Infrastructure Penetration Testing Management

by
SARAVALLI NANDHAKUMAR.

Agenda

- Introduction- PenTesting
- CIA- Triad
- Access control
- Authorization and Authentication

Penetration testing

- Security test or simulated attack
- Penetration testing (or pen testing) is a security exercise where a cyber-security expert attempts to find and exploit vulnerabilities in a computer system. The purpose of this simulated attack is to identify any weak spots in a system’s defenses which attackers could take an advantage.

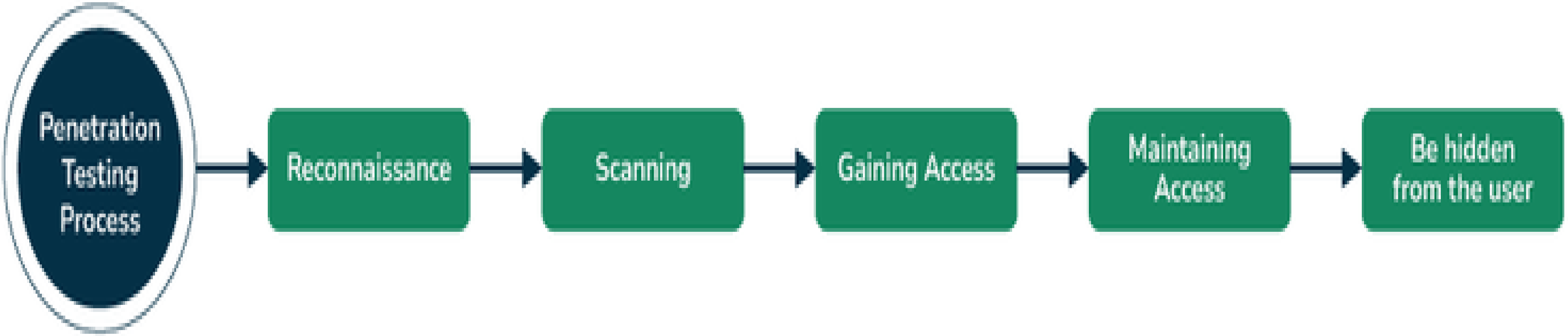
Why we need pentesting

- It can discover unknown vulnerabilities
- Pen testing can meet compliance needs.
- Customers and partners will feel secure
- It can prove your defenses are adequate
- Regular pen testing can prevent breaches or reduce their impact
- It reveals problems and solutions for security improvement

Different Types of Penetration Testing

Black Box Testing	Testers have no prior knowledge of the system, simulating a real-world scenario where attackers have limited information.
White Box Testing	Testers have full knowledge of the system’s architecture and source code, allowing for a comprehensive evaluation of internal structures and potential vulnerabilities.
Gray Box Testing	Testers have some knowledge of the system, striking a stability between the black box and white box approaches.

Phases of penetration testing



Phases of Penetration Testing

- **Reconnaissance and Planning:** Testers gather information about the target system from various sources like public and private data. They look for vulnerabilities such as network components, open ports, and operating system details.
- **Scanning:** Testers use scanning tools to further explore the system and find weaknesses. They look for vulnerabilities using tools like port scanners and vulnerability scanners.
- **Obtaining Entry:** Testers exploit vulnerabilities found in the previous stages to connect with the target. They may use attacks like denial-of-service (DoS), SQL injections, and cross-site scripting to expose weaknesses.

Phases of Penetration Testing (cont'd)

- **Maintaining Access:** Testers stay connected to the target system for as long as possible, imitating an advanced persistent threat. They continue exploiting vulnerabilities to steal data and cause damage.
- **Analysis:** Testers analyze the results and create a report detailing the exploited vulnerabilities, accessed data, and time connected to the target.
- **Cleanup and Remediation:** Testers remove all traces of their activities, and organizations start fixing any security issues found during testing.

Advantages of Pentesting

- **Identify and Resolve System Vulnerabilities:**

Penetration testing helps uncover weaknesses in your digital infrastructure before malicious attackers exploit them. By identifying vulnerabilities, you can proactively address security gaps and enhance our defenses.

- **Gain Valuable Insights into our Digital Systems:**

Pentesting provides an independent view of our security posture. It reveals how well our existing security processes and configuration management practices have been implemented.

- **Establish Trust with our Client:**

Demonstrating a commitment to security through regular penetration testing builds trust with customers and stakeholders. Clients appreciate knowing that you take their data protection seriously.

CIA

The 3 goals of information security are to maintain:

- Information **confidentiality**
  - *Making sure only approved users have access to data.*
- Information **integrity**
  - *Integrity means that data can be trusted. It should be maintained in a correct state, kept so that it may not be tampered with, and should be correct, authentic, and reliable.*
- Information **availability**
  - *Ensuring data is accessible by approved users when needed*

Protecting your C-I-A

Confidentiality
Prevent unauthorized disclosure of information

Integrity
Prevent unauthorized modification of information or files

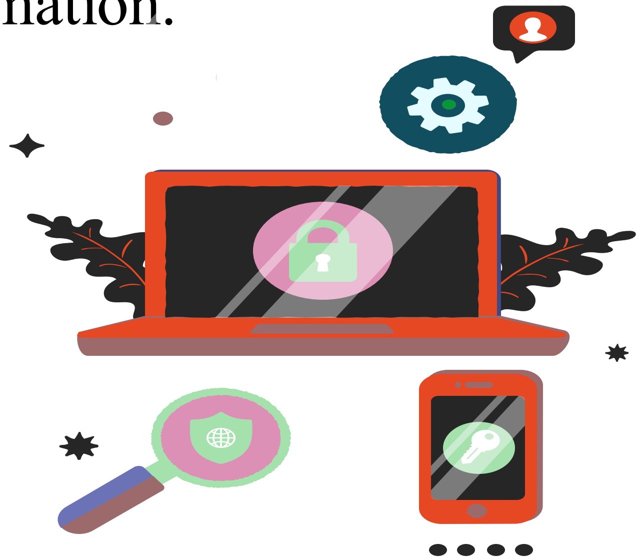
Availability
Ensuring timely access to resources

Confidentiality

- Protecting information privacy.
- Keep sensitive information off the network, if possibl
- Encrypt sensitive information.
- Protect access to your system.
- Password protection.
- Don’t share sensitive information.

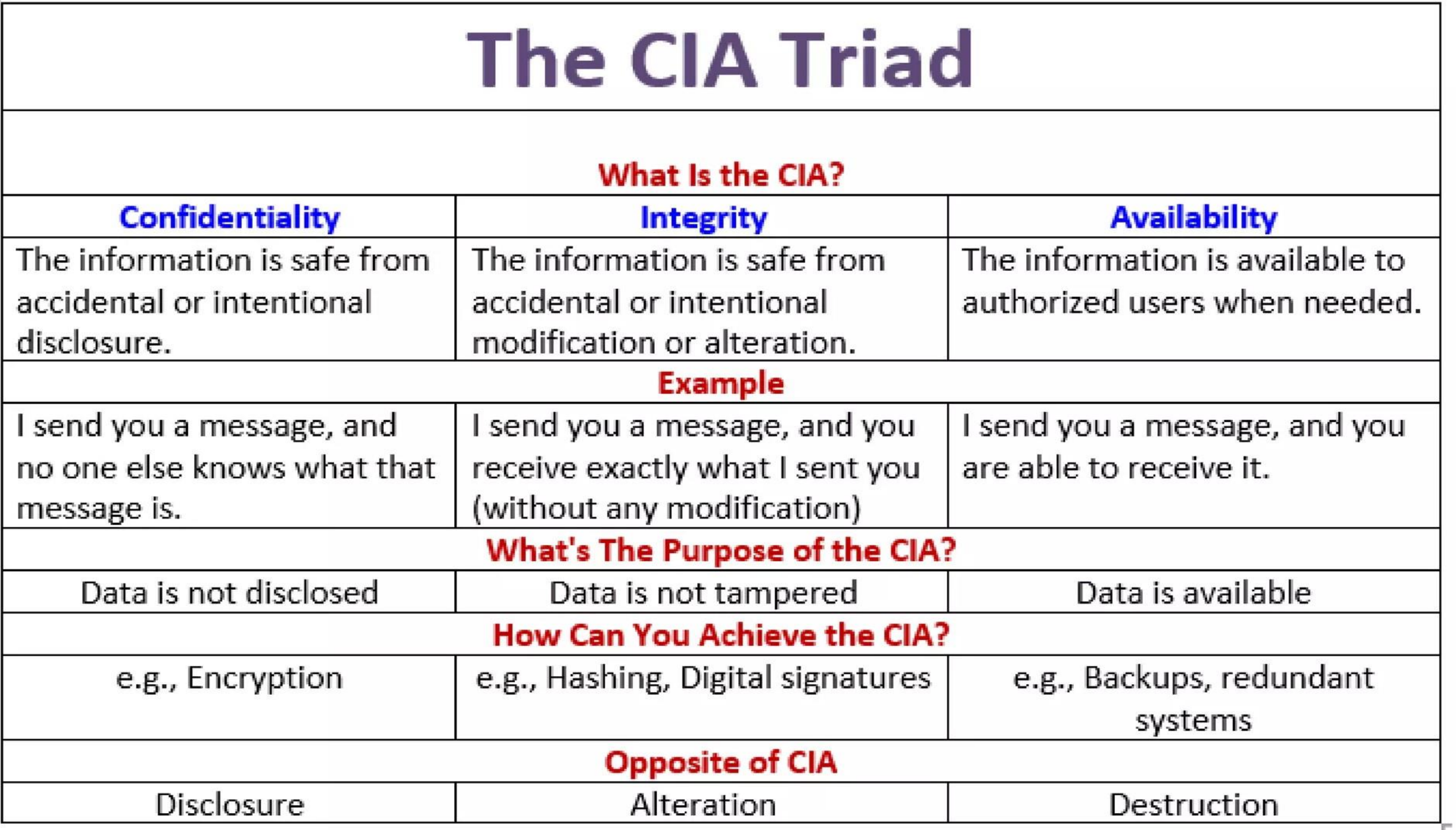
Integrity

- Preventing Unauthorized Modification of Information.
  Emails, Data,Digital Downloads.
- Reliability/Trustworthiness of information.
- Hijacked websites.
- Email with modified content.
- Corrupted files.



Availability

- Denial of Service Attacks(DOS) and Distributed Denial of Service Attacks(DDOS).
- Expect the Unexpected.
- Beware of Natural/Manmade disasters.



The CIA Triad

What Is the CIA?		
Confidentiality	**Integrity**	**Availability**
The information is safe from accidental or intentional disclosure.	The information is safe from accidental or intentional modification or alteration.	The information is available to authorized users when needed.
Example		
I send you a message, and no one else knows what that message is.	I send you a message, and you receive exactly what I sent you (without any modification)	I send you a message, and you are able to receive it.
What's The Purpose of the CIA?		
Data is not disclosed	Data is not tampered	Data is available
How Can You Achieve the CIA?		
e.g., Encryption	e.g., Hashing, Digital signatures	e.g., Backups, redundant systems
Opposite of CIA		
Disclosure	Alteration	Destruction

Access Control

- Access control systems are a fundamental aspect of security used to protect people, sites, and assets. Implementing an access control system is a critical component of security, ensuring the right people have the correct level of access to the right resources.

Access control techniques

- **Discretionary access control (DAC)** allows resource owners to control access.
- **Role-based access control (RBAC)** assigns system access to users based on their role in an organization.
- **Mandatory access control (MAC)** uses a classification system to determine who can access what.
- **Attribute-based access control (ABAC)** uses user, resource, and environment attributes to control access.

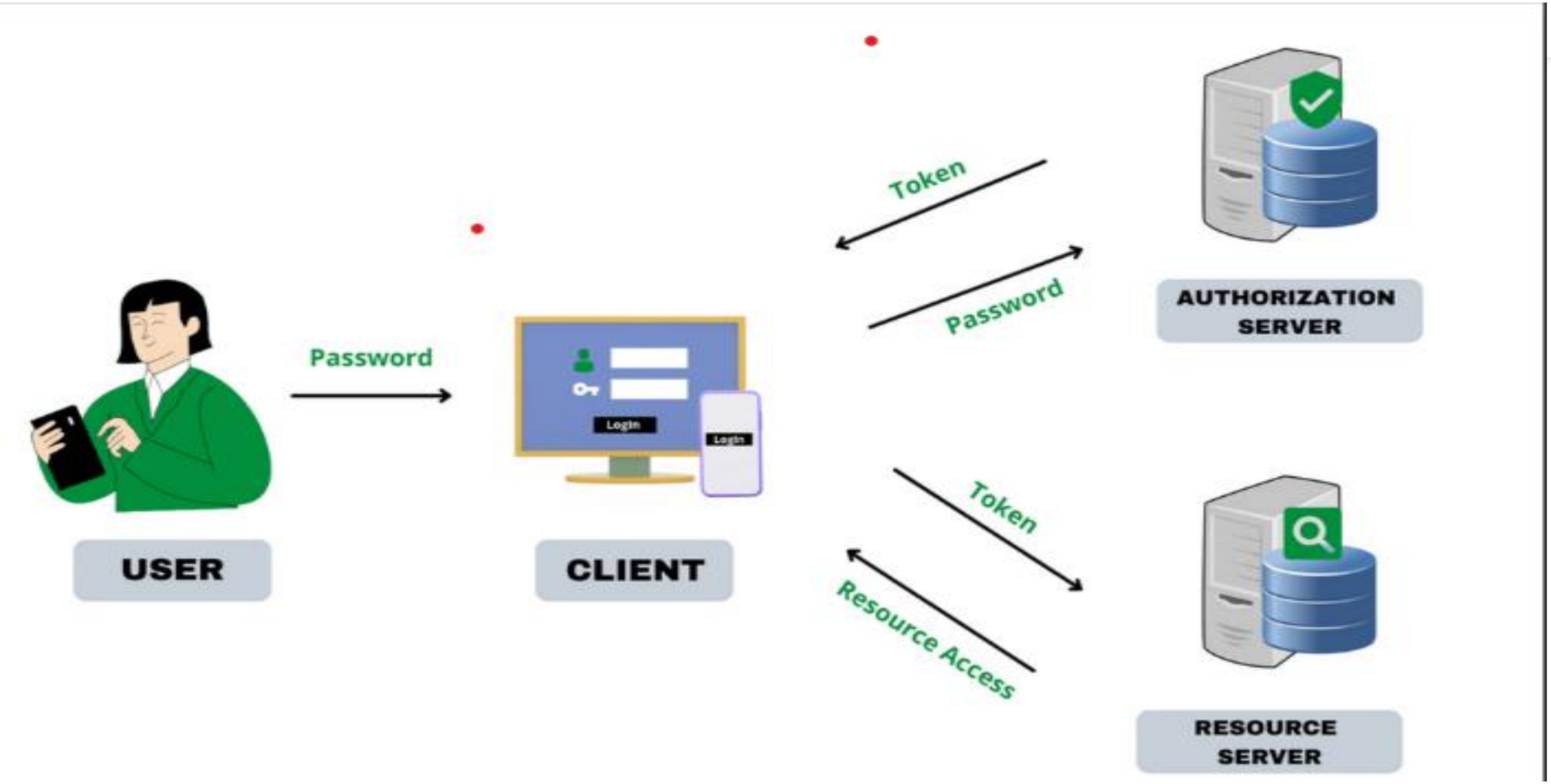
Authentication Vs Authorization

Authentication	Authorization
It is an act of identifying an user or a device	It is an act of allowing or denying users and devices access rights.
Find out whether users are who they claim to be	Based on predefined rule determines what users can and cannot access
Require the user to validate credentials using the established mechanism	Validates whether access is allowed through security policies and rules
Prerequisite process before authorization	Access after successful authentication
Transmit info through an ID Token	Send through an Access Token

Authorization token

- **A Token** is a computer-generated code that acts as a digitally encoded signature of a user. They are used to authenticate the identity of a user to access any website or application network.
- **Physical token-**A Physical token use a tangible device to store the information of a user OTP, USB
- **Web Token**- Fully digital process- Json web token(JWT)

Authorization token



Session-2

- Key Management.
- Hashes.
- Kerberos.
- Lab Introduction.

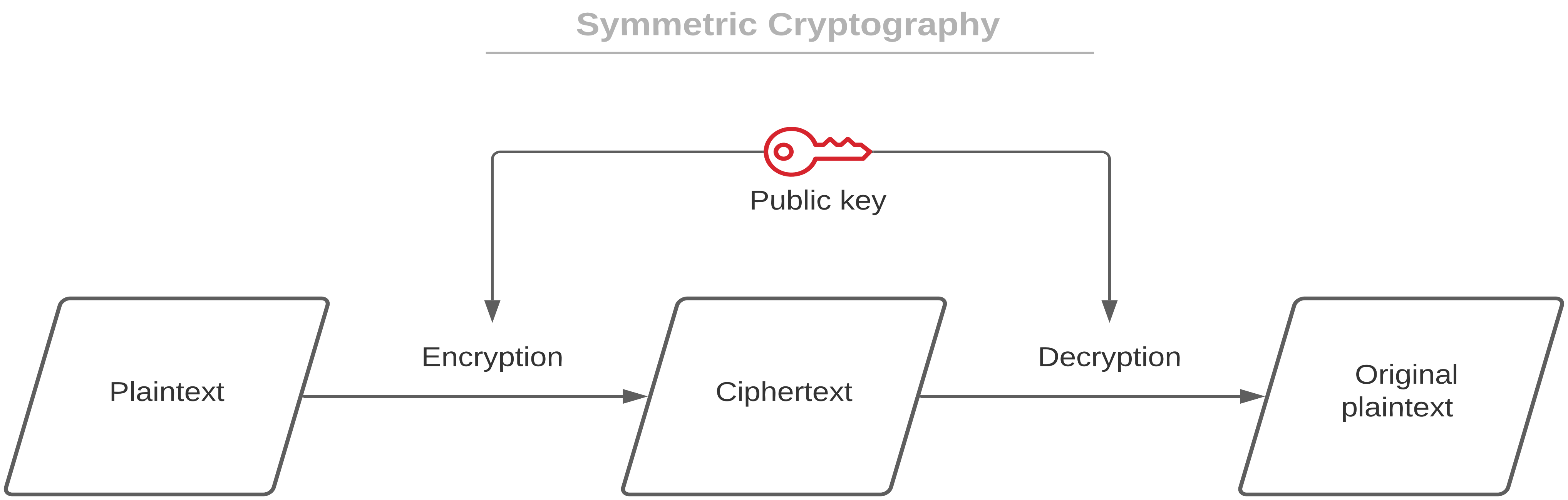
Key Mangement

- Key Management deal with the creation, exchange, storage, deletion, and refreshing of keys. They also deal with the members access of the keys.

Symmetric cryptography

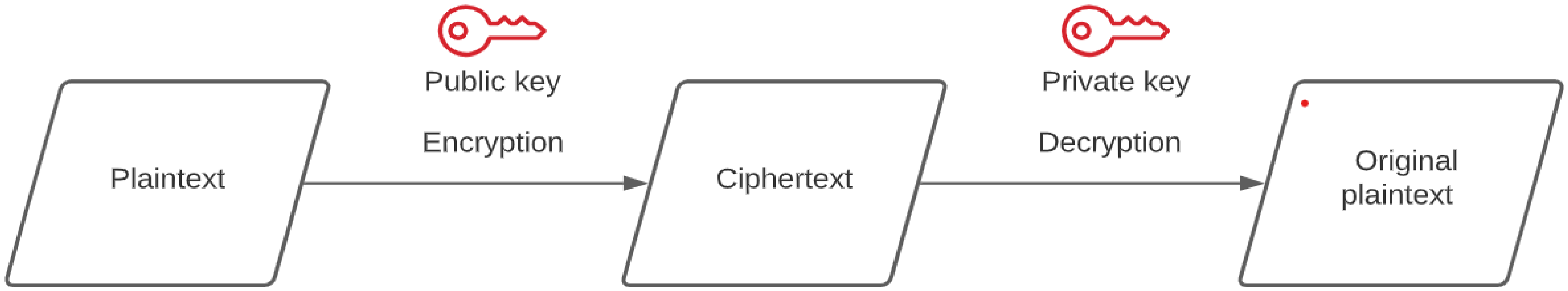
The encryption and decryption process uses the same key.

The way of providing the key to other parties should be secure to avoid any exposures.



Asymmetric Cryptography

- Asymmetric cryptography relies on a pair of two separate but mathematically connected keys.

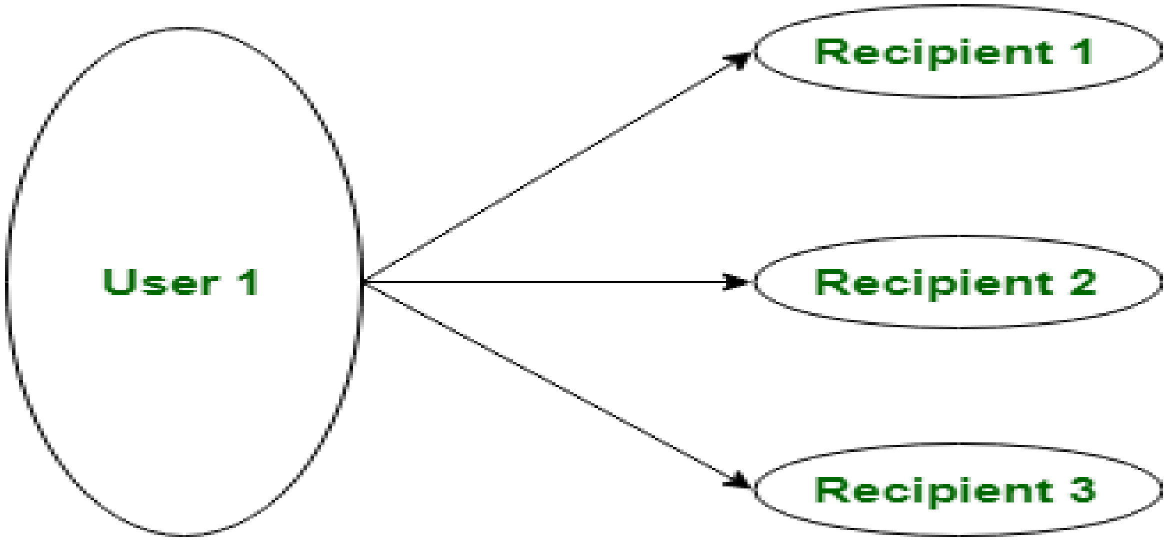


Distribution of Public Key

The public key can be distributed in four ways:

- Public announcement
- Publicly available directory
- Public-key authority
- Public-key certificates.

Public announcement



Public Key Announcement

Publicly available directory

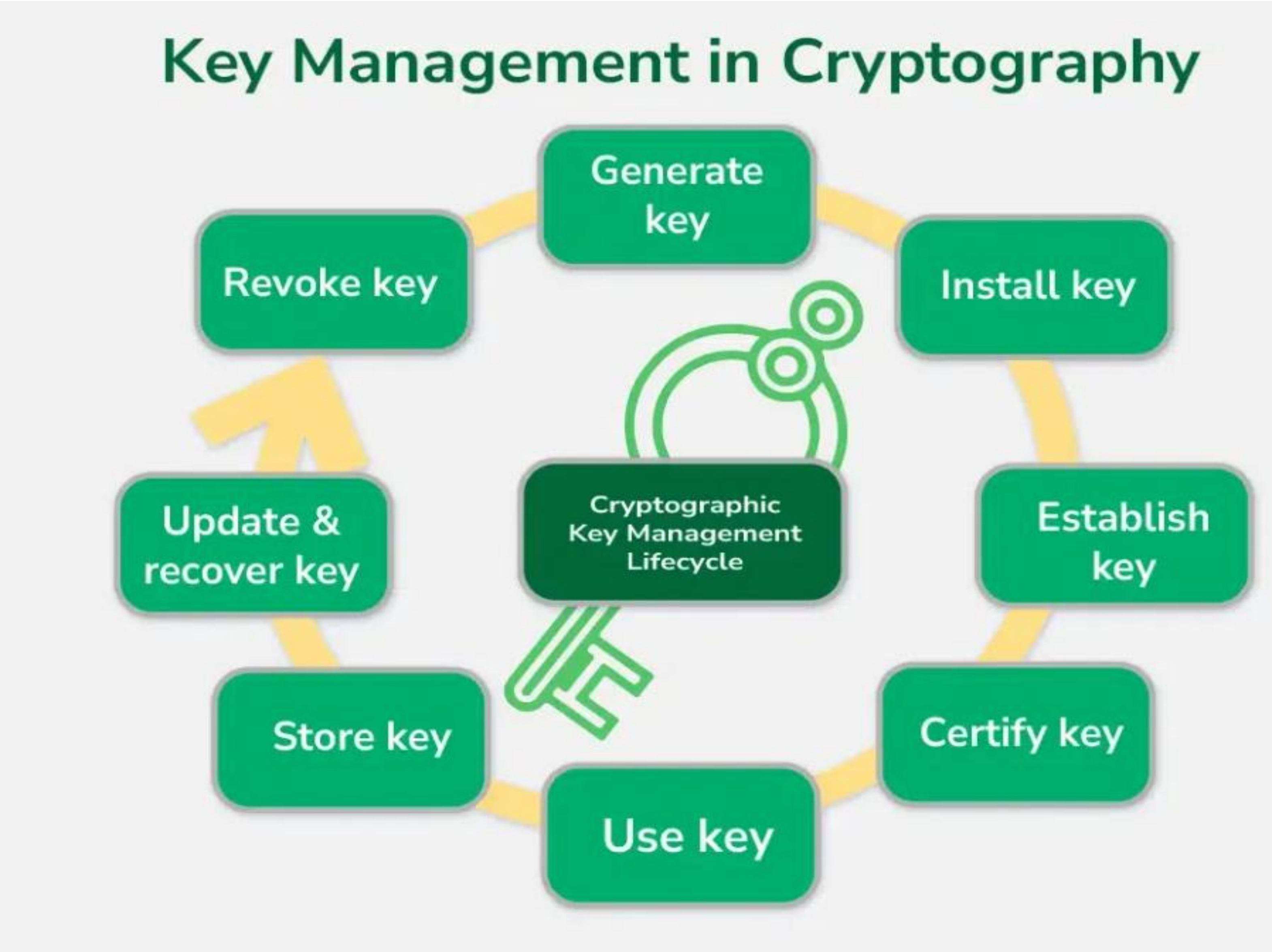
- In this type, the public key is stored in a public directory. Directories are trusted here, with properties like Participant Registration, access and allow to modify values at any time, contains entries like {name, public-key}. Directories can be accessed electronically still vulnerable to forgery or tampering.

Public-key authority

- It is similar to the directory but, improves security by tightening control over the distribution of keys from the directory. It requires users to know the public key for the directory.

Public key Certificate

- This time authority provides a certificate (which binds an identity to the public key) to allow key exchange.
- The certificate is accompanied by some other info such as period of validity, rights of use, etc. All of this content is signed by the private key of the certificate authority and it can be verified by anyone possessing the authority's public key.



Key Management in Cryptography

Hashing

- Hashing is the practice of transforming a given key or string of characters into another value for the purpose of security. Unlike standard encryption, hashed values are very difficult to decode.

What is Kerberos

- Network Authenticated protocol
- Developed at MIT in the mid 1980s
- Available as open source or in supported commercial software

Kerberos vs Firewall

- Firewall make a risky assumption: that attackers are coming from outside. In reality it comes from within.
- Kerberos assumes that network connections(rather than servers and work stations) are the weak link in network security.

Architecture

- It consists of 3 components

  1.Client

  2. Authentication Server or KDC

  3. Server

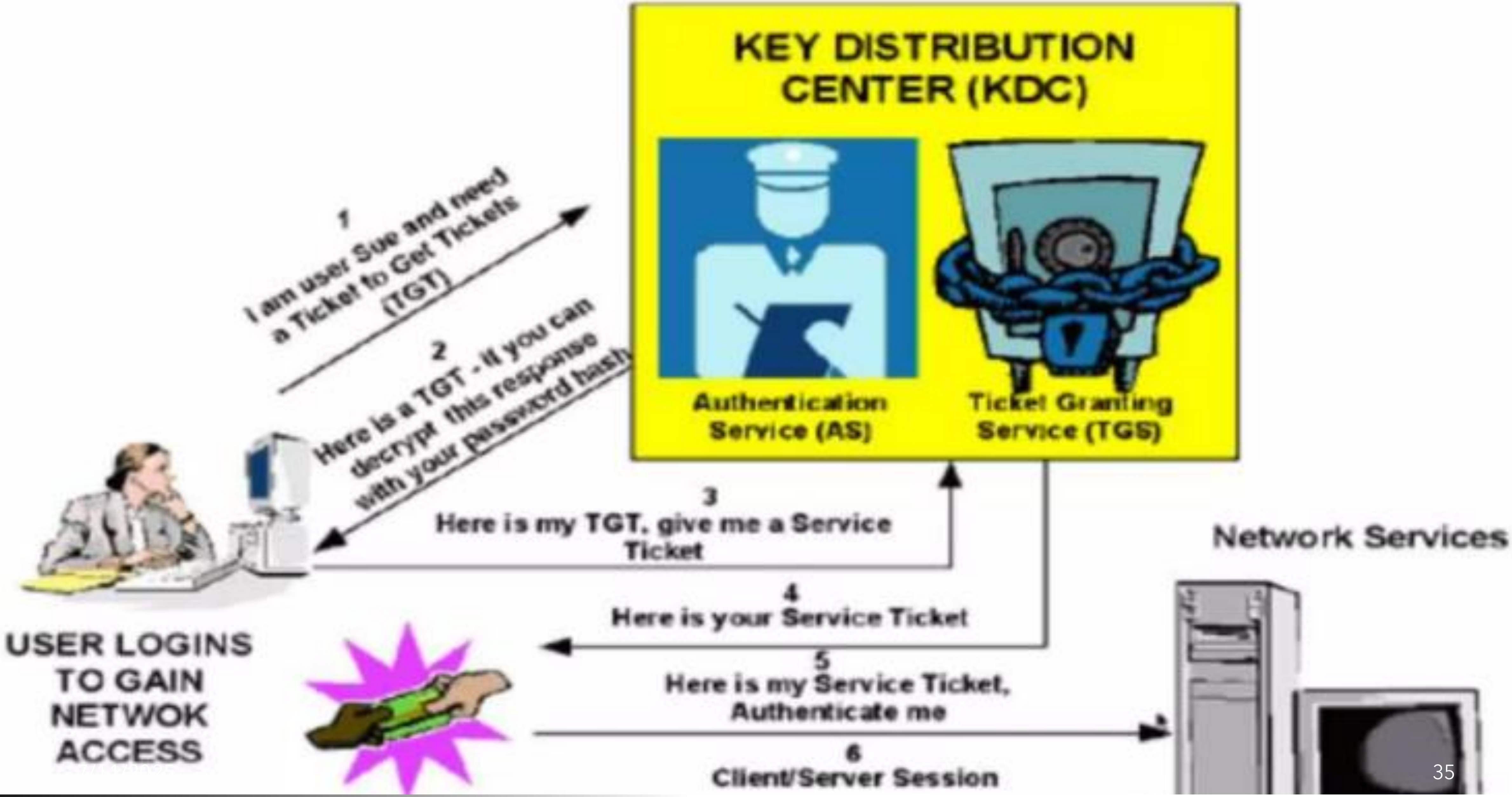
- And has three main exchanges

  1. Authentication Service(AS) Exchange

  2.Ticket Granting Service (TGS) Exchange

  3. Client Server (CS) Exchange

KERBEROS TICKET EXCHANGE



KEY DISTRIBUTION CENTER (KDC)

Authentication Service (AS)

Ticket Granting Service (TGS)

1 I am user Sue and need a Ticket to Get Tickets (TGT)

2 Here is a TGT - if you can decrypt this response with your password hash

3 Here is my TGT, give me a Service Ticket

4 Here is your Service Ticket

5 Here is my Service Ticket, Authenticate me

6 Client/Server Session

Network Services

USER LOGINS TO GAIN NETWOK ACCESS

AS Exchange

- Exchange between client and Authentication Server
- Client sends KRB_AS_REQ msg to KDC Specifying credentials it wants
- Server replies with msg KRB_AS_REP containing ticket and session key
- The session key is encrypted with client's secret key

TGS Exchange

- Client sends KRB_TGS_REQ to the TGS server
- Server replies KER_TGS_REP to the client with ticket
- TGS must have access to all secret keys
- It is used to obtain Additional tickets for the server

CS Exchange

- Client contacts with the real server
- Client sends KRB_AP_REQ to the server specifying the service
- Server validates client by decrypting ticket with server's secret key and decrypting Authenticator with sessions key contained in the ticket
- Server optionally replies with KRB_AP_REP.

Benefits of Kerberos Authentication

- 1. Access control
- 2.Mutual Authentication
- 3.Limiting ticket lifetime
- 4.Reuable Authentication
- 5. Security

Session 4(3-8-2024)

- API Security Pattern
- Vulnerability, Threat , Risk
- Vulnerability Management
- Vulnerability Management lifecycle
- Lab Continuation

API Security Pattern

- Authentication and Authorisation
- Data Protection
- Rate limiting& Throttling
- Error Handling
- Logging & Monitoring
- Token Management
- Backup & Recovery
- Secure Deployment

Vulnerability, Threat, Risk

- A **vulnerability**, as defined by the International Organization for Standardization (ISO 27002), is “a weakness of an asset or group of assets that can be exploited by one or more threats.”
- A **threat** is something that can exploit a vulnerability.
- A **risk** is what happens when a threat exploits a vulnerability. It’s the damage that could be caused by the open vulnerability being exploited by a threat.

Sources of vulnerability

- 1. Misconfigurations
- 2. Unsecured APIs
- 3. Outdated or Unpatched Software
- 4. Zero-day Vulnerabilities
- 5. Weak or Stolen User Credentials
- 6. Access Control or Unauthorized Access

Vulnerability scanner

1.What is network vulnerability scanner?

- Network vulnerability scanners monitor web servers, their operating systems, their daemons and any other services open to the internet such as database services.
- works on known vulnerabilities

2. What is web vulnerability scanner?

- Web vulnerability scanners scan application/website code to find vulnerabilities that compromise the application/website itself or its back-end services.
- These scanners work against a known list of common exploits as maintained by OWASP and others.
- These exploits use various injection and evasion techniques to “hijack” web applications and websites Some of the better known exploits are SQL injection, cross-site scripting (XSS), man-in-the-middle (MITM) attack, and malicious code.

- **What is horizontal and vertical scan?**

A horizontal scan is described as scan against a group of IPs for a single port. A vertical scan is described as a single IP being scanned for multiple ports.

- **What is Exposure?**

Exposure: The revelation of information about a system that can be used to assist an attacker in exploiting one or more vulnerabilities. Version number of an application is an example of data that may reveal potential vulnerabilities. Knowledge of a vulnerability or potential vulnerability can be considered an exposure.

- **What is a target?**

Target: A host, application, virtual host, or group of hosts that is in range of a scanning device and is designated for vulnerability assessment. When performing a scan, the scanner is directed at a target by its Internet protocol (IP) address, group of IPs, or name. A target is simply the subject of a scan. It may be specified or discovered automatically.

Vulnerability Management

- Regular process of identifying, assessing, reporting on, managing and remediating security vulnerabilities across endpoints, workloads and systems.
- A strong vulnerability management program uses threat intelligence and knowledge of IT and business operations to prioritize risks and address cybersecurity vulnerabilities as quickly as possible.

Vulnerability Management lifecycle

1. Discovery
2. Prioritize
3. Assessment
4. Reporting
5. Remediation
6. Monitoring

Vulnerability Management

What is a port?

- A port is a point on a computer where information exchange between multiple programs and the internet to devices or other computers takes place. To ensure consistency and simplify programming processes, ports are assigned port numbers.
- Each port is differentiated using an assigned port number ranging from 0 to 65535
- Port numbers 0 to 1023 are “well-known” ports and are always associated with a specific service.

What is port scan?

- A port scan is a common technique hackers use to discover open doors or weak points in a network. A port scan attack helps cyber criminals find open ports and figure out whether they are receiving or sending data. It can also reveal whether active security devices like firewalls are being used by an organization.

What is a ping scan?

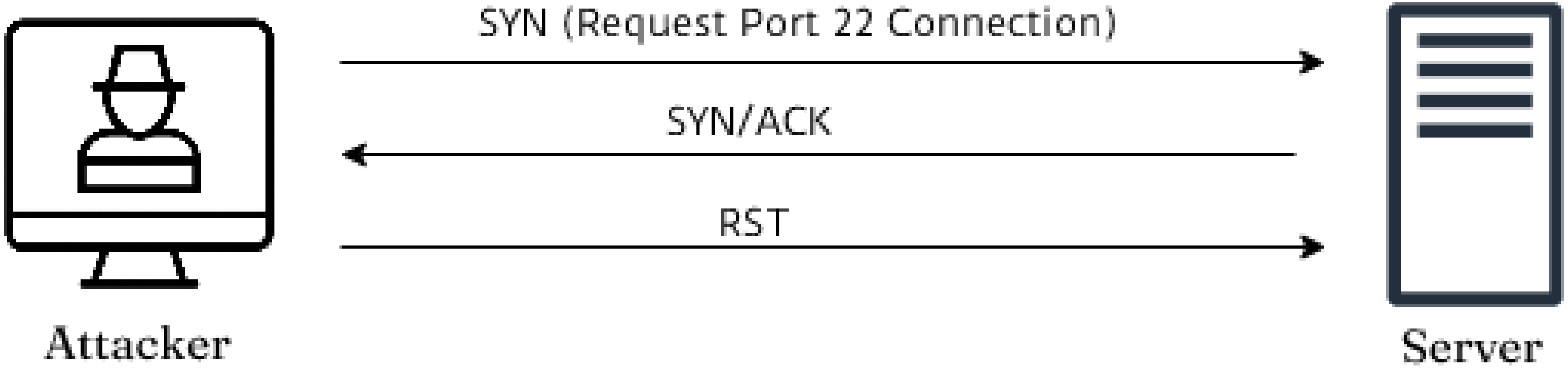
- Ping scans: A ping is used to check whether a network data packet can reach an IP address without any issues. Ping scans involve automated transmissions of several ICMP requests to various servers

Introduction to Port Scan

- Port scanning is a method of finding out which services a host computer offers.

- A closed port doesn't allow entry or access to a service. For instance, if port 80 is closed on a Web server, users can't access Web sites.

Syn Scanning



SYN (Request Port 22 Connection)

SYN/ACK

RST

Attacker

Server

TCP Connect scan

- TCP Connect scan uses the concept of a full three-way handshake to discover whether a given port is open, filtered, or closed according to the response it receives.
- What it essentially means is that if Nmap sends a TCP request to a closed port with its SYN flag set, then it receives a TCP packet with its RESET FLAG set from the target server. This tells Nmap that the specified port is "closed".
- Otherwise, if the port is actually "open", then Nmap receives a response with SYN/ACK flags set responding to the packet sent by Nmap with its SYN flag set.
- The third possibility is that if a port is filtered, most of the server's firewalls are configured to just drop incoming packets. Nmap doesn't receive any

UDP Scan

- In this type of scan, a UDP packet is sent to the target computer. If the port sends back an ICMP "Port Unreachable" message, the port is closed. Again, not getting that message might imply the port is open, but this isn't always true.

Port Scan types(cont'd)

- **TCP NULL Scan (-sN):** NULL scan, as the name implies, sends a TCP packet with no flags set. If the port is closed, the host responds with an RST.
- **TCP FIN Scan (-sF):** FIN scan, rather than sending completely empty packets, it sends a packet with its FIN flag set. If the port is closed, the host responds with an RST.
- **TCP XMAS Scan (-sX):** XMAS scan, sends a packet with URG,PSH,FIN flags set. This scan got its name from the appearance it gives of a Christmas tree when viewed as a packet capture in Wireshark. If the port is closed, the host responds with an RST.

Port scanning Tools

1.**Nmap-**

Nmap has become one of the most popular port scanners and adds new features constantly, such as OS detection and fast multiple-probe ping scanning. Nmap also has a GUI front end called Zenmap that makes working with complex options easier.

Nessus

- Remote security scanning tool which scan a computer and raises an alert, if it discovers any vulnerabilities.
- It is not a complete security solution
- It is not a prevention tool

3. Open VAS

- Open Vulnerability Assessment System (OpenVAS) is free software that is used to detect and manage vulnerabilities in computer systems and networks. It provides various services and tools for vulnerability assessment such as identifying and analyzing security issues such as misconfigurations, outdated software, and weak passwords that could be exploited by attackers.

Session 5(10.8.2024)

- Asset
- Asset valuation
- Principle of Mitigation
- Controlling Internal Vulnerabilities
- Nessus installation
- Lab practice

Asset

- Asset is anything that has a value for an organization. It may be physical or logical
- Information Asset-personal details, transactions orders etc
- Intellectual property- trade secrets, source code, policies & standards

Asset valuation

- A key part of a risk assessment is identifying the value of an asset. In the absence of an asset’s value, it is more difficult to calculate risks associated with an asset, even when qualitative risk evaluation is employed
- **Qualitative asset valuation**-The organization can assign a value using a low-medium-high scale or a numeric scale such as 1 to 5 or 1 to 10

Quantitative Asset valuation

- Replacement cost-If it is hardware asset cost of purchasing

-If it is Database –operational cost to restore from backup

- Net present value(NPV)- If the asset directly or indirectly generates revenue.
- Consequential financial cost-used to measure full impact of the breach

Mitigation principle

- **Mitigation** is the reduction of something harmful that has occurred or the reduction of its harmful effects.
- **Mitigation** in law is the principle that a party who has suffered loss (from a tort or breach of contract) has to take reasonable action to minimize the amount of the loss suffered.

Three Rules of Mitigation

- **First**, the complainant can not recover the loss resulting from the defendant’s default if the complainant could have avoided the loss by taking reasonable steps.
- **Second**, if the complainant avoids or mitigates the loss, he can not recover for such avoided loss even if he takes steps that are more than what was reasonably required of him.
- **Third**, where the plaintiff suffers loss or incurs expense by taking reasonable steps to avoid or mitigate the loss resulting from the default of the defendant, he may recover the further loss or expense from the defendant.

Types of Internal Controls Vulnerability

- **Technical internal control** weakness due to hardware and software
- **Operational internal contro**l weakness typically resulting from human error
- **Administrative internal control** weakness dependent on policies and procedures
- **Architectural control** weaknesses occur when IT systems are implemented and not adequately monitored
- Malicious actors can exploit internal control weaknesses to evade what might appear to be strong security tactics. With so much complexity and innovation in modern business, constant monitoring is necessary to identify internal control weaknesses and neutralize existing or emerging threats.

To control internal vulnerabilities, consider the following steps

- Perform penetration testing to identify vulnerabilities.
- Keep track of IT assets.
- Learn about current and emerging threats.
- Identify and fix vulnerabilities.
- Educate employees about good cybersecurity practices.

THANK YOU