Final exam in

Computer Security EIT060

Department of Electrical and Information Technology
Lund University

March, 10, 2011, 14-19

- You may answer in either Swedish or English.
- If any data is lacking, make (and state) reasonable assumptions.
- Use legible hand writing. If your answers cannot be read, you will receive zero points on that problem.
- Only pencil and eraser is allowed.
- Grading is done as follows.
  Grade 3 = 20–29 points,
  Grade 4 = 30–39 points,
  Grade 5 = 40–50 points.

Problem 1. Explain to which extent the UMTS key agreement and authentication protocol provides nonrepudiation. (3 points)

Problem 2. Explain the ideas behind a buffer overflow attack on the stack using the keywords *unsafe functions*, *return address* and *buffer size.* (3 points)

Problem 3. In a spoofing attack, the adversary masquerades as another user or program. Assume that an attacker presents a fake login screen, hoping to capture user passwords. The system can help protecting users from such attacks.

a) What can be done to prevent such attacks?

b) What can be done to detect such attacks?

(3 points)

Problem 4. The WEP protocol had an intention to provide *Confidentiality*, *Integrity* and *Authentication*. However, it failed in all three cases. Explain briefly how for each case. (3 points)

Problem 5. Explain the difference between *real UID* and *effective UID* in Linux. What are they used for? (3 points)

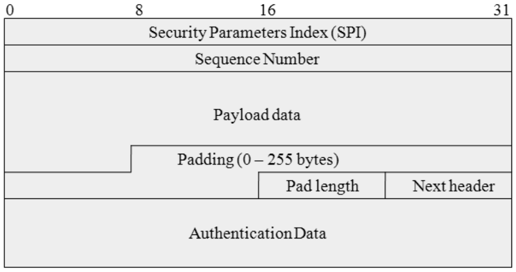
Problem 6. Allowing users to be put into groups can simplify access control. However, *policy conflicts* have to be dealt with. If a user has one set of permissions on a file, but a group that the user is a member of has another set of permissions, a decision has to be made what permissions will be effective. Compare how Windows and Linux deal with this type of policy conflicts. (3 points)

Problem 7. What are the similarities and the most important differences between the Bell-LaPadula and the Biba security models? (3 points)

Problem 8. An ESP packet used in IPsec is given below.

a) Which part of the packet is encrypted?

b) Determine the location of the original IP header in *tunnel mode* and *transport mode* respectively.



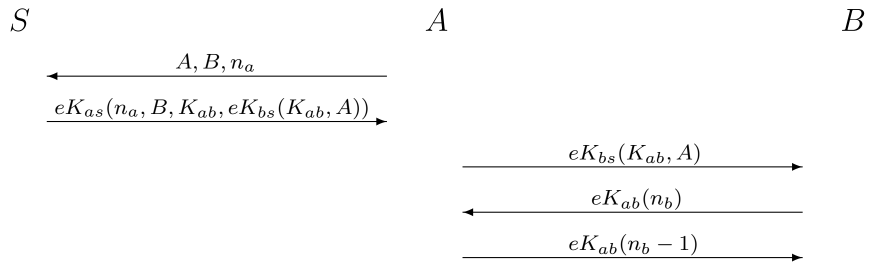
(3 points)

Problem 9. Describe and compare the *packet filter* and the *stateful packet filter* in the context of firewalls. (3 points)

Problem 10. Compare the Orange Book and the Common Criteria evaluation methods. What are the most important differences in terms of product functionality and assurance? (3 points)

Problem 11. Assume that we have the, probably familiar, situation in which we make a secure SSL connection between two computers, one client and one server. Both the client and the server has a public/private key pair and a certificate signed by the same CA, which in turn also has a public/private key pair. Thus, there are in total 6 keys involved, 3 public and 3 private keys. Explain for each of these keys its involvement when the secure connection is being set up. Assume that RSA is used and that the client is authenticated in the handshake. (5 points)

Problem 12. The Needham-Schroeder protocol is an authentication and key agreement protocol in which a client (A) can get access to a server (B) through a trusted third party (S). The protocol is given below.



a) What is the purpose of n_a?

b) In the second step, the data A and K_{ab} is encrypted with K_{bs} and then encrypted again with K_{as}. What if we move the part encrypted by K_{bs} out, i.e., the second message is instead

$$eK_{as}(n_a, B, K_{ab}), eK_{bs}(K_{ab}, A)$$

How would this affect the security of the scheme?

c) What is the purpose of the last message?

d) There is a serious security flaw in the Needham-Schroeder protocol, which has been addressed by the Kerberos protocol. Explain the flaw.

(5 points)

Problem 13. In order to measure the strength of cryptographic algorithms, the terms *empirically secure*, *provably secure* and *unconditionally secure* are commonly used. Explain and compare the terms. Also, for each security strength, give one example of a cryptographic algorithm. (5 points)

Problem 14. Explain shortly the following five terms:

a) Birthday paradox

b) Message Authentication Code

c) FRR (in biometric systems)

d) Inference (in statistical databases)

e) Chinese Wall security model

(5 points)
