Računalniške komunikacije

Omrežna varnost

Jurij Mihelič, UniLj, PeF

Omrežna varnost

- Varnost in zaščita
  - **safety** (varnost, varstvo)
    - zaščita pred **nenamernimi** aktivnostmi, ki bi škodovale varovanemu sistemu
      - človeške napake, naravne nesreče
  - **security** (varnost, varovanost)
    - zaščita pred **namernimi** aktivnostmi, ki bi škodovale varovanemu sistemu
      - kraja, poškodovanje
  - **protection** (zaščita)
    - mehanizem oz. način zagotavljana varnosti

Omrežna varnost

- Področje, ki
  - analizira možnosti vdorov v sistem
  - načrtuje tehnike obrambe pred napadi
  - snuje varne arhitekture, ki so odporne pred vdori

- Varnost interneta
  - internet **ni** bil snovan ozirajoč se na varnost
  - sprva: skupina ljudi, ki si med seboj zaupajo in so povezani v skupno omrežje

Omrežna varnost

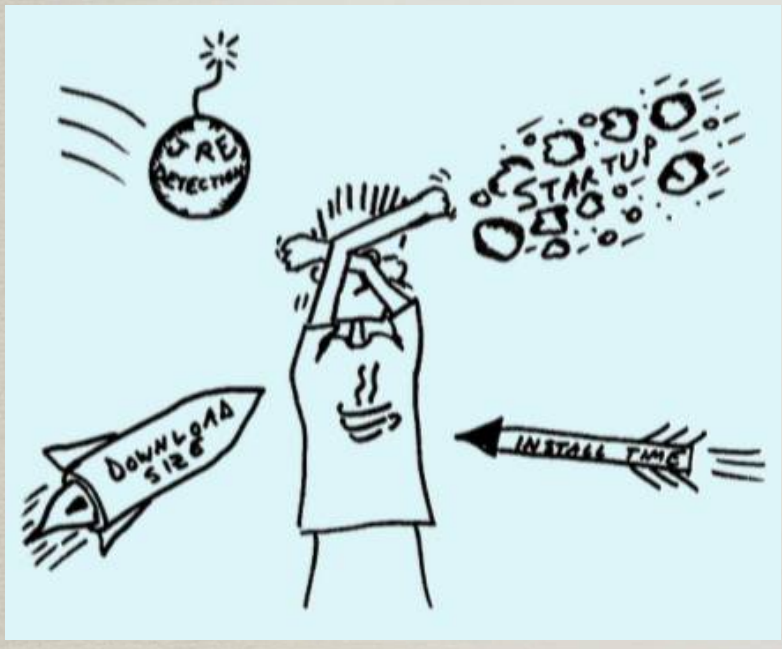
- Elementi varne komunikacije
  - **identifikacija**
    - ugotavljanje identitete (kdo si, brez dokaza)
  - **avtentikacija**
    - preverjanje identitete (dokaži, da si res tisti, za katerega se izdajaš)
  - **avtorizacija**
    - preverjanje legitimne rabe virov (ali imaš pravico, da uporabljaš nek vir)
  - **beleženje** (accounting, loging)
    - beleženje aktivnosti uporabe virov

Omrežna varnost

- Varna komunikacija
  - **zaupnost**
    - ohranjanje zaupnosti sporočila, da ga nepooblaščene osebe ne morejo razumeti
  - **integriteta**
    - ohranjanje verodostojnosti; Je bilo sporočilo med prenosom spremenjeno?
  - **onemogočanje zanikanja** (nonrepudiation)
    - zagotavljanje pošiljanja/prejema; res si poslal/prejel

Omrežna varnost

- Pogosti napadi

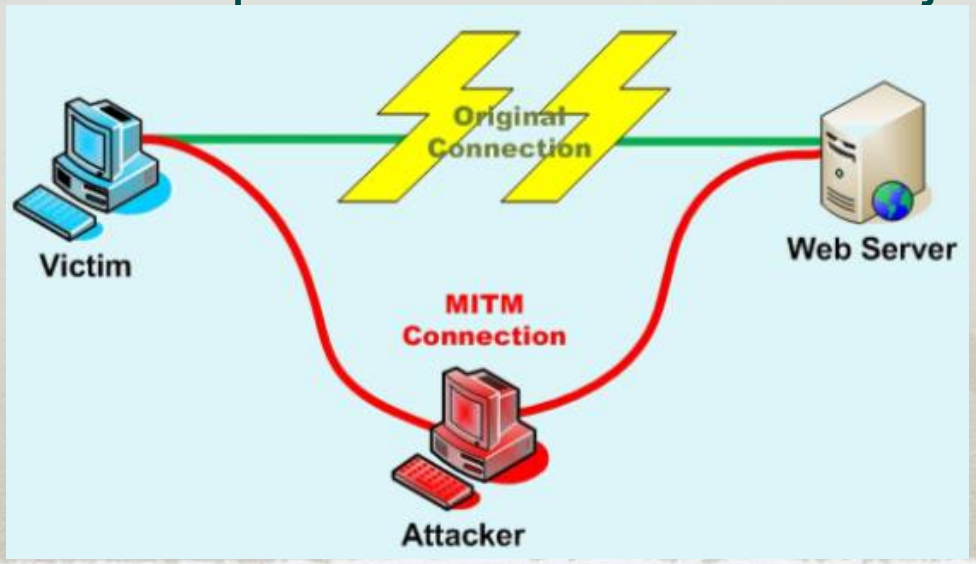


Omrežna varnost

- Pogosti napadi
  - prisluškovanje in ponarejanje sporočil
  - kriptografski napadi
    - ugotavljanje slabosti v kriptografskih algoritmih
  - ugibanje gesel
    - izčrpno preiskovanje, napadi s slovarjem
  - slabogramje: virusi, črvi in trojanski konji
  - družbeni inženiring
    - nigerijska pisma, lažne nagrade, brskanje po smeteh

Omrežna varnost

- Pogosti napadi
  - pregled vrat (port scan)
    - preverjanje vrat za prisotnost strežnikov
  - ponarejanje ARP/IP naslovov (ARP/IP spoofing)
    - napadalec prepriča ciljni sistem, da je nekdo drug
  - prestrezanje komunikacije (man-in-the-middle)
    - napadalec se postavi med izvorni in ciljni sistem

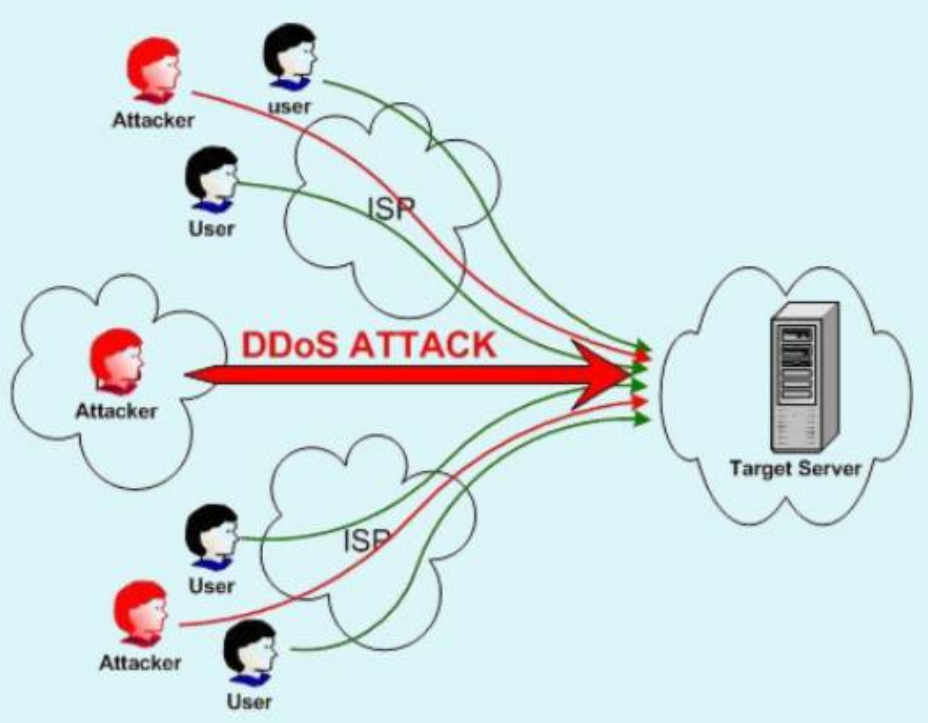


Omrežna varnost

- Pogosti napadi
  - zadnja vrata (back door)
    - nekateri programi dopuščajo možnost „skrivnega“ dostopa; ko je ta odkrit je sistem enostavno ranljiv
  - ponovitev komunikacije (replay)
    - napadalec prestreže komunikacijo in shrani stara sporočila ter jih ponovno pošlje kasneje
  - napad s fragmentacijo (fragmentation attack)
    - pretirano fragmentiranje paketa, da ga požarni zid ne zna analizirati

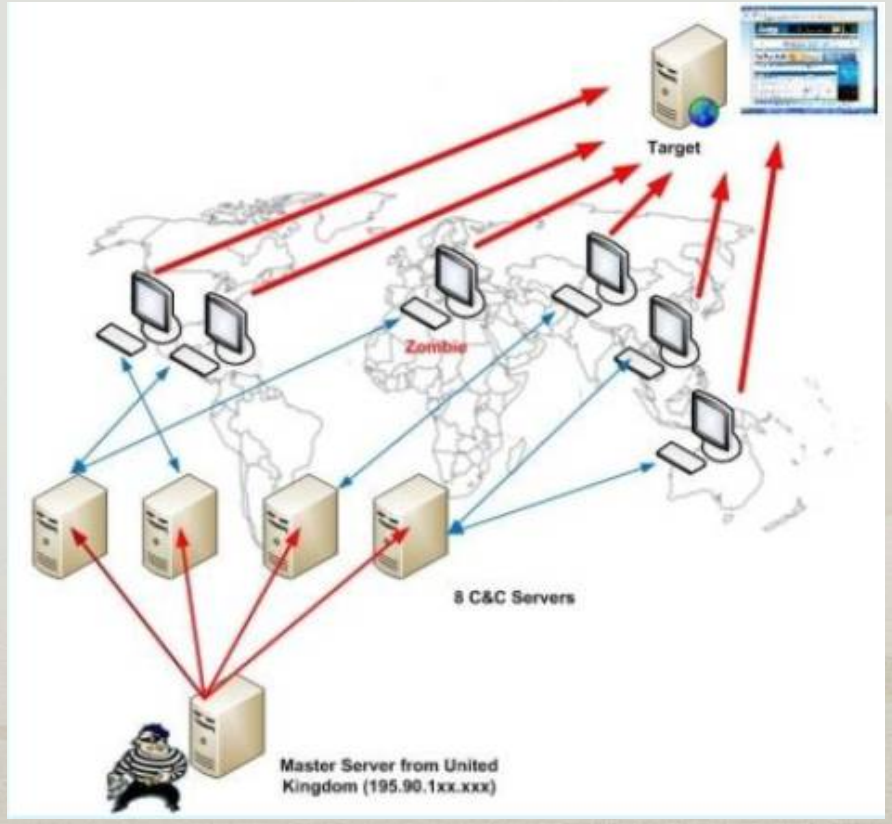
Omrežna varnost

- Pogosti napadi
  - odpoved delovanja sistema (denial-of-service)
    - obremenitev sistema preko njegovih zmogljivosti
    - sistem ne zmore več streči običajnih zahtev
    - porazdeljen napad (distributed DoS, DDoS)



Omrežna varnost

- Pogosti napadi
  - uporaba botov (web robot) za porazdeljene napade
    - bot je lahko računalnik, okužen s slabogramjem
    - lastnik takega računalnika običajno ne ve, da je okužen

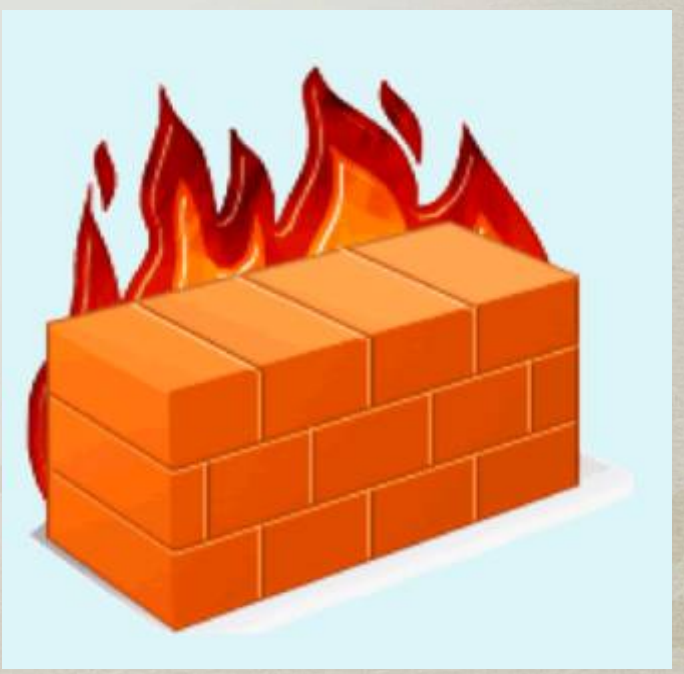


Omrežna varnost

- Operativna varnost
  - (notranje, lokalno) omrežje ima navadno samo eno točko vstopa, kjer nadzorujemo promet
  - sistemi za zaščito
    - požarni zid
    - sistem za zaznavanje vdorov
    - sistem za preprečevanje vdorov

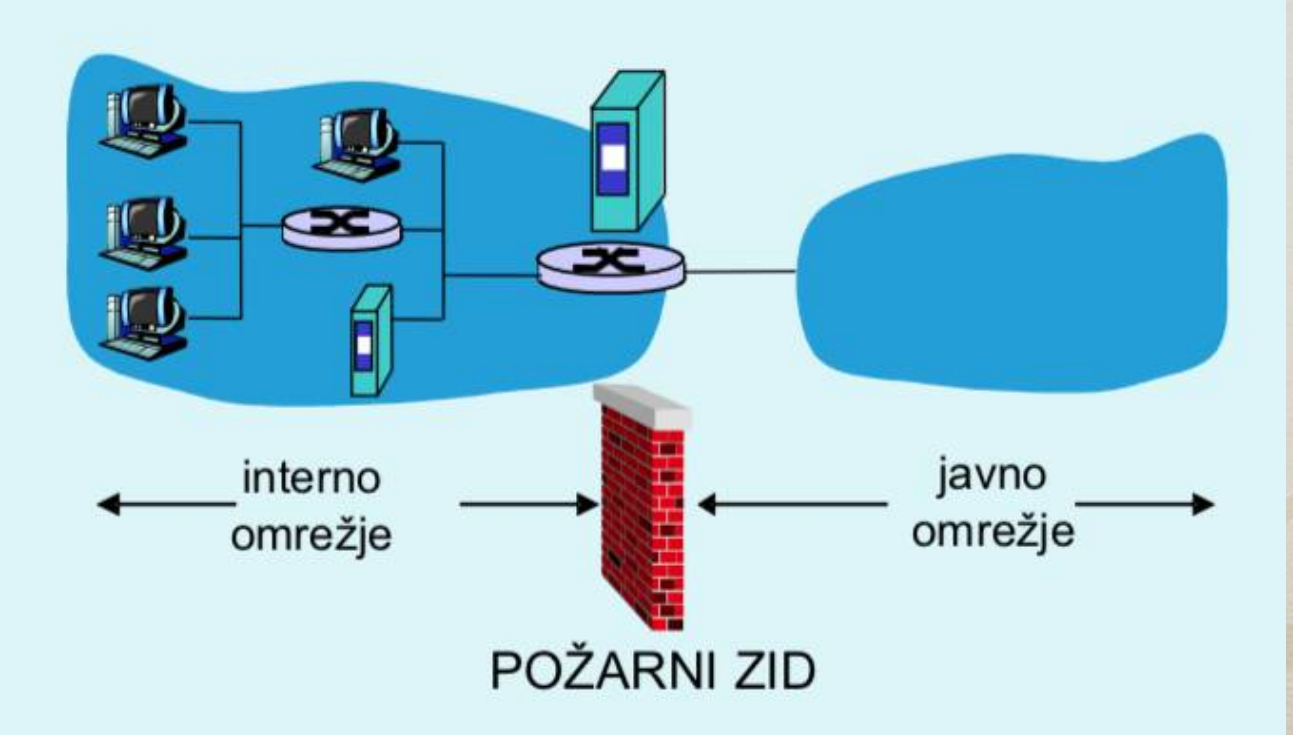
Požarni zid

- Kaj je požarni zid (firewall)
  - programska ali strojna oprema (sistem)
  - nadzoruje omrežni promet
  - preverja in filtrira *prihodne* in *odhodne* pakete
  - vzpostavi mejo med
    - zaupanja vrednim omrežjem
    - in zaupanja ne-vrednim omrežjem



Požarni zid

- Kaj je požarni zid (firewall)
  - primer
    - ločuje notranje (interno) in zunanje (javno) omrežje
    - notranje omrežje je lahko samo en računalnik



Požarni zid

- Vrste filtriranj
  - **izolirano filtriranje** paketov (stateless)
    - na podlagi podatkov v glavi paketov
  - **kontekstno filtriranje** paketov (stateful)
    - nadzoruje vzpostavljenost povezave
  - **aplikacijskih prehodi**
    - na podlagi podatkov aplikacijske plasti

Požarni zid

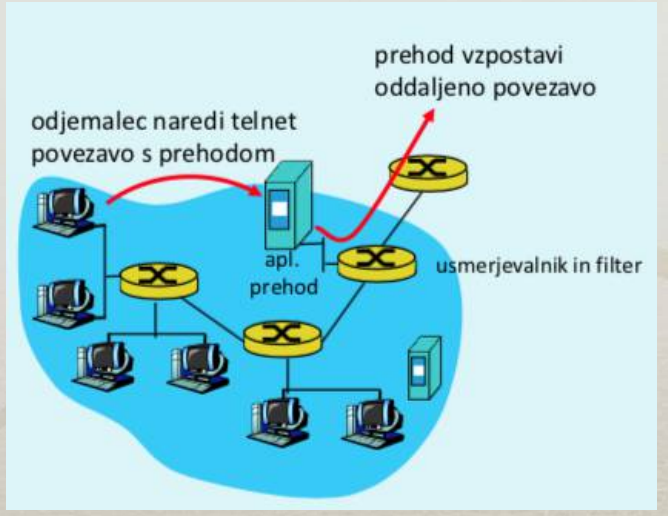
- Izolirano filtriranje
  - del usmerjevalnika, ki meji na javno omrežje
    - se odloča ali bo posredoval posamezen paket
    - drop (tiho ignorira), reject (zavrne z odgovorom ICMP), pass (prepusti)
  - mehanizmi filtriranja temeljijo na TCP/IP plasti
    - vrsta protokola (TCP, UDP, ICMP itd.)
    - IP številka izvora ali ponora
    - izvorna ali ciljna vrata
    - tip sporočila pri protokolu ICMP
    - zastavice TCP
      - SYN in ACK bit: lahko nadzorujemo dopustnost vzpostavljanja povezave

Požarni zid

- Kontektsno filtriranje paketov
  - TCP/IP plast
  - upoštevanje (vzpostavljene) povezave
  - filtriranje nesmiselnih paketov
    - npr. prepove vstop paketa na vrata 80, ACK=1, kjer predhodno še ni bilo paketa SYN (vzpostavitev povezave)
  - potrebno vodenje evidence (stanje) o povezavah
    - vzpostavitev (SYN) in rušenje (FIN) povezave
    - časovnik za posamezno povezavo, po izteku smatramo povezavo za neveljavno
    - zaradi hrambe stanja je možen napad DoS

Požarni zid

- Aplikacijski prehodi
  - filtriranje na podlagi uporabniških aplikacij
    - uporabnik najprej vzpostavi povezavo s prehodom
    - prehod uporabnika avtorizira
    - prehod posreduje podatke naprej ali pa blokira
  - vsak aplikacija potrebuje svoj aplikacijski prehod
  - odjemalce je potrebno posebej nastaviti

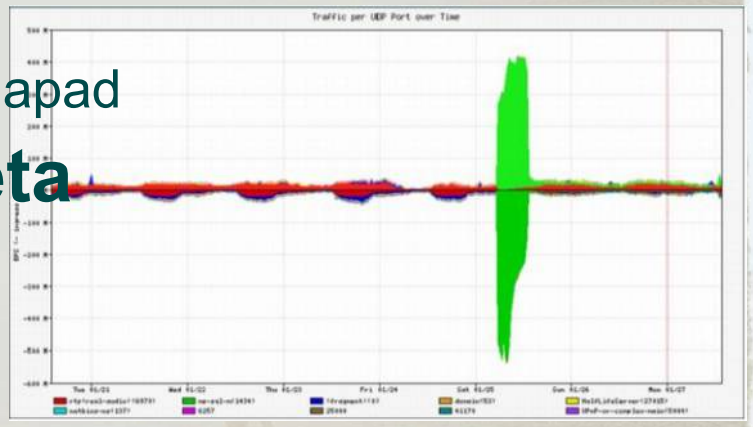


Sistem za obravnavo vdorov

- Sistem za zaznavanje vdorov
  - IDS: intrusion detection system
  - le opozori (pošilje sporočilo) na potencialno škodljiv promet
- Sistem za preprečevanje vdorov
  - IPS: intrusion prevention system
  - pri detekciji potencialnega vdora tudi ukrepa

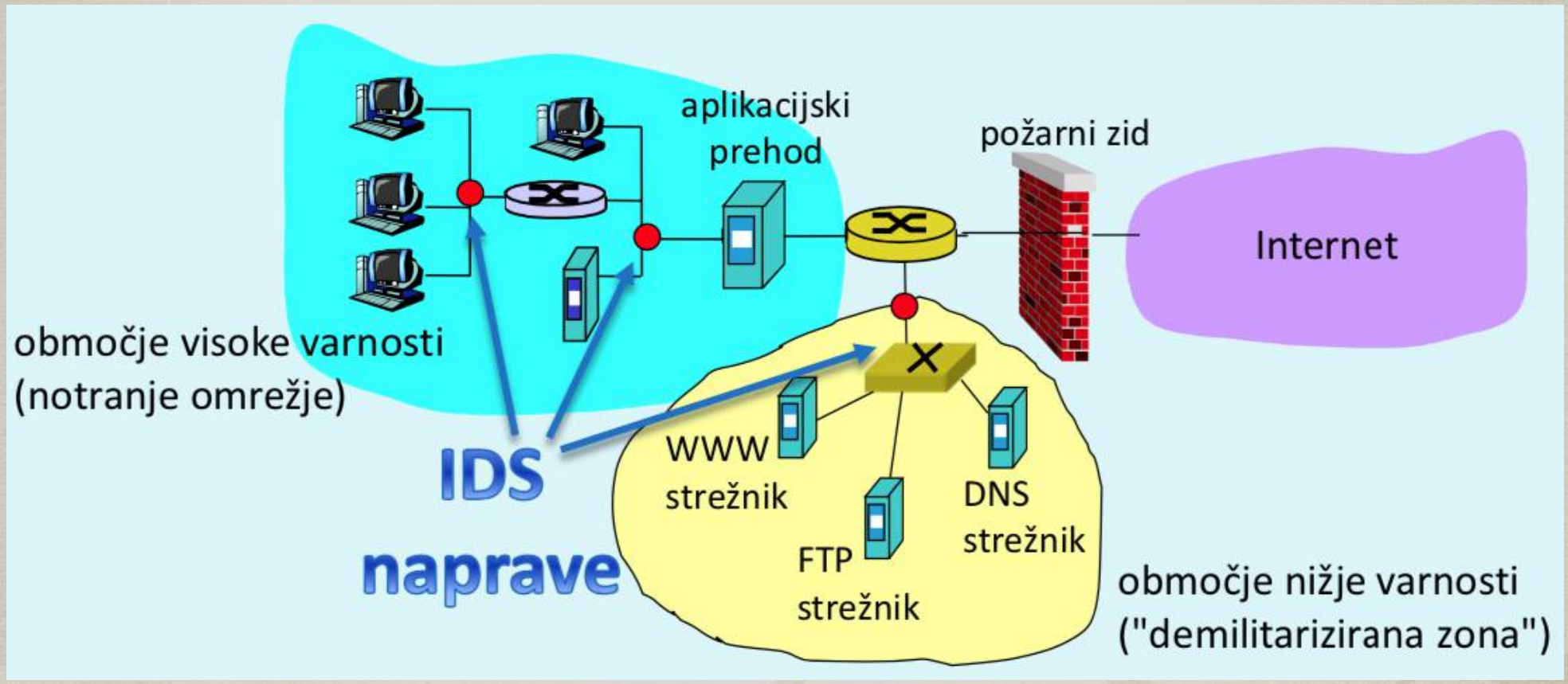
Sistem za obravnavo vdorov

- Kako deluje IDS/IPS?
  - zaznavanje z **vzorci napadov** (podpis, signature)
    - podpis (signature) napada
      - npr. izvorni/ponorni IP naslov, zaporedje bitov v podatkih paketa
    - varnost odvisna od baze znanih vzorcev, slaba zaznava še nepoznanih napadov
      - možni lažni alarmi, lahko spregleda napad
  - zaznavanje **netipičnega prometa**
    - opazovanje običajnega prometa in računanje različnih statistik
    - reagiranje na neobičajne statistike
      - npr. nenadno velik delež ICMP paketov
      - možno zaznavanje na še neznane napade, težko ločevanje med običajnim in neobičajnim prometom



Sistem za obravnavo vdorov

- Kam namestiti IDS/IPS?



Zaupnost

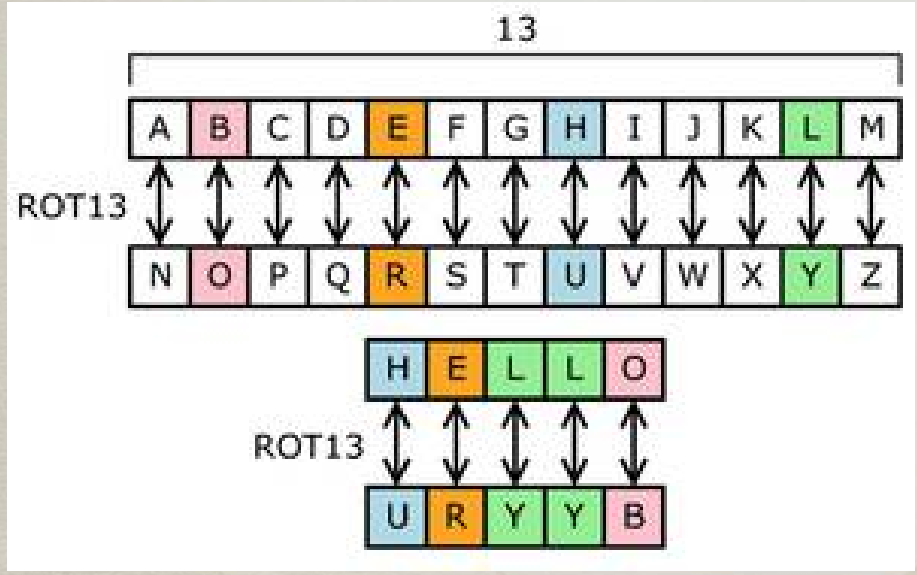
- Kriptiranje vsebine
  - zakrivanje vsebine pred nepovabljenimi uporabniki
  - **kriptiranje**
    - proces zakrivanja vsebine sporočila
    - rezultat je kriptogram
  - **dekriptiranje**
    - proces odkrivanja izvornega sporočila iz kriptograma
  - uporaba ključev
    - kriptirni/dekriptirni algoritem je pogosto znan vsem
    - skrivni so le ključi

Zaupnost

- Vrste kriptografskih metod
  - substitucijske (menjava znakov)
  - transpozicijske (menjava vrstnega reda znakov)
  - simetrične
  - asimetrične

Zaupnost

- Substitucijske metode
  - menjava znakov
  - Cezarjeva šifra



Zaupnost

- Tanspozicijske metode
  - menjava vrstnega reda znakov

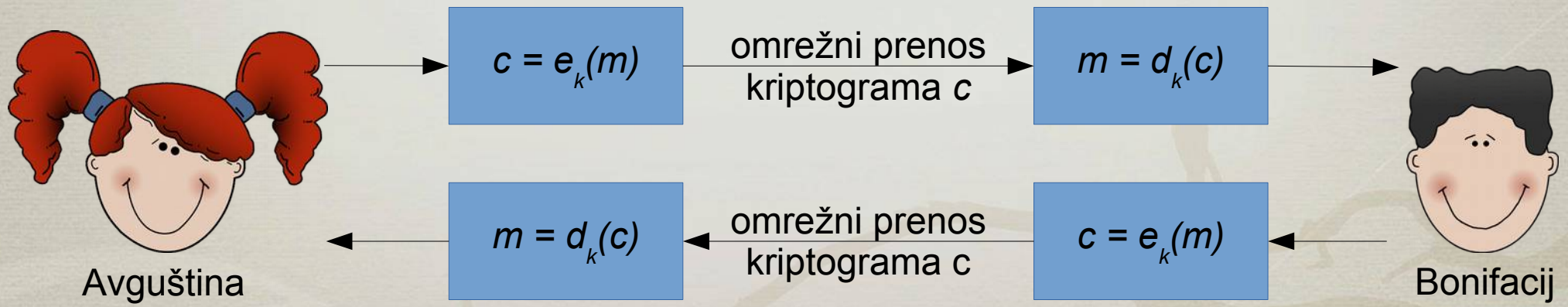
```
ORINBI
DISAEM
KLOSŽO
```

Zaupnost

- Simetrična kriptografija
  - en **skrivni ključ** *k* za kriptiranje in dekriptiranje
  - znani algoritmi
    - DES: data encryption standard, 1975; 3DES, 1995
    - AES: advanced encryption standard, 1998
    - IDEA: international data encryption standard, 1991
    - Twofish, 1997; Blowfish, 1993
  - algoritmi so običajno hitri
  - enostavno je generirati dobre ključe
    - ključi so navadno krajši kot pri asimetrični kriptografiji, za enako stopnjo varnosti
  - oba morata poznati ključ
    - Kako varno izmenjati ključ?

Zaupnost

- Simetrična kriptografija
  - $c = e_k(\mathrm{m})$ … kriptirni algoritem s ključem k
  - $m = d_k(\mathrm{c})$ … dekriptirni algoritem s ključem k
  - velja: $\mathrm{m} = d_k(e_k(\mathrm{m}))$

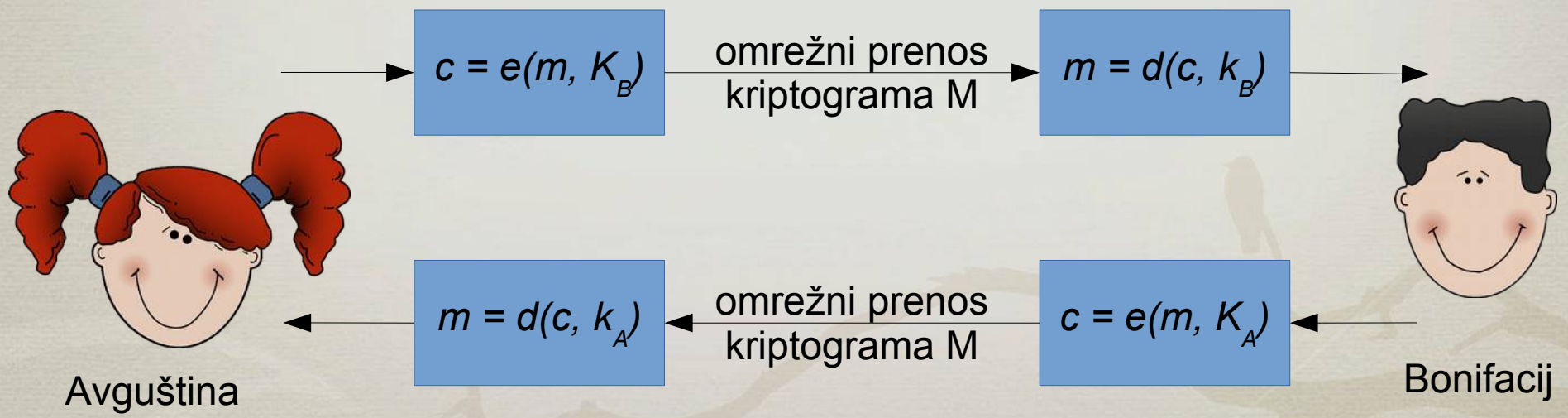


Zaupnost

- Asimetrična kriptografija (z javnimi ključi)
  - vsak ima dva ključa: javni *K* in zasebni *k*
  - javne ključe lahko javno objavimo
  - algoritmi so navadno počasni
    - zahtevajo počasne matematične operacije
  - znani algoritmi
    - RSA (Rivest, Shamir, Adelman) uporablja velika praštevila

Zaupnost

- Asimetrična kriptografija (z javnimi ključi)
  - prenos sporočila *m* od uporabnika *A* do uporabnika *B*
    - *A*: z ***B*-jevim javnim ključem** kriptiramo: c = $e(m, K_B)$
    - *B*: z ***B*-jevim zasebnim ključem** dekriptiramo: $m = d(c, k_B)$



Zaupnost

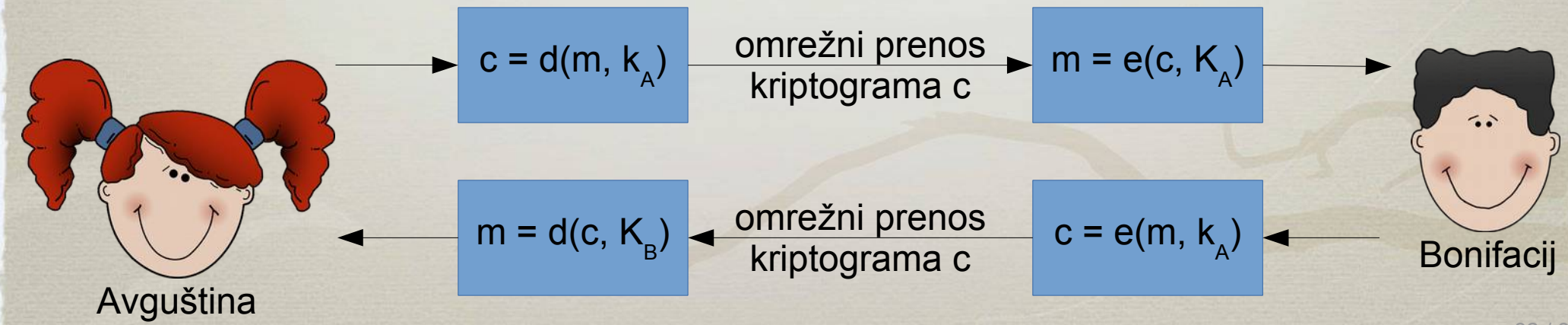
- Asimetrična kriptografija (z javnimi ključi)
  - zahteve za dobro delovanje
    - stran *A*: enostavno kriptiranje: $c = e(m, K_B)$
    - stran *B*: enostavno dekriptiranje: $m = d(c, k_B)$
    - računsko zahtevno odkrivanje zasebnega ključa k_B iz javnega K_B
    - računsko zahtevno odkrivanje sporočila *m*, če poznamo javni ključ K_B in kriptogram *c*
    - katerikoli ključ (zasebni ali javni) lahko uporabimo za kriptiranje (drugega pa za dekriptiranje)
      - $m = d(e(m, K_B), k_B) = d(e(m, k_B), K_B)$

Zaupnost

- Uporaba obeh
  - simetrična je hitra
  - asimetrična je počasna
  - rešitev
    - generiramo ključ za simetrično kriptografijo
    - uporabimo asimetrično kriptografijo, da izmenjamo generirani ključ
    - nato za glavnino komunikacije uporabljamo simetrično kriptografijo

Integriteta

- Integriteta uporabnika
  - dokazuje, kdo je sporočilo poslal
  - prenos sporočila *m* od uporabnika *A* do uporabnika *B*
    - *A*: z *A*-**jevim zasebnim ključem** kriptiramo: c = $d(m, k_A)$
    - *B*: z *A*-**jevim javnim ključem** dekriptiramo: *m* = $e(c, K_A)$
    - preverimo: m = $e(d(m, k_A), K_A)$ = m
    - vsakdo lahko dekriptira sporočilo (in ve, da je prišel od *A*)



Integriteta

- Integriteta uporabnikov in kriptiranje
  - dokazuje, kdo je sporočilo poslal in da ga bere le pravi prejemnik
  - prenos sporočila *m* od uporabnika *A* do uporabnika *B*
    - *A*: $c = e(d(m, k_A), K_B)$
      - A najprej uporabi svoj zasebni ključ k_A, nato še *B*-jev javni ključ K_B
    - *B*: $m = e(d(c, k_B), K_A)$
    - res deluje? preverimo:
      - $m = e(d(e(d(m, k_A), K_B), k_B), K_A)$ torej
      - $m = e(d(m, k_A), K_A)$
      - $m = m$

Integriteta

- Integriteta sporočila
  - dokazuje, da sporočilo ni bilo spremenjeno
  - prenos sporočila *m* od uporabnika *A* do uporabnika *B*
    - *A*: *s = sig(m)*
      - izračunamo podpis *s* sporočila *m*
    - *A*: *cs = d(s, k_A)*
      - *A* uporabi svoj zasebni ključ k_A
    - prenesemo (lahko prej še kriptiramo) *m* in *s*
    - *B*: s = *e(cs, K_A)*
      - *B* uporabi *A*-jev javni ključ, da pridobi *s*
    - B: ali je *s = sig(m)*?