Final exam in

Computer Security EITA25

Department of Electrical and Information Technology
Lund University

March 22, 2019, 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. Assume that we have the, probably familiar, situation in which we make a secure TLS 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. (3 points)

Problem 2. When encrypting information with a block cipher, it is not enough to have a secure block cipher. Explain how information can leak if the cipher is not used in a secure mode of operation. (3 points)

Problem 3. Let P be a password. Explain why

$$h = \text{SHA-1}(P)$$

is not a suitable way of storing authentication information on a server or in an operating system. (3 points)

Problem 4.

a) Describe the difference between a threat and a vulnerability.

Give an example of

b) a threat to data integrity

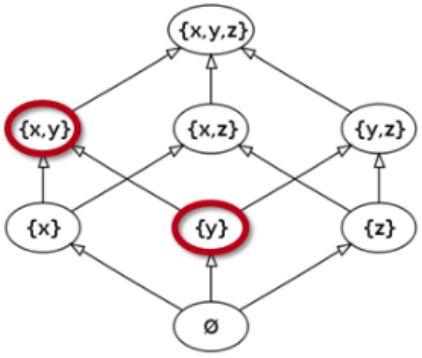
c) a vulnerability affecting data integrity

(1+1+1 points)

Problem 5. Consider the lattice below, which can be used in Mandatory Access Control.

a) Determine the Least Upper Bound and the Greatest Lower Bound of the two elements {y} and {x,y}.

b) Using this lattice as an example, explain how labels are allowed to change when dynamic integrity levels are used in the Biba model. Given one example when a user reads an object, and one example when a user writes to an object.



(1+2 points)

Problem 6. An IDS can be based on signature or anomaly detection. Highlight

a) the main differences between the two approaches,

b) the main advantages of signature based detection (compared to anomaly detection),

c) the main advantages of anomaly detection (compared to signature based detection).

(1+1+1 points)

Problem 7. The most well-known application of Time-Memory-Tradeoff attacks is to recover a password from its hashed form. However, the attack is much more general than that. Explain how a Time-Memory-Tradeoff approach can be used to conduct a chosen-plaintext attack on a block cipher. It is sufficient that you explain the offline phase of the attack. (3 points)

Problem 8. Canaries, ASLR and $W \oplus X$ are three well known and widely used protections against buffer overflow attacks. Explain each of these defense mechanisms and why they protect against the attack. (3 points)

Problem 9. The two most important protocols in TLS are the handshake and the record protocols.

a) Explain to which extent the handshake protocol supports *perfect forward secrecy*.

b) Explain to which extent the record protocol supports *non-repudiation*.

(1.5+1.5 points)

Problem 10. Assume that the value for *umask* in a Linux operating system is `027`.

a) What will be the permissions for a newly created file?

b) What will be the permissions for a newly created directory?

(1.5+1.5 points)

Problem 11. The Needham-Schroeder protocol is given below. S is a trusted third party, A is a client and B is a server.

1. $A \rightarrow S: \quad A, B, n_a$
2. $S \rightarrow A: \quad eK_{as}(n_a, B, K_{ab}, eK_{bs}(K_{ab}, A))$
3. $A \rightarrow B: \quad eK_{bs}(K_{ab}, A)$
4. $B \rightarrow A: \quad eK_{ab}(n_b)$
5. $A \rightarrow B: \quad eK_{ab}(n_b - 1)$

a) Identify all long-term keys.

b) What is the purpose of messages 4 and 5?

c) Is 2048-bit RSA a suitable encryption scheme for the above protocol? Motivate your answer.

d) Which problem with this protocol was fixed in the Kerberos protocol and how was it fixed?

(1+1+1+2 points)

Problem 12. Explain how access tokens, security descriptors, ACEs and the reference monitor are involved when a subject accesses an object in Windows. (5 points)

Problem 13. Challenge response protocols are commonly used for authentication in a network setting. In 2018, an authentication related vulnerability was reported in the Apache web server. The nonce used in a challenge response protocol was not random enough.

a) Describe an attack that takes advantages of repeated nonces in a challenge response protocol.

b) The authentication protocol used in WEP had a related, but worse, problem. What was the problem and how was it worse?

(2+3 points)

Problem 14. Explain shortly the following five terms:

a) RSA

b) Message Authentication Code

c) Second pre-image resistence

d) ABAC

e) Encapsulating Security Payload

(1+1+1+1+1 points)
