Communication Protocols and Network Security 2021/22
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. task:
Security elements.

QUESTIONS:

A) Peter Zmeda wants to set up a virtual private network using the (fictional) program *WireSentinel*. Unlike *OpenVPN*, *WireSentinel* relies solely on shared secrets, with receiving and sending secrets being different. (i.) How to set up a certification agency in such a case? (ii.) How many clients can such a system have? Justify the answer!

B) Let sides A and B want to securely communicate. (i.) Where is defined how should the individual datagram be protected?

(1) Defined in SAD.
(2) Defined through IKE.
(3) In SPD.
(4) In ESP header.

(ii.) Justify the answer by describing for each of the answers what is hidden behind the abbreviation and what the mechanism described by the abbreviation is for.

C) In the lectures, we came across three types of filtering that can be performed by a firewall. (i.) What are these types of filters? (ii.) For each of them, describe an example of an attack that can be defended with this method of filtering and how the defense is performed.

2. task: AAA and RADIUS.

QUESTIONS:

A) (i.) What is the difference between authentication and authorisation?

(a) Authentication tells us person's permissions, while authorisation tells us rules on how to use these permissions.
(b) Authentication tells us person's permissions, while authorisation tells us a person's identity.
(c) Authentication tells us person's identity, while authorisation tells us person's permissions.
(d) Authentication tells us person's identity, while authorisation logs authorship of executed commands on a system.

(ii.) Write down the authentication example and the authorization example.

B) Peter Zmeda would like to always use the same name and password on all computers. (i.) Can he use the *OpenLDAP* server for this purpose? Justify the answer. (ii.) What will he need to configure on all *GNU/Linux* and *BSD* computers to be able to authenticate with an external server? (iii.) The identification works for him, but the system returns `"unknown user"` when logging in. It also finds nothing with the `getent passwd peter` command. Which library / component will he need to set up?

C) In the PAP protocol, the server that authenticates and the client that wants to authenticate exchange messages. (i.) Write down the sequence and meaning of the messages that the client and server exchange and justify your choice. (ii.) Suggest and justify the elements (fields) contained in the messages. (iii.) Passwords are stored by the server in a file and salt is used to make them harder to decrypt. Identify the two good and two bad sides if the server uses a single salt for all users and not different salt for every user.

3. task: Information for network operation. According to the X.509 standard, the digital certificate also contains:

(1) Version Number
(2) Serial Number
(3) Signature Algorithm ID
(4) Issuer Name
(5) Validity period: Not Before, Not After
(6) Subject name
(7) Subject Public Key (PK) Info: PK Algorithm, Subject PK
(8) Issuer Unique Identifier (opt.)
(9) Subject Unique Identifier (opt.)
(10) Extensions (opt.): ...
(11) Certificate Signature Algorithm
(12) Certificate Signature

QUESTIONS:

A) The signatures are mentioned in line 3 (i.) Why twice? We have the following service configuration:

$$\text{uporabnik} \Longleftrightarrow S_1 \Longleftrightarrow \text{AAA} \Longleftrightarrow \text{LDAP} \tag{1}$$

$$\text{uporabnik} \Longleftrightarrow S_2 \Longleftrightarrow \text{LDAP} \tag{2}$$

(ii.) For each of the configurations, write two cases where it is more appropriate than the other configuration. Justify your answer.

B) Peter ran the following command:

```
ldapsearch -H ldap://ldap.zmeda.si
  -D "CN=peter,OU=peter;DC=ldap;DC=zmeda;DC=si"
  -b "O=butale,DC=zmeda,DC=si" "(CN=peter)"
```

(i.) What is the string after `-b` for in this command? (ii.) What does the abbreviation `OU` mean in English? What about `DC`? (iii.) How would you modify the command to return entries where the name is `five` and the last name is `confuse`? The abbreviation for the last name is `SN` or `surName`, and for the first name `GN` or `GivenName`.

C) Peter zmeda is a bit confused. Instead of editing the config files for the DNS and DHCP server, he has entered all the information regarding his computers - their IPs, MAC addresses and hostnames - into a directory which is available over LDAP. He would now like to use this data for his DHCP and DNS servers without having to manually copy the data. Which of the offered answrers gives the best advice? Justify your answer.

   (a) He will need the extensions to LDAP provided by the Microsoft Active Directory.
   (b) The DHCP server can use LDAP as it's backend. The DHCP server can then push data onto the DNS server. DNS servers can not use LDAP as a backend. An alternative solution is to use a common relational database (e.g. MySQL) as the backend for all three servers - DHCP, DNS and LDAP.
   (c) DHCP and DNS servers can store their data in LDAP.
   (d) He will have to copy the data manually since DHCP and DNS servers do not support LDAP.

4. task: IEEE 802.

QUESTIONS:

1. IEEE 802.1D protocol deals with MAC bridges and among others specifies protocol for building spanning trees in networks. Why do we need a spanning tree? Justify your answer.
   (a) So that we can prevent frame broadcast.
   (b) So that a frame can reach its destination in logarithmic time.
   (c) For calculaton of shortest paths.
   (d) So than we have a unique path (without cycles) between any two nodes.

2. Peter Zmeda secured the connection to his network with the IEEE 802.1x service, using Špela's RADIUS service. (i.) Draw the architecture of the entire system, which includes the network connection server, the AAA server, and of course the client. (ii.) He decided to use the CHAP protocol for authentication. Draw the format of the frame traveling from the client. Because Špela is distrustful, she changed the authentication so that the messages are tunneled through the TLS tunnel. Now the client must first set up a TLS tunnel with an AAA server. (iii.) What do they need to exchange in

order for a tunnel to be set up? Justify why they have to share this information?

3. Peter decided to take care of security on his wireless network. He will use OpenVPN instead of 802.1x. (i.) What advantages will his solution have? List at least two. (ii.) What disadvantages will his solution have? List at least two. (iii.) Can OpenVPN run on a wireless router? Justify the answer.