Komunikacijski protokoli in omrežna varnost
2011/12
Pisni izpit

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.

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: Although some questions might seem to be about a specific chapter in the lectures, you will often need the knowledge from other chapters to answer them.

VPRAŠANJA:

1. Inside a `bootp` packet, you can find the `xid` and `secs` fields. What functionality do these two fields provide at the protocol level?

2. One of the opcodes in the TFTP protocol is `ACK` (= 4). What is the meaning of a client sending a packet with the following values (writen in decimal, two bytes): `4` `210`.

3. What is the maximum file size of a file that can be transferred over TFTP? Explain your answer.

2. naloga: Peter Zmeda is a truly a confused fellow. His friend Simona is really into gardening. The plants she grows in her greenhouses require a specific temperature which must be precisely maintained. She has therefore bought a new device with a built-in thermometer and a heater. The thermometer turns the heater on and off as needed. Furthermore, the device allows the user to upgrade its firmware. This means that the user can upload her own programs to the device.

VPRAŠANJA:

1. Simona also has a home server. She has asked Peter to write for her all the programmes needed for her to be able to control the device from the server. Peter has decided to use the SNMP protocol. Which pieces of software should Peter install and where?

2. The SNMP protocol defines multiple message types. Which ones? Write a use-case for each of them in the case of Simona's greenhouses.

3. The SNMP protocol uses UDP for data transfer. We mentioned UDP when we talked about multicasting. Simona wants to increase the number of greenhouses and therefore the number of devices. To reduce the ammount of traffic on the network, Peter has come up with the wonderful idea to use *multicasting* to communicate with all the devices simultaneously. Comment on his idea.

4. One of the messages we intercepted on the network contains information about the current temperature (first) and pressure in the greenhouse. Both

values are encoded in the TLV format with the temperature in ^{o}C and the pressure in kPa. The message contains the following bytes:

12	1	2	23	0	2	2	→

What are the temperature and pressure?

3. naloga: Multicast.

VPRAŠANJA:

1. In lectures, we mentioned the division of routing protocols according to their mode of operation into dense and sparse mode protocols. What is the difference between these modes of operation? Why is one mode called dense and the other sparse?

2. Multicasting is also used to deliver TV content. The access to each channel should obviously be limited to authorized subscribers only. Suppose that the content is delivered using multicasting. Describe in as much detail as possible, how AAA and multicasting are connected.

   NAMIG: Think about who actually delivers the content to the user and that this is the content server in fact.

3. Peter Zmeda has decided to offer a new pricing scheme in his pay-per-view network. He has decided to call it PPP – Pay Per Peep. His clients subscribe to the multicast streams at their nearest router using the IGMP protocol. Which data should Peter store upon receiving which IGMP packets at the router?

4. naloga: Network security elements and AAA.

VPRAŠANJA:

1. The RADIUS protocol uses UDP for data transfer. We therefore can not guarantee that the data will be transferred safely. Nevertheless, the data provides some measure of security through signing. (i) How exactly does package signing work in the RADIUS protocol when doing authorization and/or authentication? Describe the individual steps and the content of the packages sent in each step. (ii) How would you conduct an attack on such a security system?

2. Peter Zmeda has installed a wireless network in at his company. The network is separated from the rest of his nework by a firewall. Can the firewall be used instead of the IEEE 802.1x protocol? Explain your answer.

3. The SSL protocol expects the data to be broken into records. Why would we want or even need to break the data into records?

4. One possible attack is a TCP session hijack. Cefizelj has decided to hijack one of Peter's sessions. Therefore, Peter installed SSL on top of TCP as protection. If Cefizelj still wants to hijack such a session, he must also steal some additional values from Peter. Which ones?