Komunikacijski protokoli in omrežna varnost
2010/11
Drugi kolokvij

This test must be taken individually. Any and all literature may be used while taking this test.

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

Duration of the test: 50 minutes.

Buenas suerte – veliko uspeha!

TASK	POINTS	MAX. POINTS	TASK	POINTS	MAX. POINTS
1			3		
2			4		

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga: Although this task is focused on AAA (Authentication, Authorization, Accounting), questions regarding AAA may also appear in other tasks. To answer the questions in this task you may need to show knowledge regarding other subjects covered during the course.

VPRAŠANJA:

1. Peter Zmeda (a.k.a. Peter Confusion) has once again come up with an idea. He has found out that an authentication server sold the company JCN uses a deterministic function to generate random integers:

   ```
   Init()::
     seed:= 110121;
   Random()::
     seed:= (seed * 65539) mod 2**(31);
     return seed,
   ```

   This function is actually copied from *The Art of Computer Programming* and has been proven to be good. [1] The random numbers generated by this function are used by a CHAP server to generate challenges. The CHAP server is the only process using this function on the given server. How can Peter perform a replay attack?

   HINT: Peter can restart the JNC server at will.

2. Peter's second idea is to offer his new service called KMD over the internet. In order to use the service, a user must first authenticate her/himself. Unfortunately, users tend to forget their passwords and therefore need help. Suggest at least one way Peter could solve this problem and *evaluate/ comment on* the solution from the security point of view (e.g. interception, replay, ...).

3. In our lectures we described the content of a PPP frame and the content of an IEEE 802 frame. Write down the fields in each of the frames and compare them. Which fields are present in both types of frames and which are not? Explain both answers.

2. naloga: Network secutiry.

VPRAŠANJA:

1. What is an SA (*security association*):
   - What is the purpose (role) of an SA?

[1] The operator `**` represents an exponent - 2**(31) means 2 to the 31^{st} power.

- Who are participants in an SA?
- List the fields in an SA record and explain why we need each field.

2. This time Peter wants to talk to his friend Ana over the internet using VoIP. He does not want anyone to eavesdrop on the conversation – that is to intercept the packets and "listen" to them. List at least three ways Peter can prevent eavesdroping and list the advantages of each option over the other two.

3. naloga: Network management data.

VPRAŠANJA:

1. What is LDAP? Is it a piece of software, a data format which a client can use, a protocol or something completely different? Explain your answer.

2. During the lectures we mentioned that there are two versions of LDAP: v2 in v3. List and describe at least two differences between the versions.

3. During communication, an LDAP server and client establish a *session*. During the session one can also use commands `bind` and `unbind`. Are both commands used during each session? Explain your answer, preferably by describing an example session.

4. naloga: The IEEE 802 family.

VPRAŠANJA:

1. Peter is sometimes a veritable volcano of ideas. This time he hass decided to change the IEEE 802.1x protocol so that one can use a one-time password. What does he need to do to make the idea work? For more points, explain in detail which parts of the used protocols have to be modified, extended and parametrisized.

2. We mentioned that there are three types of participants in the RADIUS protocol: (i) which are these three types; (ii) what are their roles; and (iii) how do they fit into the IEEE 802.1x protocol, more specifically EDUROAM (describe how RADIUS is used in the IEEE 802.1x protocol)?

   HINT: Is one of the participants composed of multiple actual servers?