Final exam in

Computer Security EIT060

Department of Electrical and Information Technology
Lund University

March 12, 2014, 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. Describe the connection between the terms authentication and accountability.

Answer
Authentication is the process of validating the identity of a principals/subjects. Accountability is the use of audits in order to trace actions to the responsible party. Without authentication, accountability is ineffective since it is not possible to identify the responsible party. (3 points)

Problem 2. You have seen and experimented with the time-memory tradeoff attack for hash functions. Explain how such attacks can be used to attack a block cipher in a chosen plaintext scenario. You only have to describe the offline phase in which the tables are precomputed.

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 3. What is the purpose of address space layout randomization (ASLR)? Which types of attacks is it designed to prevent?

Answer
The purpose is to randomize certain memory addresses so that they are difficult for attackers to guess. Examples of such addresses is the start address of the stack and the start of the data section in the virtual memory. This makes it much more difficult to mount buffer overflow attacks since these typically require that the return address is changed to a specific location in the virtual memory. (3 points)

Problem 4. How do Unix and Linux support controlled invocation?

Answer
It is supported by using setuid bits for executable files. When starting a program with the executable bit set, the effective UID of the process will be that of the file owner. This results in the process having the access rights of the file owner, which allows the file owner to give a process other access rights that it would otherwise have. Thus, it is possible to give other users, through a program, controlled access to files and resources that they would otherwise not have. (3 points)

Problem 5. In Windows, access control is determined both by access rights and privileges.

a) Who assigns privileges?

b) Who assigns access rights?

c) Where are they stored?

Answer
a) The administrator of the computer.
b) The owner of an object.
c) Privileges are stored in an access token and access rights are stored in a security descriptor associated with the object. (1+1+1 points)

Problem 6. SSL/TLS consists of several protocols, where the handshake and record protocols are the most interesting from a security point of view.

a) Does the record protocol offer *non-repudiation*? Motivate your answer.

b) How does the handshake protocol protect against *replay attacks*?

Answer
a) No, since a MAC is used for message authentication. A MAC requires a shared key between sender and receiver so non-repudiation is not possible.
b) New random numbers are used in the client hello and server hello messages. Since the finished messages include these random numbers it would not be possible to reuse the encrypted finished messages in a replay attack. (1+2 points)

Problem 7. Linux typically uses two separate files for storing information about users and their account, namely, the `/etc/passwd` file and the `/etc/shadow` file.

a) Why are two files used instead of putting all information in one file?

b) What *type* of information is stored in the two files?

Answer
a) This allows a separation of information that should not be hidden from users and normal processes and information that should be hidden.
b) In the /etc/passwd file, non-sensitive information is stored, e.g., full name, default shell, UID. In the /etc/shadow file, the hashed password is stored, together with specific information about the account, e.g., password expiration. (1.5+1.5 points)

Problem 8. PGP/GPG uses a combination of symmetric and asymmetric cryptography in order to encrypt emails.

a) Explain how this hybrid encryption is used.

b) In PGP/GPG, what is the purpose of combining symmetric and asymmetric algorithms like this?

Answer
a) A symmetric cipher is used to encrypt data, i.e., the email. An asymmetric cipher is used to encrypt the symmetric key, using the recipient's public key.
b) It allows public keys of a recipient to be used when sending an encrypted email. This avoids sharing symmetric long term keys with each user. At the same time, it allows efficient encryption and decryption of long messages since asymmetric encryption/decryption is very slow compared to symmetric algorithms. (1+2 points)

Problem 9. A *packet filter* is a firewall that looks at internet packets and determines if they are allowed to pass or not. The decision is based on source/destination IP address and source/destination port. All packets are examined individually and independently of each other.

a) What is the limitation of this approach?

b) What is a *stateful packet filter*?

c) How do the two types of packet filters differ from an *application level proxy*?

Answer
a) Since client programs often pick random source ports, the firewall does not know which port is chosen by the client and must thus allow all possible incoming ports (those that can be chosen by clients, typically > 1023).
b) A stateful packet filter solves the above problem by keeping a state of active connections. Incoming packets are checked against the state and only if the destination IP/port has been used before as a source IP/port, the packet is allowed to pass.
c) In an application level proxy, packets are examined at the application level. The proxy can look at the data of packets and make decisions based on that. It also sets up a new connection to the end machine so that traffic seems to be coming from the proxy instead of the actual source. (1+1+1 points)

Problem 10. The Bell-LaPadula security model is the most well known security model. It supports both mandatory and discretionary access control.

a) Explain how mandatory access control is enforced in the model.

b) Explain how discretionary access control is enforced in the model.

Answer
a) Mandatory access control is enforced by the ss-property, stating that read access is limited to subjects with security label that dominates the object's security label, and the *-property, stating that append access is limited to subjects with security label that is dominated by the object's security label.
b) Discretionary access control is enforced by the ds-property, stating that all granted access must be allowed in the access control matrix. (2+1 points)

Problem 11. The Kerberos protocol is given below.

1: A, TGS, n_a

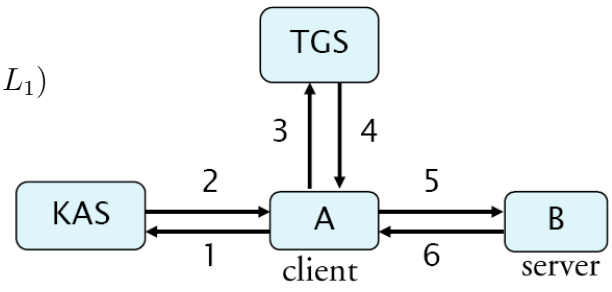
2: $eK_{as}(K_{a,tgs}, n_a, L_1, TGS), eK_{tgs}(K_{a,tgs}, A, L_1)$

3: $eK_{tgs}(K_{a,tgs}, A, L_1), eK_{a,tgs}(A, T_a), B, n'_a$

4: $eK_{a,tgs}(K_{ab}, n'_a, L_2, B), eK_{bs}(K_{ab}, A, L_2)$

5: $eK_{bs}(K_{ab}, A, L_2), eK_{ab}(A, T'_a)$

6: $eK_{ab}(T'_a)$



a) How does KAS authenticate A?

b) How does B authenticate A?

c) What is the purpose of L_1 and L_2? Describe an attack that would be possible if L_2 was removed.

Answer
a) The authentication is implicit. A is authenticated by being able to properly decrypt the session key that will be used with the TGS.
b) A uses the session key K_{ab} to encrypt a time stamp and sends this to B in step 5. Only the holder of K_{ab} will be able to encrypt a valid timestamp.
c) These are timestamps that control for how long time session keys are valid. If these were not used, a broken session key would allow a replay attack. Consider the case when the timestamp L_2 is removed. An attacker could enter the protocol at step 5, sending the encrypted session key to B together with a new valid authenticator and properly authenticate to B. (1+1+3 points)

Problem 12. In this problem we look at some different aspects of cryptography.

a) In RSA, a message is encrypted as $c = m^e \bmod n$ and decrypted as $m = c^d \bmod n$. A standard choice for e is 65537 $(2^{16} + 1)$, which is 10000000000000001 in binary notation. This allows for efficient encryption since the speed of the algorithm used for exponentiation depends on the number of ones in the exponent. If we want fast decryption instead, could we instead choose d to be 65537 then? Why or why not?

b) How many hash function invocations are needed to find a collision in a (secure) hash function? How many are needed to find a second preimage?

c) What would be a typical choice of keysize for a stream cipher?

Answer
a) Mathematically, it would be possible. Since $e \cdot d = 1 \pmod{\phi}(n)$, we could just as well pick a d with desirable properties and then compute the resulting e. On the other hand, d is part of the private key and should not be chosen as such an easily guessable value. That would make the cipher easily breakable.
b) Let n be the number of bits in the hash value. For a collision, approximately $2^{n/2}$ hashes are needed. For a second pre-image, approximately 2^n hashes are needed.
c) Typical keysizes for symmetric primitives is 64-256 bits. (Anything in this range would be a correct answer. A number outside this range must be very well motivated in order to be seen as correct.) (2+2+1 points)

Problem 13. A challenge response scheme can be used to authenticate a client to a server on a network.

a) What is the main feature of a challenge response scheme compared to just sending the password?

b) Why should a nonce be used in challenge response authentication?

c) The challenge response protocol in WEP shared key authentication was/is insecure. Explain the weakness.

Answer
a) In a challenge response scheme the password is not sent in plaintext on the network.
b) If a challenge is repeated, a replay attack using a recorded response would be possible since nonces by definition never repeat.
c) It used a stream cipher when encrypting the challenge. With a stream cipher, the response would be keystream $\oplus$ challenge. Since the challenge is known, the keystream can be computed after seeing a corresponding response. This keystream can be reused later to authenticate an attacker. The attacker can just claim to have used the same IV as was used in the eavesdropped authentication. (1+1+3 points)

Problem 14. Explain shortly the following five terms:

a) EAL
b) Security Parameters Index
c) Protection profile
d) Kerckhoffs' principle
e) Implicit key authentication

Answer
a) The assurance level used in common criteria. It indicates to which extent a product has been evaluated.
b) Integer used in IPsec to inform which keys and algorithms that should be used to decrypt a packet.
c) A document stating generic security requirements and functionality that should be met in a certain type of product (in common criteria).
d) A principle stating that only the key should be assumed unknown to an attacker. The algorithm and its implementation should be considered known.
e) The property in a key establishment protocol when one party knows that no one besides another identified party can have access to the shared key. (5 points)
