Communication Protocols and Network Security 2019/20
Written exam Weod-mōnaþ 25th, 2020

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

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

Duration of the test: 90 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. Task: Booting and Mounting.

QUESTIONS:

A) Under IPv4 the protocals BOOTP and DHCP are actually the same protocol, with the second being an extension of the first. (i.) Specify (or draw) fields of the BOOTP protocol packet. (ii.) Suppose a client sends a query for the operating system it would like to load. For three of the fields you listed above, specify the values that are in the package sent by the client. Justify why such values are in the fields as you specified. (iii.) For IPv6, we also have a version of the DHCP protocol, which is completely different from the IPv4 protocol. Why do you think they decided on a new protocol? Justify your answer.

B) (i.) What does the BIOS consist of as a whole (one answer)? Select one:

1. Software that helps stop the computer.
2. Hardware that helps start the computer.
3. Hardware (non-volatile memory) and corresponding software that helps start the computer.
4. Software that helps start the computer.

(ii.) Justify your answer.

C) Peter set up his DHCP server. (i.) Can the server assign addresses on a network it does not have an IP address on? (ii.) If not, why not? If yes, how?

2. Task: My network and its management.

QUESTIONS:

A) Peter is an entrepreneur and has upgraded the network in Butale so that subscribers can view footage of Butal Council meetings. Of course, a recording of the meeting is provided by the streaming server using the RTP protocol. Watching one meeting is presented with one session that has a beginning and an end. (i.) Is RTP protocol aware of sessions? (ii.) If so, describe how it works and if not, how can Peter then create individual sessions? (iii.) What about traffic obfuscation? How can he do it? Describe traffic obfuscation and how to create a session with obfuscated traffic.

B) One of the possible transport authentication protocols is also the PPP protocol. Assume we get PPP authentication packet, which carries authentication data. (i.) What are its first two bytes?

1. c1h 23h
2. c0h 23h

3. 00h 01h
4. c2h 23h

(ii.) Justify your answer.

C) Peter wants to manage his users' data through LDAP service, so he fixed `/etc/nsswitch.conf` as follows:

```
passwd:         ldap, compat
group:          ldap, compat
shadow:         ldap, compat
```

He can now log in the system with the username `peter`, which he has on the system, only the password in LDAP is not accepted by the system. (i.) Why? (ii.) What else does he need to change or set in LDAP for the password to work? In addition, the system no longer allows him to write to `/home/peter`. However, if he changes `/etc/nsswitch.conf` back to the old version, he can write to the home directory again. (iii.) Why could this happen?

3. Task: Multicast. In multicastin we mention protocols such as PIM.

HINT: Consider the connection between the PIM protocol and direct router multicasting of packets to its neighbors.

QUESTIONS:

A) (i.) How exactly is the PIM protocol involved in the actual multicasting of packets? (ii.) One of the basic ways of multicasting is broadcasting to all neighbors. This uses the reverse path lookup. Where does the router look when a packet arrives to decide whether to process the packet or not? On what basis does he decide that it should process the packet? (iii.) In this case, we can flood the entire Internet, but the IP packet has protection against it. Which and how does it work?

B) We have two devices A and B on the same subnet. A is subscribed to multicast address 111011010X, while B is subscribed to 111011011X, where X is a sequence of 23 bits. (i.) What does this mean for layer 2 (link layer) packet delivery? (ii.) Justify the answer.

C) Peter Zmeda wants to play the same movie on multiple information screens which are set up all over the village of Butale. On the server, he ran:

```
cvlc spincamarogla_skace.mp4
  -sout '#rtp{dst=172.31.44.6,port=5004,mux=ts}'
```

Then he ran on two information screens:

```
vlc -vvv -network-caching 200 rtp://172.31.44.6:5004/
```

but the movie started playing only on one. When he changed the address 172.31.44.6 to 225.112.213.23, the movie started playing on both. (i) Why did the commands work with one address, but not the other? Why was one of the info screens working at first? (ii) Did Peter the address (225.112.213.23) choose correctly? When could you answer yes, when no and how would you check? (iii) Which other addresses could he have used to still have a working solution? List the address range(s).

4. Task: Network operation and security.

QUESTIONS:

A) How can a client, when connecting to a network, execute the 802.1X authentication procedure if the access to the network has not been granted yet.

B) The HTTPS protocol, which is a secure version of the HTTP protocol, has a client and a server. (i.) What does the use of the certificate provide when establishing a connection from the client's point of view? (ii.) What does the use of the certificate provide when establishing a connection from the server's point of view? (iii.) Which part of the certificate is especially useful when setting up an encrypted session and why?

C) Peter Zmeda found the following lines in the 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
```

(i.) Which program recorded these lines? (ii.) What error is this and what is the direct cause of this error? (iii.) Why is it still good to ask for a password for authentication despite a wrong username?