RAČUNALNIŠKE KOMUNIKACIJE 2017/18

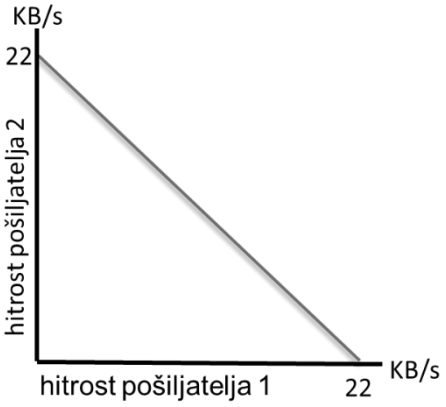
2. kolokvij, 4. 6. 2018

Literatura (prosojnice, knjige, zapiski, elektronski pripomočki) ni dovoljena. Dovoljen je 1 A4 list s poljubno vsebino.
Podpišite se na vse liste, ki jih oddate.
Na vprašanja odgovarjajte kratko (največ 2 povedi), daljši odgovori štejejo 0 točk.
Čas pisanja je 70 minut.

1. NALOGA (20t):

Dva pošiljatelja, ki uporabljata protokol TCP, si delita komunikacijski kanal. Oba uporabljata velikost segmentov MSS = 600 B in skupno povezavo s kapaciteto 22 KB/s. Na začetku opazovanja (t=0) ima prvi pošiljatelj hitrost 2400B/s, drugi pa 600 B/s. Predpostavi, da oba pošiljatelja uporabljata *TCP Tahoe* s fiksno velikostjo praga pri 16 MSS. Naloge:

a) Na graf (podoben tistemu na desni, na katerem smo na predavanjih prikazovali pravičnost protokola TCP) vriši točke, ki predstavljajo hitrosti obeh pošiljateljev v naslednjih 10 časovnih enotah (sekundah). Vseh 10 koordinat označi (ali zapiši poleg grafa).
b) Koliko podatkov se prenese v prvih 10 časovnih enotah?
c) Po koliko časovnih enotah se doseže pravična delitev kanala?



2. NALOGA (20t):

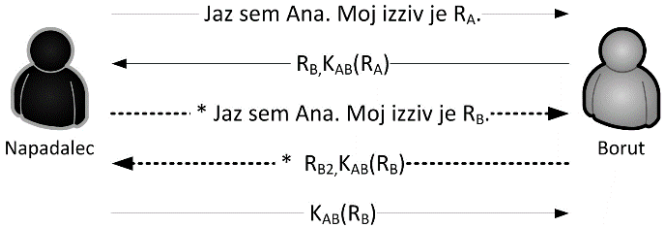
Pošiljatelj A prične s postopkom trosmernega rokovanja (TCP) z B, pri katerem se izmenja naslednje zaporedje paketov: A→B: [SYN, SEQ=42], B→A: [SYN ACK=43 SEQ=24 RWND=10200], A→B: [ACK=25 RWND=32000]. Po rokovanju si A in B začneta izmenjevati podatke. V vsaki časovni enoti pošiljatelj A prejme od B 200 B podatkov, uspe pa jih obdelati le 180 B. Podobno, v vsaki časovni enoti pošiljatelj B prejme od A 450 B podatkov, obdela pa jih 410 B. Odgovori na vprašanja:

a) V katerih časovnih enotah se zapolni sprejemno okno pošiljateljev A in B?
b) Koliko podatkov prejmeta A in B do časa zapolnitve njunih sprejemnih oken?
c) Kaj se zgodi s sprejemom novih paketov, če se sprejemno okno napolni? Ali bo pošiljatelj izvajal ponovno pošiljanje nepotrjenih paketov? Če da, kako bi to ponovno pošiljanje vplivalo na izkoriščenost komunikacijske povezave in dolžine čakalnih vrst?
d) Kaj se zgodi s paketi iz čakalne vrste ob (rednem) praznjenju sprejemnega okna?

3. NALOGA (20t):

Ana in Borut se želita vzajemno avtenticirati s postopkom izziv-odgovor in z uporabo simetrične kriptografije s ključem K_{AB}. Med njiju se vrine napadalec, ki namesto Ane z Borutom izvede komunikacijo, ki je prikazana na desni sliki (različne oblike puščic ponazarjajo dve ločeni seji). Odgovori na naslednja vprašanja:

a) V eni povedi povzemi, kaj naredi napadalec (ne na način ubesedovanja že napisane vsebine na sliki, temveč s povzemanjem napadalčevega pristopa).
b) Premisli in predlagaj dva načina, kako bi se lahko s spremembo postopka izziv-odgovor izognili zgornjemu napadu.



c) Ali lahko težavo odpravimo s požarnim zidom ali sistemom za zaznavanje vdorov? Če da, s katerim in kako?
d) Ali bi bil zgornji napad izvedljiv, če bi uporabljali kriptografijo z javnimi ključi? Odgovor pojasni v največ 2 povedih.

4. NALOGA (20t):

Nariši končni avtomat (podoben, kot smo jih risali za snovanje protokola TCP), ki prikazuje delo SMTP strežnika. Strežnik naj ne uporablja avtentikacije in kriptiranja povezave. Stanja diagrama smiselno določi in poimenuj sam-a. Pogoje za prehode med stanji naj predstavljajo prejeti ukazi s strani klienta. V diagramu tudi smiselno upoštevaj prehode, ki so posledica napačnih ali sintaktično nepravilnih ukazov in drugih napak.

5. NALOGA (20t):

Zajeli smo naslednja dva paketa (vrstni red je pomešan/naključen):

Frame a: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
Ethernet II, Src: Hewlett-_93:a9:35 Dst: Apple_02:2f:60
Internet Protocol Version 4, Src: 212.235.188.194 Dst: 212.235.188.235
User Datagram Protocol, Src Port: 53 (53), Dst Port: 55291 (55291)
Domain Name System (response)
  Transaction ID: 0x0456
  Flags: 0x8180 Standard query response, No error
    1... .... = Response: Message is a response
    .000 0... .... = Opcode: Standard query (0)
    .... .0.. .... = Authoritative:
    .... ..0. .... = Truncated: Message is not truncated
    ....1 .... = Recursion desired:
    .... 1... .... = Recursion available:
    .... .0.. .... = Z: reserved (0)
    ....0. .... = Answer authenticated:
    ....0 .... = Non-authenticated data: Unacceptable
    .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  Queries
    a.root-servers.net: type A, class IN
      Name: a.root-servers.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  Answers
    a.root-servers.net: type A, class IN, addr 198.41.0.4
      Name: a.root-servers.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 82806
      Data length: 4
      Address: 198.41.0.4 (198.41.0.4)

Frame b: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: Apple_02:2f:60, Dst: Hewlett-_93:a9:35
Internet Protocol Version 4, Src: 212.235.188.235, Dst: 212.235.188.194
User Datagram Protocol, Src Port: 55291 (55291), Dst Port: 53 (53)
Domain Name System (query)
Transaction ID: 0x0456
  Flags: 0x0100 Standard query
    0... .... = Response: Message is a query
    .000 0... .... = Opcode: Standard query (0)
    .... ..0. .... = Truncated: Message is not truncated
    ....1 .... = Recursion desired: Do query recursively
    .... .0.. .... = Z: reserved (0)
    ....0 .... = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    a.root-servers.net: type A, class IN
      Name: a.root-servers.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)

a) Kateri protokoli so bili uporabljeni in na kateri plasti delujejo?
b) Kateri paket je zahtevek, kateri odgovor?
c) Po čemu smo spraševali in zakaj oz. v katerem primeru ta podatek potrebujemo?
d) Kakšnega tipa so bile poizvedbe in kje se to vidi v analizi paketa? Bodi natančen.
e) Za protokol v teh paketih, ki je najbližje aplikacijski plasti, se v zadnjem času pojavljajo predlogi, da bi ga namesto z zgoraj uporabljanim protokolom uporabljali preko HTTPS (npr. predloga podjetij Google in Cloudflare). Naštej in zelo na kratko analiziraj prednosti in slabosti take izvedbe protokola za:
    1. zakasnitev delovanja (RTT),
    2. potrebno in porabljeno pasovno širino,
    3. varnost pred napadom MITM ("man in the middle"),
    4. vpogled podjetja, ki upravlja strežnik, v zasebnost uporabniških poizvedb.