Assessment 4 2024.

1. The university is planning to implement a smart door locking system for computer labs. The system will allow authorized students and staff to enter the lab while preventing unauthorized individuals from gaining access. The smart door locking system is to be managed remotely, allowing administrators to control access and monitor entry logs in real time. You are tasked with analysing the security of this system and ensuring it is robust enough to handle potential threats.

a. Identify and explain any two potential security threats that could affect the smart door locking system in computer labs.

Interception - Unauthorised information disclosure

Here, unauthorized individuals may intercept (eavesdrop) communication between the smart door system and authorized users. If this happens, important information like credentials of users will be exposed and the confidentiality is therefore compromised.

~~b. Propose~~

Interruption - Unauthorised denial of use

Here, if an unauthorized individual gains access to the smart door, they might deny the authorised individuals the use of the computer labs. The services/data may become unavailable, unusable or may be destroyed. This will have a huge effect on the Availability (CIA) as interruption is mapped to the availability (Authorized users cannot access the lab when required)

Modification - (Unauthorised information modification

An intruder ~~may~~ might modify the access control files or override the authorization list to add their own credentials or unlock the door remotely without permission. This compromises the integrity of both the door control system and the access user data is violated.

b. Propose two possible security policy considerations that can address each of the identified threats from (a).

To address the interception security threat, Authentication can be used.

---

b Propose two possible security policy considerations that can address each of the identified threats from (a).

Authentication:

To address the interception security threat, authentication can be used to verify that only authorised users can gain access to the smart door locking system. This means that ~~der~~ confidentiality will be maintained.

~~Monitoring and Auditing~~

Monitoring and Auditing

To address the modification security threat, monitoring and auditing security mechanism can be used by actively monitoring who accesses the door in real time with the aim to detect any unauthorised intrusions. This will preserve the system's integrity and will ensure accountability.

2. How does the use of encryption techniques such as Symmetric and asymmetric cryptography contribute to ensuring Confidentiality and integrity in distributed systems?

Symmetric cryptography

Here the same key is used to encrypt and decrypt a mesage. It is also referred to as a secret key or shared key system, i.e., $K_{A,B}$ is a key shared by and A and B.

Asymmetric cryptography

The keys for encryption and decryption are different but together form a unique pair. One of the keys is kept private and the other is made public. For this reason, it is also referred to as public-key systems. These keys protect against message interception, modification. Without the proper key, the intruders cannot read ciphertex and without first decrypting the messages, no modifation can be done. This combination ensures confidentiality and integrity.

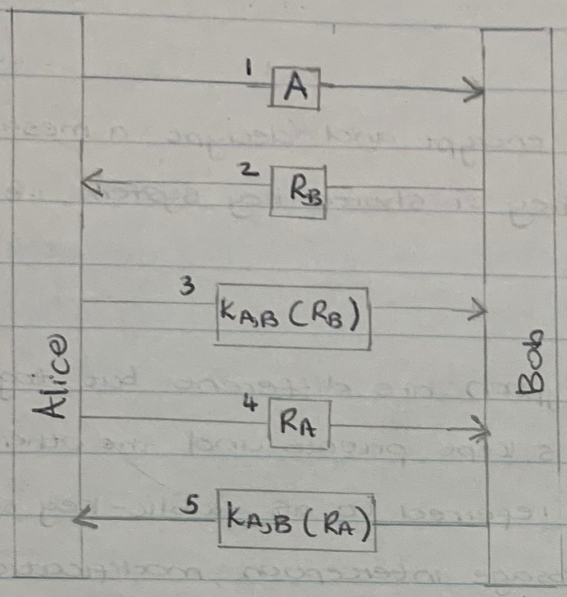
3. Why is it recommended to use session keys instead of long-lasting keys for confidentiality? (581)

Session keys are temporary, they are valid only during one communication session. (The session key is only valid as long as the channel exists). Therefore, session keys are recommended because if one key is compromised, it means only that particular session is affected.

Session keys are temporary key, they are valid only during one communication session (channel), when the channel is no longer used, the session key is safely discarded. An important reason for generating a unique key for each secure channel is to ensure protection against replay attacks, also, if a key for a particular session is compromised, only that session is affected.

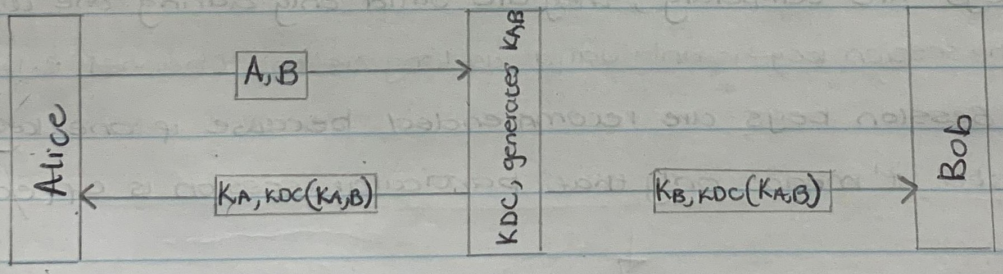
$K_{A,KDC}$ $K_{A,B}$.

4. What are the two possible implications of joining message 3 and message 4 in the authentication framework shown in the following figure?



Joining message 3 & 4 reduces the number of exchanges and speeds up the authentication processes, but it at the same time it weakens security, because it removes an important verification step that guarantee message freshness and identity confirmation.

5. Why is it not necessary in the following figure for the KDC to know for sure ~~it was taking~~ it was talking to Alice when it receives a request for a secret key that Alice can share with Bob?



The KDC does not need to verify Alice's identity because each user already shares a secret key with the KDC. When Alice requests a session key, the KDC encrypts the response using K_A, K_{DC}, which only the real Alice can decrypt. Even if an intruder pretends to be Alice, they cannot use the key without knowing this shared secret.

6. For each of the following scenarios, identify whether it is a Single-Factor Authentication (SFA) or a Multi-Factor Authentication (MFA). Provide explanations for each.

a. John logs into his company's email system by entering only his username and password. Sarah logs into her bank account online.

Single-Factor Authentication (SFA): This authentication is only based on one factor which is what she knows, his password and ~~he~~ username

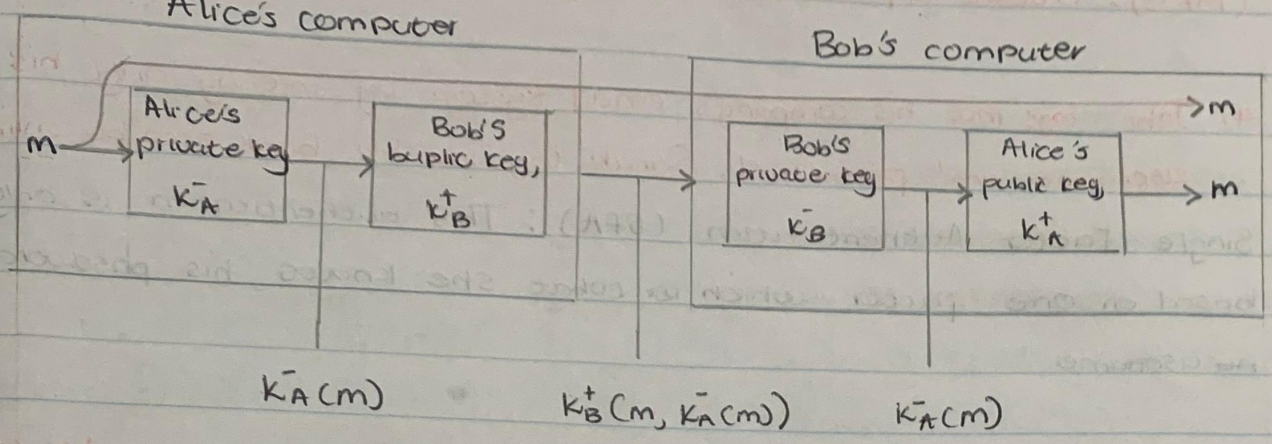
b. Sarah logs into her bank account online. After entering her username and password, she receives a text message on her phone with a verification code. She enters ~~this~~ this code to complete ~~the~~ login process.

Multi-Factor Authentication (MFA): This authentication is ~~only~~ based on what she knows which is her username and password and what she has, her cell phone (SMS code).

c. Emily accesses her workplace's secure system using a smart card that she swipes, along with a PIN code she must enter.

Multi-Factor Authentication (MFA): This authentication is based on what she has, the smart card for swiping and what she knows, the PIN code she used after swiping.

7. The following figure represents digitally signing a message using public-key cryptography. Explain the process depicted.



This process shows how Alice digitally signs and sends a secure message to Bob using public-key cryptography.

<u>One Alice's computer</u>

- The message (m) is initially signed using Alices private key (K_A^-) which creates a digital signature $K_A^-(m)$. This proves that ~~this~~ the message come from Alice. (ensuring authenticity)
- The signed message is then encrypted with Bob's public key (K_B^+) to ensure that Bob will be able to read it $K_B^+(m, K_A^-(m))$. (ensuring confidentiality)

<u>One Bob's computer</u>

- Bob decrypts the message using his private key K_B^- and gets $K_A^-(m)$
- Bob then verifies the signature by using Alice's public key K_A^+ to be able to retrieve the original message, m.

8. C - Confidentiality
   I - Intergrity
   A - Availability

9. Access rights of objects with reference to subjects are enforced using Access control Matrix approaches like the Access Control List and Capabilities. Discuss their differences.

Access Control List - This is where each object keeps a list of subjects and their respective rights. It is a column-wise implementation, making it easy to determine who can access a particular resource (object). (object-centred)

Capabilities - This distributes the matrix row-wise, giving each subject a list of the objects they are allowed to access and the operations they can perform. Each entry in this list is called a capability, and not having a capability for a resource means the subject has no rights to it. (subject-centred)

10. Discuss any two advantages and two disadvantages of using centralized servers for key management.

Assessment 4 2023

1. A financial institution wants to protect its distributed system infrastructure from potential security threats. Identify any three potential security threats that the institution should be aware of with an example.

Interception - Unauthorized information disclosure.
An intruder may intercept (eavesdrop) on the network traffic between a bank and its main server, capturing customer login or banking credentials and account numbers. This is a threat to confidentiality because essential information will be exposed.

Modification - Unauthorized information modification.
An intruder may tamper with the data or services, an example would be if a transaction request to transfer an amount of R100 is altered to transfer R10 000 before sending it to the server. This will be a threat to integrity

Interruption - Unauthorized denial of use
A denial of service (DoS) may flood the institutions web servers with traffic, this would make online banking service inaccessible to legitimate customers. This will be a threat to availability as the service or data becomes unusable, destroyed or unavailable.

2. Explain what a security policy is and then provide two security policy consideration that can be used in addressing each of the identified threats for 1 above.

A security policy describes precisely which actions the entities in a system are allowed to take and which ones are prohibited. It specifies who may perform, which actions, on which resources, under which conditions, and what must be audited.

To address interception

Encryption and authentication

Implementing a policy that mandates the use of encryption for all sensitive data. This will transform data into a ciphertext so attackers cannot understand, protecting it from interception. This will ensure that the confidentiality is maintained.

To address Modification (Integrity threat)

Encryption and Auditing

Implementing a policy that requires digital signature, which is the use of encryption, specifically public-key cryptography. The attacker will first need to decrypt the data, and if they do not have a proper key, modification will not be done. Also, a policy that uses auditing which will create a traceable record, allowing unauthorized modification to be detected and investigated.

To address interruption

4.) In the design of security for distributed systems, there are three primary design issues which are (a) focus of Control, (b) Layering of Security Mechanisms, and (c) Simplicity. Discuss these design issues.

(a) Layering of security mechanism - deciding at which level security mechanism should be placed. In this contex, a level is related to the logical organisation of a system into a number of layers.

(b) Focus of control. -

(c) Simplicity -

5. A college is implementing a new online learning platform where students can access lecture materials and submit assignment. How can the college employ security mechanism such as authorization and auditing to protect students data and ensure only authorized access?

Authorization: ; Implementing a Role-Based Access Control where the role of students is authorized to view and submit their own assignment and view or access lecture material while Lectures are authorised to upload lecture materials, delete, and grade submitted assignments.

Auditing : Implementing system logging that records who accessed the system, what resources they accessed, when they accessed it, and what action they performed. This will create an audit trail to detect and investigate any unauthorized access.

6. Suppose you were asked to develop a distributed systems application that would allow teachers to set up exams. Give at least two statements that would be part of the security policy for such an application.

- Only "authenticated teachers" may "set up" an "Exam" for cource(s) they are assigned to teach;

- Only "enrolled students" and "access (write & submit)" an "Exam" within the scheduled window from an approved device and location; the start time, end time, and all submitted answers must be audited.

7. Combining messages 3 and 4 in the authentication process reduces the number of exchanges and speeds up communication, but at the same time it weakens security because it removes important verification steps that ensure message freshness and identity confirmation. Normally, separate messages allow both Alice and Bob to validate each other's nonces (R_A and R_B) to confirm that each message is new and not reused from a previous session. When these messages are joined, Bob may no longer verify that the nonces are fresh, creating an opportunity for an attacker to replay old messages or impersonate one of the parties.