Komunikacijski protokoli in omrežna varnost
2010/11
Pisni izpit

Izpit morate pisati posamič. Pri reševanju je literatura dovoljena.

Če boste uspešno vsaj delno odgovorili na vsa vprašanja, bo možno dobiti dodatne točke.

Čas pisanja izpita je 90 minut.

Veliko uspeha!

NALOGA	TOČK	OD TOČK	NALOGA	TOČK	OD TOČK
1			4		
2			5		
3			6		

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga: Čeprav so posamezna vprašanja morda malce bolj vezana na določeno poglavje predavanj, je za reševanje vprašanja pogosto potrebno uporabiti znanje še iz drugih poglavij.

VPRAŠANJA:

1. Za protokole smo dejali, da morajo biti dovolj prožni, da omogočajo razširitve. Opišite, kako lahko (kot uporabniki) razširjamo: bootp, DHCP in RADIUS.

2. SNMP protokol je primer protokola za upravljanje z omrežji. Eno od pomembnejših upravljanj v omrežjih je upravljanje z napakami. Na kakšen način s protokolom SNMP upravljamo z napakami?

3. Peter Zmeda sporoča svoji prijateljici Ani, da je IP naslov njegovega računalnika 173.236.190.252. Zapišite ta podatek v TLV (*Type, Length, Value*(zapisu.

4. Ano seveda zanima, kaj več o skrivnostnem Petrovem IP naslovu. (i) kako lahko izve, kako je „ime“ Petrovemu strežniku; (ii) ali lahko izve še to, kje je ta strežnik (utemeljite odgovor)?

2. naloga: Promet za aplikacije v stvarnem času.

VPRAŠANJA:

1. Na predavanjih smo govorili precej o količini podatkov, ki jo moramo prenesti pri prenosu filma in zvoka. Upoštevajmo, da vsak vzorec zvoka 20 bitov. Koliko bitov na sekundo moramo prenesti, da bo ustrezalo človeškemu sluhu? Pri tem predpostavimo, da ne uporabimo nobenega kodiranja oziroma stiskanja. Opišite račun in uporabljene predpostavke.

2. Sedaj naredimo podoben izračun za prenos filma. V tem primeru predpostavimo, da vsako prenešeno piko (*pixel*) popišemo v RGB formatu (*red-green-blue*), pri čemer je vsaka od barv popisana s po 8 biti. Koliko bitov na sekundo moramo prenesti tokrat? Ponovno predpostavimo, da ne uporabimo nobenega kodiranja oziroma stiskanja. Opišite račun in uporabljene predpostavke.

3. Komentirjte velikost opisa enega vzorca (opis ene sličice z vsemi pikami) v primerjavi z velikostjo UDP oziroma IP paketa, ki ga prenašamo preko IEEE 802 ethernet okvirja.

3. naloga: AAA.

VPRAŠANJA:

1. Glej ga Petra Zmedo, spet je nekaj pogruntal. Ugotovil je, da je avtentikacijski strežniški program CHAP proizvajalca JCN napisan tako, da uporablja svoj generator naključnih števil, ki je naslednja deterministična funkcija:

   ```
   Init()::
     seed:= 110121;
   Random()::
     seed:= (seed * 65539) mod 2**(31);
     return seed,
   ```

   Dejansko je funkcija opisana v knjigi *The Art of Computer Programming* in tam dokazana, da je dobra.[1] Tako generirana naključna števila uporablja strežniški program protokola CHAP za generiranje izzivov. Kako naj Peter izvede napad s ponavljanjem na avtentikacijo?

   NAMIG: Peter lahko vedno ugasne JNC strežnik ter ga ponovno prižge.

2. Na predavanjih smo zapisali vsebino PPP okvirja in vsebino IEEE 802 okvirja. Zapišite za vsakega od okvirjev polja, ki jih vsebujeta, ter primerjajte posamezna polja v obeh okvirjih. Katera polja so prisotna v obeh okvirjih in katera ne? Obrazložite oba odgovora.

4. naloga: Varnostni elementi omrežij in razpošiljanje.

VPRAŠANJA:

1. Kaj je to SA (*security association*):
   - Kakšna je funkcija (vloga) SA?
   - Koga združuje?
   - Naštejte polja, ki jih vsebuje ter zakaj potrebujemo ta polja?

2. Tokrat bi se Peter rad pogovarjal s prijateljico Ano preko medmrežja (Internet) in pri tem uporabljal VoIP. Poleg tega ne želi, da bi lahko kdorkoli prisluškoval pogovoru – se pravi, prestrezal pakete in jih „poslušal“. Naštejte vsaj tri načine, kako se lahko pred prisluškovanjem zaščiti ter za vsak način napišite prednost, ki jo ima pred drugima dvema.

[1] Znak `**` pomeni eksponent.

3. Ana pa ni edina, s katero se Peter pogovarja. Peter in Ana sta namreč učitelja v srednji šoli. S kolegicami in kolegi uporabljajo sodobno tehnologijo VoIP, da se dva dni pred šolsko nalogo od 3h do 7h popoldne dogovorijo o vprašanjih. Kako naj zaščitijo svojo komunikacijo?[2]

   Pri odgovoru upoštevajte: (i) število kolegic in kolegov je lahko veliko; in (ii) nove kolegice ali kolegi se lahko prijavijo oziroma odjavijo.

   NAMIG: Upoštevajte, da morate zaščititi ne samo sam pogovor, ampak tudi vključitev v pogovor. Uporabite znanje iz poglavij o prometu v realnem času, o razpošiljanju in o varnosti.

5. naloga: Podatki za delovanje omrežja.

VPRAŠANJA:

1. Ko govorimo o LDAP, kaj je pravzaprav to: kos programske opreme, opis podatkov, ki jih odjemalec lahko pridobi, protokol ali nekaj tretjega? Utemeljite odgovor.

2. Na predavanjih smo omenili, da obstajata dve inačici LDAP: v2 in v3. Zapišite in opišite vsaj dve podrobnosti, v katerih se razlikujeta.

3. Med odjemalcem in strežnikom se pri LDAP vzpostavi seja. Med drugim sta ukaza, ki jih seja pozna, `bind` in `unbind`. Ali v seji oba ukaza vedno nastopata? Utemeljite odgovor – morda najbolje z opisom primera.

6. naloga: Družina IEEE 802.

VPRAŠANJA:

1. Peter je včasih neizmeren vir idej. Tokrat se je odločil, da bo spremenil protokol IEEE 802.1x tako, da bo dovolil uporabo enkratnega gesla (*one-time password*). Kaj mora narediti, da bo to delovalo. Za več točk dodajte podrobnosti, kaj je potrebno spremeniti, dopolniti, parametrizirati v uporabljenih protokolih.

2. Pri protokolu RADIUS smo omenili, da so trije udeleženci. (i) Kateri trije so ti udeleženci, (ii) kakšna je vloga vsakega od njih v protokolu RADIUS ter (iii) kje se nahajajo pri protokolu IEEE 802.1x, konkretno pri EDUROAM (t.j., kako se natančno uporablja RADIUS v protokolu IEEE 802.1x)?

   NAMIG: Ali je morda kakšen od „udeležencev“ sestavljen iz večih dejanskih strežnikov? Preverite natančno RADIUS protokol.

[2] Ne skrbite, dijaki vseeno niso tako iznajdljivi, da bi se lotili Hiperbole kot v filmu Vesna.