Final exam in

Computer Security EITA25

Department of Electrical and Information Technology
Lund University

March 22, 2019, 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. Assume that we have the, probably familiar, situation in which we make a secure TLS connection between two computers, one client and one server. Both the client and the server has a public/private key pair and a certificate signed by the same CA, which in turn also has a public/private key pair. Thus, there are in total 6 keys involved, 3 public and 3 private keys. Explain for each of these keys its involvement when the secure connection is being set up. Assume that RSA is used and that the client is authenticated in the handshake.

Answer

CA private key: Used to sign the client and server certificates that are used in the connection.

CA public key: Used to verify the signature in the client and server certificates so that these can be trusted.

Client private key: Used to sign previous messages in the handshake in order to prove that the client is in possession of the private key.

Client public key: Given in the client's certificate and used by the server to verify the signature above.

Server private key: Used by the server to decrypt the premaster secret.

Server public key: Given in the server's certificate and used by the client to encrypt the premaster secret. (3 points)

Problem 2. When encrypting information with a block cipher, it is not enough to have a secure block cipher. Explain how information can leak if the cipher is not used in a secure mode of operation.

Answer
If each block is encrypted independently of other blocks, then redundancy in the plaintext is preserved in the ciphertext. This is the case for ECB-mode, while in e.g., CBC-mode a ciphertext block will be used to modify the next plaintext block before it is encrypted. This will remove such redundancy in the ciphertext. (3 points)

Problem 3. Let P be a password. Explain why

$$h = \text{SHA-1}(P)$$

is not a suitable way of storing authentication information on a server or in an operating system.

Answer
Looking at the requirements and best practices for hashing passwords, just applying SHA-1 does (1) not provide any salt to the hashing, (2) result in a slow hash function and (3) does not consume significant amount of memory in order to make hardware acceleration infeasible. (3 points)

Problem 4.

a) Describe the difference between a threat and a vulnerability.

Give an example of

b) a threat to data integrity

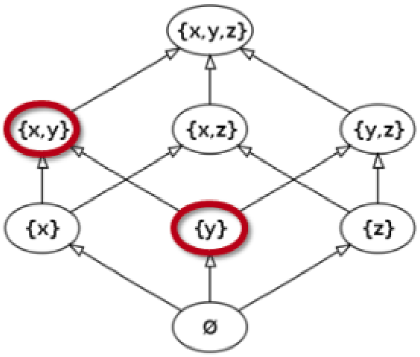
c) a vulnerability affecting data integrity

Answer
a) A threat is a potential event that can occur and that will lead to loss of confidentiality, integrity and/or availability. A vulnerability is an actual problem that has been identified that can be used to realize a threat.
b) A threat to data integrity could be that an important file is removed from a system.
c) A vulnerability could be that a programming error results in a MAC of data sent over a channel is not properly verified by the receiver. This would allow anyone to modify the data without detection. (1+1+1 points)

Problem 5. Consider the lattice below, which can be used in Mandatory Access Control.

a) Determine the Least Upper Bound and the Greatest Lower Bound of the two elements {y} and {x,y}.

b) Using this lattice as an example, explain how labels are allowed to change when dynamic integrity levels are used in the Biba model. Given one example when a user reads an object, and one example when a user writes to an object.



Answer

a) The Least Upper Bound is the label {x,y} and the Greatest Lower Bound is the label {y}.

b) In Biba, information is only allowed to flow downwards. When a user reads an object, information flows from the object to the user. Thus, if a user with label, say, {x,y} reads an object with label {y}, the user's label will be adjusted to {y}. On the other hand, if a user with label {x,y} writes to an object with label {y,z}, the object's label will be updated to {y}.

(1+2 points)

Problem 6. An IDS can be based on signature or anomaly detection. Highlight

a) the main differences between the two approaches,

b) the main advantages of signature based detection (compared to anomaly detection),

c) the main advantages of anomaly detection (compared to signature based detection).

Answer

a) Signature detection relies on a database with known attack patterns, while anomaly detection compares the current usage with a known baseline. If the usage deviates from the baseline, an attack is considered detected.

b) Signature detection will be better att detecting already existing attacks and will do that with less false positives/negatives.

c) Anomaly detection will be better at detecting new unknown attacks. Also, it does not have to keep an updated database of known attack patterns.

(1+1+1 points)

Problem 7. The most well-known application of Time-Memory-Tradeoff attacks is to recover a password from its hashed form. However, the attack is much more general than that. Explain how a Time-Memory-Tradeoff approach can be used to conduct a chosen-plaintext attack on a block cipher. It is sufficient that you explain the offline phase of the attack.

Answer

The TMTO attack can be used to "invert" a one-way function. Assuming that the plaintext is fixed, a block cipher can be seen as a one-way function with the key as input and the ciphertext as output. A table is built by picking a random key and computing the ciphertext. Then, the ciphertext is mapped to a new key using a reduction function. A new ciphertext is computed with the new key, again mapping the ciphertext to a key. This is done t times. Then a new random key is chosen and the procedure is repeated. This is done for m random keys, which gives a table that covers $t \cdot m$ keys in total. In order to avoid colliding chains, a new table with a new reduction function is computed when $N = t^2m$. This will required approximately t tables in total. (3 points)

Problem 8. Canaries, ASLR and $W \oplus X$ are three well known and widely used protections against buffer overflow attacks. Explain each of these defense mechanisms and why they protect against the attack.

Answer
A canary is a known value that is placed on the stack before the returns address. The program can verify the integrity of this value before redirecting the program to the address pointed to by the return address. This is used to detect if the return address has been overwritten. ASLR is a technique used to randomize the start address of e.g., the stack and libraries in the memory. It is used to make it more difficult to guess these addresses and thereby making it more difficult to change the program flow to a predetermined code snippet in memory. $W \oplus X$ will mark memory pages as either writeable or executable. The idea is that the stack should be writeable, but there should not be any code on the stack, so it does not have to be executable. This will make it impossible to inject code on the stack and redirect the program flow to that code. (3 points)

Problem 9. The two most important protocols in TLS are the handshake and the record protocols.

a) Explain to which extent the handshake protocol supports *perfect forward secrecy.*

b) Explain to which extent the record protocol supports *non-repudiation.*

Answer
a) The handshake protocol supports perfect forward secrecy if Diffie-Hellman is used for key establishment, but not if RSA is used.
b) The data on the record protocol is protected by a MAC, and since this is a symmetric algorithm, this does not have the nonrepudiation property (both sender and receiver share the key used to compute the MAC). (1.5+1.5 points)

Problem 10. Assume that the value for *umask* in a Linux operating system is `027`.

a) What will be the permissions for a newly created file?

b) What will be the permissions for a newly created directory?

Answer
file: rw-r—–
dir: rwxr-x— (1.5+1.5 points)

Problem 11. The Needham-Schroeder protocol is given below. S is a trusted third party, A is a client and B is a server.

$$\begin{array}{lll}
1. & A \rightarrow S: & A, B, n_a \\
2. & S \rightarrow A: & eK_{as}(n_a, B, K_{ab}, eK_{bs}(K_{ab}, A)) \\
3. & A \rightarrow B: & eK_{bs}(K_{ab}, A) \\
4. & B \rightarrow A: & eK_{ab}(n_b) \\
5. & A \rightarrow B: & eK_{ab}(n_b - 1)
\end{array}$$

a) Identify all long-term keys.

b) What is the purpose of messages 4 and 5?

c) Is 2048-bit RSA a suitable encryption scheme for the above protocol? Motivate your answer.

d) Which problem with this protocol was fixed in the Kerberos protocol and how was it fixed?

Answer
a) K_{as} is a long-term key shared by A and the trusted third party. K_{bs} is a long-term key shared by B and the trusted third party.
b) To authenticate A to the server B.
c) No, RSA is an asymmetric encryption scheme. This variant of Needham-Schröder requires a symmetric cipher.
d) The problem is that the session key K_{ab} is not guaranteed to be fresh. If an adversary can break this session key then it is possible for someone claiming to be A to enter the protocol at step 3 and renegotiate the same session key with the server B. Kerberos addresses this by including timestamps in the protocol to make sure that the key K_{ab} is a fresh key.

(1+1+1+2 points)

Problem 12. Explain how access tokens, security descriptors, ACEs and the reference monitor are involved when a subject accesses an object in Windows.

Answer
When the process started it received a copy of the user's access token. This access token has information about the process owner and groups that the owner belongs to. When requesting access to an object, the reference monitor was invoked. The reference monitor is responsible for checking the access and it is not possible to get access to anything without involving the reference monitor. The object has a security descriptor which, most importantly in this case, has a discretionary access control list (DACL). This is actually a list of access control entries (ACEs) that is traversed from the beginning until write access is granted to the process, stopping the search granting access, or until write access is explicitly denied, stopping the search denying access, or until we reach the end when access is denied. In this case there were clearly an ACE granting the user, or a group that the user belongs to, access to the object. (5 points)

Problem 13. Challenge response protocols are commonly used for authentication in a network setting. In 2018, an authentication related vulnerability was reported in the

Apache web server. The nonce used in a challenge response protocol was not random enough.

a) Describe an attack that takes advantages of repeated nonces in a challenge response protocol.

b) The authentication protocol used in WEP had a related, but worse, problem. What was the problem and how was it worse?

Answer

a) The response is typically based on the challenge and a secret shared value (key/password). If a nonce is repeated the expected response will be the same. Thus, by eavesdropping a challenge/response pair, it is possible for an attacker to use the saved response for subsequent challenges with the same nonce, without knowing the secret.

b) In WEP, the response was computed by encrypting the challenge with a stream cipher, i.e., the challenge was XORed with the keystream to form the response. An eavesdropper with access to a challenge/response pair could compute the corresponding keystream. Since the IV for the stream cipher was chosen by the sender, it was possible to send a response to *any* challenge, using the computed keystream. (2+3 points)

Problem 14. Explain shortly the following five terms:

a) RSA

b) Message Authentication Code

c) Second pre-image resistence

d) ABAC

e) Encapsulating Security Payload

Answer

a) RSA is a public key algorithm that can be used for both encryption and digital signatures.

b) A MAC is a symmetric integrity algorithm that computes a checksum based on data and a key.

c) Given x and $y = h(x)$, it is difficult to find $x' \neq x$ such that $y = h(x')$.

d) Attribute-based access control is when the access to an object is based on attributes of both the subject and the object, but also possibly on the environment, e.g., date and time.

e) An IPsec protocol that allows for both encryption and integrity protection of data at the IP layer. (1+1+1+1+1 points)
