Komunikacijski protokoli in omrežna varnost
2013/14
Drugi kolokvij

This test must be taken individually. Any and all literature may be used while taking this test. Answer *all* the questions. Diligently.

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

Duration of the test: 60 minutes.

Much success – veliko uspeha!

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

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga: AAA and RADIUS.

VPRAŠANJA:

1. Among other things, the RADIUS protocol also supports accounting. (i) Which types of accountable events does RADIUS support? (ii) RADIUS has some security elements. The main ones use the `Authenticator` field in a RADIUS packet. How exactly is this field used in accounting? (iii) Unfortunately, this mechanism does not prevent replay attacks – why? How does the RADIUS protocol and it users solve the problem of replay attacks?

   HINT: For the last part of the question, perhaps you should describe an example of an attack and then use this to formulate the general answer. Also, it might be useful to investigate the consequences of a replay attack for each type of event.

2. This time, Peter has decided to set up a virtual private network with his friend, Janez. They have decided to use certificates for mutual authentication. The first problem they ran into is the setting up of a certificate authority. Each of the two friends wants to be considered important enough for others to ask him for his autograph – this means each of the two friends wants his own certificate authority.

   (i) Can an OpenVPN client and server used to set up a virtual private network use certificates (usually `ca.crt`) from different certificate authorities? (ii) Assume that Peter created files `peter_ca.crt`, `peter_ca.key`, `peter.key` and `peter.csr`, while Janez created `janez_ca.crt`, `janez_ca.key`, `janez.key`, `janez.csr`. Which files should be on Peter's computer and which on Janez's for their network to work? (iii) Who is going to sign the public key (issue the certificate) for whom?

3. Peter Zmeda has decided to salt his saved and hashed passwords not to be vulnerable against the rainbow table attack. Unfortunately, he has lost the value of the salt. Is this important? Explain your answer.

2. naloga: Imeniške strukture in LDAP.

VPRAŠANJA:

1. The X509 standard defines certificates that Peter and Janez are using in the previous question. The standard defines a number of fields in a certificate. Some of these fields are: *Issuer*, *Subject*, *Subject Public Key Info* that includes (sub)fileds *Public Key Algorithm*, *Subject Public Key* and finally the

field *Subject Unique Identifier*. (i) What is stored in each field? Are all the listed fields mandatory? (ii) The word certificate means ”a document attesting to the truth of certain stated facts”. What is being attested with an X509 certificate and by whom? How do we know that the content of a certificate is true and can be trusted?

2. The X500 standard defines the following operations: *Bind*, *Read*, *List*, *Search*, *Compare*, *Modify*, *Add*, *Delete*, and *ModifyRDN*. The standard in RFC4511 defines the following operations: *Bind*, *Unbind*, *Search*, *Modify*, *Add*, *Delete*, *Modify DN*, *Compare*, *Abandon*, *Extended* and *StartTLS*. (i) Pair the operations from the two standards and comment on the differences. (ii) What is the difference between operations *Search* and *Compare*? Give an example of use for the first and second operation.

3. Which modes of secure communication does the LDAP protocol offer?

3. naloga: Security elements.

VPRAŠANJA:

1. Peter Zmeda heard that there exists a support protocol called IKE and that it is connected to security protocols on the Internet. (i) Describe a usage scenario for this protocol. (ii) Describe, how this protocol works. (iii) Suppose that this protocol did not exist – what would be the consequences? Would it be impossible to perform the base activity that IKE supports? Would it be more difficult to perform?

2. At home, Peter has set up a local network with a few computers. He is using an access point running OpenWRT to access the Internet. Three computers on his local network are running openssh servers. He would now like to access these computers from the public Internet. (i) What does he have to set up on the access point so that he may ssh to the computers on the internal network? Suggest at least two solutions. (ii) If the ssh server is listening on the same port on all three computers, is it even possible to access all three? (iii) Which role is the access point takes – bridge, router, firewall or application gateway? Explain your answer.

3. How does ESP prevent replay attacks?

4. naloga: Local networks.

VPRAŠANJA:

1. The IEEE 802 standard splits the data link layer into two sublayers - LLC and MAC. One of the functionalities offered by LLC is the construction of a spanning tree. (i) What would happen to the network traffic if a spanning tree was not constructed? Explain your answer with an example. (ii) Suppose that the sublayer did not support bridges, would we still need spanning trees? Explain your answer.

2. Peter Zmeda is setting up a virtual private network between his holiday house and his home. Whenever he visits the holiday house, he carries a laptop with him. He would like the laptop to get the same IP address on his network, regardless of whether he is connecting to the network at home or at the holiday house. When at home, he would like to access a security camera installed at the holiday house. On the other hand, when he is at the holiday house, he would like to watch movies stored on a disk back at home. He and his wife also enjoy old computer games from time to time and sometimes they would like to play over the network, even if one is at the holiday house and the other is at home. (i) Which of the configurations below should Peter use? Why?

   - Konfiguracija 1:
     ```
     remote vpn.zmeda.si
     dev tun
     ifconfig 192.168.5.2 192.168.5.1
     secret skrivnost.key
     ```
   - Konfiguracija 2:
     ```
     remote vpn.zmeda.si
     dev tap
     secret skrivnost.key
     ```

   (ii) What are the downsides of such a virtual private network (name at least one)?

3. When connecting to a network, how can a client even perform the 802.1X authentication, if the client is not allowed access to the network until authenticated?