Komunikacijski protokoli in omrežna varnost 2018/19 Second Midterm

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.

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) To establish a virtual private network the data stored in the SA record are required. (i.) Enumerate five elements stored in the SA record. Describe how (or for what purpose) each element is used. (ii.) Why does an SA record contains only data for establishing a unidirectional link?

B) Which of the following the most accurately describes the term *tunneling*:

   (a) a system to detect packet errors during network transfer;
   (b) a way to encrypt a packet by encrypting both the header and the payload;
   (c) a system to detect network intrusions; or
   (d) a way to encrypt a packet by encrypting only the payload.

   Explain your answer / describe the procedure.

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 set up his own certificate authority (CA). Explain your answers to the following questions. (i.) Does he have to set up the CA on a computer inside the virtual network? (ii.) The disk in the computer with the CA has failed, and all data has been lost. Can the users still connect to the virtual network? (iii.) What do the users have to do before they can use a new CA?

2. naloga: AAA and RADIUS.

VPRAŠANJA:

A) Service `syslog` recorded:

```
Jan  1 21:38:22 svarun dhcpd: uid lease 192.168.127.137
  for client 10:9a:dd:a6:dd:38 is duplicate on 192.168.127.0/24
```

   Which of the following programs requested the log: a.) `lease`; b.) `svarun`; c.) `uid`; or č.) `dhcpd`? Explain your answer.

B) Peter wants to offer a new service: printing stickers. He does not want to allow just anyone to print, so he will use the RADIUS service provided by Špela. (i.) Draw the architecture of Špela's and Peter's service and the user of Peter's service. Label the protocols used between individual components of the architecture. (ii.) Luka Kratkohlačnica wants to use Peter's service. Describe in as much detail as you can the authentication and authorization process, using the CHAP protocol.

HINT: What data (cleartext or encrypted, and how they are encrypted) is transferred between the elements of your architecture?

(iii.) Describe how Cefizelj can perform a MITM (man in the middle) attack on the CHAP protocol. For this question you can disregard the RADIUS protocol; in other words, Ana wants to authenticate Brane and Cefizelj is performing a MITM attack.

C) As said, Špela provides the RADIUS service and she is using for this the `freeradius` server. (i.) Who or what is described by the entries in the file `/etc/freeradius/3.0/clients.conf`? (ii.) Špela wants to store users in a `mysql` database. Should the `mysql` server be on the same computer as `freeradius`? Write one advantage of using the same computer, and one advantage of using a different computer for each service.

3. naloga: Information for network operation.

VPRAŠANJA:

A) Peter stores data using the LDAP service provided by Simona. Because Peter did not require any special features, Simona offered LDAP.V2. Now she has to upgrade the service to LDAP.V3. (i.) What did Peter request that could not be provided using the older version of the service? (ii.) On his system Peter found the command `ldapcompare` with the following description:

> **ldapcompare** opens a connection to an LDAP server, binds, and performs a compare using specified parameters. The DN should be a distinguished name in the directory. Attr should be a known attribute. If followed by one colon, the assertion value should be provided as a string. If followed by two colons, the base64 encoding of the value is provided. The result code of the compare is provided as the exit code and, unless ran with `-z`, the program prints TRUE, FALSE, or UNDEFINED on standard output.

Why does it return the described results? Explain your answer and describe a use case.

B) Peter Zmeda lives in Butale on Glavna ulica #5 (Main Street #5) and works at the Občina Butale (Municipality of Butale). His e-mail address is peter.zmeda@gov.bu. How does the distinguished name describing him look like according to RFC 4514?

(a) `CN=Peter Zmeda,C=Butale,STREET=Glavna ulica \#5,O=Ob. Butale,DC=gov,DC=bu`

(b) `CN=Peter Zmeda,C=Butale,STREET=Glavna ulica \#5,O=Ob. Butale,DC=gov+DC=bu`

(c) `CN=Peter Zmeda,C=Butale,STREET=Glavna ulica #5,O=Ob. Butale,DC=gov+DC=bu`

(d) `CN=Peter Zmeda C=Butale STREET=Glavna ulica #5 O=Ob. Butale DC=gov DC=bu`

Explain your answer.

C) What and where do we have to configure on a Unix system to use for resolving internet names the DNS server at `193.2.1.66`? Explain your answer.

4. naloga: IEEE 802.

VPRAŠANJA:

1. Peter Zmeda heard that IoT (Internet of Things) is becoming a reallity. Therefore he decided to use his own format of IEEE802 frames. Which parts of frame must he redefine that his frames will still travel around and that no other application will unintentionally process them: a.) destination address and payload; b.) source address and payload; c.) payload only; or č.) the field `ethertype`? Explain your answer.

2. The transport layer implemented with the IEEE.802 protocol is typically divided into two sublayers. (i.) Which layers are they? (ii.) On which sublayer do bridges operate? Explain your answer. (iii.) Routing and bridging are similar services. Which requires more resources for the same number of nodes, and why?

3. Peter has bad memory and cannot remember the MAC address of the network interface in his computer. He wants to ensure that his computer always gets the same IP when connecting to his home network. (i.) How can he determine the MAC address of his computer? (ii.) How can he ensure that his computer always gets a specific IP address? Manual assignment is out of the question. (iii.) If using the DHCP service, why can't he protect the network from unwanted guests joining it?