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)?

Answer
a) It is an attack in which the attacker tests all different keys in order to determine which one is correct.
b) The attack requires that it is possible to verify that a certain key is correct. For the OTP, all plaintexts have the same probability of being correct so it is not possible to verify the correctness of keys. (3 points)

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

Answer
Some protections include:
Canary: A word placed before the return address in the stack frame.
Randomizing stack address: Makes it difficult to predict where the stack starts and thus

to point the return address to the desired piece of code.
Check input: Make sure that the size of any input to a program is not larger than the buffer it is put into.
Avoid vulnerable languages: Buffer overflow are not possible in Java due to checks made by the virtual machine.
Check source: There are software tools available that checks for security problems in the source code.
Mark the stack as non-executable: Some CPUs support the use of an NX-bit, which the operating systems can use to mark areas of the memory as non-executable. (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.

Answer
* The function must be slow in order to make brute force attacks more time consuming. MD5 and SHA-1 are designed to be fast which is inappropriate for password hashing.
* The function should also be adaptive such that the function can be made slower if needed.
* The function must accept a salt in order to hash identical passwords to different hash values and to protect against TMTO attacks.
* The function should also be difficult to accelerate using fast hardware, e.g., graphics cards or FPGAs. This can be done by requiring the use of a large amount of memory in the hash function. (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?

Answer
a) Alice and everyone in the group students
b) Alice
c) Everyone (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.

Answer
FRR: False rejection rate. The probability that a legitimate user is rejected.
FAR: False acceptance rate. The probability that a wrong user is accepted.
EER: Equal error rate. The error probability when FRR=FAR.

In the given application the threshold should be set very high so there are no false positives. False negatives are less of a problem. (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 $d \cdot e \equiv 1 \bmod \phi(n)$.

Answer
By factoring n we get $p = 17$ and $q = 23$. Thus, $\phi(n) = 16 \cdot 22 = 352$. With $d \cdot 7 = k \cdot 352 + 1$, and testing different k we find that there is a solution when $k = 3$, namely $d = (3 \cdot 352 + 1)/7 = 151$. (3 points)

Problem 7. Explain to which extent the UMTS key agreement and authentication protocol provides nonrepudiation.

Answer
Only symmetric cryptography is used in the UMTS key agreement and authentication protocol so there is no nonrepudiation provided at all. (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.

Answer
Confidentiality: The usage of the IV in the stream cipher is flawed. Also the IV is too short.
Integrity: The integrity algorithm used is linear. Since a stream cipher adds the keystream linearly to the message it is possible to modify the message and correctly compute a new integrity check value even though the message is encrypted.
Authentication: The challenge response scheme uses a stream cipher to encrypt the response. By eavesdropping one authentication, it is easy to obtain the keystream and then authenticate as that user at any time. (3 points)

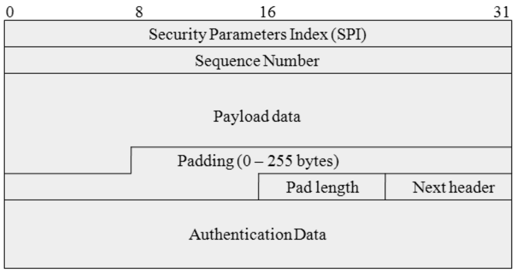
Problem 9. Allowing users to be put into groups can simplify access control. However, *policy conflicts* have to be dealt with. If a user has one set of permissions on a file, but a group that the user is a member of has another set of permissions, a decision has to be made what permissions will be effective. Compare how Windows and Linux deal with this type of policy conflict.

Answer
In Windows, if a user has one set of access rights and the user is member of a group with another set of access rights, the user will be given the union of all access rights. In Linux, if the user is the owner of the file, the access rights of the owner are the ones that determine his access. Any group access rights will not be checked at all even if the user is a member of the group that is group owner of the file. (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.



Answer
a) The payload data, padding, pad length and the next header field.
b) In transport mode, the original IP header is placed before the ESP header, i.e., before the data represented by the packet in the figure. In tunnel mode, the original IP header is part of the payload data in the figure. (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.

Answer
a) The client generates the pre-master secret and encrypts it with the public key of the server. The server uses the corresponding private key to decrypt the secret.
b) The client and the server computes their DH-values, $x^a \bmod p$ and $x^b \bmod p$ and exchanges values. The server signs the values uses its private key. The client verifies the signature. Both can compute the shared value, $x^{ab} \bmod p$.
c) In the case of a RSA handshake, the attacker can take the recorded encrypted pre-master secret and decrypt it using the leaked private key. The pre-master secret can be used to derive all communication keys, which allows the attacker to decrypt communication. In the DH handshake case, the server's values are signed using the private key, which means that the attacker can pose as the server in upcoming handshakes. However, it is not possible to decrypt previous traffic since the private key has not been used to decrypt sensitive information. (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.

Answer
a)
ss-property: This property is not broken since the subject security level dominates the object security level in all read and write access operations.
***-property:** Erika reads file_b with security level (private, {∅}) and is at the same time appending to file_d with security level (public, {A,B}). This is not allowed since it would enable information to flow from (private, {∅}) to (public, {A,B}).
ds-property: David is not allowed to write to file_c according to the access control matrix. This violates this property.
b)
In Biba, if e.g., Alice with security level (private {A,B}) reads a file at a lower level, say (public {A}), Alice's level will be adjusted such that her new lever will be the greatest lower bound of the two levels, i.e., (public {A}). This will be ok since the level will only indicate how much trust we have in Alice to provide accurate information. In Bell-LaPadula, the corresponding situation would be Alice at security level (public {A}) reading a file at a higher level, say (private {A,B}). Then we would either have to lower the file's level or increase Alice's level. As we deal with confidentiality, both alternatives are unreasonable. (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.

Answer
A digital certificate uses a digital signature in order for a CA to sign the link between a public key and a server identity. If the CA has used SHA-1 as hash function in the signature algorithm, it could be possible (although computationally very expensive) to create two certificates with colliding hashes. One real and one fake. Since the hashes collide, the CA signature will be the same. Now the attacker has the private key corresponding to a certificate "owned" by another server. In the TLS handshake, the attacker can act as a man-in-the-middle and replace the real certificate with the fake one as it is sent from the server to the client. In the case of RSA, the MitM can decrypt the pre-master secret and in the case of Diffie-Hellman the MitM can make signatures as if he was the real server in the communication. (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

Answer
a) The stream cipher used in GSM
b) Analysing data traffic in order to determine who is talking to who and when, regardless of encryption.
c) Only one of the communicating parties is authenticated.
d) In the context of hash functions, when given an input x it is computationally difficult to find another input x' such that the resulting hash value is the same for both, i.e., $h(x) = h(x')$.
e) A standard for digital certificates. (5 points)
