Final exam in

Computer Security EIT060

Department of Electrical and Information Technology
Lund University

March 15, 2017, 8-13

- 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. The brute force attack is one possible method of attacking ciphers.

a) What is a brute-force attack?

b) Why is it not possible to mount a brute force attack on the one-time-pad (OTP)?

(3 points)

Problem 2. Give three examples of protections against *buffer overflow* attacks and explain how they protect against the attack. (3 points)

Problem 3. You have been given the task to design a *password hashing* scheme. Explain and motivate some important features of your scheme and compare them to something like plain SHA-1 or MD5. (3 points)

Problem 4. In Linux, consider a file with protection mode 640 contained in a directory with protection mode 755. Both file and directory has user owner Alice and group owner Students.

a) Who can read the file?

b) Who can delete the file?

c) Who can list the directory?

(1+1+1 points)

Problem 5. What are FRR, FAR and EER in the context of biometric systems? Imagine that biometric authentication is used to activate a missile launch and the activation button is placed in a public place. How would you choose the threshold in the biometric scheme? Motivate your answer. (3 points)

Problem 6. 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 7. Explain to which extent the UMTS key agreement and authentication protocol provides nonrepudiation. (3 points)

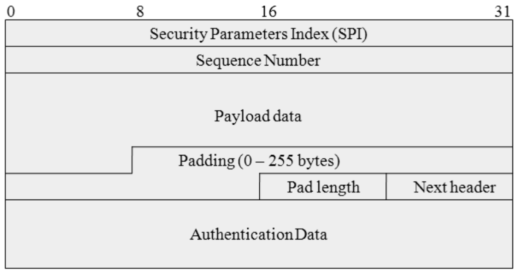
Problem 8. The WEP protocol had an intention to provide *Confidentiality*, *Integrity* and *Authentication*. However, it failed in all three cases. Explain briefly how for each case. (3 points)

Problem 9. 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 conflict. (3 points)

Problem 10. 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.



(1+2 points)

Problem 11. The TLS handshake can use both RSA and Diffie-Hellman. In this problem, we will focus on how they are used to establish a shared secret. No client authentication is assumed and you are not required to name the handshake messages.

a) How is the (pre-master) secret established when RSA is used?

b) How is the (pre-master) secret established when Ephemeral Diffie-Hellman is used?

c) Assume that an attacker has eavesdropped and recorded several subsequent handshakes and communication sessions involving the same server. At a later point in time, the private key of the server is leaked to a public forum by a pissed off employee. Is the attacker able to use this private key in order to decrypt the recorded communication? Your answer must analyze both RSA and Ephemeral Diffie-Hellman in this regard.

(1+1+3 points)

Problem 12. Consider the Bell-LaPadula state below.

Current acces set, b

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

Access Control Matrix, M

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

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

f_S:

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

f_C:

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

f_O:

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

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.

a) For each Bell-LaPadula security property, determine if it is broken or not. Motivate your answer.

b) The Biba model introduces dynamic levels, which means that levels can be adjusted after reading or modifying. Give an example of this in the Biba model and explain why dynamic levels are not appropriate for the Bell-LaPadula model.

(3+2 points)

Problem 13. It has been known for about a decade that it is possible to find collisions in SHA-1 faster than the birthday bound. However, until recently, a real collision has not been found. On February 23, 2017, at last, the first real collision between two documents were presented. Explain how a SHA-1 collision can be used to mount a man-in-the-middle attack on TLS. (5 points)

Problem 14. Explain shortly the following five terms:

a) A5/1
b) Traffic analysis
c) Unilateral authentication
d) Second Preimage Resistance
e) X.509 (5 points)
