Communication Protocols and Network Security 2019/20
Second Midterm

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. naloga: Security elements.

VPRAŠANJA:

A) One way to establish a VPN is to use IPsec. (i) With IPsec, the two parties must authenticate each other, which requires a shared secret. Where is it stored? (ii) The ESP header contains two fields. Which two? What are they and how is each of them used? (iii) The IPsec datgram also contains padding. Can the padding always be used to transmit any additional data between members of the entity pair? Justify your answer.

B) (i) How does ESP prevent replay attacks? (ii.) Justify the answer?

C) Peter Zmeda wants to set up a virtual private network using `OpenVPN`. Instead of a shared key he wants to use public-key cryptography, so he sets up his own certificate authority (CA). Explain your answers to the following questions. (i) Which certificates will he need to put on the OpenVPN server? For each of them, explain its role. (ii) What certificates will he need to put on each of OpenVPN clients? For each of them, explain its role.

2. naloga: AAA and RADIUS.

VPRAŠANJA:

A) Service `syslog` recorded the record:

```
Jan 17 10:07:27 AndyBook timed[133]:
  settimeofday({0x5e21794f,0x436ca}) == 0
```

(i) Which program requested the recording of the log? Justify the answer? (ii) What is the meaning of thelog in your opinion?

B) (i) Describe how the man in the middle attack works. (ii) Is the RADIUS protocol vulnerable to the man in the middle attack? Justify the answer. (iii) If the protocol CHAP would be vulnerable to the man in the middle attack, why we could not use it with the RADIUS service? Justify the answer.

HINT: Consider where and how (architecture) the CHAP protocol is used with the RADIUS service and who in this case knows the shared secret and who we do not want to know it.

C) As said, Špela provides the RADIUS service and she is using for this the `freeradius` server. (i) Can Špela make RADIUS work even if her computer is turned off? Justify the answer. (ii) Špela wants to store users in a way where, if someone steals her computer, the stored passwords will not be

readable. At the second to last laboratory exercises at KPOV, she heard that this could be achieved with some kind of modules. What are the modules and how do we use them with `freeradius`?

3. naloga: Information for network operation.

VPRAŠANJA:

A) Directory service is based on standard X.500. (i) Which operations does the standard define? (ii) What does each of the operations do? (iii) Choose three operations among them and describe situations (scenarios) in which they are used.

B) (i) What methods of secure communication does the LDAP protocol provide? (ii) Describe their operation.

C) Peter uses LDAP. He also entered information about himself in the database:

```
dn: cn=si,ou=users,dc=butale,dc=si
objectClass: inetOrgPerson
objectClass: person
cn: si
sn: Zmeda
gn: Peter
```

(i) Explain what do `dn`, `cn`, `ou` and `dc` in the first line mean. (ii) Since he married the beautiful Rosamunda, he now wants to have two surnames - Zmeda in Turjaški. How should he fix his database entry?

4. naloga: IEEE 802.

VPRAŠANJA:

1. (i) Which technique is one of the main reasons for increased wireless transfer bandwidth from 802.11g to 802.11n? (ii) Why or how does it increase the speed?

2. Ethernet frame has a well defined format. (i) Where in the frame is data indicating, that the frame is used to carry EAPOL protocol? (ii) What value is used to mark the EAPOL protocol? (iii) How does this field influence the bridges? Justify your answer.

3. Peter has a problem - his internet service provider (ISP) has ”locked” his router so that it only works with his old computer, which he now wants to replace. (i) Which computer-related information provider uses for locking? Justify the answer. (ii) Let us assume that Peter uses your favorite operating system on his computer. Describe which command he should run or where he should click to get this information. (iii) In addition to lock on a computer, his ISP also requires from Peter to log in with a username and password. Can a provider use the same standard (802.1x) as for authentication to wireless networks? If not, why not? If yes, what equipment should support the standard?