# Komunikacijski protokoli in omrežna varnost 2010/11
# Pisni izpit 28. prosinec 2011

The test will be taken by you alone. This is an open-book test.

Additional points will be awarded if you at least partially answer all the questions.

Test duration: 90 minutes.

Veliko uspeha!

| TASK | POINTS | MAX. POINTS | TASK | POINTS | MAX. POINTS |
|---|---|---|---|---|---|
| 1 | | | 4 | | |
| 2 | | | 5 | | |
| 3 | | | 6 | | |

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

**1. naloga:** In order to cut the cost of IT in his company, Peter Zmeda has decided to buy diskless workstations instead of normal PCs. He uses the bootp protocol to boot the computers.

Once the systems are booted, the users log in with their usernames and passwords.

VPRAŠANJA:

1. Write down the steps in the DHCP procol and the purpose of each step.
2. Some users use the *lR* operating system while others use *kHTW*. Peter has to set up his system so that users can choose which operating system to start. Describe how Peter can go about solving this task by using only the bootp and tftp protocols.
3. Miha, a malicious miscreant has somehow managed to gain control of Peter's bootp server. What can he do in order to gain access to the usernames and passwords of the users? Describe the key steps in as much detail as possible.
4. How can Peter protect his users from Miha's bootp server?

**2. naloga:** During the lectures on network management we also talked about the SNMP protocol.

VPRAŠANJA:

1. What is the difference between a MIB and MDB?
2. We have the following properties defined in a MIB:

| Object ID | ime | type |
|---|---|---|
| 1.3.6.1.2.1.7.1 | UDPInDatagrams | Counter32 |
| 1.3.6.1.2.1.7.2 | UDPNoPorts | Counter32 |
| 1.3.6.1.2.1.7.3 | UDInErrors | Counter32 |
| 1.3.6.1.2.1.7.4 | UDPOutDatagrams | Counter32 |
| 1.3.6.1.2.1.7.5 | udpTable | SEQUENCE |

   What can you say about relationship between individual entities/ objects considering their *ID*s.

3. SNMP usually uses the UDP protocol and port no. 161 or 162, Where (or to be more precise, by who) was the port to be used defined?

   NAMIG: The answer was not given during the lectures on network management.

4. Apart from SNMP, we also mentioned other network management tools. Name at least two other tools and describe a situation where it is more appropriate to use one of them instead of SNMP.

**3. naloga:** Peter wants to set up his computers so that the time on their clocks is accurate.

VPRAŠANJA:

1. To simplify things, he has decided to set up networked time servers in his company. i) Which protocol can he use? ii) Will one server be enough? Explain your answer. iii) Would it make sense for Peter to set up an atomic clock at his company? Explain your answer thoroughly – imagina that you are writing a document for the company manager and that the procurement and setup of the servers depends on your request.

2. Unfortunately, Miha, the malodorous miscreant has again decided to spit in Peter's soup and has managed to set up his own time server on the network. How can Peter defend against this?

   NAMIG: Take into account how clients are configured. Also take into account the possibility that Miha has somehow acquired the ability to configure the clients or to perform ARP poisoning attacks.

3. Peter has come up with the idea that he could synchronise the real-time clocks on his network by broadcasting the correct time in regular intervals using multicast. Will his idea work well enough?

   NAMIG: When answering, think about how accurately Peter wants to set the clocks, how his network is laid out and how often the servers send the correct time. The answer will be graded according to your arguments which should take the form of: "Because Peter's ..., it follows that ...".

**4. naloga:** As we said, Peter manages a network in a company. Although the computers boot their OS over the network, he occasiounally wants to update certain configuration parameters. He has developed his own software agents which are installed on all computers. He has decided to distribute the updates using multicast. His idea is to occasionally signal the agents that they have to download new data off a server using TFTP. The signal messages are sporadic and relatively rare - perhaps a few messages every hour.

VPRAŠANJA:

1. Because he's using multicast, which protocol will Peter have to use on the transport layer?

2. Peter's computers use IPv6 as the network layer. Write down a possible multicast address (the address of a multicast group). Explain the values in each part of the address. You will also get points if you describe the address's structure.

3. Which protocol is involved in the delivery of multicast packets: i) IGMP ii) MLD iii) PIM or iv) none of the above. Carefully read the question before answering.

**5. naloga:** Directory services.

VPRAŠANJA:

1. For a directory service to work, distinguished names are very important. What is a distinguished name and what purpose does it serve?

2. Peter has also set up a directory server for his company. He vaguely remembers hearing that the directory data can be stored on multiple servers. Which options for storing directory data exist and what is the purpose of each of the options? Which option should Peter use?

3. What is the difference between the LDAP commands `search` and `compare`?

**6. naloga:** AAA and IEEE 802.

VPRAŠANJA:

1. Peter is updating his network. Apart from booting the OS off the network, he has also decided to make accessing the network more secure. Secure access must also be provided to the computers that boot off the network. In these cases, which protocol should he use first - IEEE 802.1x or bootp? Explain your answer.

2. Oh, we almost forgot. Peter is using IPv6. Does this affect the use of RADIUS in any way? Should he switch to DIAMETER instead?

3. With IEEE 802.1x, one of the steps in the protocol is the authentication of the device or user. Peter wants to authenticate all users and has decided to use biometric data for authentication. He has installed a fingerprint reader on each of the computers. The reader returns a string of bytes, uniquely

describing each fingerprint. How should he modify the CHAP protocol to make everything work?

NAMIG: Help yourself by drawing a schematic of the whole system from the fingerprint reader up to the AAA server. On the schematic, write down the data pertinent to authentication. It might help you to start with the CHAP protocol.