Komunikacijski protokoli in omrežna varnost
2016/17
Second Midterm

The test must be taken individually. Any and all literature may be used while taking the test. Answer diligently *all* questions.

Bonus points might be awarded if you at least partially correctly answer each task.

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) Salt in Butale is a highly sought-after commodity. Peter Zmeda has therefore created an application for ordering salt seeds to be used by the Butale municipality. The Application can be used over the web. Peter has placed the application server in the *demilitarized zone*. Access is possible on TCP port 2017. Due to security considerations, Peter would like to prevent Cefizelj from accessing, let alone using the application. Which type of filtering can Peter use?

B) With IPsec, there are two modes of communication: tunnel and transport. (i) Write down a case where the first is better than the second and where the second is better than the first. Explain both answers.

   HINT: When writing the explanation, think about what you can do with one and not with the other.

   (ii) With IPsec, the packets can have either ESP or AH header. Does the AH header also require a SAD entry? Explain your answer.

   HINT: It might be easier if you describe the functionality offered by the AH header and the parts of an IP packet when it contains an AH header.

C) In Butale, people have set up a virtual private IP network, for which they are using OpenVPN. The device type was set to `tap`. In Tepanje, they have a similar network also built using OpenVPN. They would now like to improve inter-village relations by joining the two networks, for which they also intend to use OpenVPN. (i) What sort of trouble may they run into and how can they solve them (describe at least one)? (ii) How should they set up their routing tables? (iii) Can the network work without having at least one gateway in the routing tables? Explain your answers.

2. naloga: AAA and RADIUS.

VPRAŠANJA:

A) How does the CHAP protocol prevent replay attacks? Explain your answer.

B) Biometric data (fingerprints, retina scans, ...) is one of the methods that can be used for authentication. Peter Zmeda would like to use biometric data in his application, but can not decide how. He assumes that each user has a unit, which can read a piece of biometric data and sends it as a unique (for each

user) 512-bit string. He is considering the possibility of using CHAP. Describe how he could use CHAP to implement the whole authentication procedure.

HINT: When describing the solution, be careful about trust to each element of the system and how to avoid possible attacks. You may have to do something with the biometric data unit to make sure that the bit string it sends (and which is then used) is sufficiently trustworthy.

C) Peter set up a RADIUS server and created a few users. Then, Cefizelj came by, read `/etc/freeradius/users` and stole the passwords of all users. (i) How can Peter prevent such a theft in the future? (ii) How can he make sure that the passwords are not stored on the RADIUS server in plaintext? Describe at least two methods.

3. naloga: Data for network management.

VPRAŠANJA:

A) A directory contains objects. (i) What is an object described by? Give an example. (ii) What is a schema and what does it specify? Give an example. (iii) What does LDAPv3 offer that LDAPv2 does not? Give at least three additions and describe their functionality.

B) Sometimes, one may wish to find objects based on complicated queries. For example, one might want to find every person in Butale named either *Francot* or *Kozmijan*. Are such queries against LDAP databases even possible by just using the query language these databases support? Explain your answer.

C) Peter would like to allow each resident of Butale to log onto any computer in the village. He intends to store the user data in an LDAP database. (i) What will he have to configure on the computers for the users to authenticate themselves? Just listing the names of libraries is sufficient. (ii) What will he have to set up for the system to be able to translate usernames into user IDs? (iii) Peter has read that he can use the the following command for testing:

```
ldapsearch -H ldapi:/// \
  -D cn=peter,ou=people,dc=butale,dc=si\
  -W -b ou=people,dc=butale,dc=si
```

What does the string after the `-D` switch? What about the string after the `-b` switch? What about the string after the `-H` switch?

4. naloga: IEEE 802.

VPRAŠANJA:

1. With the IEEE 802.1X, we mentioned the usage of the EAPOL protocol. (i) What is it used for? (ii) The transport protocol for EAPOL is Ethernet on layer 2. Why not use the IP protocol on layer 3? Explain your answer.

2. Peter Zmeda heard that IoT (*Internet of Things*) is becoming a reallity. Therefore he decided to his own format of IEEE802 frames. Which parts of frame must he define that his frames will still travel around and that no other application will not unintentionally process them? Justify your answer.

3. Peter is a bit lazy and uses the same password on each device. He would now like to secure his wireless network but does not wish to share his password with his sister. He would rather have separate usernames and passwords. How can he set up his wireless access point? What else will he have to set up / configure?