment koda, koji zloupotrebljava svoju okolinu
  - ☞ eksploatiše mehanizme za korišćenje programa
  - ☞ napisane od strane korisnika
  - ☞ kako bi bili izvršavani od strane nekih drugih korisnika
- **Trap Door(klopka)**
  - ☞ Specificira identifikator korisnika ili lozinku
  - ☞ Koji zaobilazi normalne sigurnosne procedure
  - ☞ Može biti deo kompajlera
- **Prepunjenje steka ili bafera (buffer overflow)**
  - ☞ Koristi bug u programu
  - ☞ (može biti prepunjenje ili steka ili memorijskog bafera)

# Trojan Horse

- **Trojanski kod** predstavlja
- **podmetanje svog ilegalnog koda**
- u kod programa,
- čime se može promeniti:
  - ☞ **funkcija**
  - ☞ **ili**
  - ☞ **ponašanje originalnog programa**
- realizuje se preko **search path** podmetanja

# Trap Door (Klopka)

- **Klopka (trap door)**

- **Autor programa**

- ☞ može ostaviti **prazna mesta u svom kodu** (trap door)

- ☞ koje može kasnije koristiti

- **Ako bi napadač znao za ta mesta**

- ☞ mogao bi da podmeće svoj kod

- **Kompajleri**

- ☞ podmetnuti prevodioci

- ☞ mogu to isti da rade

- ☞ da prave rupe u objektnom kodu

# Prepunjenje Steka i Bafera

- Stek ili bafer prepunjenje je najčešći napad koji dolazi sa mreže
- Napadač korisiti grešku u programu,
  - ☞ odnosno **nedovoljne kontrole** u programu,
  - ☞ **po pitanju razdvajanja steka, podataka i koda.**
- Tada napadač šalje **više ulaznih podataka**
  - ☞ nego što program očekuje i
  - ☞ isprobava ranjivost programa na sledeći način:
    - ☞ 1. prepunjava ulazno polje, argumente komande linije ili ulazni bafer sve dok ne dođe do steka
    - ☞ 2. prepisuje **važecu adresu u steku** sa **adresom svog koda**, a **kod smešta u stek u sledećom koraku**
    - ☞ 3. puni svoj kod u prostor na steku, kao na primer, neku komandu
- Ako ovo napadač uspe da se obavi,
  - ☞ kod programa koji se nedovoljno štitio
  - ☞ preko steka će izvršiti divlji code
  - ☞ koji je ubačen prekoračenjem bafera

# Sistemske Pretnje

## ■ 1. Worms(crvi):

- ☞ Koristi mehanizam umnožavanja; samostalni program

## ■ Internet crvi

- ☞ Iskorišćen u UNIX mrežnom okruženju napravivši veliki problem
  - 📄 Napadavši pomoću finger i sendmail programa
- ☞ **Metoda udice**
  - 📄 predstavlja glavni program za učitavanje crva

## ■ 2. Virusi:

- ☞ delovi koda ugrađenih u legitimne programe

## ■ Glavni uticaj na mikroračunarske sisteme

- ☞ Download viralnih programa sa mreže
- ☞ Ili medijuma koji sadrže infekciju.

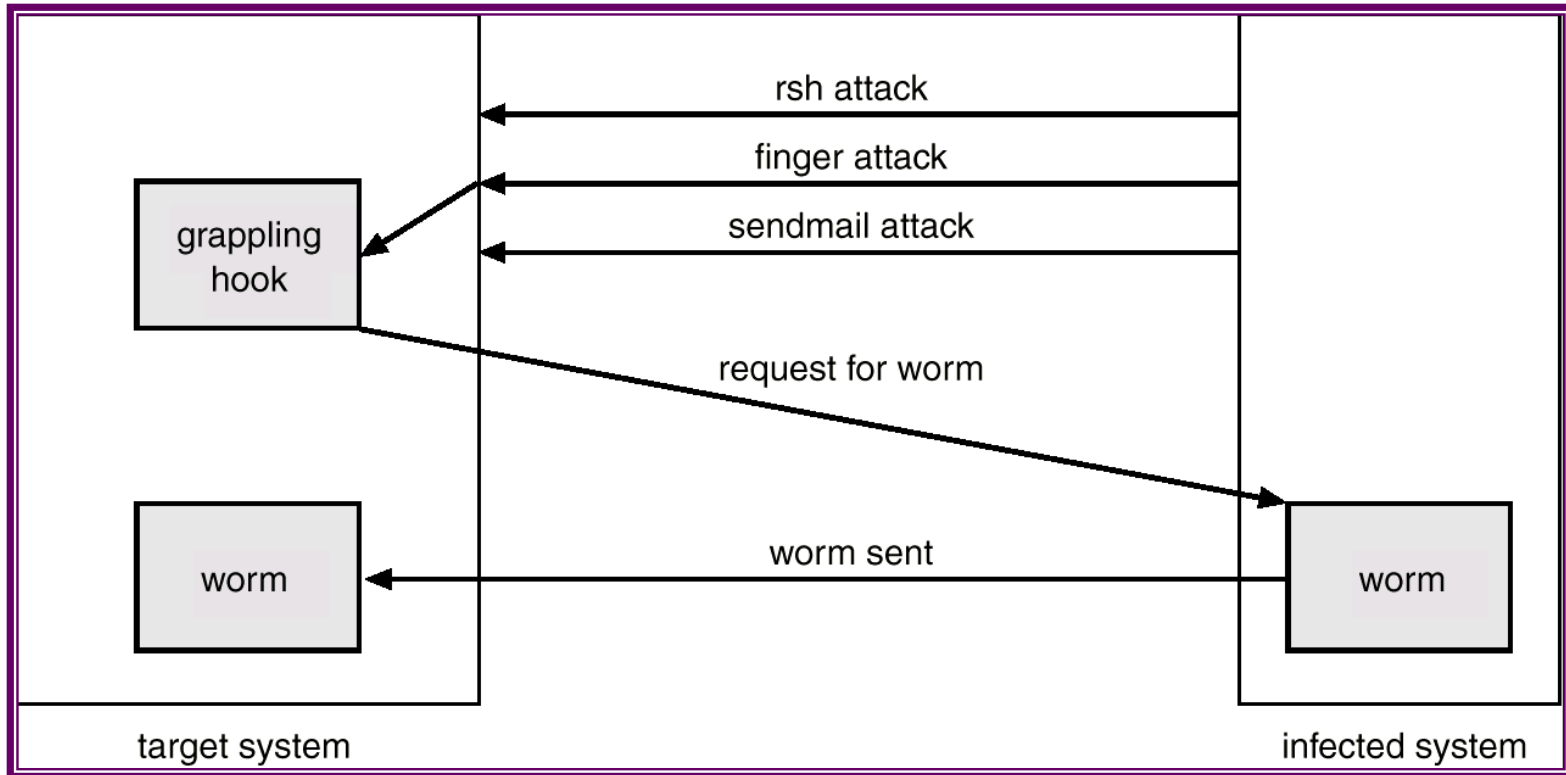
## ■ 3. Blokada usluga (DoS, DDoS):

- ☞ **Preopterećenje** ciljnog kompjutera
- ☞ sprečava
- ☞ rad bilo kog korisnog zadatka

# WORMS (Crvi)

- **Standalone program**
- **Crv je proces koji koristi**
  - ☞ mehanizam umnožavanja procesa,
  - ☞ a krajnji efekat svega je obaranje sistemskih performansi.
- **Na mreži su crvi jako opasni**
  - ☞ jer mogu da se prošire i blokiraju celu mrežu.
- **Tako je 1988. godine Morisov crv napravio veliku štetu po UNIX sistemima.**
- **Crv se sastoji od:**
  - ☞ **glavnog programa**
  - ☞ **udice (grappling hook)**
- **Zaraženi sistem tehnikom bafer-stek prekoračenja,**
  - ☞ pokušava da ubaci udicu na čist sistem
- **U to vreme ranjivi programi na UNIX sistemu su bili **rsh, finger i sendmail****
- **Ako uspe crv da progura udicu,**
  - ☞ tada udica se konektuje na zaraženu mašinu
  - ☞ kopira crva
  - ☞ obe nastavljau dalje da šire crve po mreži

# The Morris Internet Worm



# Virusi

- **Za razliku od crva**
  - ☞ koji se umnožavaju i smanjuju performanse sistema
  - ☞ **virusi su jako opasni,**
  - ☞ jer mogu da naprave razne teške destrukcije,
  - ☞ kao što je brisanje datoteka itd
- **Dok je crv samostalni program (standalone),**
  - ☞ **virusi su fragmenti koda**
  - ☞ **koji se ubacuju u druge legitimne programe**
- **Virusi su glavni problem personalnih računara.**
- **Po pravilu su dobijaju**
  - ☞ skidanjem sa mreže (downloading) zaraženih programa,
  - ☞ a takođe i kroz e-mail
- **Virusi se prate sa svojim vakcinama,**
  - ☞ raznim antivirus programima
  - ☞ a najbolji način za zaštitu od virusa je
  - ☞ kupovina legalnog softvera
  - ☞ **dober antivirus softver**

# DoS (Denial of Service-Blokada Usluga)

- **1. Blokada hosta**
- **Jedna vrsta napada**
  - ☞ je zaposliti **resurse računara**
  - ☞ da postane potpuno blokiran
- **(na primer**
  - ☞ Java aplet sa nekog web sajta
  - ☞ totalno blokira CPU)
  
- **2. Blokada servisa**
- **Drugi vrsta ovih napada je**
  - ☞ **blokada pojedinih mrežnih servisa**
  - ☞ (ftp na primer).

# Threat Monitoring - Praćenje Pretnji

- **Provera sumnjivih aktivnosti:**
  - ☞ npr. Nekoliko neuspešnih ukucavanja lozinke
  - ☞ može značiti pogađanje lozinke
- **Audit log:**
  - ☞ snima vreme, korisnika, tip
  - ☞ svih pristupa objektu;
  - ☞ koristan za oporavak od napada
  - ☞ razvoj boljih zaštitnih mera
- **Skenirati sistem povremeno**
- **zbog tzv. “sigurnosnih rupa”;**
  - ☞ koje se pojavljuju
  - ☞ kada se računar ne koristi tako često

# Threat Monitoring - Praćenje Pretnji

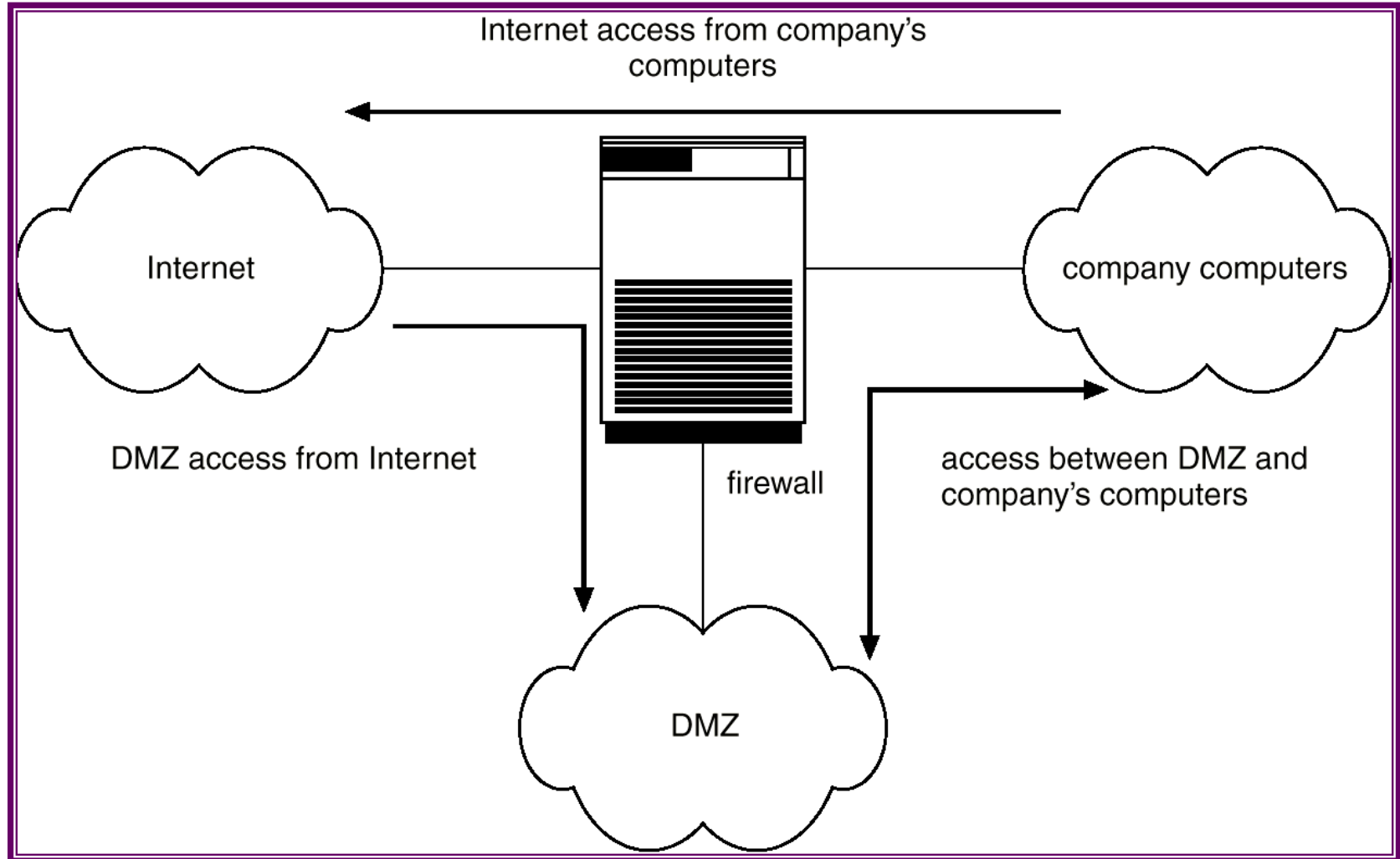
## ■ Paziti na:

- ☞ Kratke ili “lako-zapamtljive” lozinke
- ☞ Neautorizovane set-uid programe
- ☞ Neautorizovane programe u sistemskim direktorijumima
- ☞ Neočekivane long-running procese
- ☞ Neodgovarajuće zaštite direktorijuma
- ☞ Neodgovarajuću zaštitu sistemskih fajlova
- ☞ Opasne programske upade(Trojance)
- ☞ Izmene u sistemskim programima: monitor checksum values

# FireWall

- Izdvojeni sigurnosni domeni
- **Firewall** je smešten
- između
- **poverljivih i nepoverljivih hostova.**
  
- **Firewall limitira mrežni pristup**
  - ☞ Između dva sigurnosna domena
  
- U suštini **firewall tehnika** deli mrežu na **više domena.**
  - ☞ **Prvi domen je Internet**, kao krajnje nepoverljivi i nesigurni domen
  - ☞ **Drugi domen je polusigurna mreža DMZ (demilitarized zone)**
  - ☞ **Treći najsigurniji domen su lokalni računari (company computers)**

# Mrežna Sigurnost Kroz Domensko Razdvajanje uz Pomoć Firewall-a



# FireWall

- Po pravilu, **konekcije su dozvoljene**
  - ☞ sa interneta do DMZ
  - ☞ sa lokalnih računara do Interneta
- **ali nisu dozvoljene**
  - ☞ sa Interneta ili DMZ do lokalnih računara
  - ☞ **osim nekih kontrolisanih komunikacija**
- **Firewall ne štiti**
  - ☞ od napada na komunikacijama koje su dozvoljene
  - ☞ pa su tu mogući napadi tipa prepunjenja bafera
- **Spoofing:**
  - ☞ Postoji još jedna vrsta napada koja se zove **spoofing**,
  - ☞ gde neautorizovani host
  - ☞ pokušava da u svojim paketima podmetne IP adresu
  - ☞ **koja može da prođe kroz firewall**
- **Sniffing**

# Detekcija Napada

- **IDS (Intrusion Detection System)** bavi se
  - ☞ detekcijom napada
  - ☞ reakcijom na pokušaj napada na sistem
- Metode se dele na dve vrste a to su
- **1. detekcija bazirana na oznaci (signature-based detection)**
  - ☞ u kojoj se analizira ulaz ili mrežni saobraćaj i
  - ☞ traži se karakterističan uzorak
  - ☞ koji otkriva napad,
  - ☞ kao što je tipična sekvenca višetrukog pogrešnog logovanja
- **2. druga detekcija bazirana na anomaliji (anomaly detection),**
  - ☞ koja otkriva anomalije u sistemu,
  - ☞ na primer sistemski poziv
  - ☞ sa velikom količinom ulaznih podataka
  - ☞ koji verovatno pokušava prepunjenje steka ili bafera.

# Detekcija Napada

- Ukazaćemo na **3 razvijene metode** koje se koriste za detekciju napada
- **1. Vođenje statistike u log formatu (Auditing and logging).**
- **2. Tripwire softver**
- **3. Monitorisanje sistemskih poziva (System call monitoring)**
- **1. Vođenje statistike u log formatu (Auditing and logging).**
  - ☞ U ovoj metodi
  - ☞ upusuju se u log datoteku svi događaji
  - ☞ koji su potencijalno opasni po sigurnost,
  - ☞ kao što je logovanje,
  - ☞ da bi se kasnije analizirali ima li tu napada ili ne

# Detekcija Napada

## ■ 2. Tripwire softver

- ☞ To je softver pod UNIX sistemom
- ☞ koji proverava **da li su neke bitne datoteke promenile**
- ☞ kao na primer datoteka sa lozinkama (**/etc/passwd**)

## ■ 3. Monitorisanje sistemskih poziva (System call monitoring)

- ☞ Ovaj metoda se bazira na **anomalijama**
- ☞ Funkcioniše tako sto monitoriše sistemske pozive
  - 📄 gde pored neobičnih parametara za sistemske pozive
  - 📄 mogu se detektovati normalne sekvence zbivanja
  - 📄 ili neobične sekvence koje ukazuju na potencijalni napad
- ☞ **Za jedan program se napravi sekvenca sistemskih poziva u vidu tabele**
  - 📄 tabela se zapamti
  - 📄 pa kada se program ponovo izvršava
  - ☞ proverava se **da li sekvenca ista ili slična**

# Data Strukture Izvedene iz System-Call Sekvence

system call	distance = 1	distance = 2	distance = 3
open	read getrlimit	mmap	mmap close
read	mmap	mmap	open
mmap	mmap open close	open getrlimit	getrlimit mmap
getrlimit	mmap	close	
close			

# Kriptografija

- Kada poruka putuje po mreži
  - ☞ između izvornog i odredišnog IP,
  - ☞ do poruke mogu doći i ostali sajtovi
  - ☞
- Kako bi poruka postala **poveljiva**,
  - ☞ ona se **kriptuje**,
  - ☞ odnosno izmeni
  - ☞ da mogu da je koriste samo oni kojima je namenjena
- Poenta kriptografije je **uvođenje ključa**,
  - ☞ kojim se originalna poruka
  - ☞ šifruje na izvornoj strani
  - ☞ i dešifruje na odredišnoj strani

# Autentifikacija

## ■ Algoritam za **autentifikaciju**

- ☞ omogućava primaocu poruke,
- ☞ da proveri,
- ☞ pomoću ključa,
- ☞ da li je poruka generisana na određenom računaru ili ne.

## ■ Preciznije, **algoritam za autentifikaciju** zahteva **sledeće komponente**:

- ☞ **skup ključeva K**
- ☞ **skup poruka M**
- ☞ **skup autentifikatora A**
- ☞ funkcija **S: K->(M->A)**
  - 📄 koja znači za svaki ključ k iz skupa K
  - 📄 **S(k)** je funkcija za generisanje autentifikatora iz poruke
- ☞ funkcija **V: K->(MxA->true or false)**,
  - 📄 koja znači za svaki ključ k iz skupa K,
  - 📄 **V(k)** je funkcija za proveru autentifikatora za poruku

# Autentifikacija

## ■ Samo računari

- ☞ koji poseduju  $S(k)$  i  $V(k)$

- ☞ mogu međusobno da identifikuju svoj poruke na mreži

## ■ Postoje dve glavne varijante za autentifikaciju:

- ☞ **MAC** (message authentication code)

- ☞ **digitalna signatura-potpis**

# Enkripcija

- **Enkripcija** znači ograničenje
  - ☞ za potencijalne primaocce poruke
  - ☞ zato što omogućava šifrovanje poruka.
- **To znači**
  - ☞ kada se šalje poruka
  - ☞ samo onaj ko ima ključ
  - ☞ može pročitati poruku.
- **Preciznije, algoritam za enkripciju zahteva sledeće komponente:**
  - ☞ **skup ključeva  $K$**
  - ☞ **skup poruka  $M$**
  - ☞ **skup šifara  $C$**
  - ☞ **funkcija  $E: K \rightarrow (M \rightarrow C)$ ,**
    - 📄 koja znači za svaki ključ  $k$  iz skupa  $K$ ,
    - 📄  $E(k)$  je funkcija za generisanje šifre iz poruke
  - ☞ **funkcija  $D: K \rightarrow (C \rightarrow M)$ ,**
    - 📄 koja znači za svaki ključ  $k$  iz skupa  $K$ ,
    - 📄  $D(k)$  je funkcija za generisanje poruke iz šifre

# Enkripcija

- To znači da bi sistem došao do poruke,
  - ☞ mora da zna funkciju  $D(k)$  i
  - ☞ da ima ključ  $k$
- Postoje 2 tipa ovakvih algoritama:
- **simetrični**
  - ☞ kod kojih se funkcija  $E(k)$  se izvodi iz  $D(k)$
- **asimetrični**
  - ☞ gde je  $E(k)$  javni ključ, a  $D(k)$  privatni ključ
  - ☞ Tipičan primer je SSL

# Enkripcija

- Enkripcija običnog teksta u šifrirani tekst.
- Osobine dobrog enkriptovanja:
  - ☞ Relativno jednostavna za autorizovane korisnike
    - 📄 Da šifruju i dešifruju podatke
  - ☞ Šema enkripcije zavisi
    - 📄 ne od poverljivosti algoritma
    - 📄 već od parametara algoritma
    - 📄 korišćenih u šifrovanom ključu.
  - ☞ Veoma teško za upadača da utvrdi šifrovani ključ.
- Data Encryption Standard
  - ☞ zamena karaktera
  - ☞ i preuređivanje njihovog redosleda
  - ☞ **na bazi ključa**
  - ☞ omogućenu od strane autorizovanih korisnika preko sigurnih mehanizama
  - ☞ šema je sigurna koliko i mehanizam

# Enkripcija

- Enkripcija javnog ključa
- bazirana na pravilu da svaki korisnik ima dva ključa:
  - ☞ **javni ključ**
    - 📄 ključ korišćen da šifrira podatke.
  - ☞ **privatni ključ**
    - 📄 ključ poznat samo pojedinim korisnicima u dešifrovanju podataka.
- Mora postojati šema enkripcije
  - ☞ koja će javno biti napravljena
  - ☞ bez lakog shvatanja
  - ☞ šeme enkripcije

# Encryption Example – SSL (Primer Enkripcije)

- **SSL – Secure Socket Layer**
- **Kriptografski protokol**
  - ☞ limitiran na samo dva kompjutera
  - ☞ kako bi razmenjivali poruke međusobno.
- **Korišćen između**
  - ☞ **web servera i browser-a**
  - ☞ Za sigurnu komunikaciju
  - ☞ (broj credit card-a)
- **Server se verifikuje sertifikatom**
- **Komunikacija između svakog kompjutera**
  - ☞ koristi simetrični kriptografski ključ

# Klasifikacija Računarske Sigurnosti

## ■ Ministarstvo odbrane SAD

- ☞ Odredilo je 4 vrste računarske sigurnosti:

- ☞ A, B, C, and D.

## ■ D – Minimalna sigurnost (MS-DOS, MS Windows 3.11).

## ■ C – Omogućuje diskretnu zaštitu kroz revizije

- ☞ Podeljena na C1 i C2

- ☞ C1 identifikuje kooperativne korisnike sa istim nivoom sigurnosti

- ☞ C2 dozvoljava user-level kontrolu pristupa

## ■ B – Sve osobine C

- ☞ Ipak svaki objekat može imati jedinstvene osetljive oznake.

- ☞ Podeljena na B1, B2, i B3.

## ■ A – Koristi zvanične principe i verifikacione tehnike

- ☞ da bi se obezbedila sigurnost