Komunikacijski protokoli in omrežna varnost
2018/19
Exam February 6^{th} 2019

This test must be taken individually. Any and all literature may be used while taking this test. Answer diligently *all* questions.

Bonus points might be awarded if you at least partially correctly answer each question.

Duration of the test: 60 minutes.

We wish you a lot of success – veliko uspeha!

TASK	POINTS	MAX. POINTS	TASK	POINTS	MAX. POINTS
1			3		
2			4		

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga: Basics.

VPRAŠANJA:

A) Peter has connected his computer to the network, but cannot access the Internet – the web browser reports that it cannot find the server www.google.com. He used `ifconfig` to check his address, which is 192.168.1.1. The DNS server is set in `/etc/resolv.conf`. (i.) What else should he check to ensure his computer is set up correctly? Explain your answer. (ii.) Once he is sure the computer is set up correctly, how should he proceed to look for the source of the error?

B) When can a computer with BIOS boot over the network? Explain your answer.

C) `tftp` uses the `udp` protocol, which does not have sessions and does not ensure data transfer. (i.) How does `tftp` on application layer use the fields in `tftp` header to transfer the whole file? (ii.) Peter Zmeda already has a `tftp` server and wants to use it to transfer files of arbitrary size. How should he do that?

2. naloga: Time, TV and multicasting.

VPRAŠANJA:

A) How does a program which receives music over RTP and plays it back through a sound card know which format the music is in? Explain your answer.

B) While playing video of a song over the network we captured the (abbreviated) packet:

```
HTTP/1.0 200 OK
  Content-type: video/webm
  Content-Length: 7456250
  Last-Modified: Mon, 04 Feb 2019 18:09:57 GMT
  .E.....B..webm..B...C*..B@{..Lithium Flower..
  .Lavf58....V_VP9...#.."..eng..A_OPUS...c
  ..V.. c..OpusHead..8..g..E..ARTISTD..Raj Ramayya..
  .ENCODERD..Lavf58.."E..DURATIOND..00:03:18.706000000.
```

(i.) How long is the song? Who is the artist, and what is the title of the song? (ii.) Which format is the song in? Write the container format and the codecs for video and audio parts of the recording. (iii.) Which protocol (on the topmost layer) is used to transfer data? Write one advantage and one disadvantage of using this protocol to transfer video and explain your answer.

C) We wish to transmit the song to multiple listeners. The PIM protocol can function in dense and sparse modes. (i.) Are the multicast trees built by the protocol equal in both modes? Explain your answer, focusing on the question *why* they should or should not be the same. (ii.) In class we talked about the RPL (revers path lookup) algorithm. Does PIM use this algorithm? Explain your answer. (iii.) Is it even possible to multicast video using `http`? Explain your answer.

3. naloga: Network management.

VPRAŠANJA:

A) When using LDAP, sometimes one may wish to find objects based on complex queries. For example, one might want to find every person in Maribor named either Janez or Borut. Are such queries against LDAP databases even possible by just using the query language these databases support? Explain your answer.

B) Peter uses LDAP. He added an entry for himself to the database:

```
dn: cn=si,ou=users,dc=butale,dc=si
objectClass: inetOrgPerson
objectClass: person
cn: si
sn: Zmeda
givenName: Peter
```

(i.) Explain the meaning of `dn`, `cn`, `ou`, and `dc` in the first line. (ii.) Since marrying the beautiful Rosamund he wants two record two surnames - Zmeda and Turjaški. How should he modify his entry in the database?

C) SNMP uses `udp` to transmit messages. (i.) How does the protocol ensure that the client knows it got a response to its query? Explain your answer by describing the communication. (ii.) To transmit data it uses TLV notation. Describe it. (iii.) What is the content of the following TLV record (the rightmost value is the first byte, bytes are given in hexadecimal):

```
00x E3x 07x 02x 02x 02x 01x 02x 06x 01x 02x
```

4. naloga: Security. Peter Zmeda found the following lines in his system log:

```
Dec 31 06:29:28 colin sshd[25212]: Invalid user xc from 106.12.37.232
port 58944
Dec 31 06:29:28 colin sshd[25212]: input_userauth_request: invalid
user xc [preauth]
Dec 31 06:29:28 colin sshd[25212]: pam_unix(sshd:auth): check
pass; user unknown
Dec 31 06:29:28 colin sshd[25212]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=106.12.37.232
Dec 31 06:29:30 colin sshd[25212]: Failed password for invalid
user xc from 106.12.37.232 port 58944 ssh2
```

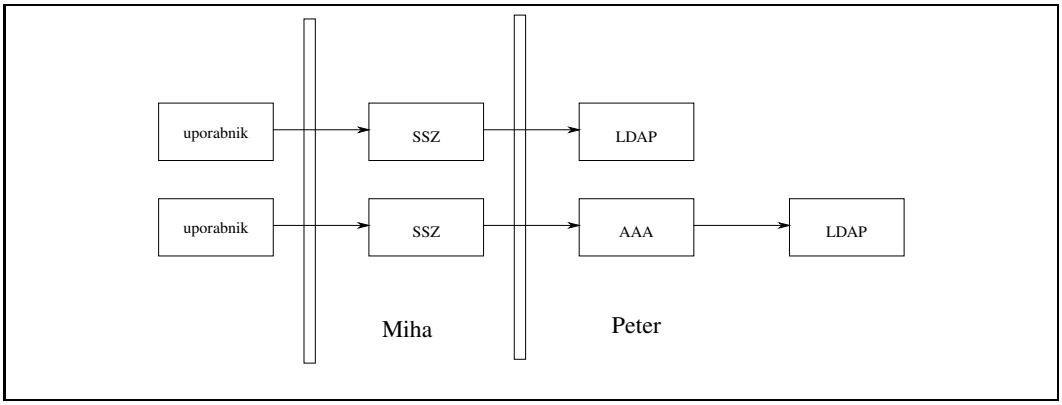
It appears something is going on with users on his system.

VPRAŠANJA:

A) Help him understand these records. (i.) Which program logged these lines? (ii.) What kind of error are they about, and what is the immediate cause of this error? (iii.) When authenticating users, why is it good practice to request a password even if a non-existing username is given?

B) Now Peter wants to establish a VPN between his and Špela's systems. Among the RFCs he read was the one about IKE. This RFC mentions two phases. What is the purpose of the second phase?

C) The system is now set up, including an `ldap` service. Miha wants to use this service for authentication in his CD-recording service called SSZ. Peter is not entirely sure if he should allow Miha's service to access LDAP or not. He is deciding between two possible architectures in Figure 1. (i.) Which option se-



Slika 1: Možni topologiji za storitev SSZ.

ems more secure to you, considering who has the shared authentication secret? Explain your answer. (ii.) What would it mean for Miha's implementation of SSZ if Peter offers a CHAP service instead of AAA? Explain your answer.