# Komunikacijski protokoli in omrežna varnost
# 2020/21
# Drugi kolokvij

Kolokvij morate pisati posamič. Pri reševanju je literatura dovoljena. Odgovorite pazljivo na *vsa* vprašanja.

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 | | | 3 | | |
| 2 | | | 4 | | |

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

**1. naloga:** Varnostni elementi.

VPRAŠANJA:

A) Peter Zmeda želi postaviti navidezno zasebno omrežje s pomočjo `OpenVPN`. Namesto skupnega ključa želi uporabiti asimetrično kriptografijo in je zato postavil svojo certifikatno agencijo (CA). (i.) Ali na strežniku s certifikatno agencijo potrebuje OpenVPN odjemalca? Kaj pa OpenVPN strežnik? Odgovor utemeljite. (ii.) Ali mora na odjemalce spraviti tudi zasebni ključ certifikatne agencije? Kaj pa OpenVPN strežnik? Odgovor utemeljite. (iii.) Če ima Peter pet odjemalcev (A, B, C, D in E) ter en strežnik (S), koliko datotek s certifikati bo moral imeti na strežniku? Ne pozabite še na certifikatno agencijo.

B) Kako protokol CHAP preprečuje napade s ponavljanjem? Utemeljite odgovor s tem, da razložite *zakaj* ne more napadalec izvesti napada. Izberite eno možnost.

   (a) Z uporabo zgoščevalne funkcije.
   (b) Z uporabo naključnega izziva.
   (c) Z uporabo TLS šifriranja.
   (d) Z uporabo trosmernega rokovanja.

C) Omenili smo štiri tipične vrste napadov, ki ogrožajo zaupnost, celovitost in razpoložljivosti omrežnih sistemov. (i.) Katere so te štiri vrste napadov? (ii.) Za vsako od njih opišite primer napada. (iii.) Za vsakega od primerov napada opišite, kako se pred njim branimo.

**2. naloga:** AAA in RADIUS.

VPRAŠANJA:

A) Storitev RADIUS uporablja za transport UDP protokol. Odločite se za najboljši razlog, čemu tako (prim. RFC 2865) in utemeljite svoj odgovor.

   (a) Protokol RADIUS je brezstanjski.
   (b) Raba protokola UDP poenostavlja implementacijo strežnika RADIUS.
   (c) V IP skladu naprave mora biti implementiran vsaj protokol UDP, medtem ko je TCP neobvezen.
   (d) protokol UDP je bil razvit pred protocolom TCP.

B) Peter Zmeda bi rad na vseh računalnikih vedno uporabljal isto ime in geslo. (i.) Ali lahko v ta namen uporabi strežnik freeradius? Utemeljite odgovor. (ii.) Kaj bo moral nastaviti na vseh GNU/Linux in BSD računalnikih, da se bo

lahko avtenticiral s pomočjo zunanjega strežnika? (iii.) Kaj bo moral nastaviti, da bo računalnik vedel, katera identifikacijska številka (UID) je povezana s posameznim uporabniškim imenom?

C) Eden od najstarejših protokolov je protokol PPP (*point to point protocol*). Protokol PPP lahko uporabimo, da preko njega prenašamo podatke za CHAP protokol. (i.) Recimo, da bi Peter Zmeda rad avtenticiral Špelo Hitro s protokolom, ki uporablja izziv. Zapišite, kdo komu pošlje kakšne podatke (lahko večkrat), da lahko na koncu Peter res verjame, da ima opravka s Špelo. (ii.) Narišite in opišite paket protokola PPP, ki prenaša podatke protokola CHAP. (iii.) Narišite in zapišite vsebino vseh paketov PPP, ki potujejo med Petrom in Špelo, ko Peter avtenticira Špelo z uporabo protokola CHAP.

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

VPRAŠANJA:

A) Peter je pognal spodnjinaslednji ukaz:

```
ldapsearch -H ldap://ldap.zmeda.si
  -D "CN=peter,OU=peter;DC=ldap;DC=zmeda;DC=si"
  -b "DC=zmeda,DC=si" "(givenName=peter)"
```

(i.) Kaj je v tem ukazu niz za `-D`? (ii.) Kaj v angleščini predstavlja kratica `CN`? Kaj pa `DC`? (iii.) Kako bi ukaz predelali, da bi vrnil vnose, kjer je ime `peter` in priimek `zmeda`? Kratica za priimek je `SN` ali `surName`.

B) X.509 certifikat vsebuje polji *Signature Algorithm* kar dvakrat in sicer RFC5280 enega imenuje *signatureAlgorithm* in drugega *Signature*. (i.) V kakšnem odnosu sta? Izberite eno mo¸nost.

(a) V nikakršnem.
(b) Ime algoritma v polju *Signature Algorithm* določi uporabnik za svoje podpisovanje, medtem ko ime algoritma v polju *Signature* določi podpisovalec, ki z njim podpiše certifikat.
(c) Ime algoritma določi uporabnik in sme biti v obeh primerih enako, saj uporabnik tudi posreduje svoj podpis kot del zapisa *Signature*.
(d) Imeni morata biti enaki, saj algoritem določi podpisovalec za podpisovanje certifikata.

(ii.) Zakaj imamo dve polji?

C) Recimo, da RADIUS strežnik uporablja LDAP strežnik kot shrambo podatkov o uporabnikih. (i.) Opišite vsaj tri primere (situacije), ko RADIUS strežnik

potrebuje pridobiti podatke. (ii.) Na kakšen način (s katerimi ukazi) bere podatke iz LDAP strežnika in zakaj z njimi? (iii.) Podajte primer LDIF zapisa in opišite, kaj so posamezna polja ter opišite, kje se LDIF zapisi uporabljajo.

**4. naloga:** IEEE 802.

VPRAŠANJA:

1. (i.) Med katerima dvema stranema poteka pogajanje po EAP protokolu pri protokolu IEEE 802? Izberite eno mo¸nost.
   (a) Med avtentikacijskim strežnikom in avtentikatorjem.
   (b) Med odjemalcem in avtenitakcijskim strežnikom.
   (c) Med odjemalcem in avtentikatorjem.
   (d) Med odjemalcem in RADIUS strežnikom.

   (ii.) Kako izgledajo datagrami/paketi/okvirji EAP protokola? Narišite jih in opišite posamezna polja.

2. Peter Zmeda se je za storitev omogočanja dostopa do omrežja odločil sprogramirati svojo lastno avtentikacijo. (i.) Ali lahko uporabi namesto protokola EAP protokol PAP? Kako *uporabna* (ne *varna*) bo rešitev s protokolom PAP? Utemeljite odgovor. (ii.) Če pa le uporabi protokol EAP, opišite vse pakete, ki potujejo med njegovo napravo in napravo, ki se želi priklopiti v omrežje.

3. Peter ima težavo - nekateri uporabniki njegovega domačega omrežja si nikakor ne morejo zapomniti dodatnega gesla. Da bi vseeno omejil dostop do omrežja, bi rad vsakemu uporabniku dodelil svoje uporabniško ime in geslo. (i.) Kateri protokol bo uporabil, če je omrežje brezžično? Poznate kakšno implementacijo, ki je prosto dostopna? (ii.) Kateri protokol bo uporabil, če je omrežje ožičeno? Poznate kakšno implementacijo, ki je prosto dostopna? (iii.) Ali ima podatke lahko v bazi, dostopni po protokolu LDAP? Odgovor utemeljite.