Communication Protocols and Network Security 2020/21
Written exam 22. Æfterra Geola 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: 105 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: Basics. There are enterprising but also cautious people in Butale. The newspaper *Butalske novice* decided to offer even more local news to its readers. For this purpose, they intend to set up a service to which the residents of Butale would send news up to 1000 characters long. The sender should send a message to a specific port on the `Butalske-novice.but` server, which should contain the content of the message, the time and date of the event, and the name and surname of the sender. The service must then acknowledge receipt of the message to the sender. The service should be stateless so as not to overload the server unnecessarily. Help people of Butale set up this service.

QUESTIONS:

A) Let's start with the hardware. They have BIOS on the service server. Which of the following descriptions best describes what BIOS as a whole consists of? Justify the answer.
   (a) Software that helps stop the computer.
   (b) Hardware that helps start the computer.
   (c) Hardware (non-volatile memory) and corresponding software that helps start the computer.
   (d) Software that helps start the computer.

B) On the server, Peter would like to run Linux, but his booting computer stops with a black screen and the caption `(initrd)#`. He is booting Ubuntu and uses `atftpd` and `pxelinux`. (i.) Does `atftpd` work? Justify the answer. (ii.) Does `pxelinux` work? Justify the answer. (iii.) If we know he set something wrong in `default.cfg`, what could it most likely be?

C) And finally the service protocol. This should be directly above transport layer. (i.) Which protocol should they choose on the transport layer? Justify the answer. (ii.) Draw the fields in the message (packet, datagram) as accurately as possible. Justify why each field is in the message. (iii.) The people of Butale heard that the world was flooded with fake news and decided that it must be possible to verify that the news received was in fact written by a person posing as a sender. Describe how to extend the protocol from the previous point so that verification can be done.

2. task: My network and its management.

QUESTIONS:

A) Peter Zmeda is a bit confused. Instead of editing the config files for the DNS and DHCP server, he has entered all the information regarding his computers

- their IPs, MAC addresses and hostnames - into a directory which is available over LDAP. He would now like to use this data for his DHCP and DNS servers without having to manually copy the data. Which of the following tips is best? Justify the answer.

  (a) He will have to copy the data manually since DHCP and DNS servers do not support LDAP.
  (b) The DHCP server can use LDAP as it's backend. The DHCP server can then push data onto the DNS server. DNS servers can not use LDAP as a backend. An alternative solution is to use a common relational database (e.g. MYSQL) as the backend for all three servers - DHCP, DNS and LDAP.
  (c) DHCP and DNS servers can store their data in LDAP.
  (d) He will need the extensions to LDAP provided by the *Microsoft Active Directory*.

B) Peter and Manca share the physical part of the network. Each of them has its own list of computers and would like to assign IP addresses to them, each in her/his own area. (i.) How would they solve the problem if they have a shared DHCP server? (ii.) Can they also have two separate DHCP servers? If so, how would you set them up? If not, why not? (iii.) BYOD problem. Peter and Manca occasionally get a visitor who has a computer that is not on any of their lists. What happens when you connect this computer?

C) The SNMP protocol transmits data in the form of messages. (i.) What fields does a message of type request or response have and what is the role or purpose of each of them? (ii.) Let's say the content of the message are numbers `1000` and `500`. Where in the message are they located? (iii.) How are they encoded? Write them appropriately encoded.

3. task: Time and world wide web.

QUESTIONS:

A) Peter Zmeda noticed a REGISTER packet of PIM-SM protocol on his network. (i.) Who is sending it to whom?

  (a) Arbitrary router to the router to which the source of the data stream is connected.
  (b) Client that wants to join group to the client that is already member of a group.
  (c) Router to which the source of the data stream is connected to some other router.

(d) Client that wants to join group to its router.

(ii.) What does the sender with the packet communicate to the recipient?

B) Peter Zmeda maintains hundreds of computers, all connected to an internal, local area network. Every morning, when employees arrive at work and turn on computers, they first trigger the NTP protocol to synchronize time, which completely occupies the local network. Peter got the idea to set up a service that would multicast the current time every ten seconds on the local network while the computers would be in the recipient group. The sent packet contains only one field, namely the time in nanoseconds from January 1, 1900. (i.) What IPv4 multicast address should he use for group and what in the case of IPv6? Justify the answer. (ii.) Peter has decided to encrypt the time data and intends to use the same approach as the SRTP protocol - chaining. Can he? If so, how and if not, what should he do to be able to do it?

C) Peter Zmeda is setting up *Butale Television*. He would like to use multicasting to distribute the video material. It intends to use addresses between 224.0.5.3 and 224.0.5.33 for this purpose. The server has the address 192.168.1.31. (i.) Are these addresses appropriate? Justify the answer. (ii.) If he has 10 viewers, how many addresses will he spend? (iii) His streaming is currently not working. He is currently running:

```
vlc --sout="#transcode{acodec=mp4a,ab=128,channels=2,
  samplerate=44100,scodec=none}:rtp
  {dst=192.168.1.31,port=5004,mux=ts}"
  --no-sout-all --sout-keep Cin\ cin\ to\ sem\ jaz
  \(Kosmatko\ Ver\ by\ Butn8\).mkv
```

and on the client:

```
vlc rtp://192.168.1.31:5004
```

(iv.) Correct the two commands that streaming will work using multicasting.

4. task: Security.

QUESTIONS:

A) Peter Zmeda is planning a web service NekiNeki. The users will need to authenticate to use it. Which of the following approaches is the best for keeping the passwords for this purpose? Justify the answer.

(a) Database of users with their hashed salted passwords.
(b) Database of users with salts for their passwords.

(c) Database of users with their encrypted passwords.
(d) Database of users with their passwords.

HINT: The justification must be based on the property the chosen solution has and others do not have.

B) (i.) In addition to the firewall, what other service do we use for local network security? (ii.) How do this service and the firewall work together? Describe an example of an attack and how this service secures the local network with the help of a firewall. (iii.) In the lectures we learned about three types of firewalls. What are they and how they differ?

C) Peter Zmeda is setting up a VPN in his company with the help of OpenVPN. He will use certificates for authentication. He uses EasyRSA for this purpose. He creates all the necessary files for each user and then delivers them to the user on optical disk, which he sends by regular mail. Cefizelj laughs at this and thinks that doing so is dangerous. (i.) Who is right? Justify the answer. (ii.) What files does each user get? (iii.) How would Peter achieve that in the event that someone steals the letter, the company would not be endangered? Describe the procedure that Peter and employees would use.