Komunikacijski protokoli in omrežna varnost
2016/17
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) Can a device with IP address 192.168.2.10 send a network packet to device with IP address 192.168.3.15? If yes, how? If not, why?

B) Peter is setting up a local network and will require a DHCP server. There will be at most 50 computers in the network. (i) Suggest an address range for the DHCP server's address pool and the netmask such that the smallest possible number of addresses will be used. Explain your suggestions. (ii) If he has 50 computers, how many addresses will remain unassigned? Explain your answer.

C) There is in each `bootp` packet a field called `xid` – request identifier. What is the field used for? Which problems would arise if this field did not exist? Explain your answer.

Peter Zmeda is, as we all know, an inovative fellow. He now wants to replace `tftp` with a real `ftp`. (ii) Is this possible? Explain your answer.

HINT: If you believe it is not possible, explain why. If you believe it is possible, explain what would have to be done for the replacement to work.

2. naloga: Network management.

VPRAŠANJA:

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

B) Our friend Peter Zmeda has learned to use the net-snmp tools during lab exercises. He knows how to read any piece of data which is available on a computer over SNMP. Unfortunately, he does not even know which data are available. How can he find that out? Write down a complete command and explain each of its arguments.

C) Peter has finally set up SNMPv3 on all the agents on his network. He would now like to monitor them over some sort of web interface.

(i) Which MIB files will he need on the web server? Explain your answer. (ii) Suggest at least one existing web application for monitoring the state of the network and drawing graphs which he could use. (iii) Which part of the settings must he protect from Cefizelj so that Cefizelj will not be able to eavesdrop on the traffic between the agents and the monitoring system? Explain your answer.

3. naloga: Real-time.

VPRAŠANJA:

A) We have developed our own application protocol ABC. At the transport layer, we have decided to use UDP. How does this affect the reliability of communication between two participants in the ABC protocol?

B) NON-OBLIGATORY AND NOT TO BE GRADED. Peter Zmeda was the producer of a concert during which Luka Brezhlachnice played French and English suites on a Harpsychord. Peter was enchanted by the music but is now angry with himself for not hearing the name of the author. Help him eith the name of the composer.

C) They used RTP for streaming the concert. To make Peter's predicament even worse, his sound technician Špela was actually listening and has written down the name of the composer. She has also included the name of the composer in the transmission. (i) Where in the transmission can Peter find the name of the composer? (ii) Before the concert, Peter was explaining to Špela thath they would also use SIP. Do you think this makes sense? Explain your answer.

   HINT: The more detailed your answers, the more points you will get. For example, under (i), name not only the protocol but the place(s) in the transferred protocols which may contain the author's name.

D) Peter has decided that NTP is too complicated. He has therefore decided to extend the rdate protocol so that the time is transferred as a 48-bit unsigned integer representing the number of miliseconds since midnight, 1. 1. 1970. He will use port 3700 for his protocol. Write a client for the new protocol in a programming language of your choice. Feel free to use the code below (a not-quite-working rdate client) as inspiration.

```
import java.util.Date; import java.io.*; import java.net.*;
class RDate {
  public static void main(String[] args) throws IOException
{
    Socket s = new Socket("ntp1.arnes.si", 73);
    long d;
    d = new DataInputStream(s.getInputStream()).readInt();
    System.out.println(new Date(d * 1000 - 2208988800l));
  }
}
```

4. naloga: Multicast.

VPRAŠANJA:

A) How can we determine whether any computer on a network is a member of a particular multicast group – for example 224.6.1.2?

B) Peter has unpacked two programs for managing a *rendezvous point* in his home directory. The first is called `setrp` and is located in the subdirectory `nastaviRP`. The second is called `findrp` and is located in the subdirectory `poisciRP`. He has learned that he can use the following sequence of commands to run `setrp`: `cd ~/nastaviRP; ./setrp`. (i) How could he re-write the command so that all paths start with `/`? Assume that his username is `peter` and that his home directory is in the usual location. (ii) How could he run the `findrp` command without using absolute paths or the `~` shortcut if he is currently in the directory containing `setrp`?

C) In the previous question we mentioned a rendez-vous point. (i) What role does it play in multicasting? (ii) We mentioned that there are two basic modes of multicasting. In which mode is the rendez-vous point used? (iii) Why only in this mode and not in the other? (iv) Suppose you had to help Peter write the two programs mentioned in the previous question, which arguments should `setrp` and `findrp` accept to make the program names appropriate? Explain your answer.