Final exam in

Computer Security EIT060

Department of Electrical and Information Technology
Lund University

March 12, 2014, 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. Describe the connection between the terms authentication and accountability. (3 points)

Problem 2. You have seen and experimented with the time-memory tradeoff attack for hash functions. Explain how such attacks can be used to attack a block cipher in a chosen plaintext scenario. You only have to describe the offline phase in which the tables are precomputed. (3 points)

Problem 3. What is the purpose of address space layout randomization (ASLR)? Which types of attacks is it designed to prevent? (3 points)

Problem 4. How do Unix and Linux support controlled invocation? (3 points)

Problem 5. In Windows, access control is determined both by access rights and privileges.

a) Who assigns privileges?

b) Who assigns access rights?

c) Where are they stored?

(1+1+1 points)

Problem 6. SSL/TLS consists of several protocols, where the handshake and record protocols are the most interesting from a security point of view.

a) Does the record protocol offer *non-repudiation*? Motivate your answer.

b) How does the handshake protocol protect against *replay attacks*?

(1+2 points)

Problem 7. Linux typically uses two separate files for storing information about users and their account, namely, the `/etc/passwd` file and the `/etc/shadow` file.

a) Why are two files used instead of putting all information in one file?

b) What *type* of information is stored in the two files?

(1.5+1.5 points)

Problem 8. PGP/GPG uses a combination of symmetric and asymmetric cryptography in order to encrypt emails.

a) Explain how this hybrid encryption is used.

b) In PGP/GPG, what is the purpose of combining symmetric and asymmetric algorithms like this?

(1+2 points)

Problem 9. A *packet filter* is a firewall that looks at internet packets and determines if they are allowed to pass or not. The decision is based on source/destination IP address and source/destination port. All packets are examined individually and independently of each other.

a) What is the limitation of this approach?

b) What is a *stateful packet filter*?

c) How do the two types of packet filters differ from an *application level proxy*?

(1+1+1 points)

Problem 10. The Bell-LaPadula security model is the most well known security model. It supports both mandatory and discretionary access control.

a) Explain how mandatory access control is enforced in the model.

b) Explain how discretionary access control is enforced in the model.

(2+1 points)

Problem 11. The Kerberos protocol is given below.

1: A, TGS, n_a

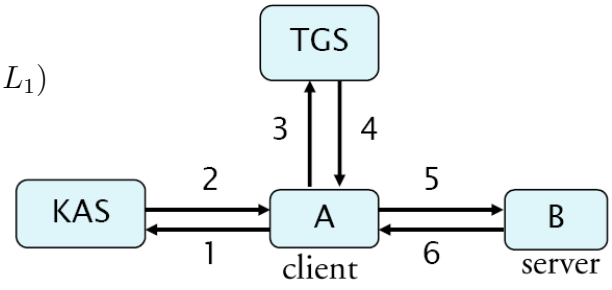
2: $eK_{as}(K_{a,tgs}, n_a, L_1, TGS), eK_{tgs}(K_{a,tgs}, A, L_1)$

3: $eK_{tgs}(K_{a,tgs}, A, L_1), eK_{a,tgs}(A, T_a), B, n'_a$

4: $eK_{a,tgs}(K_{ab}, n'_a, L_2, B), eK_{bs}(K_{ab}, A, L_2)$

5: $eK_{bs}(K_{ab}, A, L_2), eK_{ab}(A, T'_a)$

6: $eK_{ab}(T'_a)$



a) How does KAS authenticate A?

b) How does B authenticate A?

c) What is the purpose of L_1 and L_2? Describe an attack that would be possible if L_2 was removed.

(1+1+3 points)

Problem 12. In this problem we look at some different aspects of cryptography.

a) In RSA, a message is encrypted as $c = m^e \bmod n$ and decrypted as $m = c^d \bmod n$. A standard choice for e is 65537 ($2^{16} + 1$), which is 10000000000000001 in binary notation. This allows for efficient encryption since the speed of the algorithm used for exponentiation depends on the number of ones in the exponent. If we want fast decryption instead, could we instead choose d to be 65537 then? Why or why not?

b) How many hash function invocations are needed to find a collision in a (secure) hash function? How many are needed to find a second preimage?

c) What would be a typical choice of keysize for a stream cipher?

(2+2+1 points)

Problem 13. A challenge response scheme can be used to authenticate a client to a server on a network.

a) What is the main feature of a challenge response scheme compared to just sending the password?

b) Why should a nonce be used in challenge response authentication?

c) The challenge response protocol in WEP shared key authentication was/is insecure. Explain the weakness.

(1+1+3 points)

Problem 14. Explain shortly the following five terms:

a) EAL
b) Security Parameters Index
c) Protection profile
d) Kerckhoffs' principle
e) Implicit key authentication (5 points)
