

## RK 2. kolokvij 2. 6. 2010

- 1) TCP oddajnik s širino okna 4000 bytov odda segmente z zaporednimi številkami 3000, 4000, 5000 in 6000. Nato sprejme potrditev ACK 6000. Katere od naslednjih trditev so resnične in katere ne? Vse odgovore utemeljite!

- Vsi oddani paketi so sedaj potrjeni.
- Po prejemu naslednje potrditve (ACK 7000) se bo zamašitveno okno povečalo.
- Max. velikost segmenta je najverjetneje 1000 bytov.
- Če bo naslednja potrditev ACK 6000, pomeni da prejemnik dobil segment 6000 podvojen.
- Če bo naslednja potrditev ACK 6000, pomeni da je bilo s segmentom 6000 najbrž nekaj narobe.
- Če bo naslednja potrditev imela vrednost Receive window nastavljeno na več kot 1000, lahko oddamo naslednji segment.
- Če bo namesto naslednje potrditve zazvonil alarm časovne kontrole za segment 6000, je to lažni alarm in segmenta ni treba ponovno oddati, saj smo že 2x dobili njegovo potrditev.

- 2) Navedite naloge transportne plasti in en standardni protokol transportne plasti. Na transportni plasti se med transportnima entitetama vzpostavi:

- fizična povezava
- logična povezava
- virtualna zveza
- aplikacijska povezava

- 3) Navedite 3 od petih metod, ki jih uporabljamo v http zahtevi po http 1.1, ter pojasnite njihovo uporabo.

- 4) Hash funkcije

- Kaj je hash funkcija?
- Navedite tri lastnosti dobre hash funkcije.
- Navedite dva hash algoritma.
- Kje se uporablja na področju varnosti (zadošča en primer)?
- Kaj je rojstnodnevni napad (navedite le namen napada, ne mehanizma izvedbe)?

- 5) Elektronski podpis

- Kaj je elektronski podpis in kako ga izvedemo s pomočjo kriptografije? Opišite le osnovno različico brez centralne avtoritete in navedite tudi slabosti takega načina podpisovanja.
- Ali vidite kako možnost napada na opisani mehanizem?
- Je podpisano besedilo je varno pred napadalčevimi očmi?

- 6) Needham- Schroeder:

- Za kakšen namen in v kakšnih sistemih se uporablja Needham-Schroeder-jev protokol?
- Ali uporablja simetrično ali asimetrično kriptografijo?
- Za kateri napad je občutljiv (kratak oris izvedbe napada)?

- 7) Brskalnik prenaša s spletnega strežnika html datoteko, ki vključuje še tri majhne objekte, npr. jpeg sličice.

Čas vrnitve (RTT) naj bo  $r$ , časi prenosa datotek pa naj bodo kar vsi enaki in sicer  $t$ . Predpostavimo, da na omrežju ni zamašitev. Koliko http zahtev je potrebnih? Koliko časa preteče, da brskalnik dobi vse objekte, če

- Uporablja ne-trajne povezave in vzporedne prenose po več TCP povezavah?
- Uporablja ne-trajne povezave brez vzporednih prenosov?
- Uporablja trajne povezave, okno je ob vzpostavitvi povezave enako 1 in se povečuje v skladu s pravili delovanja TCP?

- 8) S programom Wireshark smo zajeli spodnjo sejo SMTP:

```
220 ns.fri.uni-lj.si ESMTP Postfix (Debian/GNU)
EHLO fri.uni-lj.si
```

```
250-ns.fri.uni-lj.si
250-PIPELINING
250-SIZE 60000000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM: <mojca.cigliaric@fri.uni-lj.si>
250 2.1.0 Ok
RCPT TO: <andrej.krevl@fri.uni-lj.si>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: Janez Novak <janez@example.com>
To: Andrej Krevl <andrej.krevl@fri.uni-lj.si>
Subject: Domaca naloga
```

Zal nisem uspel narediti domace naloge.

Lp, Janez

250 2.0.0 Ok: queued as 6FAE48322

- Kaj bo kot pošiljatelj sporočila prikazal prejemnikov odjemalec za e-pošto (npr. Thunderbird)?
- Kako se lahko zavarujemo pred poneverjanjem pošiljatelja?
- Vidimo, da protokol SMTP prenaša podatke kot golo besedilo. Kaj lahko storimo, da naši podatki ne bodo vidni morebitnim prisluškovalcem na omrežju?

- 9) S programom Wireshark smo zajeli spodnji promet:

Št	Čas	Izvorni IP	Ponorni IP	Info
71	53.256762	212.235.189.155	193.2.1.66	DNS Standard query A www.fri.uni-lj.si
72	53.259022	193.2.1.66	212.235.189.155	DNS Standard query response A 212.235.188.25
97	69.926157	212.235.189.155	193.2.1.66	DNS Standard query MX fri.uni-lj.si
98	69.929198	193.2.1.66	212.235.189.155	DNS Standard query response MX 10 ns.fri.uni-lj.si
117	85.699318	212.235.189.155	193.2.1.66	DNS Standard query PTR 158.189.235.212.in-addr.arpa
118	85.702795	193.2.1.66	212.235.189.155	DNS Standard query response PTR marvin.fri.uni-lj.si

- Za kateri protokol gre?
- Strežnik sprašujemo po 3 različnih tipih zapisih v tem protokolu. Po katerih treh?
- Čemu so namenjeni zapisi PTR (po takšnem zapisu sprašuje paket št. 117)?

- 10) S programom Wireshark smo zajeli spodnjo zahtevo in odgovor HTTP:

```
GET / HTTP/1.1
Host: marvin.fri.uni-lj.si
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.3)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
If-Modified-Since: Fri, 20 Feb 2009 14:41:51 GMT
If-None-Match: "076195e6993c91:ae8"
Cache-Control: max-age=0
```

```
HTTP/1.1 304 Not Modified
Content-Location: http://marvin.fri.uni-lj.si/Default.htm
Last-Modified: Fri, 20 Feb 2009 14:41:51 GMT
Accept-Ranges: bytes
ETag: "076195e6993c91:ae8"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Wed, 02 Jun 2010 08:15:28 GMT
```

- Zahtevo smo zajeli pri dostopu do spletnega naslova <http://marvin.fri.uni-lj.si>. Zakaj nam strežnik odgovori s takšnim odgovorom namesto s spletno stranjo (navedite tudi ustrezne vrstice zahteve, ki so »krivi« za to)?
- Kakšno programsko opremo (spletni strežnik) uporablja marvin.fri.uni-lj.si? Kje lahko to preberemo?