Komunikacijski protokoli in omrežna varnost
2011/12
Drugi kolokvij

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.

A lot of success – veliko uspeha!

NALOGA	TOČK	OD TOČK	NALOGA	TOČK	OD TOČK
1			3		
2			4		

IME IN PRIIMEK: ______________________________

ŠTUDENTSKA ŠTEVILKA: ______________________________

DATUM: ______________________________

PODPIS: ______________________________

1. naloga: This time, Peter Zmeda has decided to implement the CHAP protocol. Unfortunately, he was a bit sloppy while reading the RFC describing CHAP. His implementation for Borut authenticating with Ana looks as follows:

1. Borut sends Ana a message stating that he wishes to authenticate;
2. Ana sends Borut a random 192-bit message X as a challenge;
3. Borut uses a common secret S which is also 192-bits long and calculates a bitwise `xor` between S and X, producing the response Y:

   $$Y = X\,\texttt{xor}\,S \ ,$$

   which he returns to Ana;
4. Ana now knows the challenge X, the common secret S and Borut's reply Y and can therefore verify whether the person on the other side of the line is truly Borut.

VPRAŠANJA:

1. How can Ana check that Borut truly is the person on the other side of the line? Explain your answer.
2. Peter's scheme has a huge flaw. Which is it? Explain your answer. Suggest a solution.
3. What is a rainbow-table attack and how does it work?
4. How do we defend against such an attack?

   NAMIG: A single-line answer will not be enough. Explain your answer thoroughly.

2. naloga: Network security elements.

VPRAŠANJA:

1. The Butale municipality has issued a decree according to which all traffic over computer networks on it's territory must be unencrypted[1]. Soon after the passage of the decree, the municipality tried to set up an e-public affairs infrastructure. The residents started complaining that the municipality is

[1] This means that users are forbidden to use even the SSL layer and therefore can not use the `https` protocol, for example.

charging them for services that they (the residents) did not request. What should the municipality do so that the residents will no longer be able to deny the data they sent to the municipality office?

Explain your answer!

NAMIG: The more thorough your answer, the more points you will get.

2. When talking about IPsec datagrams, we mentioned two modes of operation. Which ones? Describe the main difference.

3. Assume that in the first step of the SSL protocol the server sends client only its public key instead of certificate. What does this imply? Elaborate.

3. naloga: Network operations data.

VPRAŠANJA:

1. One of the DNS record types is the TXT record. How are TXT records related to data describing e-mail infrastructure?

2. Peter is sometimes a peculiar fellow. This time he has stubbornly decided not to upgrade his LDAP server, which would allow him to use LDAPv.3 instead of LDAPv.2. Describe three cases when his stubborness will *not* come to bite him back. Explain your answers.

3. After a short discussion, we realised why he does not want to upgrade the server – he wrote it's code himself. Reluctantly, he agreed to upgrade. During the upgrade, he got stuck implementing the `bind` command, but was able to implement all the other commands and features successfully. Comment on this flaw. Can he replace the functionality of bind with something else? Explain your answer.

4. naloga: The IEEE 802 family.

VPRAŠANJA:

1. Apart from the RADIUS server, two other entities are present in the IEEE 802.1x scenario. Which ones?

2. Which role does each of these two entities play? What is the role of the RADIUS server?

3. In the scenario we are dealing with three entities. What is the *smallest* number of computers in the scenario? Explain your answer.

4. This time, Peter has signed a contract with the Butale municipality, to set up access points which allow users to connect to a LAN using the IEEE 802.1x protocol. He has set up the RADIUS server at his company, which is located in Spodnji Gozd. The only link between his company and the municipality building is over the Internet. This presents a problem, since the local villain, Cefizelj, has just finished a course on the use of the *wireshark* program and can therefore listen in on the traffic going over the network. Suggest two possible solution Peter could use. Explain each solution, why and when it could be used. Evaluate each solution's quality and applicability in the given situation[2].

[2] In this case, the municipality has issued a special decree allowing Peter to use encryption just this once.