Communication Protocols and Network Security 2019/20
Written exam 31. 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: 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. task: Basics of Networking. Cefizelj is a shrewd man and made plans to attack the server of Butale authorities, which has IP address 197.44.41.204. First, he will acquire a botnet and then each of the bots will send a ping request to address 23.192.3.212, by putting the IP address 197.44.41.204 as a source address.[1] For starters, Cefizelj tried to ping the above mentioned address and got the following result

```
Cefizelj > ping 23.192.3.212 -c 8
PING 23.192.3.212 (23.192.3.212): 56 data bytes
64 bytes from 23.192.3.212: icmp_seq=0 ttl=47 time=230.110 ms
64 bytes from 23.192.3.212: icmp_seq=1 ttl=47 time=268.099 ms
64 bytes from 23.192.3.212: icmp_seq=2 ttl=47 time=307.391 ms
64 bytes from 23.192.3.212: icmp_seq=3 ttl=47 time=116.082 ms
64 bytes from 23.192.3.212: icmp_seq=4 ttl=47 time=182.987 ms
64 bytes from 23.192.3.212: icmp_seq=5 ttl=47 time=222.148 ms
64 bytes from 23.192.3.212: icmp_seq=6 ttl=47 time=266.222 ms
64 bytes from 23.192.3.212: icmp_seq=7 ttl=47 time=306.350 ms
--- 23.192.3.212 ping statistics ---
8 packets transmitted, 8 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 116.082/237.424/307.391/60.612
ms
Cefizelj >
```

QUESTIONS:

A) (i) Describe what a botnet is and how it works. (ii) According to Cefizelj's plan, Where should the answers to the ping request supposedly go? Why? How? (iii) Where and how can defense be put against such an attack? (iv) Describe two possible reasons why the times in Cefizelj's ping experiment are so different?

B) What is *SecureBoot* supposed to protect? How?

C) Peter has connected his computer to the network, but he has no Internet access. The web browser immediately tells him that the server `www.google.com` it cannot find. With the program `ifconfig` he verified that his IP address is 192.168.1.1. He also verified that he has a DNS server IP address written in `/etc/resolv.conf`. (i) What else should he check to make sure the settings on his computer are correct? (ii) When he is sure that the computer is set up correctly, how can he continue to search for the source of the error?

[1] After the exam, try to find out who has this IP address. Please describe on the forum how you found this out. At least in two ways.

2. task: My network and its management.

QUESTIONS:

A) (i) What are the categories of network management? (ii) For each category give one examaple of network management.

B) Peter uses DHCP on his network. Due to hardware issues, he decided to replace the server. He added a new computer to the network and installed ISC DHCP3 on it. He set up the range of addresses that it can assigns. A few hours after replacing the server, he noticed that the network was running smoothly. Furthermore, the address of most computers have not changed, even though the lease duration has been set to 30 minutes. (i) Why the IP address generally did not change? How did the server get the current addresses? (ii) Describe at least one instance, where the IP address of a computer on the network might change.

C) The TFTP protocol is usually used to load the operating system. (i) Draw a protocol packet and describe what is in each field of the packet. (ii) The TFTP protocol is a lockstep protocol. Describe how a lockstep is executed? Give an example. (iii) How does the client know when the file transfer started and how does it know when it ended?

3. task: Time and television.

QUESTIONS:

A) SRTP is a secure RTP protocol. (i) What part(s) of RTP packet does it encrypt? (ii.) Why these parts and not the others?

B) Peter Zmeda is setting up *Butale Television*. He would like to use broadcasting to distribute the video. For this purpose, he intends to use addresses between 172.18.0.1 and 172.19.255.254. The server has the address 192.168.1.31. (i) Are these addresses appropriate? Justify the answer. (ii) What addresses could he (still) use? Justify the answer. (iii) He is currently watching a movie successfully if he runs the following command on the server

```
vlc --sout="#transcode{acodec=mp4a,ab=128,channels=2,
  samplerate=44100,scodec=none}:rtp
  {dst=172.18.0.2,port=5004,mux=ts}"
  --no-sout-all --sout-keep Cin\ cin\ to\ sem\ jaz
  \(Kosmatko\ Ver\ by\ Butn8\)-zy6qR1q2RvM.mkv
```

and on the client

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

(iv) Correct the commands in such a way that the VLC will use the selected (multicast) addresses.

C) Peter Zmeda came up with a brilliant idea, he was always annoyed with the fact that the protocol RTP did not know anything about the session. Therefore, he wanted to define a PRTP (Peter RTP) protocol that would allow a client-server session to be established and broken. (i) Let us say you would have to implement this protocol. Suggest the format of the packets and the meaning of each packet field. (ii) Is the protocol so defined useful for multicasting? Justify your answer.

4. task: Security.

QUESTIONS:

A) Peter and Maja want to talk online, but jealous Maša wants to eavesdrop on their conversations, so they decide to use public-private key encryption. Do they have to protect the key exchange against Maša and how?

- yes, with the Diffie-Hellman protocol;
- no, because the connection is over SSL and is sufficiently secure;
- yes, they exchange the keys through a certificate authority (CA);
- yes, with RSA+MD5

Justify the answer.

B) When discussing VPN we mentioned the term *tunneling*. (i) What is tunneling and describe an example of it. (ii) In addition, we mentioned the possibility of establishing VPN in *tunnel* and in *transport* mode. Describe two examples for each mode, where it is better than the other.

HINT: If one way is better than another at something, it means that in the second mode this cannot be done or it is very cumbersome.

C) Gregor Copatka, Peter Zmeda and Jure¸ Pismouk would like to communicate safely over a network which Peter has set up between the Butale hiking cottage on Veliki Hrib and the Tepanje owned cottage on Mala Planina. Peter beleives that the easiest solution will be to use OpenVPN with a shared secret. Gregor and Jure¸ would prefer to use certificates. (i) Which solution is better and why? (ii) How till their choice affect the type of virtual network device they should use (tun or tap)? (iii) If the gateway to the rest of the Internet is on Veliki Hrib, where should they set up the VPN server and why?