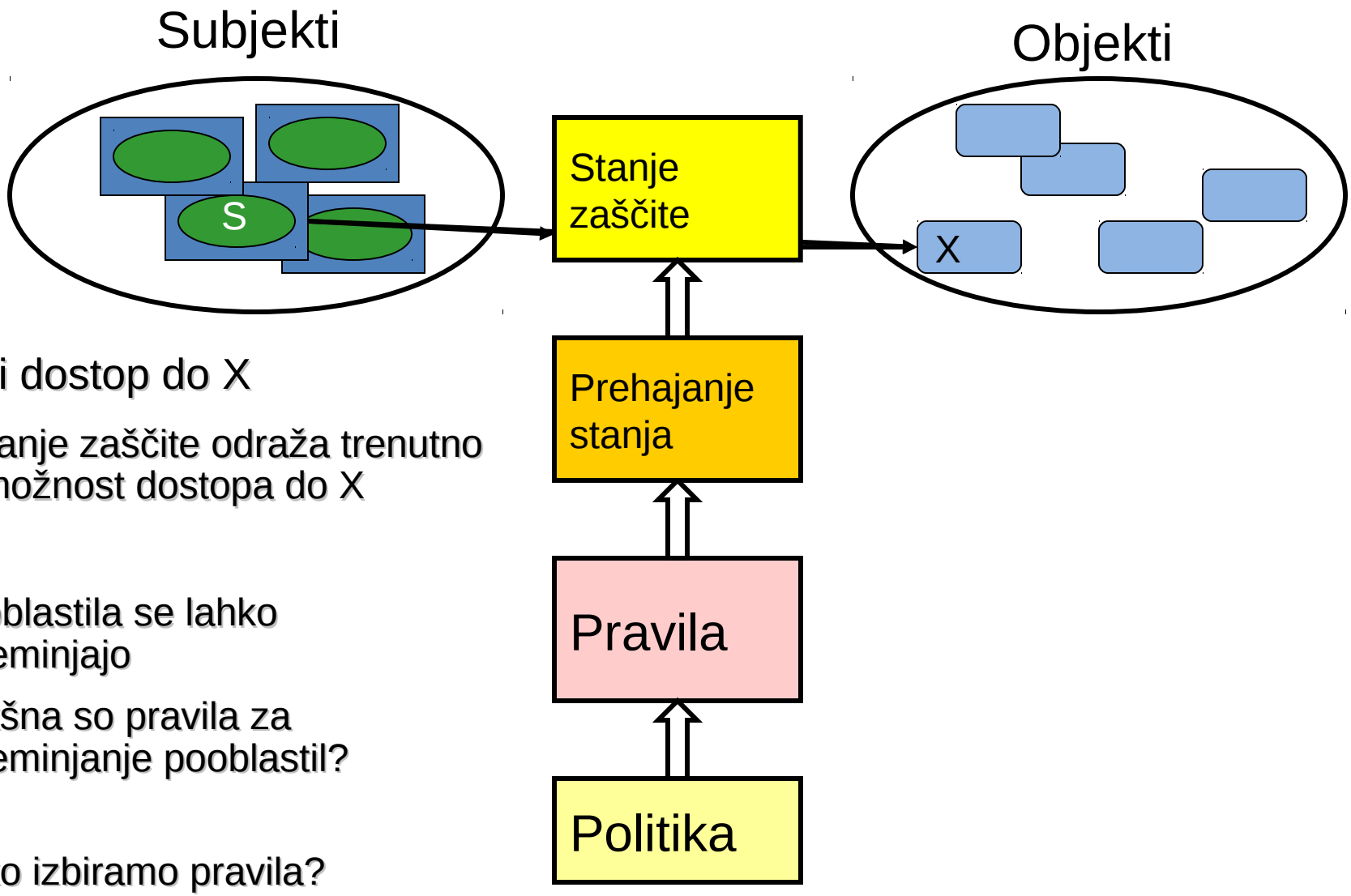
# Zaščita
# in varnost
# operacijskih sistemov

# Lampsonov model zaščite

- Aktivni deli (na primer procesi)
  - Delujejo v različnih domenah
  - Subjekt  je proces v domeni
- Pasivnim delom pravimo objekti
  - Procesi dostopajo do objektov glede na pravice, ki jih procesi imajo
- Želimo mehanizem zaščite, ki naj omogoča različne varnostne politike za subjekte, ki dostopajo do objektov
  - Možno je več različnih politik
  - Politike se s časom spreminjajo

# Sistem zaščite




- S želi dostop do X
  - Stanje zaščite odraža trenutno zmožnost dostopa do X
  - Pooblastila se lahko spreminjajo
  - Kakšna so pravila za spreminjanje pooblastil?
  - Kako izbiramo pravila?

# Primer z matriko dostopnosti (Access Matrix) in stanji zaščite

- Matrika dostopnosti subjektov do objektov/subjektov
- Specificira pravice, dodeljenene subjektom za subjekte in objekte
- Pred izvedbo operacije mora sistem preveriti matriko dostopnosti
  - (**$S_2$**, spreminja, **$F_2$**) dovoljeno
  - (**$S_2$**, izvaja, **$F_2$**) prepovedano

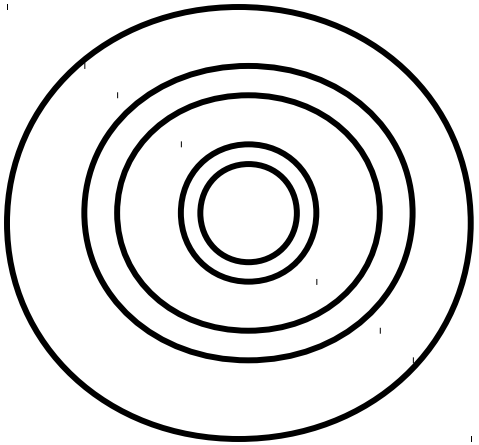
| | $S_1$ | $S_2$ | $S_3$ | $F_1$ | $F_2$ | $D_1$ | $D_2$ |
|---|---|---|---|---|---|---|---|
| $S_1$ | nadzor | blok zbudi lastnika | nadzor lastnika | branje pisanje* | | iskanje | last |
| $S_2$ | | nadzor | stop | last | spremi njanje | last | iskanje* |
| $S_3$ | | | nadzor | brisanje | izvajaj lastnika | | |

# Pravila politike za stanje zaščite

- Pravila politike krmilijo, kako lahko sistem zaščite spremeni stanje zaščite
  - Pravila specificirajo prehajanja stanj zaščite
  - Kažejo, kako proces prenaša, sbriše in dodeljuje privilegije
- Zakaj je prenos in dodeljevanje pravil politike  nevarno?
  - Lahko dovoli procesu (subjektu) prenos privilegijev drugemu procesu
    - Tak privilegij lahko krši politiko varnosti
    - Prenos takih privilegijev drugemu procesu ne smemo dovoliti

# Domene zaščite

- Lampsonov model uporablja procese in domene
- Kako implementiramo domeno?
  - Aparaturno: Supervisor/User Mode Bit
  - Programske razširitve -- obroči
- Notranji obroči imajo večja pooblastila
  - Obroč 0 ustreza režimu administratorja
  - Obroči 1 do S imajo manjšo zaščito in jih potrebujemo za implementacijo OS
  - Obroči S+1 doN-1 imajo manjšo zaščito in jih potrebujemo za aplikacije



# Domene zaščite (2)

- Prečkanje obroča pomeni spremembo domene
- Prečkanje notranjih obročev⇒ večanje pooblastil
  - Proces pridobi “Strožja” pooblastila
  - Proces se mora izvajati v obroču notranje domene
  - Prečkanje pri posebnih vratih
  - Zaščita s mehanizmom avtentikacije
- Prečkanje zunanjih obročev –manj zaščiteni objekti
  - Ni avtentikacije
  - moramo se vrniti nazaj

# Uporaba matrike dostopnosti

- Matrika je običajno redko posejana
  - Draga implementacija kot tabela
  - Uporabimo raje seznam
- Seznam po stolpcih imenujemo Seznam nadzora dostopa (***Access Control List (ACL))***
  - Seznam vzdržujemo pri objektu
  - Tipičen primer: zaščitni biti pri datotečnem sistemu Linux
- Seznam po vrsticah imenujemo  seznam zmožnosti (***Capability List***)
  - Seznam vzdržujemo pri subjektih (na primer procesih)
  - primer "Kerberos Ticket" je zmožnost (Capability)

# Še o zmožnostih

- Omogočajo naslavljanje objekta iz zelo obsežnega naslovnega prostora
- Lastništvo zmožnosti predstavlja avtorizacijo do dostopa
- Zato mora veljati:
  - Zmožnosti naj bo težko uganiti
  - Zmožnosti morajo biti unikatne in ne ponovno uporabljene

# Varnost in Java

- Kako lahko apleti postanejo aplikacije?
  - Zaupen ponudnik(tvorec apleta)
  - Podpisani aplet je overovljen
  - "Java Security Manager" lahko dovoli apletu, da je aplikacija izven peskovnika
- Kako lahko podatke prenašamo in izmenjujemo?
  - JAR: arhivske, zgoščene datoteke
  - Kodo in podatke vežemo v javanski arhiv
  - Pridružimo digitalni podpis za overovitev
  - Prenos preko serializacije objektov

# Varnostne zmožnosti Javinih ACL (Access Control List)

- Z dovoljenji nadzorovan dostop do virov
- Klasične varnostne tehnike za
  - Podatkovne strukture za zaščito virov
  - Definiranje dovoljenj za branje / pisanje za uporabnike in skupine uporabnikov
  - Rokovanje s seznami pooblastil dostopa
  - Podpora pozitivnim in negativnim dovoljenjem
  - Posamezna dovoljenja prekrijejo skupinska

- Implementacija na nivoju programskega jezika za funkcije, tipične za operacijske sisteme

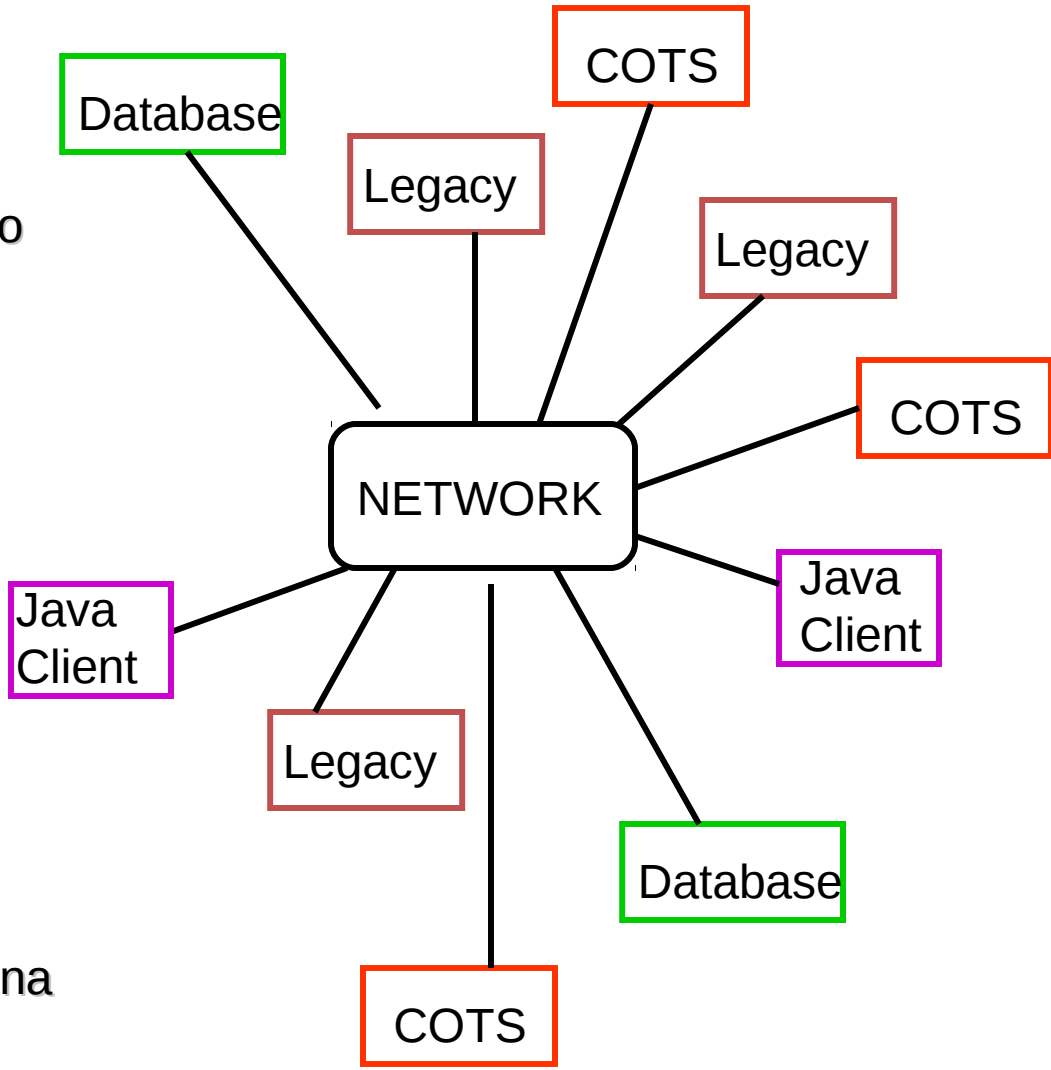
# Varnost za porazdeljeno računanje

Kako varnost obravnavajo posamezni sistemi?

Kaj, če ni varnosti pri starejših in komercialnih programih?

Varnost novih odjemalcev? novih strežnikov? vzdolž omrežja

Kaj pa porazdeljena varnost?



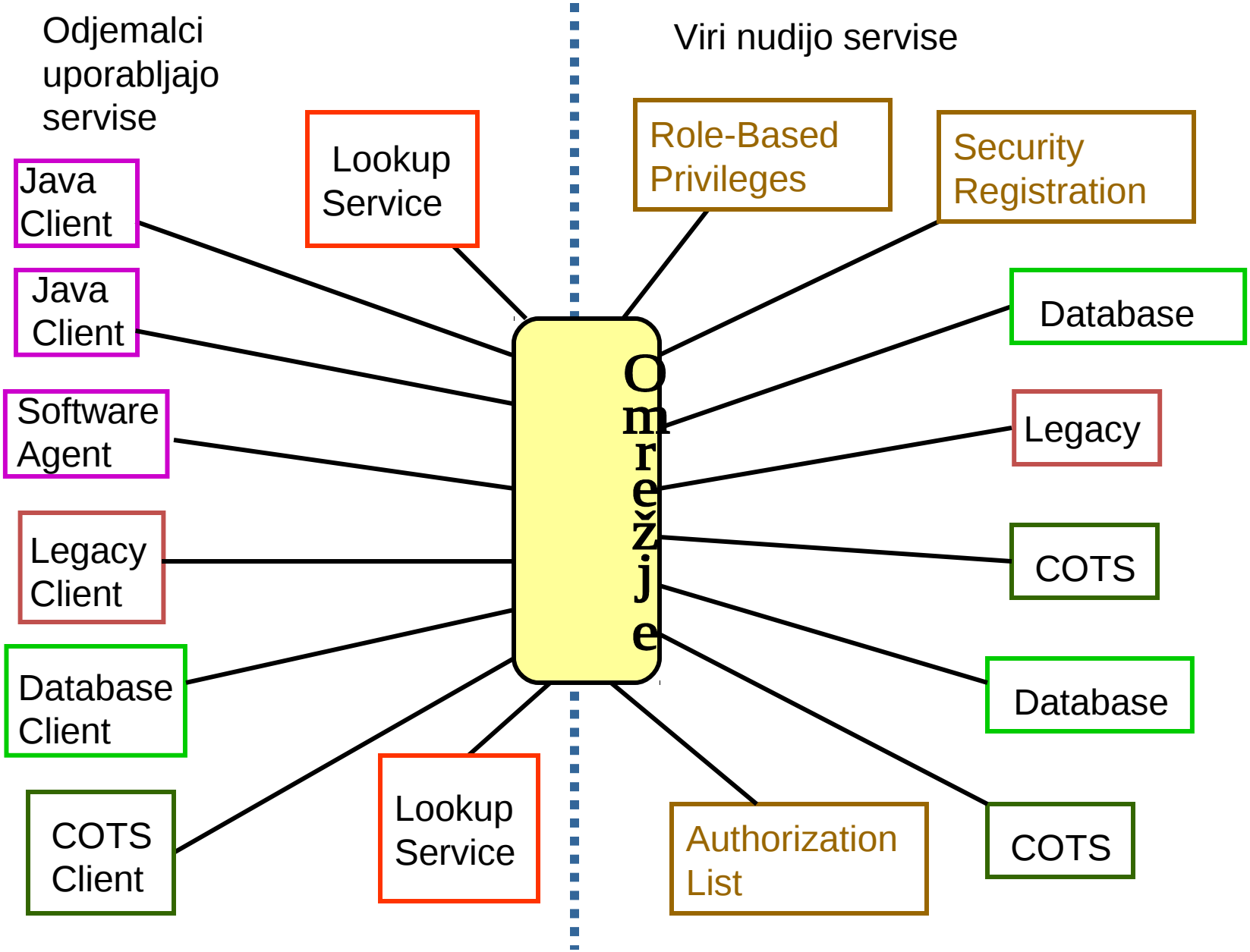

legacy sw – starejši programi
COTS –commercil off the shell sw

# Varnost in porazdeljeno računanje

- Avtentikacija (overovitev)
  - Ali je odjemalec res ta, za katerega se izdaja?
- Avtorizacija
  - Ali ima odjemalec dovoljenje za to, kar želi?
- Privatnost
  - Ali kdo prestreza komunikacijo med strežnikom in odjemalcem?
- Ojačitev (Utrditev)
  - Centralizirana in porazdeljena "koda"

# Varnost in porazdeljeni sistemi

- Zavarovanje
  - Ali so varnostni privilegiji vsakega odjemalca primerni za podporo njegove aktivnosti?
  - Ali varnostni privilegiji vsakega odjemalca dosegajo, ne pa presegajo njegovih zmožnosti?
- Konsistenca
  - Ali so definirani privilegiji vsakega odjemalca interno konsistentni?
    - Princip ravno dovolj visokih pooblastil
  - Ali so definirani varnostni privilegiji za klijente globalno konsistentni?
    - Medsebojno izobčenje: Nekateri smejo brati, drugi lahko pišejo




Splošna zgradba odjemalcev in virov.

# Varnost v omrežjih

Implementacija varnosti je bolj pomembna kot pred leti. Zakaj?

1. Napadalci so bolj usposobljeni in izobraženi ter imajo boljša orodja
2. Bolj smo odvisni od IT in več izgubimo kot nekdaj
3. Implementacija in upravljanje varnostne tehnologije je cenejše
4. Svet postaja manj vreden zaupanja

# Osnovna terminologija

- *Host*
  - Gostiteljski računalniški sistem
- *Service*
  - Program v uporabniškem prostoru, ki izvaja kakšno nalogo
- *Vulnerability* - ranljivost
  - Pomanjkljivost, hiba v programu, ranljivost, kritična s strani varnosti
  - Napadalec išče take pomanjkljivosti v programih s ciljem, da si poviša pravice na sistemu
- An *intrusion detection system* (IDS) poskuša odkriti oziroma preprečiti napade

# Ranljivost

- Ranljivost: šibkost, ko jo lahko izkoristimo za povzročanje škode.
- Napad: metoda izkoriščanja ranljivosti.
- Grožnja (threat): napadanje s strani motiviranega in sposobnega nasprotnika

- Tipična ranljivost v računalniških programih:
  - s prekoračitvijo medpomnilnikov (buffers) omogočeno izvajanje poljubne kode

# SANS lestvica 20 najpogostejših ranljivosti

Operacijski sistemi:

- W1. Internet Explorer
  - ranljivosti, ki omogočajo izvajanje poljubne kode z obiskom spletne strani napadalca
- W2. Windows Libraries
  - luknje v knjižnicah DLL predstavljajo tudi luknje v aplikacijah, ki uporabljajo te knjižnice
  - tipičen primer je bila letos napaka v Windows Graphics Rendering Engine, kjer si s posebno narejeno WMF sliko lahko izvedel poljubno kodo
- W3. Microsoft Office
  - dokumenti vsebujejo napadalsko kodo. Odprtje takega dokumenta je problematično
- W4. Windows Services
  - veliko strežnikov omogoča dostopnost funkcionalnosti preko RPC – izkoriščanje napak preko omrežja
- W5. Windows Configuration Weaknesses
  - šibko ščitena gesla ...
- M1. Mac OS X
  - podobno kot v Windows – Safari brskalnik, knjižnice za delo s slikami, Bluetooth wireless podsistem ...
- U1. UNIX Configuration Weaknesses
  - šibka gesla, uporaba nekriptiranih mrežnih servisov (npr. telnet)

SANS+NIPC+FBI (2006)

# SANS lestvica 20 najpogostejših ranljivosti

## Cross-Platform Applications

- C1 Web Applications
  - ranjivosti v PHP, SQL injection, XSS ...
- C2. Database Software
  - šibka gesla, prekoračitev medpomnilnika v mrežnih servisih ...
- C3. P2P File Sharing Applications
  - napake v programih za razne file-sharing mreže in sisteme grid
- C4 Instant Messaging
  - širjenje črvov, virusov, kraja zaupnih informacij ...
- C5. Media Players
  - napake v predvajalcih omogočajo dostop do sistema
- C6. DNS Servers
  - napadi DOS (denial of service) in spoofing (pretvarjanje)
- C7. Backup Software
  - napake v programih za komunikacijo med backup strežniki in odjemalci
- C8. Security, Enterprise, and Directory Management Servers
  - vdori v imeniške strežnike (dostop do uporabniških imen in gesel)
  - strežnki za preverjanje virusov in spam pošte – dostop omogoči pošiljanje virusov in spama

SANS+NIPC+FBI (2006)

# SANS lestvica 20 najpogostejših ranljivosti

## Network Devices

- N1. VoIP Servers and Phones
  - prisluškovanje, pretvarjanje ...
- N2. Network and Other Devices Common Configuration Weaknesses
  - operacijski sistemi usmerjevalnikov, omrežnih tiskalnikov ...

## Security Policy and Personnel

- H1. Excessive User Rights and Unauthorized Devices
- H2. Users (Phishing/Spear Phishing)
  - Phishing – pretvarjanje; web strani, ki izgledajo kot prave; napadalec dobi dostop do gesel ... Lahko so web strani, VoIP, lažnivi e-maili

## Special Section

- Z1. Zero Day Attacks and Prevention Strategies
  - zero day attacks – napadi še preden je napaka odkrita in popravljena s strani proizvajalca programske ali strojne opreme

SANS+NIPC+FBI (2006)

# Najpogostejši tipi napadov

- **Odklanjanje storitve** (Denial of Service)
  - ni neposrednje grožnje za podatke
  - napadalec onesposobi nek računalnik (storitev), da ni uporabna
- **Vohljanje paketov** (Packet Sniffing)
  - na Ethernet omrežjih (velik del današnjih) vidi vsak računalnik celoten promet na istem delu omrežja
  - vsak lahko torej prisluškuje nekriptiranemu prometu (vidi gesla ... )
- **Puščanje informacij** (Information Leakage)
  - pridobivanje podatkov brez neposrednega vdora na računalnik
  - napad na vire podatkov (npr. spletne strežnike), da dajo podatke, do katerih neavtorizirani uporabniki sicer ne morejo priti (npr. SQL Injection ... )
- **Zlonamerna koda** (Malicious Code)
  - virusi, črvi ... , torej koda, ki lahko škodi bodisi delovanju računalnika bodisi se uprabi za pridobivanje informacij
- **Social Engineering**
  - zavajanje uporabnikov, da izdajo zaupne informacije. Lahko preko telefonov, lažnih spletnih strani ...
- **Razbijanje gesel** (Password Cracking)
  - programi za generiranje gesel na podlagi slovarjev ...

# Odklanjanje storitve
## Denial of Service (DoS)

- Računalniški sistem naj bi zagotavljal storitve pooblaščenim uporabnikom.
- Ko zaradi napada sistem pade ali pa postanejo programi tako počasni, da so neuporabni, pravimo, da je prišlo do napada tipa “odklanjanje storitve” ("denial of service“)
- Napadalec to doseže s primernimi programi in se dobro zaveda posledic.

# Denial of Service

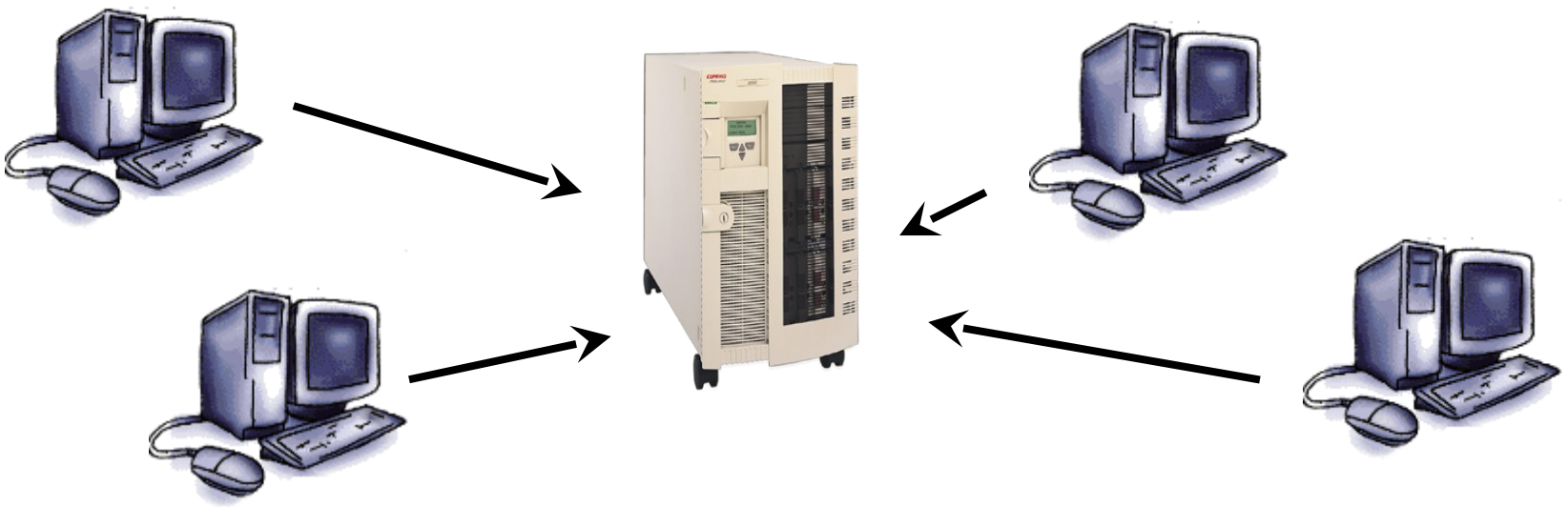
- Variante DoS
  - Doseči prevelike porabe virov, npr. omrežja, prostora na disku ali CPE časa
  - Pokvariti konfiguracijo npr. usmerjevalnikov v omrežju
  - Fizično pokvariti omrežno infrastrukturo
- Tehnike DoS
  - Poplavljanje omrežja s paketi, kar prepreči normalen promet in dostopnost storitve
  - Preobremenitev strežnika s pošiljanjem prevelikega števila zahtev
  - Preprečitev točno določenemu uporabniku dostop do storitve
  - Napad na strežnik, da točno določenemu uporabniku ne nudi strežbe

# Nekaj tipov DoS

- SYN floods: poplava paketov SYN
  - pošiljanje zahtev za odprtje povezave (SYN) s pokvarjenim izvornim naslovom – strežnik zaman čaka na potrditev
  - lahko je izvorni naslov kar naslov napadenega računalnika, kar lahko vodi do sesutja (LAND attack)
- ICMP floods: poplava paketov ICMP (ping)
  - pošiljanje ping paketov velikemu številu računalnikov s potrditvenim naslovom napadenega računalnika (smurf attack)
  - tip odbojnega napada (reflected attack)
- DoS na nivoju aplikacij
  - buffer overflow napadi, ki izkoristijo napake na strežnikih in povzročijo prekomerno porabo diska ali CPE časa
  - IRC floods ...
- Porazdeljeni DoS napadi (DDoS)
- Nenamerni napadi
  - popularne web strani, napake v OSih usmerjevalnikov ...

# Distributed Denial of Service (DDoS)

- Več strojev lahko sodeluje v napadu DoS na izbrani računalnik, npr. če se preobremeni strežnik
- Ti stroji so pogosto kompromitirani nedolžni računalniki, ki sedaj služijo napadu.
- Oddaljeni klijent (ali časovna bomba) sproži napadalne raćunalnike.



# Prevare in IPv4

- Večina DoS napadov zlorablja lastnosti paketov protokola IPv4 (so nekriptirani) in storitev IPv4
- Tehnika IP sleparstva (IP spoofing)
  - IP paket vsebuje IP naslove pošiljatelja in prejemnika.
  - Vse je nekodirano: IP naslov: a.b.c.d: 4 bajti
  - IP sleparstvo nadomesti IP naslov (običajno) pošiljatelja ali (redko) naslovnika z drugimi naslovi.
  - To lahko zmede določene storitve in povzroči napačno delovanje (sesutje ali preobremenitev ...)
- DNS sleparstvo (DNS spoofing)
  - ponaredi DNS informacije
  - promet, ki bi šel na nek računalnik se posledično preusmeri na drug računalnik

# Vohljači (Sniffers)

- V Ethernet omrežjih gredo vsi paketi preko vseh računalnikov v istem delu omrežja
- Vohljač paketov (packet sniffer) je program, ki prisluškuje prometu na omrežju.
- Kopira pakete, ko prehajajo  NIC.
- NIC normalno bere pakete, namenjene na njen specifičen MAC naslov, vse ostale pakete pa ignorira.
- NIC v zmešanem režimu sprejema vse pakete ne glede na naslov MAC.
- Napadalec lahko vidi nekodirana gesla, zaupne informacije ...

NIC  =Network Interface card
MAC =Media Access Control

# Puščanje informacij

- Napad na vire podatkov (npr. spletne strežnike), da dajo podatke, do katerih neavtorizirani uporabniki sicer ne morejo priti
- Primer: SQL Injection
  - vrivanje stavkov v SQL ukaze, ki se uporabljajo v npr. spletni aplikaciji
- Primer: preobširna sporočila o napakah
  - programerji ob napakah uporabnikom povedo preveč informacij, ki jih lahko le-ti izkoristijo za napad
- Primer: mož v sredini/kraja seje (man in the middle)
  - pri komunikaciji med dvema računalnikoma se vzpostavi seja;
  - napadalec onesposobi enega od obeh in se v nadaljnji komunikaciji pretvarja, da je onesposobljen rač.

# Primer: SQL injection

string userName = TextBox.Text;

string statement =

"SELECT * FROM users WHERE name = '" + userName + "';"

Če v TextBox vpišemo: *matic*, vrne vse uporabnike z imenom *matic* (SELECT * FROM users WHERE name = 'matic')

Če v TextBox vpišemo: *a' or t = 't*, vrne vse uporabnike

(SELECT * FROM users WHERE name = 'a' or t='t')

Kaj se zgodi, če v TextBox vpišemo:

*a'; DROP TABLE users; SELECT * FROM data WHERE name LIKE '%*

# Primer: preobširna sporočila o napakah

npr. pove nam sestavo query stringa:

An Error Has Occurred. Error Message:
System.Data.OleDb.OleDbException:
Syntax error (missing operator) in query expression 'username = '' and password = 'g''.
at System.Data.OleDb.ExecuteCommandTextErrorHandling ( Int32 hr)
at System.Data.OleDb.ExecuteCommandTextForSingleResult ( tagDBPARAMS dbParams, Object& executeResult)
at ...

# Zlonamerna koda

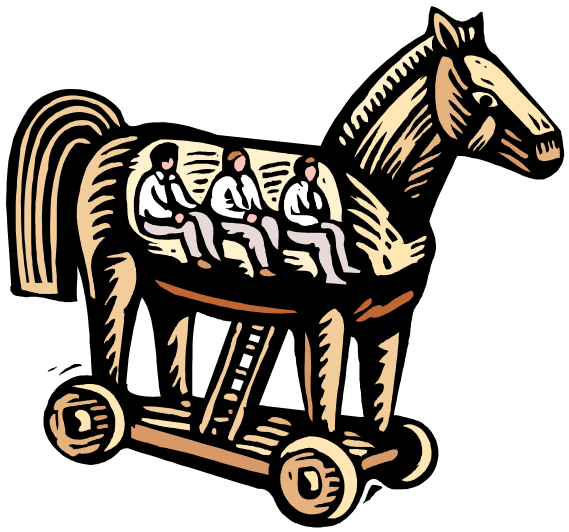
- Koda, ki lahko škodi bodisi delovanju računalnika bodisi se uprabi za pridobivanje tajnih informacij
- Nekatere vrste zlonamerne kode:
  - Trojanski konji
  - Črvi
  - Virusi
  - Logične bombe ...
- Zlonamerna koda se lahko uporablja za npr.:
  - dostop do zaupnih informacij
  - DoS napade
  - enkripcijsko izsiljevanje (cryptovirus extorsion)
  - pušča odprta zadnja vrata (back doors) za vstop v računalnik
- Tehnike napada, ki se velikokrat uporabljajo pri napadih z zlonamerno koda:
  - Napadi s prekoračitvijo polja (Buffer Overflow)
  - Rootkit-i

# Zadnja vrata

- Po angleško *trap doors ali backdoors*.
- Omogočajo dostop do sistema s preskokom običajnih vstopnih (login) postopkov – nepooblaščen dostop
- Velikokrat posledica poganjanja zlonamerne kode, ki jih pusti odprta za seboj
- Pojem: remote administration tool
  - dopušča napadalcu, da iz oddaljenega računalnika nadzoruje napaden računalnik
  - npr. sproži DDoS napad
  - pošilja SPAM ePošto
  - ...

# Trojanski konji

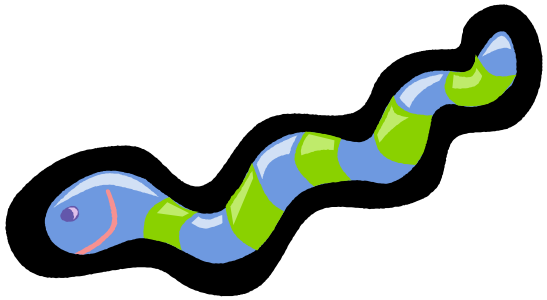
- Trojanski konj oponaša funkcionalnost legitimnega istoimenskega programa.
  - lahko ga napadalec vključi v nek legitimni program
  - lahko je samostojen program, ki izgleda kot legitimen program
- Vendar ima skrito “poslovanje.” Ima torej v resnici (še) drugo funkcijo, ki je uporabniku neznana.
- Ne more delovat sam od sebe, uporabnik ga mora pognati
  - mora delovati privlačno, da ga uporabnik požene
- Primeri opravil, ki jih počnejo:
  - brisanje ali prepisovanje podatkov
  - upload/download datotek
  - dovoljevanje oddaljenega dostopa (remote administration)
  - širjenje druge kode (virusi ...)
  - DDoS



# Poznana Trojanska vrata

- Nekatera vrata, ki jih pustijo odprta, ko se poženejo:
  - 22 TCP Shaft
  - 23 TCP Fire Hacker
  - 41 TCP Deep Throat
  - 41 TCP Deep Throat
  - 456 TCP Hacker's Paradise
  - 901 TCP Backdoor.Devil
  - 999 TCP DeepThroat
  - 6712 TCP Sub Seven
  - 8879 TCP UDP BackOrifice 2000
  - 27444 UDP Trin00/TFN2K
  - 40412 TCP The Spy
  - 65535 TCP Adore Worm/Linux

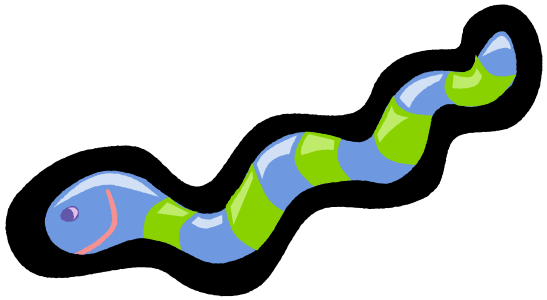
# Črvi



- Črvi so programi, ki se po omrežju širijo od računalnika do računalnika.
- Črvi lahko tečejo samostojno brez intervencije uporabnika
- Črvi imajo lahko (različne) dele svojih kopij, ki tečejo na več različnih računalnikih.
- V nasprotju z virusi se ne navezujejo na obstoječe datoteke

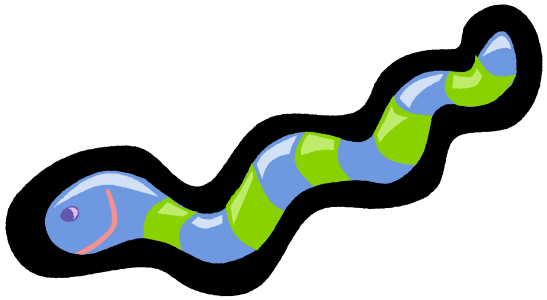
•Definition from RFC 1135: A *worm* is a program that can run independently, will consume the resources of its host [machine] from within in order to maintain itself and can propagate a complete working version of itself on to other machines.

# Črvi



- Prva implementacija že leta 1978 za koristna opravila
- Glavni tipi:
  - poštni črvi se širijo kot priponke ePošti. Ko je pognan, se razpošlje na druge naslove (npr. Anna Kournikova)
  - messaging črvi se širijo preko programov tipa Messenger in se razpošiljajo po kontaktih
  - file sharing črvi se širijo preko file sharing mrež
  - širjenje neposredno preko ranljivosti v TPC storitvah, npr. RPC (Blaster)

# Črvi



- Tipično škodijo omrežjem, saj povzročijo preobremenitev s svojim širjenjem
- Lahko nosijo tudi kake druge naloge, npr. brisanje datotek ali pošiljanje dokumentov po ePošti
- Pogosto puščajo odprta zadnja vrata
- Koristni črvi
  - lahko počnejo kaj koristnega (npr. najde proste računalnike in na njih izvaja računske operacije)

# Kaj počnejo virusi

- Virusi ne morejo teči samostojno
- Kaj lahko virus naredi (poleg tega, da se širi) ko se izvede.
  - ničesar
  - naredi kaj navihanega
  - zlonamerno škodo (na primer zbriše tabelo particij).
- Nekateri virusi imajo poseben sprožilec.
  - datum
  - število uspešnih okužb
  - pametni virusi uporabljajo časovno redke sprožilce, tako da imajo dovolj časa, da se primerno razširijo, preden so uporabniki opozorjeni nanje.

# Splošni tipi virusov

- Datotečni virusi oz. parazitni virusi
- Zagonski sektor (Boot Sector)
- Multi-partitni
- Makro
- Omrežni
- ePoštni
- ...

# Boot Sector virusi

- Najpogostejši v obdobju 1980 do 1990
- Prenašajo se preko prenosljivih medijev (diskete ipd.)
- Vpišejo se na področje zagonskega sektorja medija in trdega diska (MBR)
- Sprožijo se pri zagonu sistema, opravijo svoje delo, okužijo vse medije) in prenesejo nadzor na relocirano kodo, ki so jo sami nadomestili.
- Enostavno odstranjevanje virusa
  - Zagon z neokuženo disketo
  - Zamenjava MBR (master boot record)
- Z zatonom disket, jih je precej manj

# Datotečni/parazitni virusi

- Pripnejo se datotekam (izvršljive datoteke, gonilniki, kompresirane datoteke)
- Poženejo se, ko poženemo datoteko
- Ob tem okužijo ostale podobne datoteke na disku
- Če okuženo datoteko prenesemo na drug računalnik in jo tam poženemo, bo okužila tudi tega

## Multi-partitni virusi

- uporabljajo tako datoteke, kot boot sektorje za širitev

# Makro virusi

- 60-80 procentov vseh virusov
- Niso specifični za nek operacijski sistem, ampak za programsko opremo (npr. Microsoft Word ...)
  - Za aplikacije Word, Access, Excel, PowerPoint, and Outlook so pisani v Visual Basic
- Širjenje: priponke elektronski pošti, diskete, kopiranje s spletnih strani, prenosi datotek
- Nekateri jih imenujejo za črve, čeprav potrebujejo gostiteljski program

# Makro virusi - Primer

- Primer: Melissa
- Word Makro virus pisan v Visual Basicu
  - okuži Word dokumente in se pošilja preko Outlook Address Booka prvim 50 kontaktom
- l. 1999 je povzročil sesutje velike količine eMail strežnikov zaradi preobremenitve
  - pojavil se je v Usenet grupi alt.sex pod pretvezo da vsebuje gesla za dostop do porno strani
  - avtor D. Smith je bil obsojen na 10 let zapora in 5000$ kazni

# Omrežni virusi

- Se širijo preko omrežja
  - npr. preko souporabljenih  diskov ali direktorijev

# E-mail virusi

- se širijo preko elektronske pošte kot priponka
- se razpošiljajo na naslove v kontaktih bralca

# Logične bombe

- Logična bomba:  se izvede, ko nastopi določen pogoj.
  - s sprememba datoteke
  - posebno zaporedje tipk
  - z nastopom nekega datuma ...

# Struktura virusov

Namesto glavne main funkcije programa, se zažene funkcija virusa V()

```
V() {
 infectExecutable();
 if (triggered()) doDamage();
 jump to main of infected program;
}

void infectExecutable() {
   file = chose an uninfected executable file;
   prepend V to file;
}

void doDamage() { ... }
int triggered() { return (some test? 1 : 0); }
```

# Iskanje virusov – virus skenerji

- Viruse iščemo s posebno programsko opremo
- Skenerji preverjajo bralno pisalne metode za datotečni sistem.
- Iščejo specifična imena datotek
- Iščejo določene vzorce v vsebinah datotek
- Uporabljajo statistične metode za iskanje polimorfnih virusov
- Lahko dajejo tudi napačen rezultat.
- Lahko spregledajo zlonamerne programe.

# Pametni virusi

Virusi se znajo ogibati detekciji

- izogibanje infekciji datotek antivirusnih programov
- prestrezanje sistemskih klicev antivirusnih programov
- samo-spreminjanje
- enkripcija s spreminjajočim ključem:
  - le dekripcijski modul ostane enak, ostali deli virusa so vsakič drugačni
- polimorfna koda
  - tudi dekripcijski modul je vsakič drugačen – virus pri vsaki okužbi izgleda drugače
- metamorfna koda
  - virus se vsakič na novo napiše – prevede kodo v začasno drugo obliko in nazaj
  - so kompleksni ker je logika spreminjanja kompleksna

# Prekoračitev polja (Buffer Overflow)

## Računalniška ranljivost desetletja

- Tehnika, ki jo uporablja veliko zlonamerne kode za svojo širitev ali pridobitev administratorskih pravic
- Izkorišča slabo napisano kodo v jezikih, kot so C, C++, itd. (večina OS je pisanih v teh jezikih)
- Buffer overflow pomeni, da nek proces poskuša shranjevati podatke preko meja bufferja fiksne širine (npr. polja v Cju)
  - proces se lahko sesuje
  - lahko pa je to narejeno namerno in povzroči posledično proženje zlonamerne kode
- Primer: če shranimo predolg niz v A, povozimo B

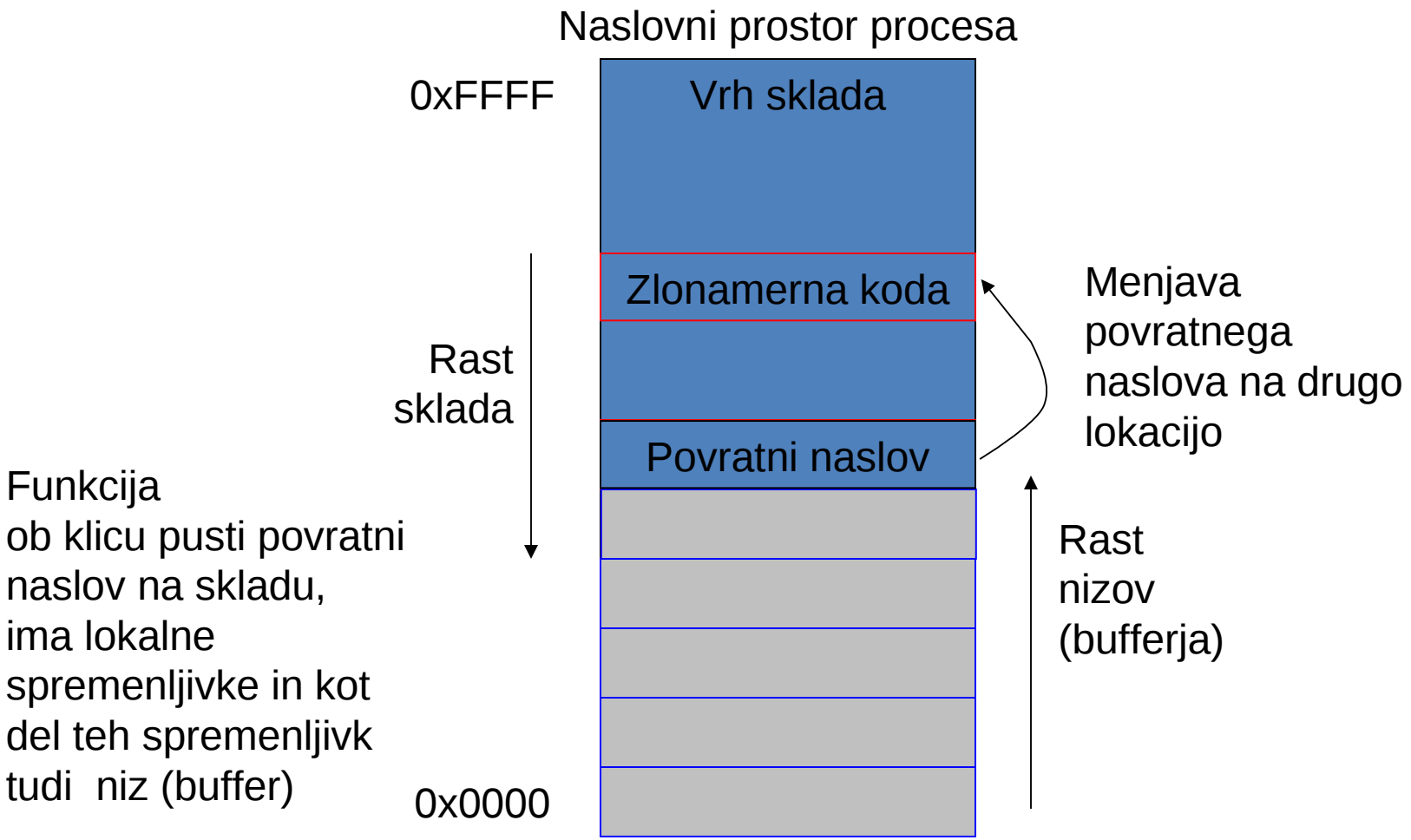
| A | A | A | A | A | A | A | A | B | B |
|---|---|---|---|---|---|---|---|---|---|
| x | z | c | d | e | q | a | f | e | 0 |

# Prekoračitev polja (Buffer Overflow)

## Prekoračitev na skladu

- Izvedljivo zlonamerno kodo vstavimo v programski proces.
- Povratni naslov trenutno izvajajoče-se funkcije, ki je na skladu, z namernim Buffer Overflowom spremenimo tako, da kaže na začetek te kode
- Namesto normalnega povratka iz funkcije, se sproži koda na spremenjenem povratnem naslovu

# Napad s prekoračitvijo polja



# Rootkit

- “rootkit” je zbirka orodij, ki jih uporabljajo napadalci za zakrivanje svoje prisotnosti in za zbiranje podatkov, potrebnih za nadaljnjo infiltracijo v omrežju.
- “Rootkit” orodja krpajo obstoječe programe, pa tudi vstavljajo zadnja vrata, nameščajo trojanske konje ...
  - npr. na unixu zakrpa ukaze *ls*, *ps*, da ne prikažejo datotek in procesov napadalca
  - onemogoči pregledovanje (auditing), ko je v sistem prijavljen napadalec.
  - dovoli vstop komurkoli, če uporabljamo posebno geslo za stranska vrata (backdoor password).
  - rootkit lahko “pokrpa” tudi samo jedro operacijskega sistema in tako omogoči komurkoli izvajanje privilegirane kode
- Rootkit namesti napadalec potem, dobi dostop.
- Navadno ga ne moremo odkriti s požarnimi zidovi ali protivirusnimi programi

# Windows Rootkit

- Windows rootkit tipično nadomesti API in ne binarnih programov.
- Vsak program, ki kliče tako zamenjane API, je potencialno pod njihovim vplivom.
- Tipični Windows rootkit lahko skriva datoteke, direktorije, procese, servise in vstopne točke v registry
- Zloglasni Sony BMG XCP copy protection
  - Sony je izdal Audio CDje, ki so na sistem avtomatsko namestili rootkit, ki je skrival njihov program za “ščitenje” vsebine CDja, ko je uporabnik predvajal CD
  - skrival je vse datoteke, procese in ključe v registru, ki so se začeli z nizom $sys$

# Linux rootkit

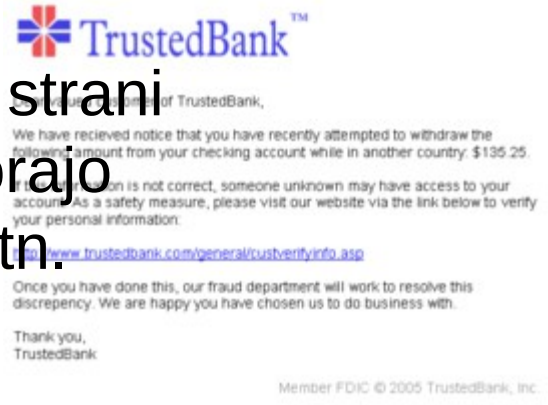
- chfn Trojaned! User->r00t
- chsh Trojaned! User->r00t
- inetd Trojaned! Remote access
- login Trojaned! Remote access
- ls Trojaned! Hide files
- du Trojaned! Hide files
- ifconfig Trojaned! Hide sniffing
- netstat Trojaned! Hide connections
- passwd Trojaned! User->r00t
- ps Trojaned! Hide processes
- top Trojaned! Hide processes
- rshd Trojaned! Remote access
- syslogd Trojaned! Hide logs
- linsniffer Packet sniffer!
- fix File fixer!
- z2 Zap2 utmp/wtmp/lastlog eraser!
- wted wtmp/utmp editor!
- lled lastlog editor!
- bindshell port/shell type daemon!
- tcpd Trojaned! Hide connections, avoid denies

# Social engineering

- Pogost del napadov na sisteme vključuje komponento “social engineering”
- Lažje je prevarati uporabnika, da posreduje svoje geslo, kot vdreti v sistem
- Pri tem gre za to, da napadalec uporabnika prepriča, da:
  - mu izda neko tajno informacijo (npr. številko kreditne kartice)
  - odpre e-mail z virusom
  - vtipka geslo v lažni program
  - ...

# Social engineering – kako prevarati uporabnika

- Zakriti zlonamerni program kot nekaj kar ni
  - Anna Kournikova virus se je širil kot priponka, ki je obljubljala slike tenisačice
- Lažne spletne strani – phishing
  - spletne strani, ki izgledajo kot prave strani bank ipd. in kamor se uporabniki morajo prijaviti, vtipkati št. kreditne kartice, itn.


TrustedBank™

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

- Predstavljanje za lažno osebo
  - lažni telefonski klic administratorja ...
- Pogosto ni potrebno veliko
  - raziskava Infosecurity l. 2003: 90% uradnikov je izven delovnega mesta v anketo vpisala svoje geslo v zameno za kemični svinčnik

# Problem varnosti

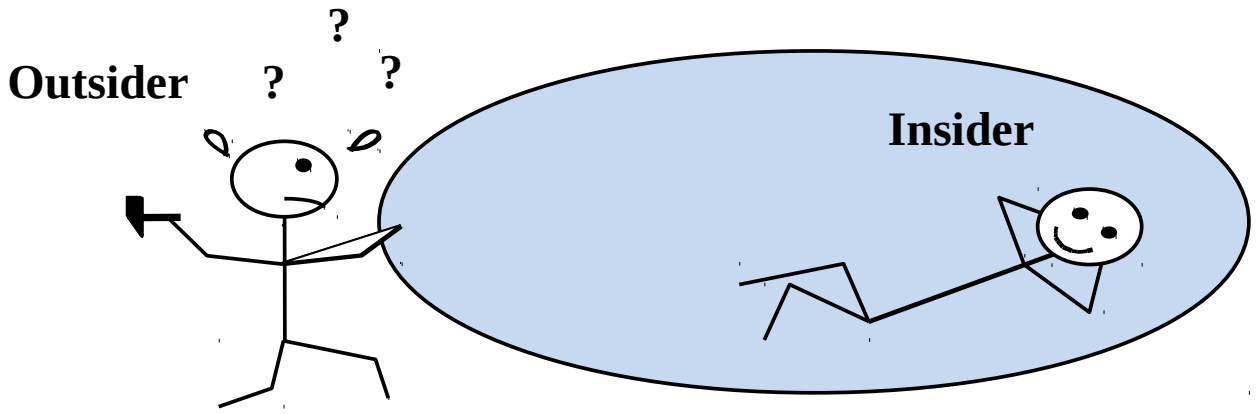
- Varnost mora upoštevati zunanje okolje sistema in sistem zaščititi pred:
  - Neavtoriziranim dostopom.
  - Zlonamernim spreminjanjem ali uničevanjem
  - Nenamernim, slučajnim vnašanjem nekonsistentnosti

- Lažje se zaščitimo pred slučajno, nenamerno napačno uporabo kot pred zlorabo.

# Kaj vpliva na nas

- Zunanji napadi
  - Napadi virusov, spam in kraja računalnikov
- Notranji napadi
  - Finančne goljufije, sabotaže, posredovanje privilegiranih podatkov izven organizacije
- Zavračanje in pomanjkanje odgovornosti
  - “Tega nisem storil jaz!”, “Te e-pošte nisem nikoli prejel…”
- Zaupanje v IT
  - Telefon in faks sta bolj zanesljiva

# Zunanji in notranji napadalci




## – Outsider

- Potrebuje dostop do sistema
- Deluje hitro, da ga ne bi odkrili
- Vgradi “zadnja vrata” (trapdoors) za nadaljni dostop
- Deluje v okolju, ki ga ne pozna

## Insider

- Ima dostop do sistema
- Deluje lagodno
- Ima zagotovljen dostop v prihodnosti
- Dela v znanem okolju
- Ve, kaj je pomembno

# Black Hats - White Hats

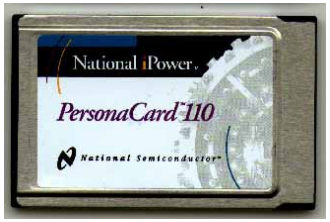
- Črni klobuki so “hudobneži“, ki uporabljajo svoje znanje za nepooblaščeno vdiranje v druge sisteme in posredovanje svojega znanja drugim “insiderjem”
- Beli klobuki so “dobri” ljudje. Delujejo v odkrivanju in v preprečevanju napadov.

# Kako zagotoviti varnost

- Preventiva pred napadom
  - avtentikacija
  - avtorizacija
  - kriptografija
  - požarni zidovi
  - utrjevanje ...
- Odkrivanje med napadom
  - IDS – Intrusion Detection Systems
  - beleženje - vodenje sistemskih dnevnikov
- Reakcija po napadu
  - krpanje lukenj
  - sporočanje ustreznim organom

# Avtentikacija

- Ugotavljanje uporabnikove identitete
  - uporabnik je oseba ali drug računalnik/storitev, ki uporablja neko zaščiteno storitev
- Uporabnikovo identiteto največkrat ugotavljamo z geslom
- Avtentikacija človeka:
  - Nekaj, kar veš (na primer geslo ali kako drugo skrivnost)
  - Nekaj, kar imaš (na primer smart card, varnostni žeton)
  - Nekaj, kar si (prstni odtisi, skeniranje zenice, glas)


# Gesla

- Ne smejo biti preprosto uganljiva
- Vedno je prisotna komponenta “social engineering”.
- Če potujejo nezaščitena po mreži jih je mogoče prebrati
- Bolj varna so začasna gesla (novo geslo ob vsakokratni prijavi)
  - zunanji generatorji gesel, sinhronizirani s strežnikom

# Tvorimo varna gesla

- Implementacija varnostne politike ustanove
- e-mail naslovi naj ne bodo del gesla
- Spreminjajmo vsakih 30 - 45 dni
- Vzdržujmo zgodovino zadnjih 8 gesel, izogibajmo se ponovni uporabi starih gesel
- Vedno uporabljajmo gesla, nikoli praznih
- Izogibajmo se znanim besedam - slovarji
- Uporabljajmo znake ALT - ALT-130 for é, ALT-157 za ¥, itd.
- Nikoli si ne zapisujmo gesel
- Tvorimo gesla s kompleksnimi akronimi:
  (I eat 3 pizzas on Tuesday) Ie_#3poT

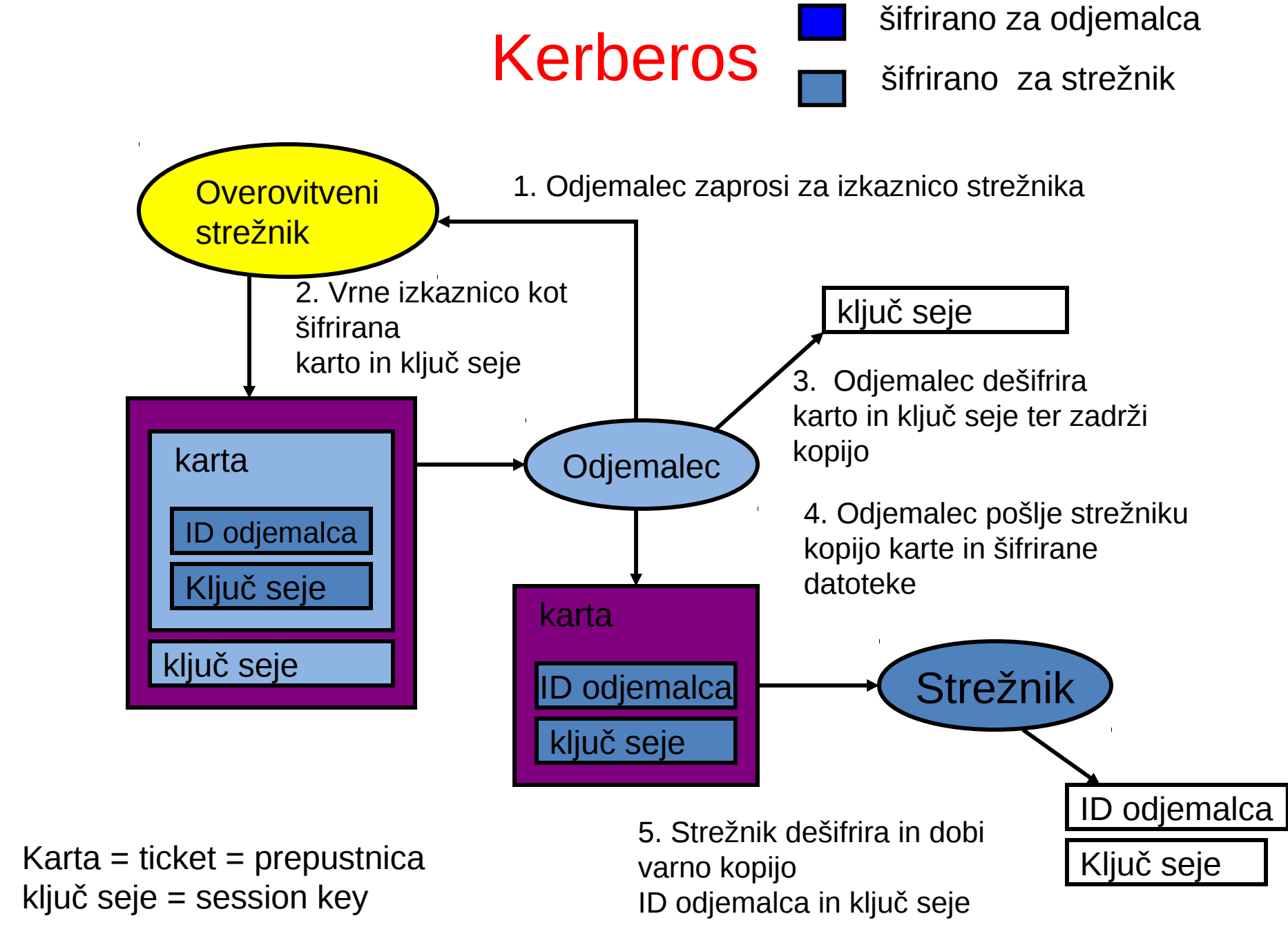
# Avtorizacija

- Kaj lahko uporabnik počne
- OS omejuje dostop uporabnikov do virov glede na privilegije uporabnikov
- ACL – Access Control List
  - določa dostopne pravice do objektov v sistemu
  - lahko do datotek, procesov, omrežnih virov ...
- Trostopenjski proces:
  - avtentikacija uporabnika
  - ugotavljanje pravic uporabnika
  - odločitev ali uporabnik ima pravice za dostop do vira ali ne

# Kerberos

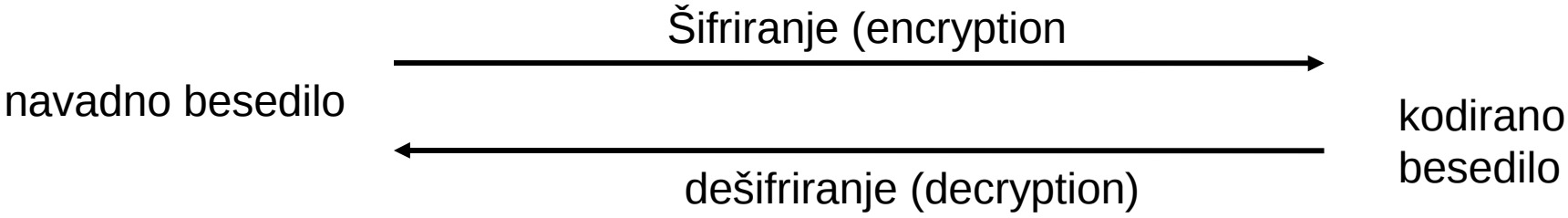
- Kerberos
  - predpostavlja zmešanje podatkov, ki potekajo po omrežju
  - OS na dveh računalnikih nista nujno varna
- Kako deluje Kerberos?
  - Proces na odjemalcu hoče storitev procesa na strežniku
  - Sredstvo komunikacije je omrežje
  - Kerberos nudi strežnik overovitve in protokol
    - Odjemalec in strežnik lahko oddajata  overovljena sporočila
    - Overovitvenemu strežniku moramo zaupati!

# Kerberos

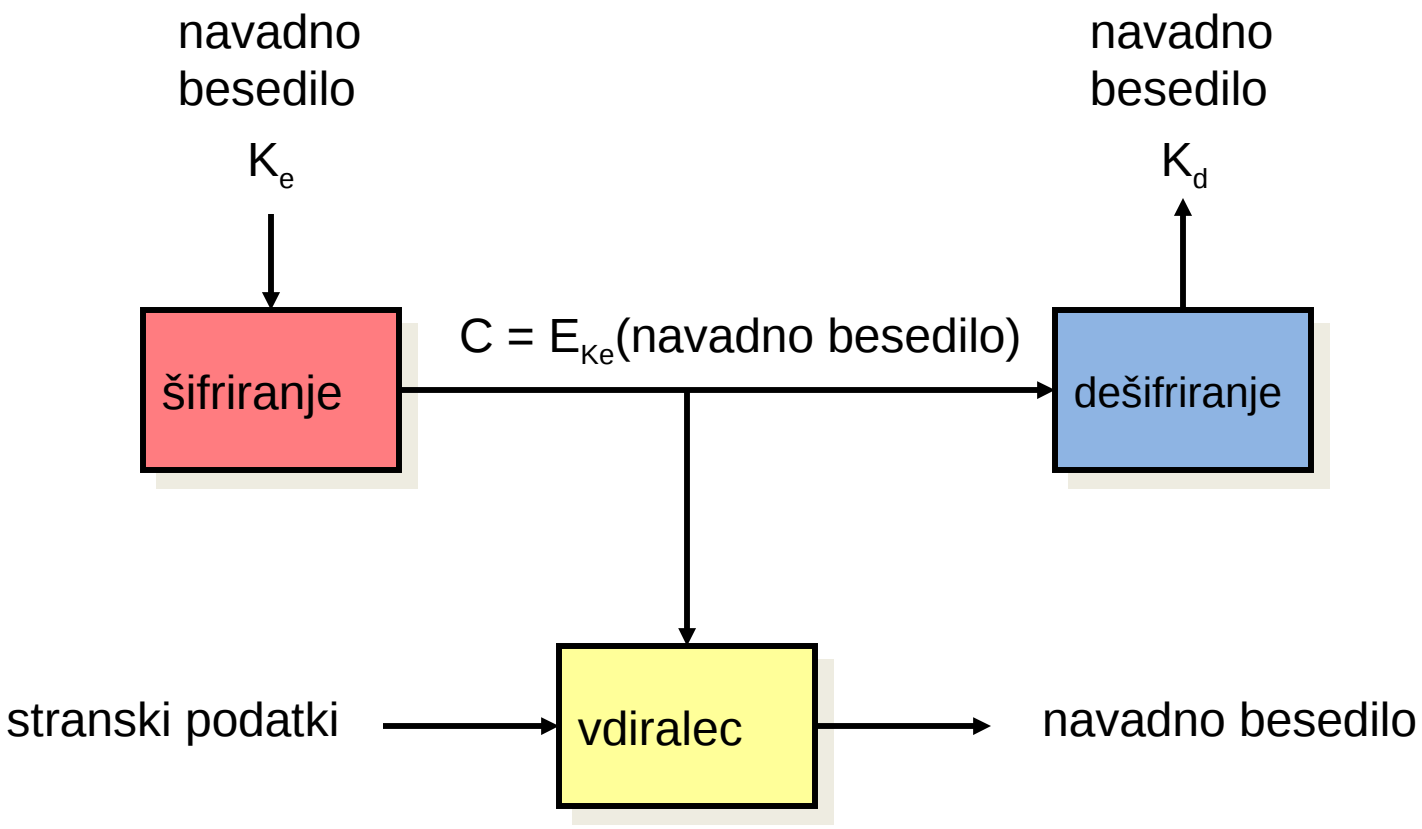

šifrirano za odjemalca
šifrirano za strežnik
Overovitveni strežnik
1. Odjemalec zaprosi za izkaznico strežnika
2. Vrne izkaznico kot šifrirana karto in ključ seje
ključ seje
3. Odjemalec dešifrira karto in ključ seje ter zadrži kopijo
karta
ID odjemalca
Ključ seje
ključ seje
Odjemalec
4. Odjemalec pošlje strežniku kopijo karte in šifrirane datoteke
karta
ID odjemalca
ključ seje
Strežnik
ID odjemalca
Ključ seje
5. Strežnik dešifrira in dobi varno kopijo ID odjemalca in ključ seje
Karta = ticket = prepustnica
ključ seje = session key

# Kriptografija

- Šifriranje: podatke zakodiramo s pomočjo ključa in pošljemo ali zapišemo
- Dešifriranje: pri branju ali sprejemu podatke dekodiramo s pomočjo ključa
- Pogosta uporaba pri varnem prenosu po omrežju
- Matematično ozadje – Tvorba praštevil



# Še o kriptografiji



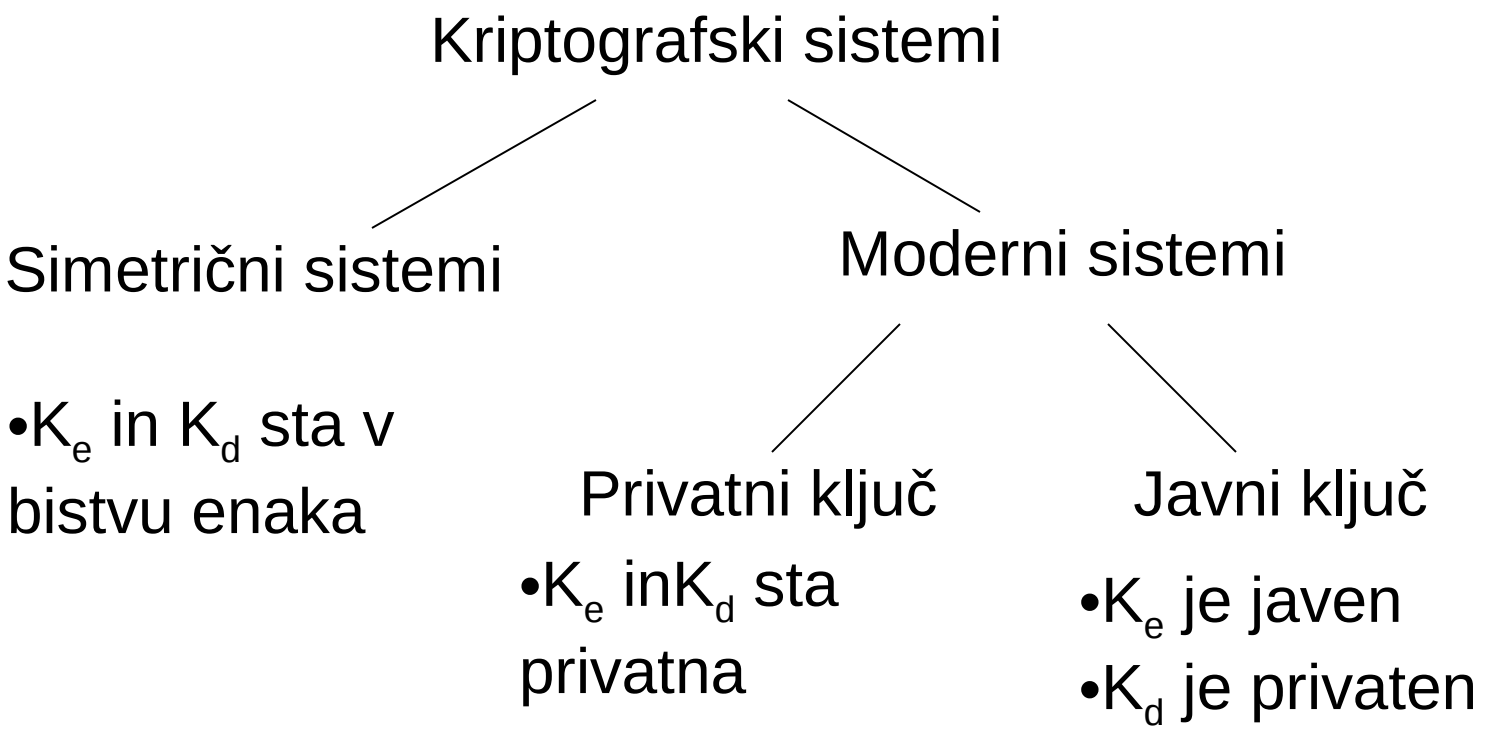
# Primer:
## Enostavna enkripcija z enojnim ključem

- Obvestilo = “Hello”, Ključ enkripcije = 7
- “Hello” = “72  69  76  76  79” (ASCII)
- Enkripcija: formula  C = MxE
- C = “504  483  532  532  553”
- Dekripcija: formula D = C/E
- D = “72  69  76  76  79”
- Obvestilo = “Hello”

# Kriptografija

- Se ukvarja s skrivanjem pravega pomena sporočil
- Enkripcija: sporočilo zakodiramo, da ni berljivo brez dodatnega znanja
- Lastnosti dobre enkripcije:
  - avtoriziranemu uporabniku omogoča relativno enostavno kodiranje in dekodiranje podatkov.
  - shema enkripcije ni odvisna od tajnosti algoritma temveč od parametra algoritma , ki mu pravimo ključ enkripcije (encryption key)
  - vdiralec naj ima pri ugotavljanju ključa enkripcije čim večje težave
- Enkripcija zagotavlja neberljivost sporočila, ne zagotavlja pa nujno integritete in avtentičnosti sporočila
  - to lahko zagotavljamo npr. z digitalnimi podpisi
- Enkripcijske algoritme delimo v dve skupini:
  - simetrične (s privatnimi ključi)
  - nesimetrične (z javnimi ključi)

# Kriptografski sistemi

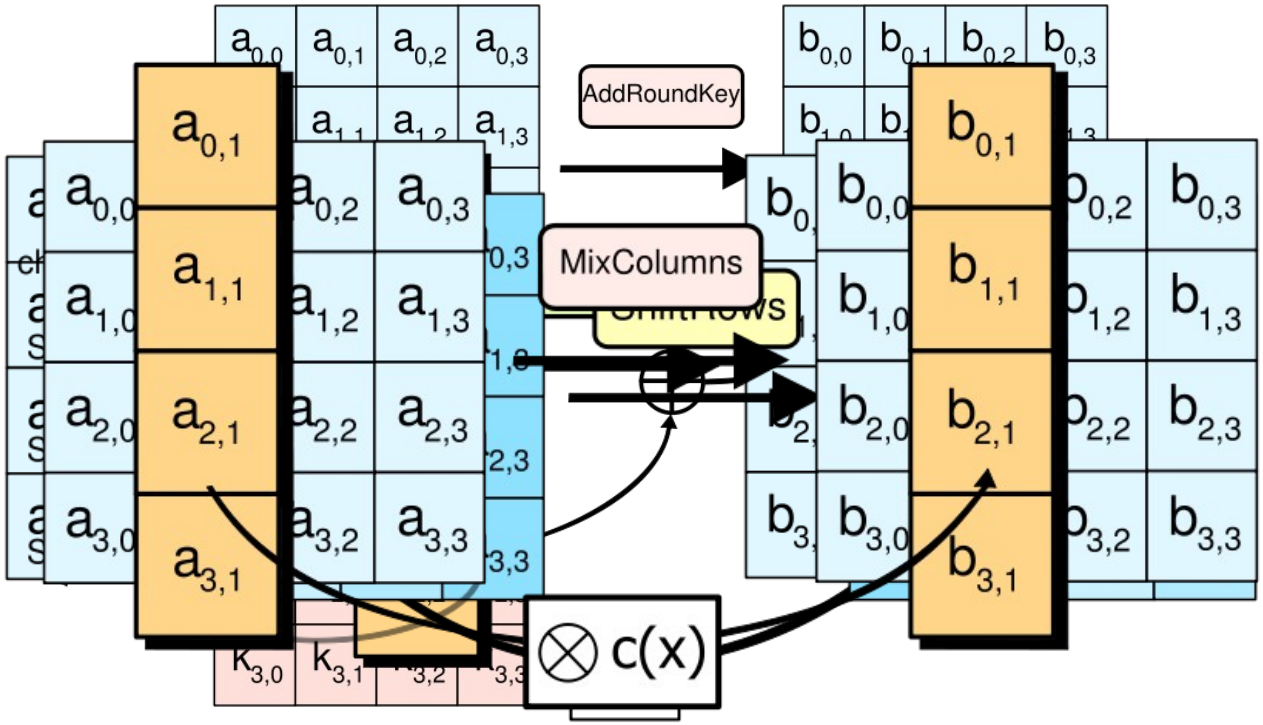


# Simetrični algoritmi za enkripcijo

- Tako pošiljatelj kot prejemnik imata isti enkripcijski ključ
  - ali zelo podoben oz. se da iz enega enostavno dobiti drugega
- Primeri algoritmov: DES, AES (Advanced Encryption Standard ali Rijndael)
- So hitri algoritmi
- Simetrični algoritmi tipično nadomeščajo znake v tekstu in spreminjajo njihov vrstni red na osnovi ključa enkripcije
- Ključ enkripcije se med pošiljateljem in prejemnikom navadno izmenja preko drugega varnega mehanizma.
  - Algoritem je znan -> taka shema je le toliko varna, kolikor je varen mehanizem izmenjave ključa

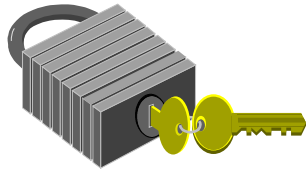
# Primer:
# AES

- 4 operacije nad matrikami 4x4 bajte
  - dodaj ključ (z XOR)
  - transformiraj matriko (s funkcijo, ki vnaša nelinearnost)
  - zamakni vrstice
  - premešaj stolpce



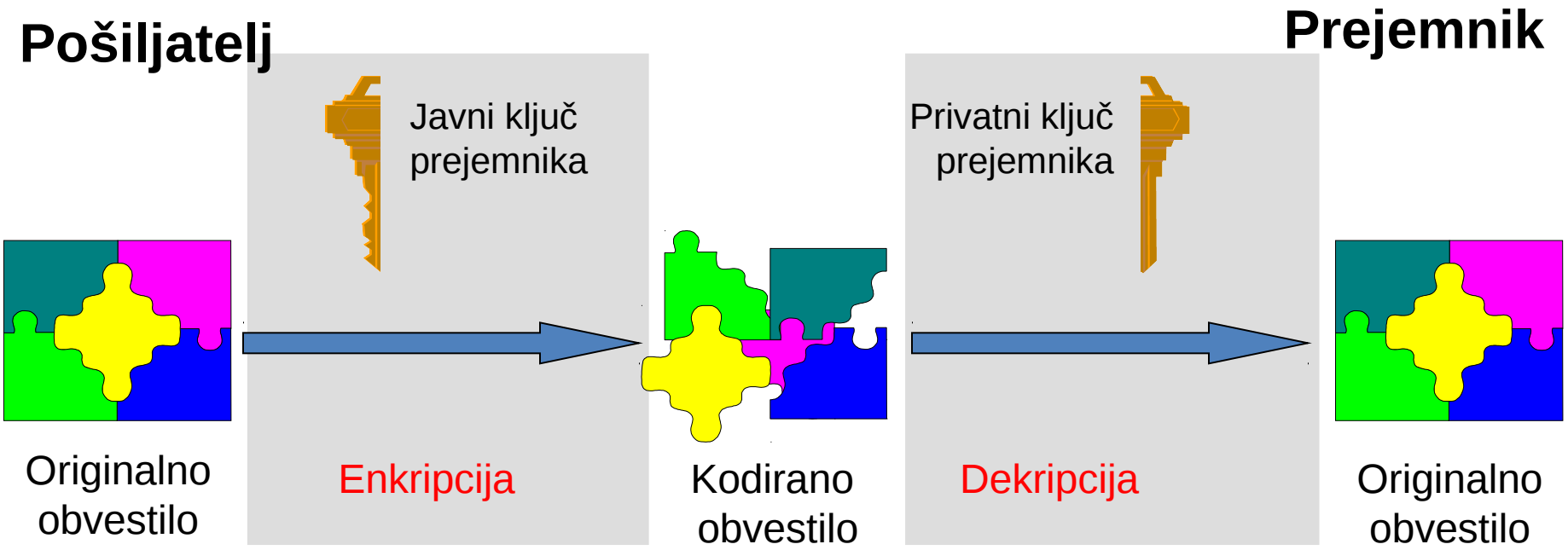
# Nesimetrični algoritmi

- Enkripcija z javnim ključem, temelji na tem, da ima vsak uporabnik dva ključa:
  - javni ključ – objavljen ključ za enkripcijo podatkov.
  - privatni ključ – Ključ, ki ga pozna le posameznik , ki z njim lahko dekodira podatke.
- Shema kodiranja je javna, vendar iz nje ne sme biti lahko odkriti sheme dekodiranja.
  - iz javnega ključa ne sme biti enostavno dobiti privatnega ključa!
- Kar zakodiramo z enim ključem (javnim ali privatnim), lahko odkodiramo z drugim ključem
- Bolj računsko zahtevni od simetričnih algoritmov
- Velikokrat se uporabljajo za izmenjavo simetričnega ključa, po izmenjavi pa pošiljatelj in prejemnik uporabljata simetrični algoritem (npr. AES)
- Primer: RSA algoritem



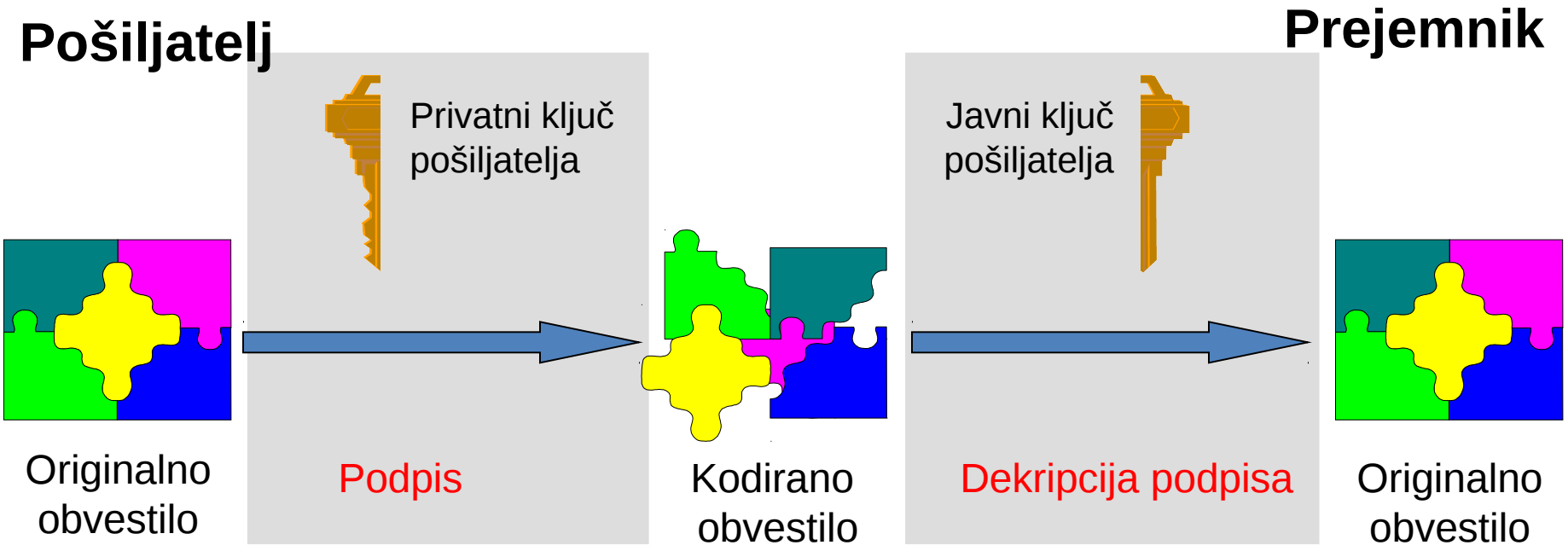
# Enkripcija z javnim ključem

- Postopek zagotavlja tajnost sporočila



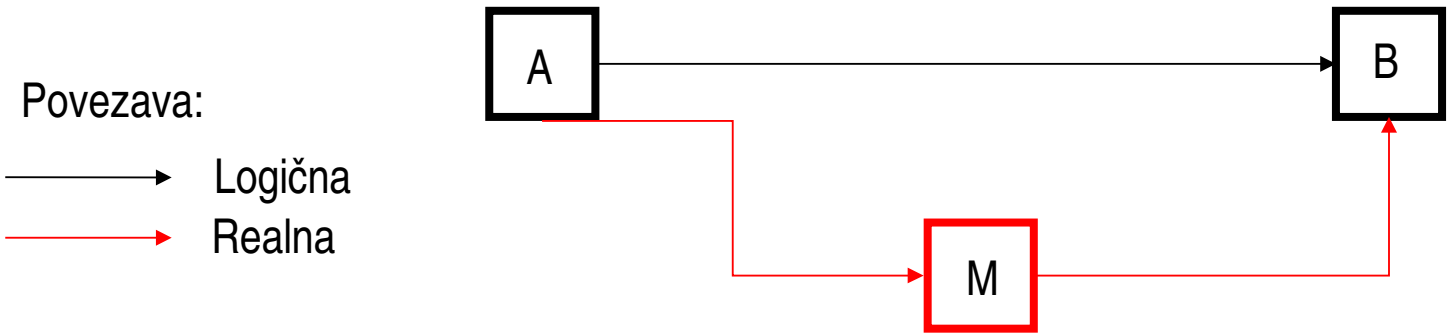
# Digitalni podpis z javnim ključem

- Postopek zagotavlja, da je pošiljatelj tisti, ki je poslal sporočilo



# Napad “moža v sredini”

- Se tipično uporablja za krajo seje
- Tipologija napada, ki mu pravimo “man-in-the-middle” je v preusmeritvi prometa med dvema računalnika proti tretjemu (napadalcu), ki se dela, da je legitimna komunikacijska točka.
- Napadalec lahko tako bere, ustvarja in spreminja sporočila med dvema točkama, brez da bi žrtvi to vedeli
- Lahko ogrozi tudi zaščito z javnim ključem



# Napad “moža v sredini” – kraja seje

- Možen napad na shemo javnega ključa
- Predpostavimo, da vdiralec Pepe lahko prisluškuje tako Jankotu kot Metki, lahko pa tudi spreminja, briše in nadomešča sporočila ter ustvarja nova.
  - Janko pošlje Metki svoj javni ključ
  - Pepe ga prestreže in pošlje Metki svoj javni ključ.
  - Metka kodira svoje sporočilo z Jankovim javnim ključem (ki je v resnici Pepetov) in ga pošlje Janku
  - Pepe prestreže njeno obvestilo, dekodira ključ s svojim privatnim ključem, spremeni, zakodira ga z javnim ključem Janka in mu ga pošlje.
  - Janko sprejme sporočilo, za katerega misli,  da je od Metke. Dekodira ga s svojim privatnim klučem in dobi napačno sporočilo
  - Janko in Metka si začneta izmenjevati sporočila z uporabo ključa seanse. Pepe, ki sedaj prav tako ima ta ključ, lahko nemoteno dešifrira kompleten pogovor.

# Certifikati

- Zaščita pred napadi moža v sredini
- Public key certificate – uporablja digitalni podpis, da poveže javni ključ in osebo ali organizacijo, ki ji javni ključ pripada
- Digitalni podpis tipično pripada znani CA – Certificate Authority (npr. VeriSign)
- Certifikat tako vsebuje:
  - javni ključ, ki se podpisuje
  - ime osebe/računalnika/organizacije
  - veljavnost
  - digitalni podpis certifikata, ki ga je s svojim privatnim ključem naredila CA
- S preverbo digitalnega podpisa (preko javnega ključa CA) lahko ugotovimo, ali uporabljeni javni ključ res pripada pravi osebi

# Primer: kako deluje HTTPS

- HTTPS: varen HTTP protokol, ki temelji na asimetričnih in simetričnih algoritmih in podpisovanju s strani CA
- Kriptira se ves promet
- Spletni strežnik potrebuje certificiran par privatni/javni ključ
- HTTPS po korakih:
  - odjemalec pošlje strežniku seznam algoritmov, ki jih podpira in naključno zaporedje N1
  - strežnik vrne naključno zaporedje N2, izbrani algoritem in svoj certifikat
  - odjemalec preveri certifikat, ki vključuje javni ključ strežnika KP1
  - odjemalec generira “premaster” ključ P1, ga kodira z javnim ključem strežnika KP1 in pošlje na strežnik
  - če je potrebno, se preveri certifikat odjemalca
  - strežnik in odjemalec iz naključnih zaporedij N1 in N2 in “premaster” ključa P1 generirata “master“ ključ za izbrani simetrični algoritem (DES, MD5 ...), ki ga uporabljata do konca seje
  - odjemalec pošlje sporočilo, da bo začel uporabljati ta novi ključ in od tu naprej je povezava kriptirana

# Varnost na omrežju

## (network security)

- Na mreži smo vedno v nevarnosti
  - Manj varno: brezžično omrežje
  - Drugo najmanj varno: stalno ožičene povezave
  - Tretje najmanj varno: Občasne povezave (na primer dial-up)
- Najbolj varno: Nikoli povezan
- Povečanje varnosti:
  - kriptirani mrežni protokoli (IPsec)
  - uporaba programov, ki uporabljajo kriptografske protokole nad TCP/IP, npr. SSL ali TLS (SSH, ipd.)
  - požarni zidovi

# Problemi TCP/IP

- Pri načrtovanju niso mislili na varnost.
- Vse podatke, vključno s polji v zaglavjih protokolov, posredujemo nekodirano.
- Prevarana sta lahko tako pošiljatelj kot prejemnik
- Prijemi kot npr. IP spoofing in razne DoS tehnike kažejo na veliko ranljivost protokola

# IPsec

Protokoli za povečevanje varnosti IP, ki omogočajo enkripcijo in avtentikacijo vsakega IP paketa

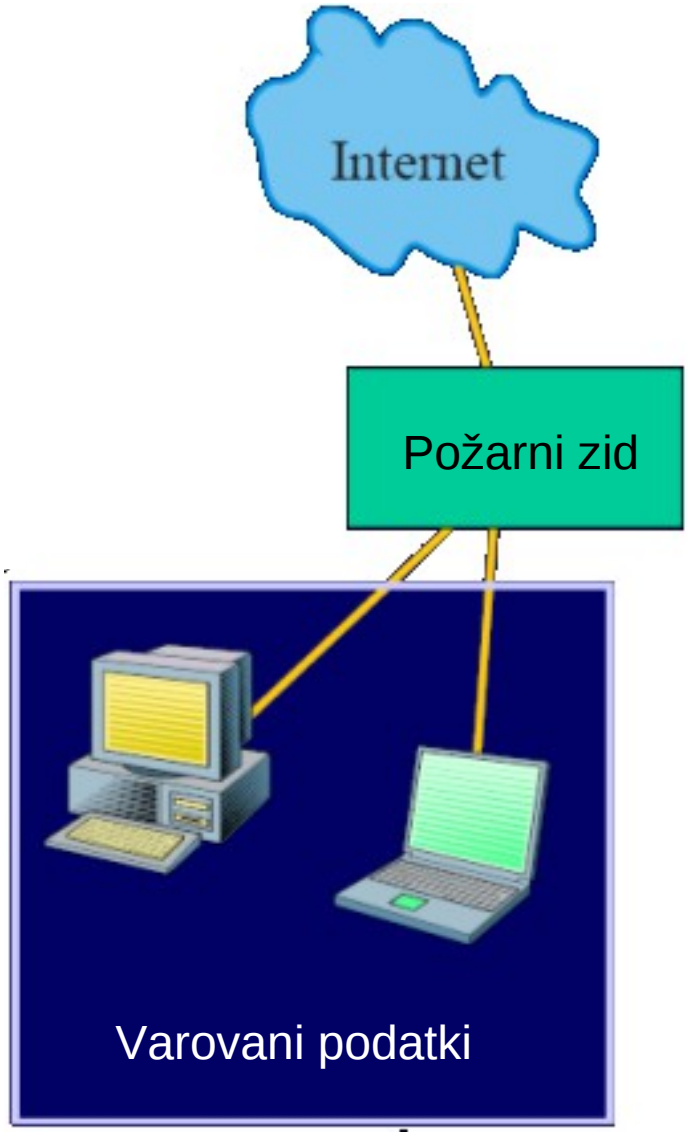
- Zaupnost podatkov: IPSec pošiljatelj lahko enkriptira pakete, preden jih pošlje preko omrežja.
- Neoporečnost podatkov: IPSec prejemnik lahko preveri pakete, sprejete od IPSec pošiljatelja, da se prepriča, če niso bili med prenosom kaj spremenjeni.
- Avtentikacija izvora podatkov: IPSec sprejemnik lahko preveri izvor poslanih paketov. Ta storitev je odvisna od servisa za ugotavljanje neoporečnosti podatkov.
- Anti-Replay: IPSec sprejemnik lahko odkrije in zavrne ponovljene pakete.
- Dva načina enkripcije:
  - Transport: enkripcija samo sporočila (ne tudi glave paketa)
  - Tunnel: tako glava kot sporočilo sta kriptirana

# IPv6

- Novi IP standard, ki se počasi uveljavlja
- IPsec je njegov obvezen del
- Poleg tega nudi:
  - Razširjene možnosti naslavljanja (128 bitni naslov)
  - IP naslovi navadno niso fiksni
  - Multicast podpora
  - Enostavnejša zaglavja paketov vodijo v hitrejše usmerjanje (routing)
  - Rezervacija pasovne širine
  - ...

# SSH (Secure Shell)

- Omogoča varno prijavo na oddaljen računalnik
- telnet, rlogin, … ne avtenticirajo oddaljenega računalnika;  SSH pa ga.
- Geslo, ki ga tipka uporabnik, je pri telnet in rlogin posredovano kot nekodiran tekst.  SSH ga pošilja kodirano.
- Podatki, ki jih pošiljamo ali sprejemamo preko RTF, so prav tako nekodirani;  SSH jih pošilja in sprejema v kodirani obliki.
- SSH zlorabe obstajajo
  - Občutljivo na napad “moža v sredini”



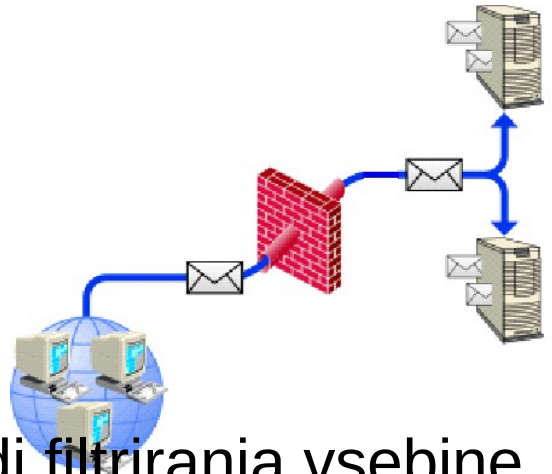

# Omrežna zaščita z uvedbo požarnega zidu (firewall) za izolacijo domene

# Kaj je požarni zid

- Je omrežna naprava, ki omejuje dostop do virov (informacijskih storitev) v skladu z varnostno politiko
- Požarni zid ni “čarobna rešitev” varnostnih problemov na omrežju niti popolna rešitev pred oddaljenimi napadi ali neavtoriziranim dostopom do podatkov
- Služi za povezavo dveh delov omrežja preko nadzora prometa (podatkov), ki sme potekati med obema
- Filtrira le tisti promet, ki poteka preko njega
- Tako lahko ščitimo pred zunanjim omrežjem (npr. internetom) celotno ustanovo, oddelek ali posamezni računalnik

# Kaj lahko filtriramo

- Moderni požarni zidovi lahko npr. filtrirajo promet glede na:
  - IP naslov pošiljatelja in vrata pošiljatelja
  - IP naslov in vrata prejemnika
  - storitev (npr. splet, ftp ...)
  - parametre protokola, npr. TTL
  - domena pošiljatelja
  - ...



- Filtriranje podatkovnih paketov ne nudi filtriranja vsebine podatkov
- Tudi če bi pregledovali vsebino, enkriptiranih podatkov ne moremo pregledovati (https, ssh)
- Določene storitve oziroma aplikacije, ki jih nudi internet, ne bodo več dostopne

Varnost ali prikladnost ?

# Utrjevanje sistema

- Postopek povečanja varnosti sistema, da bi ga čimbolj zaščitili pred napadi
- Utrjevanje je posledica neprimernih privzetih konfiguracij OS
  - privzete (Out of the box) namestitve so redkokdaj pravilno konfigurirane.
  - standardna uporabniška imena s standardnimi gesli.
  - izvajanje nepotrebnih (tudi omrežnih) servisov.
  - puščanje občutljivih sistemskih datotek, odprtih za branje ali pisanje

# Utrjevanje

Postopek bi lahko bil sledeč:

- Začni s primerno konfiguriranim sistemom.
- Odstrani nepotrebna up. imena in gesla
- Odstrani šibke in nepotrebne komponente/storitve (npr. print spooler na Windowsih, če ni v uporabi)
- Dodaj zaščitne plasti – požarne zidove, popravke jedra (PaX za Linux, Bastille Linux ...)
- Vodi podroben zapis dogodkov (log).

# Utrjeni OS

- Pogosto izenačevano z “utrjevanjem”.
- Ponovna izgradnja operacijskega sistema iz iste izvorne kode, vendar z bolj strogim prevajalnikom.
- Predelava delov operacijskega sistema za večjo varnost

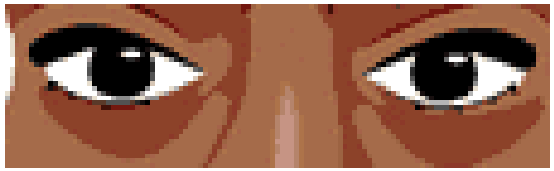
# Odkrivanje med napadom - IDS

## IDS = Intrusion Detection System

- Splošen pomen
  - Pridobivanje podatkov o okolju, potrebnih za analizo obnašanja sistema
  - Odkrivanje varnostnih lukenj, vdorov, odprtih ranljivosti
- Tipi podatkov
  - dolgoročni podatki. – baza znanja o napadih (statično)
  - Podatki o konfiguraciji. – model trenutnega stanja sistema (statično)
  - Revizorski podatki. – opisujejo dogodke v sistemu (dinamično)

# Odkrivanje med napadom - IDS

- Kaj IDS opazuje:
  - opazuje mrežni promet npr. opazi lahko DoS napade, skeniranje vrat, poskuša najti buffer-overflow napade
    - npr. če ugotovi, da se naenkrat poskuša odpreti veliko povezav na različna vrata, gre najbrž za skeniranje vrat
  - opazuje protokole – poskuša najti zlorabe na nivoju protokolov, npr. HTTPS
    - odkrivanje man in the middle in podobnih napadov
  - opazuje komunikacijo med aplikacijami in strežnikom (npr.  SQL povpraševanja na strežniku)



# Odkrivanje med napadom - IDS

- IDS opazuje tudi dogajanje na računalniku
  - Pozor na sumljive vzorce aktivnosti – na primer večkratno vnašanje napačnih gesel kaže na ugibanje gesel.
  - analiza dnevnikov (Audit log) – notri je zapisan čas, uporabnik in tip dostopa do objektov na sistemu
  - analiza sistemskih datotek: gledanje sprememb z opazovanjem “checksum” vrednosti
  - odkrivanje napačnih nastavitev (zaščite sistemskih direktorijev in datotek)
  - iskanje nepričakovanih programov, ki tečejo
  - iskanje nenavadnih datotek v sistemskih imenikih
  - analiza sistemskih klicev
  - ...
- Ko odkrije sumljivo dogajanje
  - reagira pasivno: obvesti pristojne
  - reagira aktivno (npr. blokira vse omrežne povezave ...) – Intrusion Prevention System

# Omejitve trenutnih pristopov

- Obstoječe tehnike odkrivanja vdorov so usmerjene v nizkonivojsko opazovanje
  - Oprema je enostavna, imamo pa ogromne količine podatkov
  - Veliko računanja
  - Difuzen pomen aktivnosti uporabnika
- Odkrivanje vdora terja sintezo teh podatkov
- Največkrat se še vedno odkriva po dejanju

# Kaj še narediti: dobra praksa

- Izolirajmo svoje podatke od aplikacij
  - Application folder
  - Data folder
- Uporabnik naj ima pravico pisati le v svoj podatkovni imenik
- Imejmo podatke na datotečnem strežniku
  - Vsak dan delajmo rezervne kopije
  - Imejmo več rezervnih kopij
- Imejmo načrt za izhod iz razdejanja
  - Operacijski sistem
  - Uporabniški programi
  - Podatki

# Dobra praksa

- Ne vstopaj v sistem kar tako s pravicami administratorja
- Sistemski servisi naj ne tečejo pod pravicami administratorja
- Uporabljaj protivirusne programe
- Imej ažuriran operacijski sistem
  - Servisni popravki (Service patches)
- Imej ažurirane uporabniške programe
  - Servisni popravki

# Dobra praksa

- Ne odpiraj pošte z neznanim naslovom
- Ne uporabljaj piratskih kopij programov
- Če ne veš, kaj neka datoteka naredi ali čigava je, je ne izvajaj
- 99% virusov se razširja tako, da jih poganjajo uporabniki

# 10 zakonov varnosti

- Če te zlobnež prepriča, da poženeš njegov program na svojem računalniku, to ni več tvoj računalnik.
- Če lahko zlobnež spremeni operacijski sistem na tvojem računalniku, to ni več tvoj računalnik
- Če ima zlobnež neomejen fizični dostop do tvojega računalnika, to ni več tvoj računalnik
- Če dovoliš zlobnežu, da nalaga programe (upload) na tvojo spletno stran, to ni več tvoja spletna stran
- Slaba gesla zahtevajo močno zaščito
- Računalnik je le toliko varen, kolikor je zanesljiv njegov administrator
- Enkriptiran podatek je le toliko varen, kolikor je varen ključ za dekripcijo
- Neaužuriran skener virusov je le nekaj več vreden od nobenega virusnega skenerja
- Absolutna anonimnost ni praktična ne v realnem življenju in ne na spletu
- Tehnologija ni zdravilo za vse