Communication Protocols and Network Security 2020/21
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: 90 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 with help OPENVPN. He wants to use asymmetric cryptography instead of a shared secret, so he has set up his own certificate authority (CA). (i.) Does he need an OPENVPN client on a server with a certificate authority? What about an OPENVPN server? Justify the answer. (ii.) Does he also have to put the private key of the certificate authority on the clients? What about on an OpenVPN server? Justify the answer. (iii.) If Peter has five clients (A, B, C, D, and E) and one server (S), how many certificate files will he need to have on the server? Don't forget the certificate authority.

B) How does the CHAP protocol prevent replay attacks? Justify your answer by an explanation *why* the attacker can not execute such an attack. Select one:

   (a) By using a hash function.
   (b) By using a random challenge.
   (c) By using TLS encryption.
   (d) By using three-way handshake.

C) We mentioned four typical types of attacks that threaten the confidentiality, integrity, and availability of network systems. (i.) What are these four types of attacks? (ii.) For each of them, describe an example of an attack. (iii.) For each case of an attack, describe how we defend ourselves against it.

2. task: AAA and RADIUS.

QUESTIONS:

A) RADIUS uses UDP as a transport protocol. Decide for the most appropriate reason for such a decision (cf. RFC 2865) and justify your answer. Select one or more:

   (a) RADIUS protocol je state-less.
   (b) Use of UDP protocol simplifies implementation of RADIUS server.
   (c) In IP stack only implementation of UDP protocol is mandatory, while implementation of TCP protocol is optional.
   (d) UDP protocol was developed before TCP protocol.

B) Peter Zmeda would like to always use the same name and password on all computers. (i.) Can a `freeradius` server be used for this purpose? (ii.) What will he need to set up on all GNU/Linux and BSD computers to be able to authenticate using an external server? (iii.) What will he need to set so that the computer knows which identity number (UID) is associated with each username?

C) One of the oldest protocols is the PPP protocol (*point to point protocol*). The PPP protocol can be used to transfer data for the CHAP protocol. (i.) Let us say Peter Zmeda would like to authenticate Špela Hitra with a protocol that uses a challenge. Write down who sends what information to whom (maybe several times) so that in the end Peter can really believe that he is dealing with Špela. (ii.) Draw and describe a PPP protocol packet that transmits CHAP protocol data. (iii.) Draw and write down the contents of all PPP packets traveling between Peter and Špela when Peter authenticates Špela using the CHAP protocol.

3. task: Information for network operation.

QUESTIONS:

A) Peter ran the command below:

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

(i.) What is the string after `-D` in this command? (ii.) What does the abbreviation `CN` mean in English? What about `DC`? (iii.) How would you rework the command to return entries where the name is `peter` and the surname is `zmeda`? The abbreviation for the surname is `SN` or `surName`.

B) *X.509* certificate contains record *Signature Algorithm* twice, where RFC5280 one of the records defines as *signatureAlgorithm* the second one as *Signature*. (i.) In what relation they are? Select one:

(a) In no relation.
(b) The name of the algorithm in the field *Signature Algorithm* defines user for his own signing procedure, while the name in the field *Signature* is defined by the signing authority who also uses it to sign the certificate.
(c) The name of the algorithm may be the same as it is provided by the user including with her/his signature that is part of the field *Signature*.
(d) The names must be the same and it is defined by the signing authority in order to sign the certificate.

(ii.) Why do we have two fields?

C) Let's say the RADIUS server uses LDAP server as a store of user data. (i.) Describe at least three cases (situations) when the RADIUS server needs to retrieve data. (ii.) How (with which commands) it reads data from LDAP server and why with these commands? (iii.) Give an example of a LDIF record and describe what the individual fields are and describe where the LDIF records are used.

4. task: IEEE 802.

QUESTIONS:

1. (i.) Between which two parties does the EAP protocol negotitation take place in protocol IEEE 802? Select one:
   (a) Between authentication server and authenticator.
   (b) Between the client (supplicant) and authentication server.
   (c) Between the client (supplicant) and authenticator.
   (d) Between the client and RADIUS server.

   (ii.) What do datagrams/packets/frames of the EAP protocol look like? Draw them and describe the individual fields.

2. Peter Zmeda decided to program his own authentication for the network access service. (i.) Can he use the PAP protocol instead of the EAP protocol? How *useful* (not *secure*) will the solution with the PAP protocol be? Justify the answer. (ii.) However, if he decides to use the EAP protocol, describe all the packets that travel between his device and the device that wants to connect to the network.

3. Peter has a problem - some users of his home network can't remember the additional password. However, in order to restrict access to the network, he would like to assign each user a username and password. (i.) Which protocol will he use if the network is wireless? Do you know any implementation that is openly available? (ii.) Which protocol will he use if the network is wired? Do you know any implementation that is openly available? (iii.) Can he have data in a database accessible via LDAP? Justify the answer.