# Komunikacijski protokoli in omrežna varnost
# 2011/12
# Drugi kolokvij

Kolokvij 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 50 minut.

Veliko uspeha!

| NALOGA | TOČK | OD TOČK | NALOGA | TOČK | OD TOČK |
|---|---|---|---|---|---|
| 1 | | | 3 | | |
| 2 | | | 4 | | |

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

**1. naloga:** Peter Zmeda se je tokrat lotil implementacije CHAP protokola, vendar je malce površno prebral RFC, ki opisuje CHAP. Njegova implementacija avtentikacije Boruta pri Ani je bila naslednja:

1. Borut pošlje Ani sporočilo, da se želi avtenticirati;
2. Ana Borutu pošlje kot izziv naključno 192-bitno sporočilo $X$;
3. Borut vzame skupno skrivnost $S$, ki je prav tako 192-bitna in izračuna bitni `xor` med $S$ in $X$ ter dobi odgovor $Y$:

   $$Y = X \texttt{ xor } S \ ,$$

   ki ga vrne Ani;
4. Ana sedaj pozna tako izziv $X$, skupno skrivnost $S$ in Borutov odgovor $Y$ ter lahko preveri, ali je res na drugi strani Borut.

VPRAŠANJA:

1. Kako Ana preveri, če je na drugi strani res Borut? Utemeljite odgovor.
2. Petrova shema ima veliko napako. Katero? Utemeljite odgovor in predlagajte rešitev.
3. Kaj je to napad z mavričnimi tabelami in kako deluje?
4. Kako se branimo pred takšnim napadom?

   NAMIG: Enovrstični odgovor ne bo dovolj, ampak se pričakuje podrobnejša razlaga rešitve.

**2. naloga:** Varnostni elementi omrežij.

VPRAŠANJA:

1. Občina Butale je sprejela odlok, da mora biti ves promet po računalniških omrežjih v občini nekriptiran[1]. Kmalu po sprejemu odloka je občina želela postaviti infrastrukturo za e-poslovanje. Vendar so se pričeli občani pritoževati, da si občina zmišljuje, da so zahtevali različne usluge od njih. Kaj naj naredi občina, da občani ne bodo mogli preklicati mrežnega prometa, ki so ga pošiljali na občino. Utemeljite odgovor!

   NAMIG: Podrobneje kot boste razložili rešitev, več točk boste dobili.

[1] To pomeni, da ne moremo uporabljati SSL plasti in posledično ne moremo uporabljati protokola `https`.

2. Pri IPsec datgramih smo govorili o dveh načinih dela. Katerih? Opišite bistveno razliko.

3. Kaj bi pomenilo, če bi v prvi komunikaciji protokola SSL strežnik poslal namesto certifikata samo svoj javni ključ?

**3. naloga:** Podatki za delovanje omrežja.

VPRAŠANJA:

1. Eden od prilastkov DNS protokola je TXT. Kako je prilastek TXT povezan s podatki o elektronski pošti?

2. Peter je včasih prav čuden možakar. Tokrat si je vbil v glavo, da ne bo nadgradil svojega LDAP strežnika, da bi uporabljal protokol LDAPv.3 namesto LDAPv.2. Napišite tri primere, ko ga njegova trdoglavost *ne bo* prizadela. Utemeljite svoj odgovor.

3. Po krajšem pogovoru, smo ugotovili, zakaj nima namena nadgraditi svojega strežnika – njegovo kodo je napisal sam. No, končno se je le dal prepričati, da ga bo nadgradil. Pri nadgradnji se mu je zataknilo pri izvedbi ukaza `bind`, medtem ko je vse ostale spremembe uspešno implementiral. Komentirajte omenjeno pomankljivost. Jo lahko kako drugače nadomesti? Utemeljite odgovor.

**4. naloga:** Družina IEEE 802.

VPRAŠANJA:

1. V scenariju protokola IEEE 802.1x nastopata poleg RADIUS strežnika še dve stranki. Kateri?

2. Kakšno vlogo imata obe stranki in kakšno RADIUS strežnik?

3. Opravka imamo s tremi strankami. Koliko računalnikov *najmanj* nastopa v omenjenem scenariju? Utemeljite odgovor.

4. Peter je tokrat sklenil pogodbo z Občino Butale, kjer je namestil dostopne točke, ki dovoljujejo uporabnikom priklop na LAN z uporabo protokola IEEE 802.1x. RADIUS strežnik ima postavljen v svojem podjetju, ki je v Spodnjem Gozdu. Edina povezava med njegovim podjetjem in občinsko stavbo poteka po medmrežju (Internetu). Pri tem je naletel na veliko težavo, saj je občinski nebodigatreba Cefizelj ravno končal tečaj uporabe programa *wireshark* in tako lahko prisluškuje prometu na omrežju. Predlagajte Petru dve možni rešitvi in ju utemeljite ter ocenite kakovost in primernost.[2]

[2]Občina je s posebnim odlokom Petru dovolila rabo kriptiranega prometa za ta primer.