Računalniške komunikacije

2020/21

operativna varnost

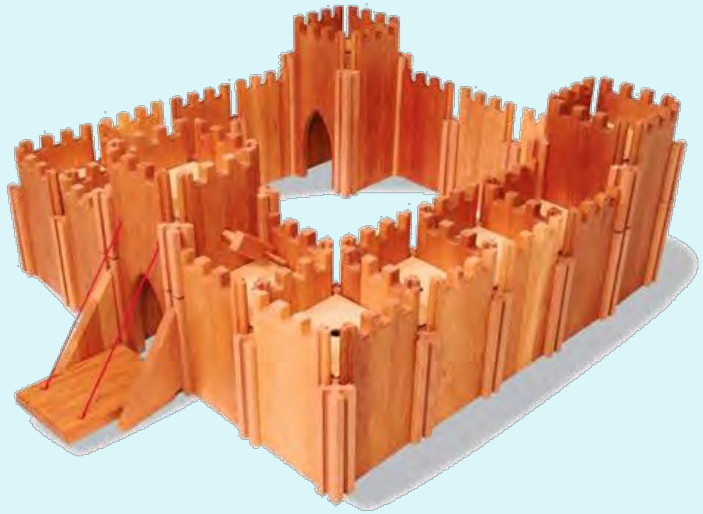
požarni zidovi, zaznavanje vdorov,
napadi in grožnje

Operativna varnost:

požarni zidovi in sistemi za zaznavanje vdorov

Varnost v omrežju

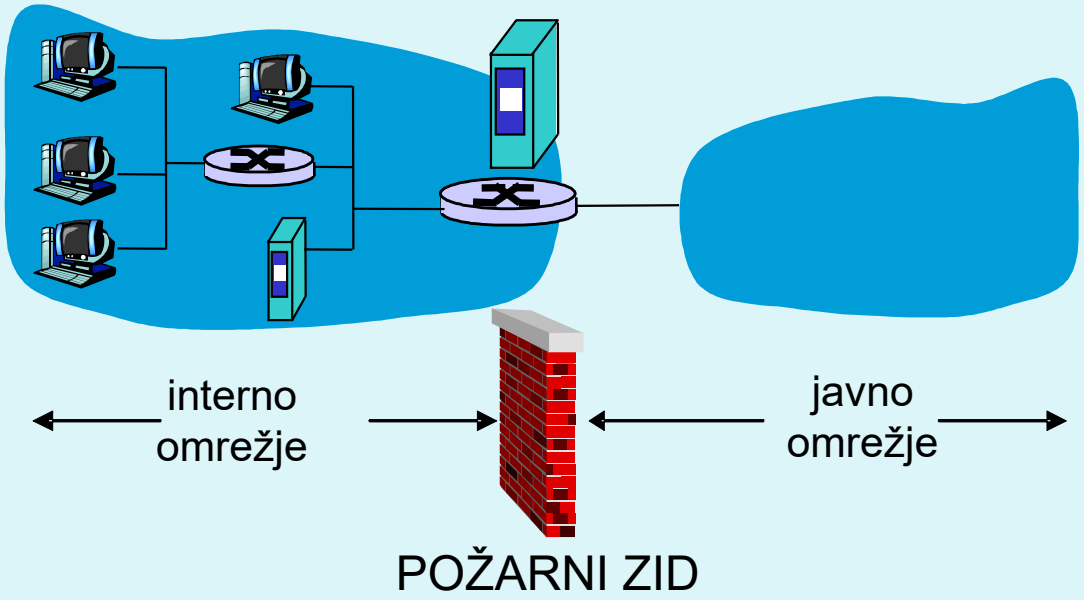
- Administrator omrežja lahko uporabnike deli na:
  - **good guys**: uporabniki, ki legitimno uporabljajo vire omrežja, pripadajo organizaciji,
  - **bad guys**: vsi ostali, njihove dostope moramo skrbno nadzorovati
- Omrežje ima običajno eno samo točko vstopa, kontroliramo dostope v njej:
  - **požarni zid** (firewall)
  - **sistem za zaznavanje vdorov** (*IDS, intrusion detection system*)
  - **sistem za preprečevanje vdorov** (*IPS, intrusion prevention system*)



Požarni zid (firewall)

izolira interno omrežje od velikega javnega omrežja, določenim paketom dovoli prehod, druge blokira. Ima 3 naloge:

- filtrira VES promet,
- prepušča samo promet, ki je DOPUSTEN glede na politiko,
- je IMUN na napade



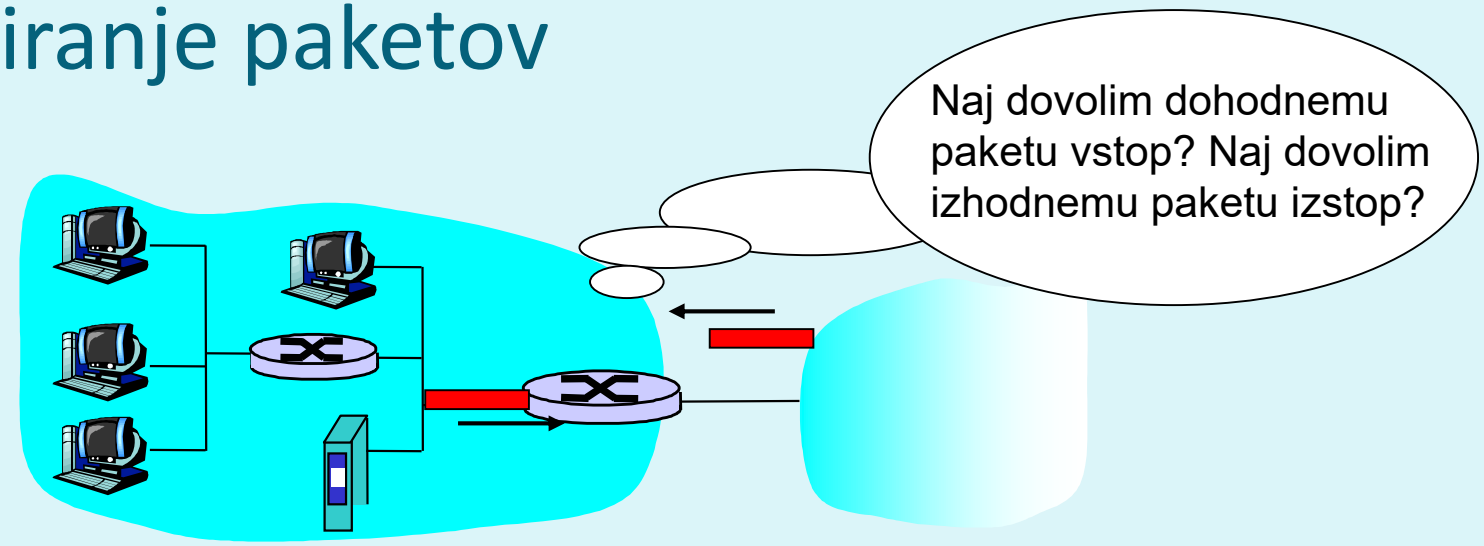
Požarni zid: vrste filtriranj

1. **izolirano filtriranje** paketov (angl. *stateless, traditional*)
   - pretežno filtriranje na podlagi podatkov v glavi: izvorni in ponorni naslovi ter vrata

2. **filtriranje paketov v kontekstu** (angl. *stateful filter*)
   - nadzoruje vzpostavljenost povezave

3. **aplikacijski prehodi** (angl. *application gateways*)
   - filtriranje z vpogledom v podatke aplikacijske plasti (vsebina, aplikacijski protokol, uporabniško ime, …)

Izolirano filtriranje paketov



- filtriranje običajno izvaja že usmerjevalnik, ki meji na javno omrežje. Na podlagi vsebine paketov se odloča, ali bo posredoval **posamezen paket**,
- odločitev na podlagi:
  - IP izvornega/ponornega naslova
  - številke IP protokola: TCP, UDP, ICMP, OSPF itd.
  - TCP/UDP izvornih in ciljnih vrat
  - tip sporočila pri protokolu ICMP
  - zastavice TCP: SYN in ACK bit (sta aktivni za prvi segment pri povezovanju, nadzorujemo dopustnost vzpostavljanja povezave)

Izolirano filtriranje: dostopovni seznami

- dostopovni seznam (angl. access control list, ACL)
- tabela pravil, upošteva (procesira) se jo od vrha proti dnu
- zapisi so par *(pogoj, akcija)*
- primer: onemogoči ves promet razen WWW navzven in DNS v obe smeri

tabelo bere od zgoraj navzdol, prvo pravilo, ki ga najde, uporabi, če pravilo ne ustreza, gre naprej

izvorni naslov	ciljni naslov	protokol	izvorna vrata	ciljna vrata	zastavica	akcija	
222.22/16	izven 222.22/16	TCP	> 1023	80	any	dovoli	dopusti izhodni HTTP
izven 222.22/16	222.22/16	TCP	80	> 1023	ACK	dovoli	dopusti dohodni HTTP
222.22/16	izven 222.22/16	UDP	> 1023	53	---	dovoli	dopusti izhodni DNS
izven 222.22/16	222.22/16	UDP	53	> 1023	----	dovoli	dopusti dohodni DNS
all	all	all	all	all	all	zavrzi	

Filtriranje paketov v kontekstu

- angl. *stateful filter*, upošteva povezavo
  - izolirano filtriranje lahko dovoli vstop nesmiselnim paketom (npr. vrata = 80, ACK =1; čeprav notranji odjemalec ni vzpostavil povezave)

npr. napadalec s trojancem komunicira preko porta 80, čeprav je to samo za HTTP ...
tj. prej bi moral biti request od userja, nato šele reply

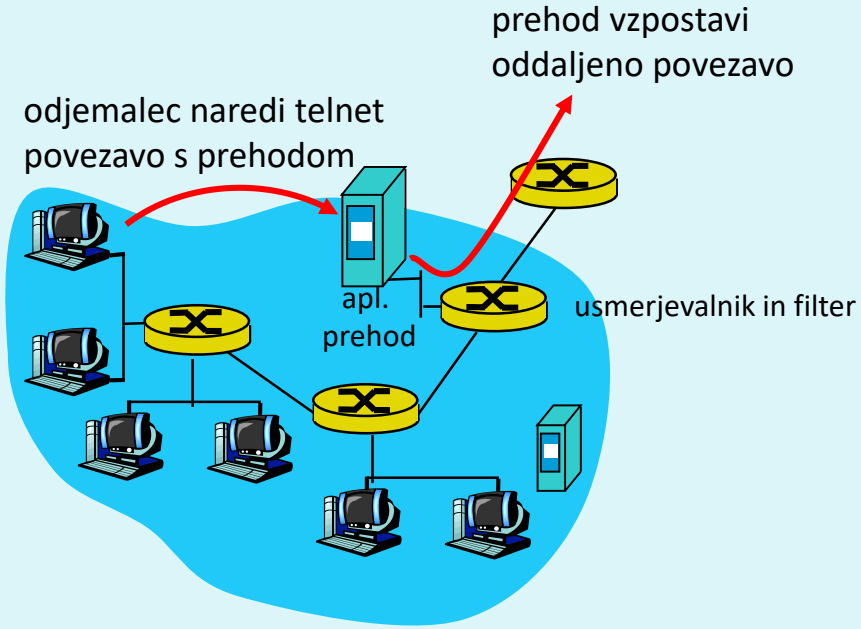
- IZBOLJŠAVA: **filtriranje paketov v kontekstu** spremlja in vodi evidenco o vsaki vzpostavljeni TCP povezavi
  - zabeleži vzpostavitev povezave (SYN) in njen konec (FIN): na tej podlagi odloči, ali so paketi smiselni
  - po preteku določenega časa obravnavaj povezavo kot neveljavno (timeout)
  - uporabljaj podoben dostopovni seznam, ki določa, kdaj je potrebno kontrolirati veljavnost povezave (angl. *check connection*)

Filtriranje paketov v kontekstu

izvorni naslov	ciljni naslov	protokol	izvorna vrata	ciljna vrata	zastavica	akcija	preveri povezavo
222.22/16	izven 222.22/16	TCP	> 1023	80	any	dovoli	
izven 222.22/16	222.22/16	TCP	80	> 1023	ACK	dovoli	X
222.22/16	izven 222.22/16	UDP	> 1023	53	---	dovoli	
izven 222.22/16	222.22/16	UDP	53	> 1023	----	dovoli	X
all	all	all	all	all	all	zavrzi	

Aplikacijski prehodi

- omogočajo dodatno filtriranje glede na izbiro uporabnikov, ki lahko uporabljajo določeno storitev
- omogočajo filtriranje na podlagi podatkov na aplikacijskem nivoju poleg polj IP/TCP/UDP.



1. vsi uporabniki vzpostavljajo povezavo preko prehoda
2. samo za avtorizirane uporabnike prehod vzpostavi povezavo do ciljnega strežnika
3. prehod posreduje podatke med 2 povezavama
4. usmerjevalnik blokira vse povezave razen tistih, ki izvirajo od prehoda

Aplikacijski prehodi

Tudi aplikacijski prehodi imajo omejitve:

- če uporabniki potrebujejo več aplikacij (telnet, HTTP, FTP itd.), potrebuje vsaka aplikacija svoj aplikacijski prehod,
- kliente je potrebno nastaviti, da se znajo povezati s prehodom (npr. IP naslov medstrežnika v brskalniku)

Sistemi za zaznavanje vdorov

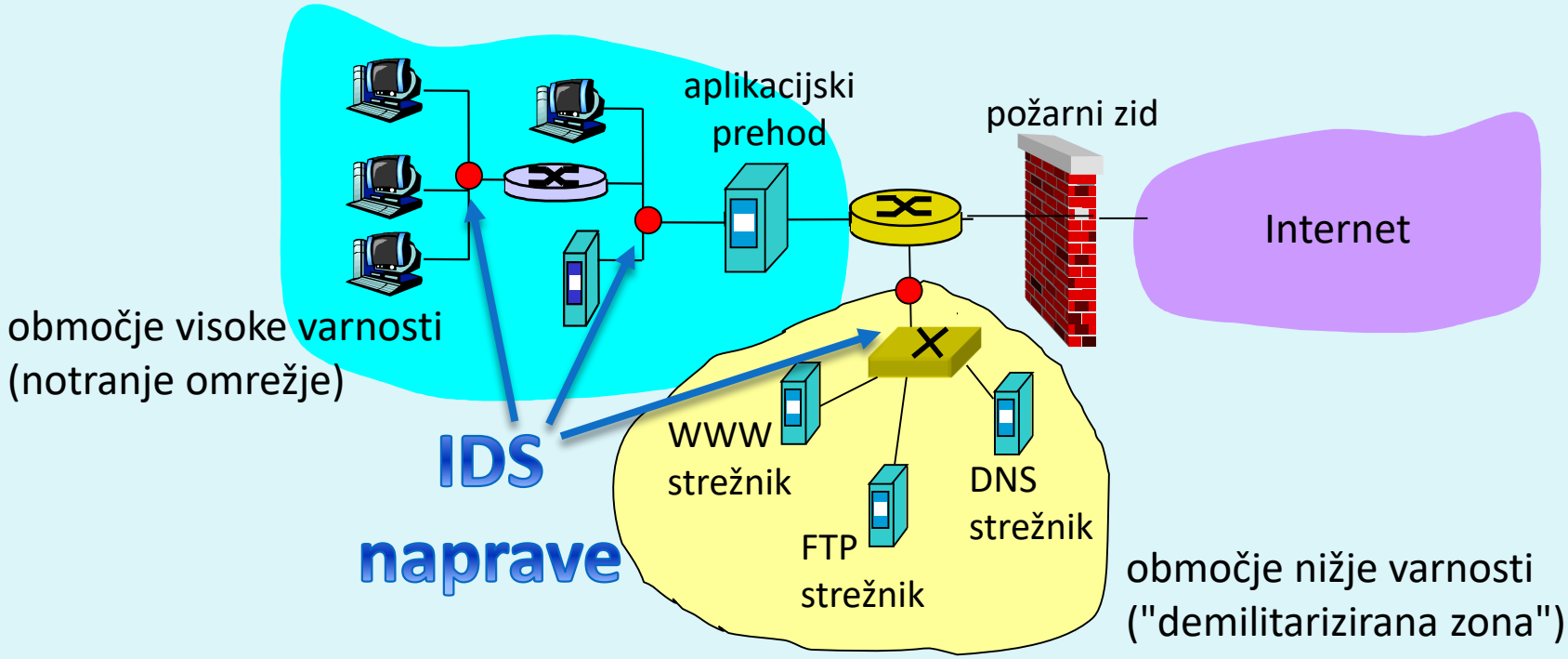
- dodatna naprava - IDS, ki izvaja **poglobljeno analizo paketov**. Na podlagi vstopa sumljivih paketov v omrežje lahko naprava prepreči njihov vstop ali razpošlje obvestila.
  - sistem za zaznavanje vdorov (IDS) pošlje sporočilo o potencialno škodljivem prometu
  - sistem za preprečevanje vdorov (IPS) ukrepa pri pojavitvi sumljivega prometa

  - primeri: Cisco, CheckPoint, Snort IDS

Načini zaznavanja vdorov

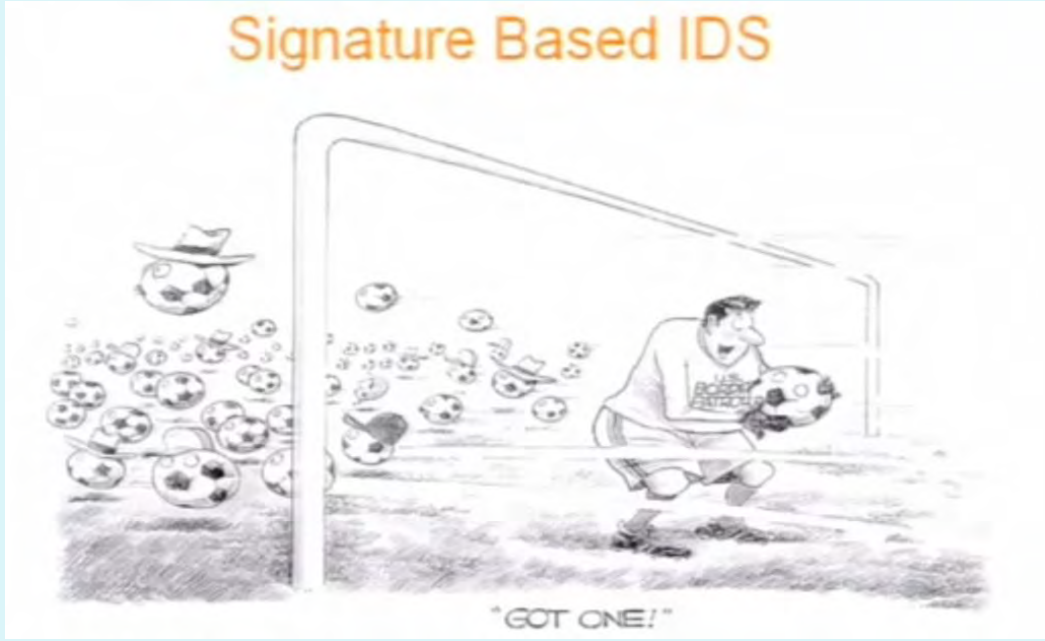
Kako deluje IDS/IPS?

- primerjava s shranjenimi vzorci napadov (angl. **signatures**)
- opazovanje netipičnega prometa (angl. **anomaly-based**)



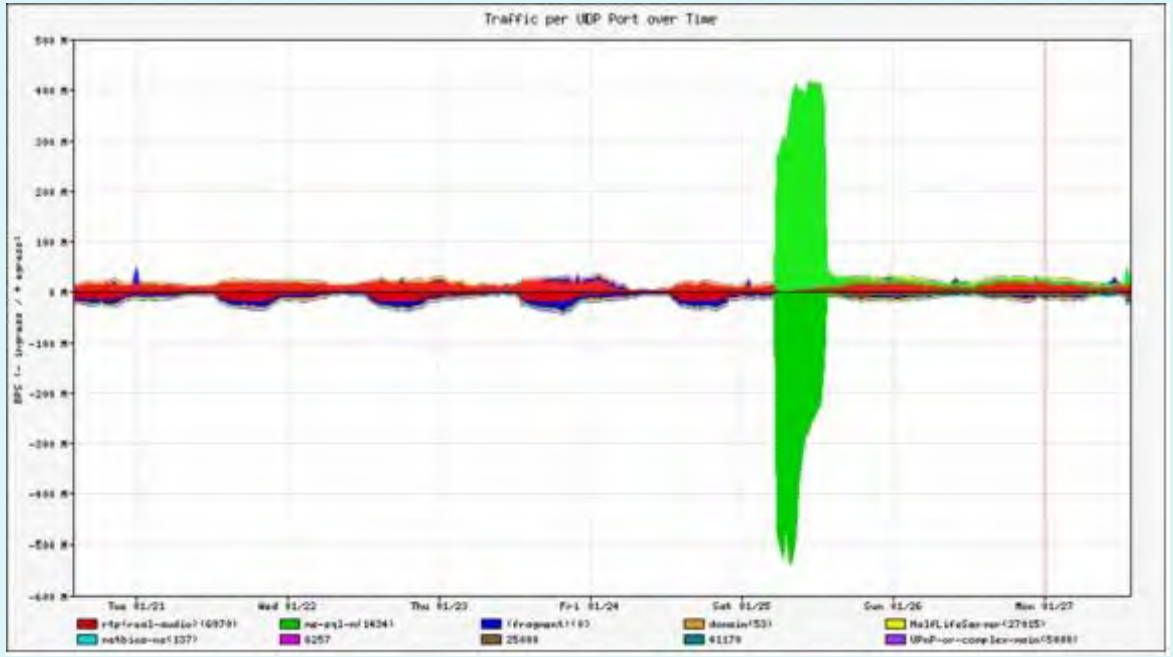
Zaznavanje z vzorci napadov

- vzorci napadov lahko hranijo izvorni IP, ponorni IP, protokol, zaporedje bitov v podatkih paketa, lahko so vezani na serijo paketov
- varnost je torej odvisna od baze znanih vzorcev; IDS/IPS slabo zaznava še nevidene napade
- možni lažni alarmi
- zahtevno procesiranje (lahko spregleda napad)

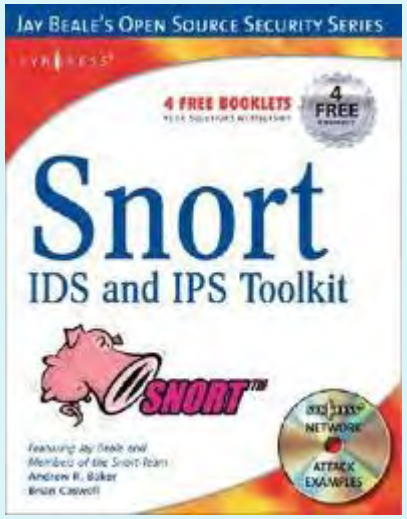


Zaznavanje netipičnega prometa

- sistem opazuje običajen promet in izračuna statistike, vezane nanj
- sistem reagira na statistično neobičajen promet (npr. nenadno velik delež ICMP paketov)
- možno zaznavanje še nevidenih napadov
- težko ločevanje med normalnim in nenavadnim prometom



Primer IDS/IPS sistema



- Snort IDS
  - public-domain, odprtokodni IDS za Linux, UNIX, Windows (uporablja isto knjižnico za branje omrežnega prometa kot Wireshark)
  - primer vzorca napada

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any
(msg:"ICMP PING NMAP"; dsize: 0; itype: 8;)
```

sporočilo za administratorja

prazen paket (dolžina 0) in ICMP tip 8 (=PING) sta lastnosti NMAP napada

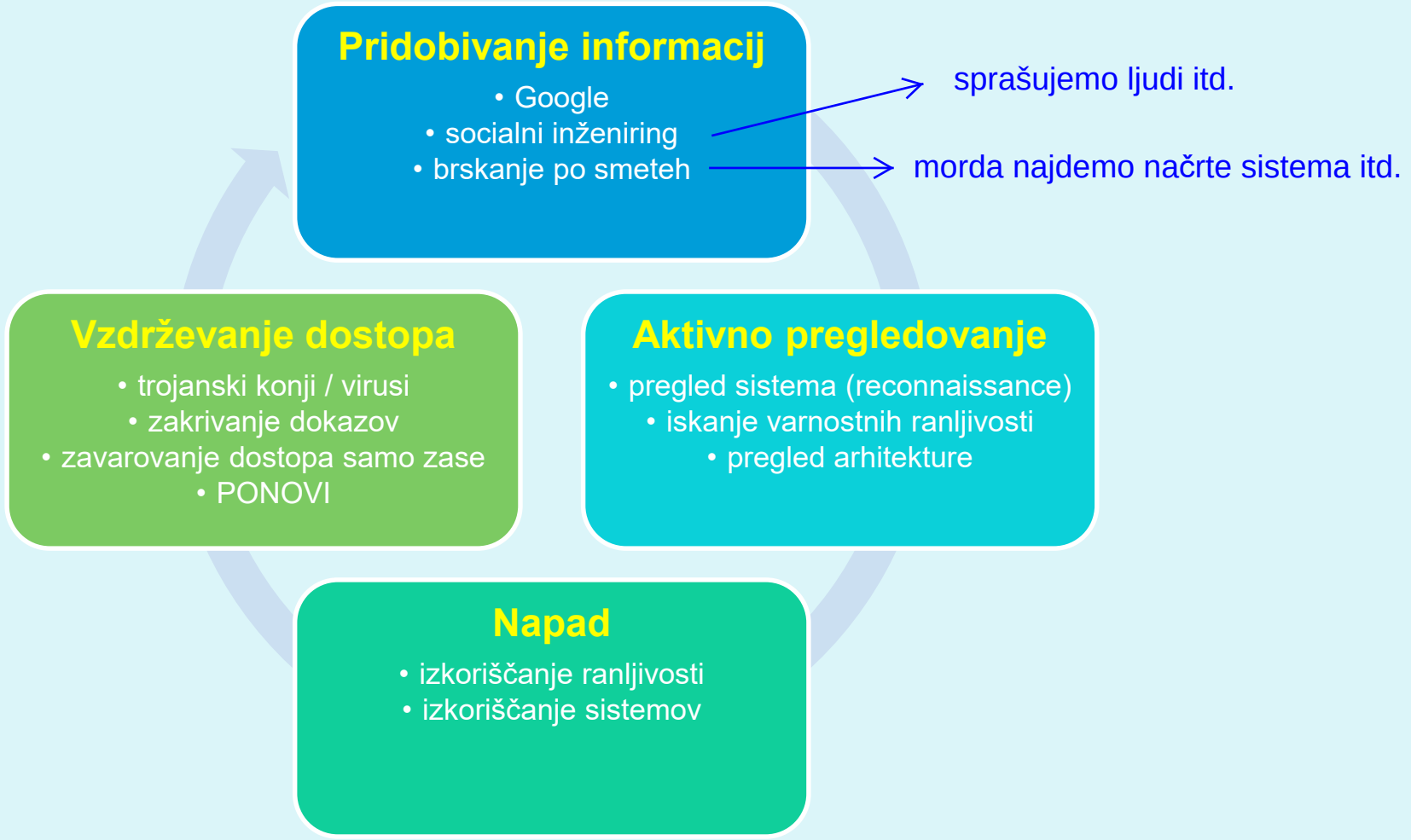
reagiraj na VES DOHODNI ICMP promet

Napadi in grožnje

Pogosti napadi na omrežne sisteme

- **NAMEN?** Namenjeni so škodovanju ali obhodu računalniških in omrežnih funkcij.
- **ZAKAJ?** Denarna dobrobit, škodovalnost, poneverbe, ekonomske dobrobiti, čast in slava?
- **KAKO?** Ogrožanje zaupnosti, integritete in razpoložljivosti omrežnih sistemov
  - napadi s spreminjanjem informacij (*modification attack*)
  - zanikanje komunikacije (*repudiation attack*)
  - odpoved delovanja sistema (*denial-of-service attack*)
  - nepooblaščen dostop (*access attack*)
  - …

Pogosti napadi na omrežne sisteme



Pogosti napadi

1. **prisluškovanje in ponarejanje sporočil**
2. **matematični napadi** na kriptografske algoritme in ključe
3. **ugibanje gesel** (brute force, napad s slovarjem)
4. **virusi, črvi, trojanci**
5. **izkoriščanje šibkosti v programski opremi**
6. **socialni inženiring** (preko e-maila, telefona, servisov)


THE NEW PAPER/Wednesday, October 6, 2004

SINGA

Hacker's polite approach works like a charm

BY ARUL JOHN

reveal computer system passwords during happy hours.

Last year, he said computer fraud.

Pogosti napadi

7. **pregled vrat** *(port scan)*: napadalec testira, kateri strežniki so delujoči (npr. ping) in katere storitve ponujajo. Napadalec lahko pridobiva podatke o sistemu: DNS, storitve, operacijski sistemi)

8. **brskanje po smeteh** *(dumpster diving)*: način, s katerim lahko napadalci pridejo do informacij o sistemu (navodil za uporabo, seznamov gesel, telefonskih številk, opisa organizacije dela)

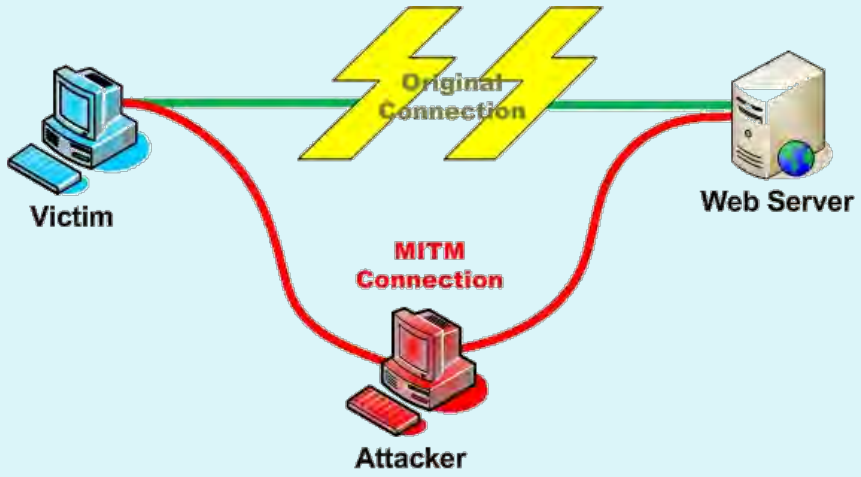
9. **rojstnodnevni napad** *(birthday attack)*: je napad na zgoščevalne funkcije, za katere zahtevamo, da nobeni dve sporočili ne generirata iste zgoščene vrednosti. Pri slabših funkcijah napadalec išče sporočilo, ki bo dalo isto zgoščeno vrednost.

Pogosti napadi

10. **zadnja vrata** (*back door*): napadalec zaobide varnostne kontrole in dostopi do sistema preko druge poti,

11. **ponarejanje IP naslovov** (*IP spoofing*): napadalec prepriča ciljni sistem, da je nekdo drug (poznan) s spreminjanjem paketov,

12. **prestreganje komunikacije** (*man-in-the-middle*): napadalec prestreže komunikacijo in se obnaša, kot da je ciljni sistem (pri uporabi certifikatov lahko žrtev uporablja tudi javni ključ napadalca)



Pogosti napadi

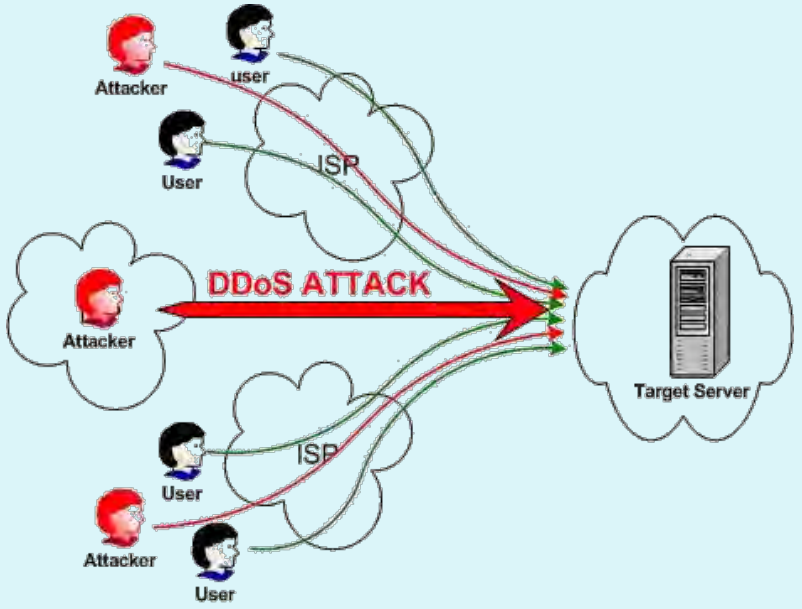
13. **ponovitev komunikacije** (*replay*): napadalec prestreže in shrani stara sporočila ter jih ponovno pošlje kasneje, predstavljajoč se kot eden izmed udeležencev
    - kako preprečimo napade s ponovitvijo komunikacije?

14. **ugrabitev TCP sej** (*TCP hijacking*): napadalec prekine komunikacijo med uporabnikoma in se vrine v mesto enega od njiju; drugi verjame, da še vedno komunicira s prvim
    - kaj napadalec pridobi s tem?

15. **napadi s fragmentacijo** (*fragmentation attack*): z razbijanjem paketa na fragmente razdelimo glavo paketa med fragmente tako, da jih požarni zid ne more filtrirati
    - tiny fragment attack: deli glavo prvega paketa
    - overlapping fragment attack: napačen offset prepiše prejšnje pakete

Napadi DoS (1/5)

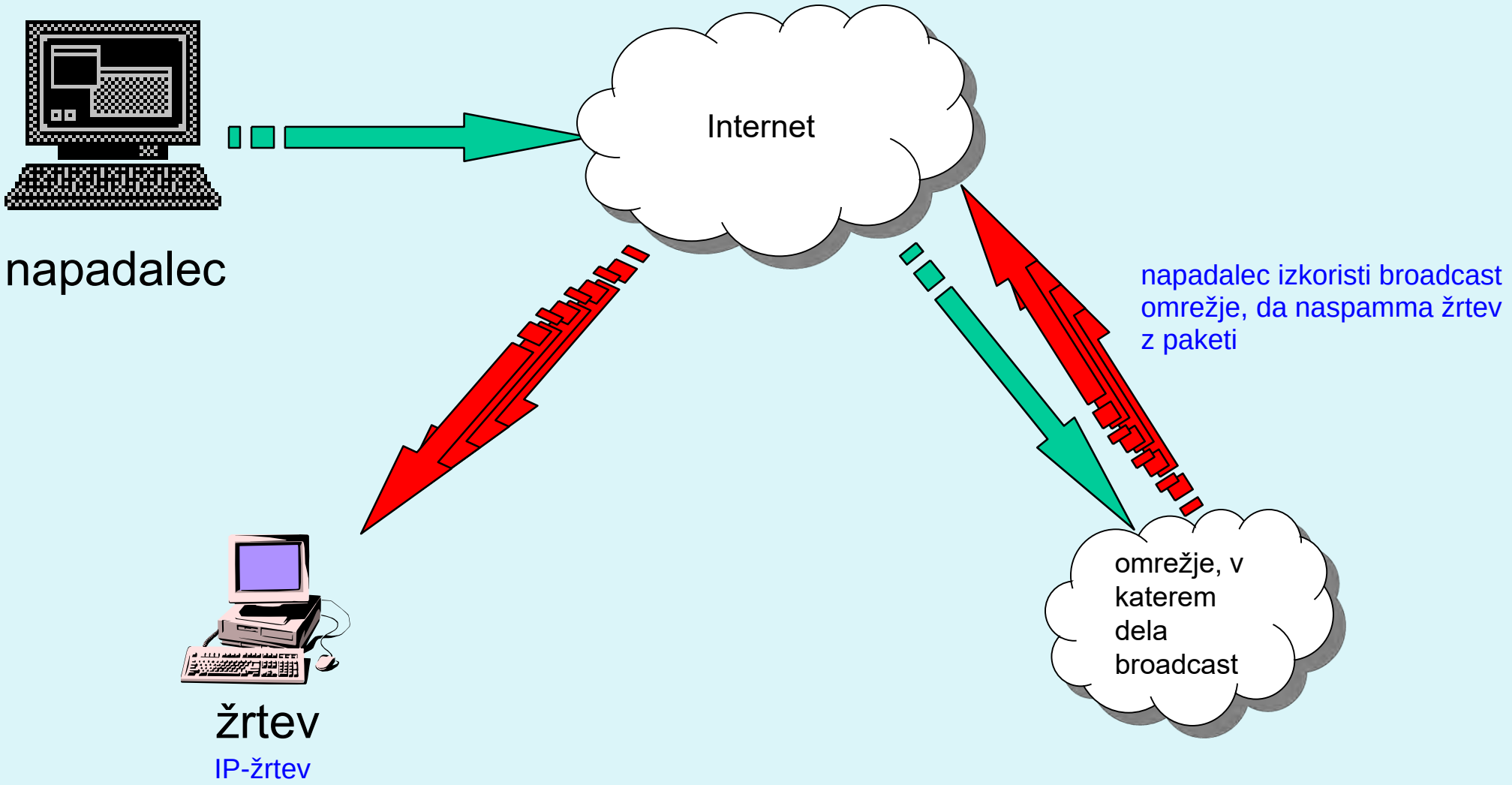
16. **odpoved delovanja sistema** (*Denial-of-Service)*
    - cilj napadalca: obremeni omrežne vire tako, da se nehajo odzivati zahtevam regularnih uporabnikov (npr. vzpostavitev velikega števila povezav, zasedanje diskovnih kapacitet, ...)
    - lahko je porazdeljen (distributed DOS = DDoS)



Napadi DoS (2/5)

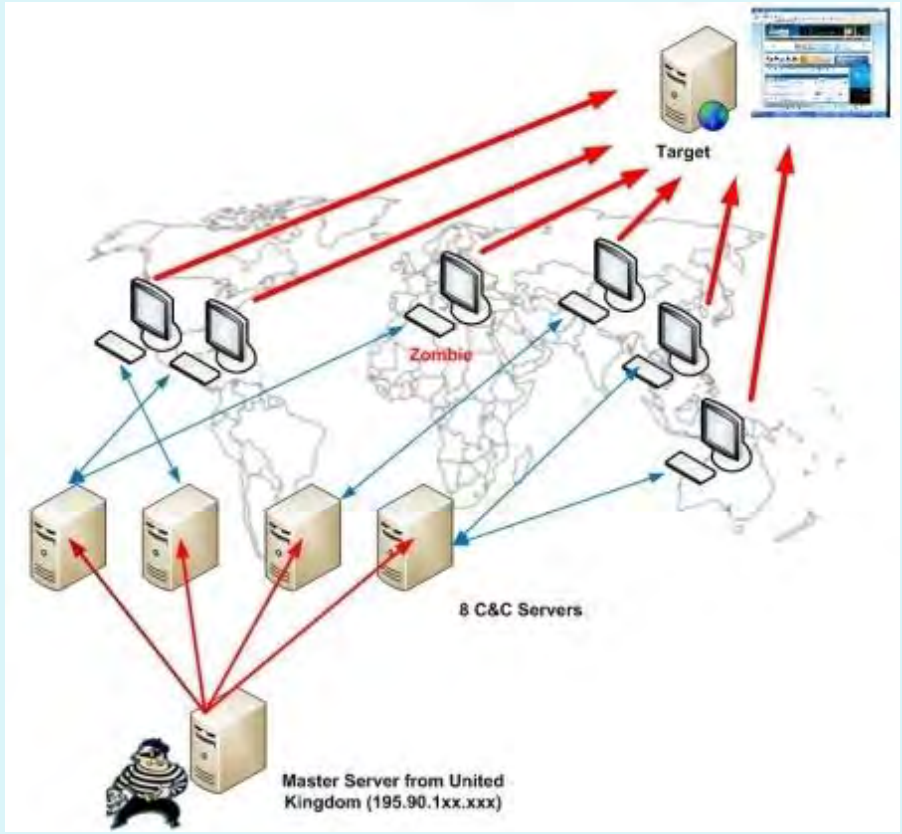
- primeri:
  - **prekoračitev medpomnilnika** (*buffer overflow*): procesu pošljemo več podatkov, kot jih lahko sprejme (Ping of death: ICMP z več kot 65K podatkov je povzročil sesutje sistema)
  - **SYN napad**: napadalec pošlje veliko število zahtev za vzpostavitev povezave in se na odgovor sistema ne odzove; pride do preobremenitve vrste zahtev v sistemu
    - rešitev: omejitev števila odprtih povezav, timeout
  - **napad Teardrop**: napadalec spremeni podatke o številu in dolžini fragmentov v IP paketu, kar zmede prejemnika
  - **napad Smurf** (naslednja prosojnica): uporaba posrednega broadcasta za preobremenitev sistema
    - porazdeljen DDoS
    - uporabniki porazdeljenih omrežnih sistemov lahko da ne vejo, da je napadalna oprema nameščena pri njih

DoS Smurf (3/5)


napadalec
Internet
napadalec izkoristi broadcast omrežje, da naspamma žrtev z paketi
omrežje, v katerem dela broadcast
žrtev
IP-žrtev

Napadi DoS (4/5)

- Uporaba *bot*-ov (*web roBOT*) za organizacijo napadov na ciljni sistem
  - boti so lahko računalniki, okuženi s trojanskimi konji
  - njihovi uporabniki običajno ne vejo, da sodelujejo v napadu



Napadi DoS (5/5)

- subjekti v napadu: **napadalec**, centralni računalnik za **krmiljenje botov** (*herder*), **boti** (zombie), **cilj**