PRACTICE QUESTION 1

SECURITY, ATTACK AND MITIGATION

1. **Explain how public key cryptography may be used for identification. [4 marks]**

Public-key cryptography may be used for identification as follows:

- If Bob wants to identify himself to Alice he asks Alice for a random number
- Bob encrypts this random number with his private key and sends the cipher text to Alice
- Alice decrypts the cipher text using Bob's public key and compares the result with the number she sent.
- If there is a match then she accepts this as proof of identity.

For this challenge response system to work Alice must be sure that she has the authentic public key of Bob.

2. **Describe how a man-in-the-middle attack may be performed on a Wi-Fi network and the consequences of such an attack. [10 marks]**

Wi-Fi is a wireless technology that provides simple broadband access using a laptop and an access point to which the laptop has authenticated itself.

Suppose an attacker has a modified Wi-Fi card designed to intercept data. All information coming from the access points within wireless range can be read. Suppose an attacker wishes to authenticate to a corporate access point they should not be able to use.

In a man-in-the-middle attack the attacker sets up a bogus access point:

- The bogus access point identifies a real corporate access point in advance.
-

- When a corporate laptop sees the bogus access point and tries to associate to it the bogus access point copies all the messages it receives to the valid corporate access point, substituting its own Medium Access Control (MAC) address for the source address.
-
- The bogus access point copies all the messages received from the valid access point back to the mobile device again substituting its own Medium Access Control (MAC) address for the source address. This intervention is possible even when the data is encrypted and without the enemy knowing the secret keys.
-
- If the message content is encrypted very little can be achieved without some knowledge of the contents of the messages before they were encrypted. More can be achieved if the attacker is allowed to replay captured messages.
-

In particular, if a simple challenge response scheme were used for authentication by replaying captured messages the bogus access point could associate itself to the corporate access point.

3. **Explain how a man-in-the-middle attack on a Wi-Fi network can be defeated. [4 marks]**
   A man-in-the-middle attack on a Wi-Fi network can be defeated by requiring mutual authentication between the corporate user and the access point and providing protection against replay attacks. The security methods for Wi-Fi called Wireless Protected Access (WPA) and Robust Security Network (RSN/WPA2) do this.

4. **a) In general, there are three types of identity authentication tasks. List these tasks. [4 marks]**

In general, there are three types of identity authentication tasks which are:

- Identity authentication for something known, such as a password;
- Identity authentication for something possessed, such as a smart card;

- Identity authentication for some personal characteristics, such as fingerprints.

b) Explain the role of the logic of authentication. [4 marks]

The logic of authentication formally describes the operation of an authentication protocol. It does this by formally describing the knowledge and the beliefs of the legitimate parties involved in authentication, and while analyzing the authentication protocol step by step, describes how their knowledge and beliefs change at each step. After the analysis, all the final states of the protocol are set out.

5. **a) An ideal password authentication scheme has to withstand a number of attacks. Describe five of these attacks. [10 marks]**

Any five of the following:

SR1. Denial of Service Attacks An attacker can update false verification information of a legal user for the next login phase. Afterwards, the legal user will not be able to login successfully anymore.

SR2. Forgery Attacks (Impersonation Attacks) An attacker attempts to modify intercepted communications to masquerade the legal user and login to the system.

SR3. Forward Secrecy It has to be ensured that the previously generated passwords in the system are secure even if the system's secret key has been revealed in public by accident or is stolen.

SR4. Server spoofing attacks Mutual authentication can help withstand the server spoofing attack where an attacker pretends to be the server to manipulate sensitive data of the legal users. Mutual authentication means the user and the server can authenticate each other. Not only can the server verify the legal users, but the users can also verify the legal server.

SR5. Parallel Session Attacks Without knowing a user's password, an attacker can masquerade as the legal user by creating a valid login message out of some eavesdropped communication between the user and the server.

SR6. Password Guessing Attacks Most passwords have such low entropy that they are vulnerable to password guessing attacks, where an attacker intercepts authentication messages and stores them locally and then uses a guessed password and seeks verify the correctness of their guess using these authentication messages.

SR7. Replay Attacks Having intercepted previous communications, an attacker can replay the intercepted messages to impersonate the legal user to login to the system.

b) Describe the goals an ideal password authentication scheme should achieve. [10 marks]

An ideal password authentication scheme should achieve the following goals:

- The passwords or verification tables are not stored in the system.
- The passwords can be chosen and changed freely by the users.
- The passwords cannot be revealed by the administrator of the server.
- The passwords are not transmitted in plain text over the network.
- The length of a password must be appropriate for memorization.
- The scheme must be efficient and practical.
- Any unauthorized login can be quickly detected when a user inputs a wrong password.
- A session key is established during the password authentication process to provide confidentiality of communication.
- The ID should be dynamically changed for each login session to avoid partial information leakage about the user's login message.

- The proposed scheme is still secure even if the secret key of the authentication server is leaked out or stolen.

6. **a) Describe the three main concerns with the use of passwords for authentication. Explain what is meant by a social engineering attack on a password. [4 marks]**

There are three main concerns with the use of passwords for authentication:

- Will the user disclose the password to another person intentionally, accidentally, or because they were deceived?
- Will the user be able to regularly enter the password correctly?
- Will users be able to remember their passwords or will they have to record them somewhere or choose easily guessed passwords? When an attacker obtains a password directly from its user by deceit the attack is known as social engineering.

b) Explain how attacks on passwords are broadly classified. [4 marks]

Attacks on passwords can be broadly classified as:

- A targeted attack on one account: The attacker tries to obtain a particular user's password.
- Attempt to penetrate any account on a system: The attacker tries to steal any password for the system, for example, by a dictionary attack.
- Attempt to penetrate any account on any system: This is when an attacker is seeking access to any system within a given domain.
- Service denial attack: An attacker may want to prevent a specific user from using the system.

c) Explain how access control lists are use to represent access control matrices. Describe the environments in which they are widely used and their advantages and disadvantages. [6 marks]

Access control lists are used to simplify access rights management by storing the access control matrix a column at a time along with the resource to which the column refers. ACLs are widely used in environments where the users manage the security of their own files such as Unix systems.

Their advantages are:

- Easy to understand
- Easily answer the question "who has what kind of access to this resource"
- Work well in distributed systems;
- Rights stored together with resources

Their main disadvantage is:

- May be inefficient. Determining rights may require searching a long list [6 ma

d) Suppose the following groups are defined to shorten a system's access control lists:

– Group1: Alice, Bob, Cynthia, David, Eve

– Group2: Alice, Bob, Cynthia – Group3: Bob, Cynthia

Suppose the access control list for File 1 is:

– File 1: Group 1, R; Group 2, RW If Alice wants to write to File 1 giving your reasoning state whether Alice will be allowed to do so if:
i) The first relevant entry policy is applied
ii) The any permission in list policy is applied Suppose the access control list for File 2 is: – File 2: Group 3, RWE
iii) Show how the need for a Group 3 for File 2 can be removed using access none. [6 marks]

The first relevant entry is Group 1 because Alice is a member of Group 1. Group 1 has read only access to File 1 son Alice has read only access to File 1. Alice is a member of Group 1 and Group 2. As Group 2 has read and write access to File 1, Alice has write access to File 1. The access control list for File 2 may be written:
– File 2: Alice, None; Group 2, RWE

7. **Describe how a one-way hash function may be used for message authentication.**

   In a symmetric key system, a one-way hash function is used as the fundamental component of a key dependent Hash-Based Message Authentication Code that takes as its input the whole message and outputs a message authentication code that is appended to the message. Only those with knowledge of the key may generate or check the message authentication code. In a public key system the message is input into a one way hash function the output of which is a message digest. A private key is used to encrypt the message digest to give digital signature which is attached to the message. The corresponding public key may be used to check the signature. An adversary will be unable to create a valid signature.