Komunikacijski protokoli in omrežna varnost
2018/19
First Midterm

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: bootp and DHCP.

VPRAŠANJA:

A) We have network devices with IP addresses 192.168.2.10 and 192.168.3.15. When can they send packets to each other directly, and when do they need a intermediate? Explain your answer.

B) Peter has two networks - 192.168.1.64/26 and 192.168.1.128/26. (i) At least how many DNS servers does he need so that his users can access the world wide web normally? (ii) What and how will he have to configure (besides the servers themselves) if he wants to offer the correct DNS to his users as simply as possible?

C) (i) As above, Peter has two networks. How many servers with an operating system does he need to offer the tftp service? Explain your answer. (ii) We learned about bootp and tftp services in connection with system boot. Can we also use them while the system is running? Explain your answer.

HINT: If you believe the answer is yes, explain why and how, and if you believe the answer is no, explain why not.

2. naloga: Peter heard that he can check the available disk space by running:

```
snmpget -v1 -c studentje localhost .1.3.6.1.4.1.2021.9.1.9.1.
```

VPRAŠANJA:

A) He wants to know what other information about the disk he can get. (i) What command can he use for this? Write the whole command with all arguments. (ii) What is `studentje` in the above command? (iii) Are the commands he is using safe? Explain your answer.

B) SNMP has three forms of communication: request/response between manager and agent, messages from agent to manager, and messages between managers. There are also several message types (*PDU Type*, *Protocol Data Unit Type*). (i) Which message types do you know and what forms of communication are they used for? Add an example of their use. (ii) SNMP is not a very safe protocol. How do we protect it from replay attacks? What resources, on which devices, are needed for this defense?

C) Can the state of a network (IEEE 802.3) switch be monitored without the use of SNMP? Explain your answer.

3. naloga: Real time

VPRAŠANJA:

A) Can we use the SSL/TLS protocol to encrypt RTP traffic? Explain your answer.

B) The RTP protocol provides two basic functionalities. (i) Which and how? (ii) Suppose we agreed that instead of using UDP as the transport protocol, we will use TCP. Which part of the RTP header would we no longer need and why? (iii) Peter has set up a videophone system using RTP in his company. To set up a connection, he is using a SIP service. How can he ensure the integrity of the data flow? Describe your proposed solution with as much detail as possible.

C) The TIME (`rdate`) can use either TCP or UDP as the transport layer. In which cases would you pick one over the other? Explain your answer.

4. naloga: Multicast

VPRAŠANJA:

A) Does the DHCP protocol use multicast addresses? Explain your answer.

HINT: Take into account which protocol is used on the network layer

B) There is a device with the address 1.4.6.7 which is joining the multicast group 224.0.24.32. (i) Write down the source and destination addresses in the IP header and the contents of the IGMPv2 packet. Explain why the field values are the ones you have written down. (ii) During lectures, we mentioned that the TTL value is set to 1. When would it make sense to have a TTL larger than 1? Describe an example. (iii) Does the IGMP protocol contain any mechanism for ensuring the integrity of messages? Explain your answer.

HINT: If you beleive it contains such a mechanism, describe how it works. If not, describe how an attacker can change the contents of a message without the recepient knowing.

C) OPTIONAL AND WILL NOT BE GRADED This year marks 100 years since the end of the World War I. (i) Name three countries which fought on the side of the central powers and three countries which fought on the side of the antante. (ii) Why was Russia not one of the signatories of the peace treaty 100 years ago?

D) In Butale is a red alert again. Something is going really wrong and Peter Zmeda suspects that it is Cefizelj who is responsible for the problems. Consequently he captured the network traffic and got the following log:

```
Frame 1543: 62 bytes on wire (496 bits),
  62 bytes captured (496 bits) on interface 0
Ethernet II, Src: 00:6c:bb:2f:30:00 (00:6c:bb:2f:30:00),
  Dst: IPv4mcast_16 (01:00:5e:00:00:16)
Internet Protocol Version 4, Src: 10.0.0.2, Dst: 224.0.0.22
Internet Group Management Protocol
    [IGMP Version: 3]
    ...
    Num Group Records: 1
    Group Record : 224.1.1.1  Mode Is Include
        Record Type: Mode Is Include (1)
        Aux Data Len: 0
        Num Src: 2
        Multicast Address: 224.1.1.1
        Source Address: 192.168.1.2
        Source Address: 8.8.8.8
```

(i) What is the IP address that Peter thinks that Cefizelj iz using? Explain your answer. (ii) What exactly Cefizelj is doing considering the captured log? FOr more precise answer you get more points.

HINT: Examine the captured packet content and based on it draw your own conclusions considering the type of packet and what is it used for.