Unit 5

Authentication

MKK

Basic concepts

- Authentication can be defined as determining an identity to the required level of assurance. Authentication is the first step in any cryptographic solution.
- There is no use of encryption without authentication.
- We see authentication checks many times every day. We are required to wear and produce our identity cards at work, whenever demanded. To use our ATM card, we must make use of the card as well as the PIN.
- The whole idea of authentication is based on secrets. Most likely, the entity being authenticated and the authenticator both share the same secret (e.g. the PIN in the ATM example). Another variation of this technique is the case where the entity being authenticated knows a secret, and the authenticator knows a value that is derived from the secret.

Passwords

- Passwords are the most common form of authentication. A password is a string of alphabets, numbers and special characters, which is supposed to be known only to the entity (usually a person) that is being authenticated.

Something Derived from Passwords

- Several requirements need to be met to ensure that this scheme works correctly:
  - Each time the algorithm is executed for the same password, it must produce the same output.
  - The output of the algorithm (i.e. something derived from the password) must not provide any clues regarding the original password.

The Problems with Passwords

- Password maintenance is a very big concern for system administrators. A study shows that system administrators spend about 40% of their time creating, resetting or changing user passwords! This can truly be a nightmare for them.
- Organizations specify password policies, which mandate the structure of passwords. For instance, an organization policy could have some of the following policies governing the passwords of its users:
  - The password length must be at least 8 characters.
  - It must not contain any blanks.
  - There must be at least one lower-case alphabet, one upper-case alphabet, one digit and one special character in the password.
  - The password must begin with an alphabet.

MKK

Authentication Tokens

- An authentication token is an extremely useful alternative to a password. An authentication token is a small device that generates a new random value every time it is used.
- This random value becomes the basis for authentication.
- The small devices are typically of the size of small key chains, calculators or credit cards. Usually, an authentication token has the following features:
  - Processor
  - Liquid Crystal Display (LCD) for displaying outputs
  - Battery
  - (Optionally) a small keypad for entering information
  - (Optionally) a real-time clock
- Each authentication token (i.e. each device) is pre-programmed with a unique number, called a random seed, or just seed. The seed forms the basis for ensuring the uniqueness of the output produced by the token

MKK

Working of Authentication token

- Step 1: Creation of a Token
- Step 2: Use of Token
- Step 3: Server Returns an Appropriate Message back to the User

Types of Authentication Token:

- ***Response/Challenge Token***

  1. User sends a login request by providing only his user id and not the one-time password.

  2. Server checks whether the user id is valid. If it is not valid, it responds with an error message otherwise if it is valid, then the server creates a random challenge. Then sends the random challenge to the user.

  3. User receives the random challenge. Open the authentication token using the PIN and keys in the random challenge using the small keypad.

- ***Time-Based Token***

  In a time-based token, the server need not send any random challenge to the user. The token need not have a keypad for entry. In fact, it uses time in place of a random challenge. The tokens automatically generate a password every 60 seconds and display the latest password on the LCD output for the user.

Biometric Authentication

- Biometric-authentication mechanisms are receiving a lot of public attention. A biometric device works on the basis of some human characteristics, such as fingerprint, voice, or pattern of lines in the iris of your eye. The user database contains a sample of the user's biometric characteristics.
- Biometric techniques are generally classified into two sub-categories, namely physiological and behavioral. Let us discuss these in brief.

1. Physiological Techniques

- As the name suggests, these techniques rely on the physical characteristics of human beings. Since the aim is to identify humans uniquely, these characteristics must be very prominent and distinguishable from one person to another. Several such techniques are used, as mentioned below.

(a) Face: In this technique, the idea is to check and measure the distance between the various facial features such as eyes, nose, and mouth.

(b) Voice: Human voice can be uniquely identified based on the characteristics of the sound waves of a voice.

(c) Fingerprint: The fingerprint-based authentication uses two approaches: *minutiae-based* and *image-based*. In the minutiae-based technique, a graph of the individual ridge positions is drawn. In the image-based technique, an image of the fingerprints is taken and stored in the database for subsequent comparisons

(d) Iris: Amazingly, each person has some unique pattern inside the iris. This technique is based on identifying a person uniquely based on this pattern.

(e) Retina: Retina scanning is not very common. The main reason behind this is its high cost. In this mechanism, the vessels carrying blood supply at the back of a human eye are examined. They provide a unique pattern, which is used to authenticate an individual.

2. Behavioral Techniques

- The idea in behavioral techniques is to observe a person to ensure that he/she is not trying to claim to be someone else. Two main techniques are used here:

(a) Keystroke: Several characteristics such as the speed of typing, strength of keystrokes, time between two keystrokes, error percentage and frequency, etc., can be measured for identifying users. However, it is not as reliable as many other authentication mechanisms.

(b) Signature: This is an old technique. Cheques and many other documents are expected to be physically signed by the authorizer. This is now extended by keeping a scanned copy of a person's signature and comparing this computer-based scanned signature with the paper signature as and when the need arises.

Kerberos

- Many real-life systems use an authentication protocol called Kerberos. The basis for Kerberos is another protocol, called *Needham-Shroeder*. Designed at MIT to let workstations allow network resources in a secure manner, the name Kerberos signifies a multi-headed dog in Greek mythology (apparently used to keep outsiders away).
- Version 4 of Kerberos is found in most practical implementations. However, Version 5 is also in use now.

The Working of Kerberos

There are four parties involved in the Kerberos protocol:

- The *client* workstation.
- *Authentication Server (AS)* Verifies (authenticates) the user during login.
- *Ticket Granting Server (TGS)* Issues tickets to certify proof of identity.
- The *server* offering services such as network printing, file sharing or an application program.
  - The job of AS is to authenticate every use at the login time. AS shares a unique secret password with every user. The job of TGS is to certify to the servers in the network that a user is really who he/she claims to be. For proving this, the mechanism of tickets (which allow entry into a server, just as a ticket allows parking a car or entering a music concert) is used.

There are three primary steps in the Kerberos protocol.

Authentication Server (AS):

- The Authentication Server performs the initial authentication and ticket for Ticket Granting Service.

Database:

- The Authentication Server verifies the access rights of users in the database.

Ticket Granting Server (TGS):

- The Ticket Granting Server issues the ticket for the Server

Kerberos Overview:

- **Step-1:**
  User login and request services on the host. Thus user requests for ticket-granting service.
- **Step-2:**
  Authentication Server verifies user's access right using database and then gives ticket-granting-ticket and session key. Results are encrypted using the Password of the user.
- **Step-3:**
  The decryption of the message is done using the password then send the ticket to Ticket Granting Server. The Ticket contains authenticators like user names and network addresses.
- **Step-4:**
  Ticket Granting Server decrypts the ticket sent by User and authenticator verifies the request then creates the ticket for requesting services from the Server.
- **Step-5:**
  The user sends the Ticket and Authenticator to the Server.
- **Step-6:**
  The server verifies the Ticket and authenticators then generate access to the service. After this User can access the services.

Key Distribution Center (KDC).

- Key Distribution Center (KDC) is a central authority dealing with keys for individual computers (nodes) in a computer network.
- It is similar to the concept of the Authentication Server (AS) and Ticket Granting Server (TGS) in Kerberos.
- The basic idea is that every node shares a unique secret key with the KDC.
- Whenever user A wants to communicate securely with user B, the following happens:

  1. The background is that A has a shared secret key KA with KDC. Similarly, B is assumed to share a secret key KB with the KDC.

  2. A sends a request to KDC encrypted with KA, which includes

  (a) Identities of A and B

  (b) A random number R, called a *nonce*

  3. KDC responds with a message encrypted with KA, containing

  (a) One-time symmetric key KS

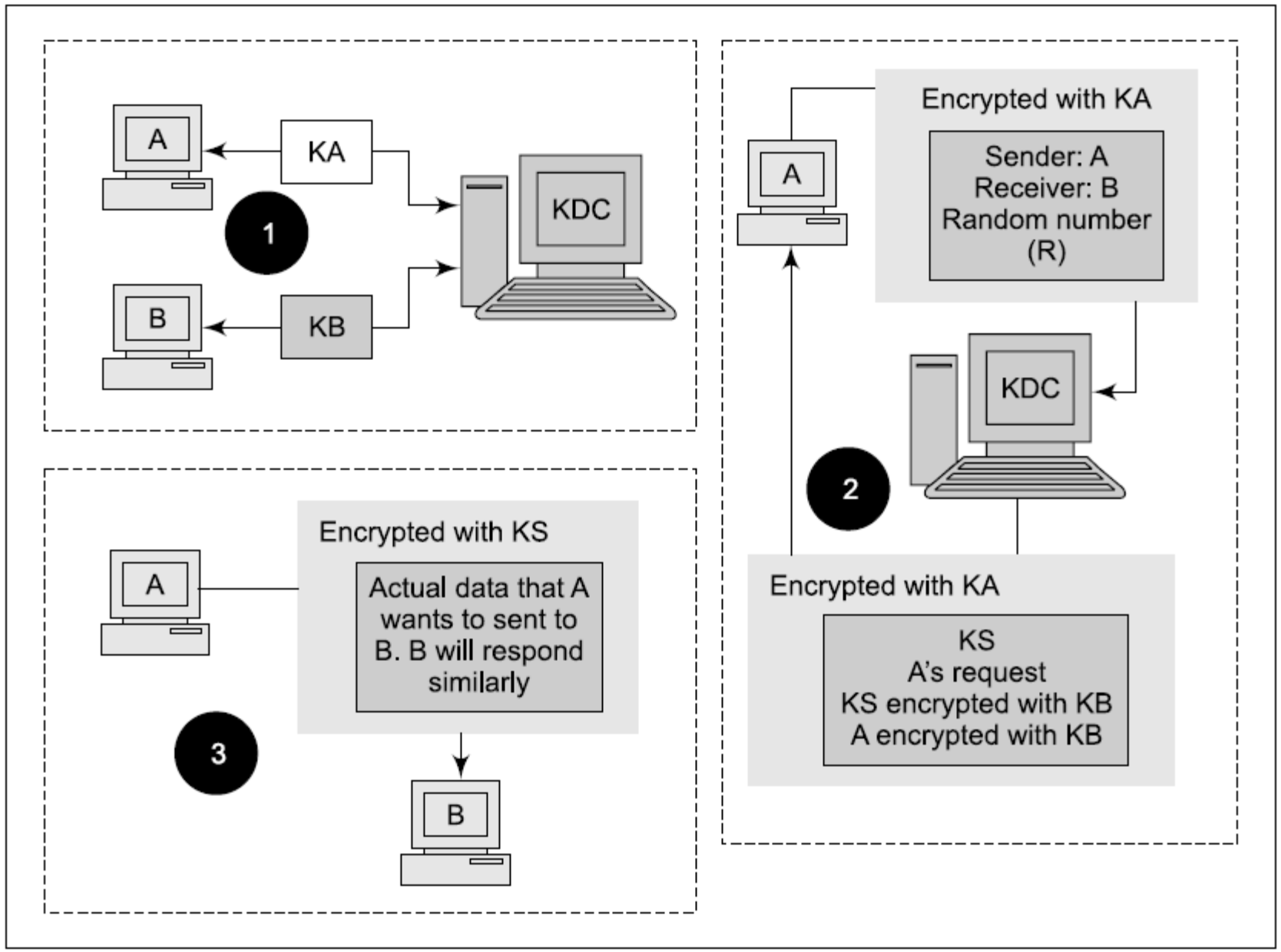
  (b) Original request that was sent by A, for verification

  (c) Plus, KS encrypted with KB and ID of A encrypted with KB.

  4. A and B can now communicate by using KS for encryption.

MKK

Key Distribution Center (KDC) concept



MKK

Network Security

E-mail Security

- Basically, Email security refers to the steps where we protect the email messages and the information that they contain from unauthorized access, and damage. It involves ensuring the confidentiality, integrity, and availability of email messages, as well as safeguarding against phishing attacks, spam, viruses, and another form of malware. It can be achieved through a combination of technical and non-technical measures.

Steps to Secure Email:

- Choose a secure password that is at least 12 characters long, and contains uppercase and lowercase letters, digits, and special characters.
- Activate the two-factor authentication.
- Use encryption, it encrypts your email messages so that only the intended receiver can decipher them.
- Keep your software up to date.

MKK

Email Security Policies

The email policies are a set of regulations and standards for protecting the privacy, accuracy, and accessibility of email communication within the organization.

- Appropriate Use
- Password and Authentication
- Encryption
- Virus Protection
- Retention and Detection
- Training
- Incident Reporting
- Monitoring
- Compliance
- Enforcement

Firewall

- A firewall is defined as the system which analyzes and filters incoming or outgoing data packets based on pre-defined rules.
- Firewalls can be *hardware and software or* both. The router is an example of a physical firewall, and a simple firewall program on the system is an example of a software firewall. Hence a firewall can be implemented either way.
- A firewall is usually defined as a network controlling system. It means that firewalls are primarily responsible for monitoring and filtering network traffic.
- Because the firewall supports both types of implementations, hardware, and software, therefore, it is more scalable than anti-virus.
- A firewall is mainly used to prevent network related attacks. It mainly includes external network threats? for example- Routing attacks and IP Spoofing.

IP Security

- IP Sec (Internet Protocol Security) is an Internet Engineering Task Force (IETF) standard suite of protocols between two communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted, and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

Components of IP Security

1. Encapsulating Security Payload (ESP): It provides data integrity, encryption, authentication, and anti-replay. It also provides authentication for payload.
2. Authentication Header (AH): It also provides data integrity, authentication, and anti-replay and it does not provide encryption.
3. Internet Key Exchange (IKE): It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication.

VPN

- VPN stands for Virtual Private Network. It allows you to connect your computer to a private network, creating an encrypted connection that masks your IP address to securely share data and surf the web, protecting your identity online.
- A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.

Types of VPNs

- *Router VPN:* The first type uses a router with added VPN capabilities. A VPN router cannot only handle normal routine duties, but it can also be configured to form VPNs over the internet to other similar routers located in remote networks.
- *Firewall VPN:* The second type of VPN is one built into a firewall device. Firewall VPN can be used both to support remote users and also to provide VPN links.
- *Network Operating System:* The third type of VPNs include those offered as part of a network operating system like Windows NT, Windows 2000, and Netware 5. These VPNs are commonly used to support remote access, and they are generally the least expensive to purchase and install.

Intrusion

- Any illicit behavior on a digital network is known as a network intrusion. Network incursions frequently include the theft of important network resources, which virtually always compromise the network and/or data security.
- An illegal entrance into your network or an address in your assigned domain is referred to as a *network intrusion*. An intrusion can be passive (in which access is achieved quietly and undetected) or *aggressive* (in which access is gained overtly and without detection).
- Intrusions might occur from the outside or from within your network structure (an employee, customer, or business partner). Some intrusions are just aimed to alert you that an intruder has entered your site and is defacing it with various messages or obscene graphics.
- Some intruders will try to implant code that has been carefully developed. Others will infiltrate the network, stealthily siphoning out data on a regular basis or altering public-facing Web sites with varied messages.

MKK

Intrusion detection system

An intrusion detection system (IDS) is a monitor-only program that detects and reports irregularities in your network architecture before hackers may do damage.

Intrusion detection systems employ two detection methods −

- *Signature-based detection* matches data activity to a signature or pattern in a signatures database. A new harmful behavior that is not in the database, for example, is overlooked when using signature-based detection.
- Unlike signature-based detection, *behavior-based detection* recognizes any abnormality and issues alarms, making it capable of identifying new sorts of threats. It's referred to as an expert system since it learns what regular behavior looks like in your system.

That's all about

UNIT 5

MKK