Final exam in

Computer Security EIT060

Department of Electrical and Information Technology
Lund University

March, 7, 2012, 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. What is the difference between access control lists and capabilities?

(3 points)

Problem 2. A (long) listing of the information about the /tmp directory in a typical Linux distribution is shown below.

```
drwxrwxrwt 16 root root 4096 2012-03-07 14:00 tmp/
```

Why is there a `t` in the permissions list? What would be the difference if it is replaced by an `x`? (3 points)

Problem 3. How does the Orange Book, ITSEC and Common Criteria differ in their treatment of functionality and assurance of products. (3 points)

Problem 4. What is a replay attack? How does the SSL handshake protocol protect against replay attacks?

(3 points)

Problem 5. In the original Encrypted Key Exchange protocol (EKE), a public key is encrypted using a password. This will protect against offline dictionary attacks on the password. Breaking this scheme will require breaking either the symmetric key, or finding the private key corresponding to K_a. But if the security does not depend on the strength of the password, it should be ok to just omit the use of the password, shown in the modified EKE below. This is of course not true, why?

Original EKE

1. $A \rightarrow B: \quad eP(K_a)$
2. $B \rightarrow A: \quad eP(eK_a(K_s))$

Modified EKE

1. $A \rightarrow B: \quad K_a$
2. $B \rightarrow A: \quad eK_a(K_s)$

(3 points)

Problem 6. Why is the ESP header not encrypted in IPsec transport mode? (3 points)

Problem 7. Explain the idea behind SQL injection attacks. What is the main implementation mistake that allows the attack to succeed? (3 points)

Problem 8. An intrusion detection system (IDS) is based on *misuse detection* or *anomaly detection*. A *honeypot* has many similarities with an IDS. Describe when false positives and false negatives occur for each type of IDS and a honeypot. (3 points)

Problem 9. The Biba security model uses the notion of *clean* and *dirty* subjects and objects. Explain what is meant by this. (3 points)

Problem 10. In an RSA scheme, the public modulus is given by $n = 391$ and the public exponent is $e = 7$. Break this RSA scheme by finding the private exponent d. Recall that $d \cdot e \equiv 1 \bmod \phi(n)$. (3 points)

Problem 11. The Diffie-Hellman protocol is probably the most well-known key agreement protocol. Variants of the protocol has been implemented in numerous applications.

a) Describe the basic Diffie-Hellman protocol.

b) The basic protocol is vulnerable to a man-in-the-middle attack. Describe this attack.

c) Describe one way to fix this vulnerability.

(5 points)

Problem 12. Passwords are treated and stored in Windows and Linux systems in similar ways, but there are some important differences. In addition to this, there are differences between different Windows configurations and also between different Linux configurations. We are of course here only interested in differences related to the security of passwords.

a) What is the difference of storing the hash in /etc/passwd and /etc/shadow?

b) Windows Vista and Windows 7 by default only store the NTLM hash. Previous versions additionally stored the LM hash. What is the difference?

c) How does the use of salt differ between Windows and Linux?

d) Why does a random unique salt for each user protect against time-memory-tradeoff attacks?

(5 points)

Problem 13. Not only clients need to be authenticated, but also the servers. This can be done in several ways.

a) What is it called when *both* entities in the communication are authenticated?

b) How is the network authenticated in UMTS?

c) How is the server authenticated in SSL when RSA is used as handshake method?

(5 points)

Problem 14. Explain shortly the following five terms:

a) Controlled invocation

b) HMAC

c) Chinese wall model

d) Spoofing attack

e) Canary value

(5 points)
