Final exam in

Computer Security EIT060

Department of Electrical and Information Technology
Lund University

March 18, 2016, 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 how an attacker could (try to) forge a digital signature. (3 points)

Problem 2. Two communicating parties (A and B) are negotiating a session key. They both share a long term *symmetric* key, K_{long}. The picture shows how the session key, K_{sess}, is computed. The random value, R, is sent as part of the handshake protocol and thus known to both A and B at the time of computation.

a) What would be a suitable algorithm, to use inside the box in the figure, i.e., how should f such that $K_{\text{sess}} = f(K_{\text{long}}, R)$ be chosen?

b) Suggest a reasonable handshake protocol that provides *implicit key authentication* and *unilateral authentication*, using the long term symmetric key.

(1+2 points)

Problem 3. The TLS handshake protocol protects against replay attacks. Explain how this is achieved. (3 points)

Problem 4. The IP header includes a 16-bit checksum. Basically, you take the header and divide it into 16-bit words and add these together. The checksum is the complement of this sum. However, the details are irrelevant to this problem.

a) Does this checksum provide integrity protection? Motivate your answer!

b) Assume that, instead of this checksum, a modern state-of-the-art hash function is used. How would this affect the integrity protection in the presence of a man-in-the-middle? Motivate your answer!

(1.5+1.5 points)

Problem 5. PGP uses the notions *validity* and *trust*.

a) When Alice signs Bob's public PGP key, what happens to the *trust* and *validity* of Bob's public key?

b) Further, assume that Bob has signed Charlie's public key. What is required in order for Alice to use Charlie's public key with very high confidence that the key is actually Charlie's?

(1+2 points)

Problem 6. Consider an executable file in Linux with the following permissions

```
-rwsrws--x 2 10 Alice Students prog
```

Assume that the user Bob successfully executes the program. List the different IDs that are associated with the running process and determine their values. (3 points)

Problem 7. When authenticating to a computer or web service, a user often submits a password. How should, according to best practice, the password-related information be treated by the computer or web service? (3 points)

Problem 8. Compare how functionality and assurance are treated in Orange book and Common Critera evaluations. (3 points)

Problem 9. Consider the Bell-LaPadula state below.

Current acces set, b

(Alice, file_b, w)
(Alice, file_a, r)
(Charlie, file_e, a)
(David, file_c, r)
(Erika, file_d, w)

Access Control Matrix, M

	file_a	file_b	file_c	file_d	file_e
Alice	r,w,a	r,w		e	a
Bob			a	r,e	
Charlie	r	r		r	r,e
David			r,w,a	r	r,w
Erika	a			r,w,e	

Functions, $f = (f_S, f_C, f_O)$

f_S:

Alice: (private {A,B}), Bob: (public, {A,B}), Charlie: (private, {A}), David: (private, {A,B}), Erika: (private, {A})

f_C:

Alice: (private, {∅}), Bob: (public, {A,B}), Charlie: (public, {B}), David: (public, {A,B}), Erika: (public, {∅})

f_O:

file_a: (private, {A}), file_b: (private, {∅}), file_c: (public, {A,B}), file_d: (public, {A,B}), file_e: (private, {A,B})

Assume that we have a lattice with two classifications, public and private, and two categories, A and B. These are used in the Bell-LaPadula model. Determine which security properties are broken and motivate why they are broken (if any). (3 points)

Problem 10. In WEP, a challenge-response protocol based on a stream cipher (RC4) was used. What was the fundamental flaw in this protocol? (3 points)

Problem 11. Several well-known antivirus products install a CA certificate on the user's computer. This is used to mount a man-in-the-middle attack on TLS connections involving the computer.

a) Explain how the attack is performed and why it succeeds.

b) Why would an antivirus product mount an attack like this on the user?

(3+2 points)

Problem 12. The buffer overflow attack is still one of the most common attacks. Both the attack and mitigation techniques have evolved since its first discovery.

a) What is the purpose of introducing NOP instructions in the program code in a buffer overflow attack?

b) What is a canary value and how does it protect against the attack?

c) How does ASLR make the attack more difficult?

(2+2+1 points)

Problem 13. RSA is based on the problem of factoring large numbers. The public parameters of an insecure RSA scheme are:

- Modulus: $n = 221$
- Public exponent: $e = 7$

Recall that, in RSA, the private exponent d is chosen such that $e \cdot d \equiv 1 \mod \phi(n)$. Find d and decrypt the ciphertext $c = 2$.

The following table might be helpful:
$2^2 \equiv 4 \mod 221$
$2^4 \equiv 4^2 \equiv 16 \mod 221$
$2^8 \equiv 16^2 \equiv 35 \mod 221$
$2^{16} \equiv 35^2 \equiv 120 \mod 221$
$2^{32} \equiv 120^2 \equiv 35 \mod 221$

(5 points)

Problem 14. Explain shortly the following five terms:

a) HMAC

b) ECB mode for block ciphers

c) Encapsulating Security Payload (ESP)

d) Honeypot

e) Reference monitor

(5 points)
