4. Security and Protection (8+10 hours)

4.1 Network Security

4.1.1 Network Infrastructure Analysis

4.1.2 Encryption and Decryption in Network

4.1.3 Firewall and its types

4.1.4 Wired and Wireless Security

4.1.5 Virtual Private Network

4.2 System Security

4.3 Email, Web and Database Security

4.4 User Security

4.4.1 Access

4.4.2 Files and Devices

4.4.3 Electronic Communications

4.5 Program Security

4.5.1 Common Security-Related Programming Problems

<u>Practical Works</u>

- **Configure routers, switches, and other network devices to enhance security.**
- **Assess and secure web applications against common security threats. Use tools like OWASP ZAP or Burp Suite for web application security testing.**

Configure firewalls to control and monitor network traffic.

Security and Protection:

The measure of resistance to or protection from harm is referred to as **security**. It revolves around the external environment of a system and requires a suitable protection system. The security of a computer system involves the protection of its resources like information stored, memory, processing unit, etc. from inconsistency, unauthorized access, and malicious changes, etc.

Security mainly emphasizes on the protection of physical resources of the system and the integrity of the information stored in it. Hence, security is a mechanism that protects the system and user's data stored in it against the interference caused by an external threat on the system.

The CIA Triad (Confidentiality, Integrity, and Availability) is a common model that forms the basis for the development of security systems. Confidentiality and Integrity are concerned with

keeping the data private and protected from malicious entities. Availability refers to the prevention of data being withheld by unauthorized actors.

The part of security mechanism that controls access to a system is referred to as **protection**. Protection defines the types of file access allowed to the users of the system. Thus, protection ensures the authorization of process and access to data.

Protection measures restrict the unauthorized users from accessing the resources and information stored in the system. Protection is required to intercept the intentional violation of an access restraint by a user. Therefore, protection is important to ensure the reliable access of resources.

Network Security:

All the measures used to safeguard a computer network's integrity and the data on it are collectively referred to as network security. Network security is crucial because it protects sensitive data from online threats and guarantees the network's dependability. Multiple security measures are used in successful network security plans to shield users and organizations from malware and online threats like distributed denial of service.

Computers, servers, wireless networks, and other associated devices make up a network. Many of these gadgets are open to possible intruders. Utilizing a range of hardware and software tools on a network or as software as a service is necessary for network security. As networks get increasingly complicated and businesses rely more on their networks and data to operate, security becomes more crucial. As threat actors develop new ways to target these more complex networks, security techniques must change.

Security is typically described as everyone's duty since every user on the network represents a potential vulnerability in that network, regardless of the exact method or business security plan.

Network Infrastructure Analysis:

Network security analysis is the process of maintaining the integrity and privacy of your organization and workers. It includes everything from creating strong passwords, installing antivirus and antimalware software to ensuring firewall protection and integrating best practices to protect the system from harmful spyware.

While no network is immune to attacks, network security allows you to create a barrier against hackers and intruders. It ensures that the data shared within the network is secure and protected from potential threats.

Besides this, by running the network security analysis, you get a close inspection of a network's structure, traffic, and data as it works in a collaborative environment. This way, you can easily detect and eliminate any potential vulnerabilities from the system by learning from other systems facing a similar issue.

Benefits of Network Security Analysis

1. Improved Speed

If we look at the current system, it takes several days for the network and system administrators to detect an anomaly and remove it from the system. This sometimes causes enormous data loss and results in a legitimate threat for all the network programs.

However, it is easier to get the data traffic synopses with network security analysis and detect suspicious traffic without any hassle. Moreover, you can share the data with all users on the network and resolve the issue as soon as possible.

2. Improved Detection, Reduced Damage

While many organizations still use the conventional approach to detect threats and anomalies, they still recognize peer-to-peer techniques to be useful and beneficial.

Here, ransomware attacks are the prime examples. If your organization has siloed cyber defense, you can never identify the root cause of the ransomware. But in the P2P approach, you can quickly learn from systems facing a similar issue and take measures to protect yourself from future vulnerabilities.

Encryption and Decryption in Network

Encryption

Encryption is the process of transforming plaintext data into ciphertext with the help of an algorithm and an encryption key. Ciphertext is basically unreadable without the decryption key, adding another degree of security to sensitive data. Encryption methods differ in complexity, with some being more secure than others.

Decryption

Decryption is the process of transforming ciphertext back into plaintext using the decryption key. Only persons or entities that have the right decryption key may access the original data. Decryption should be done securely to avoid unauthorised access to sensitive information.

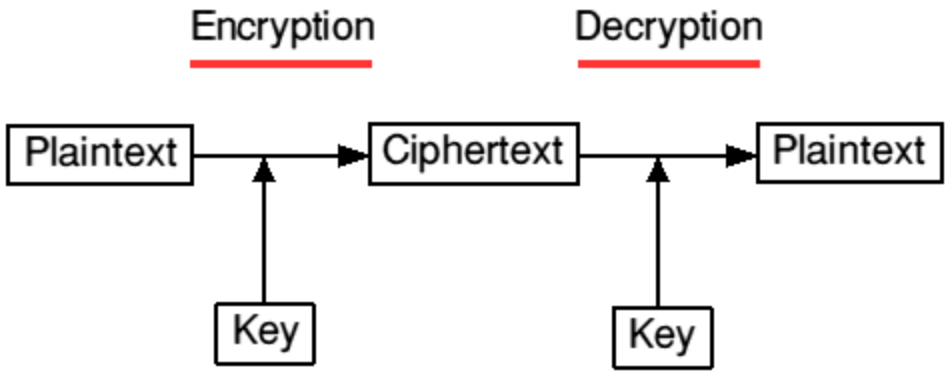


Fig. 2. Components of Encryption and Decryption

Firewall and its types:

A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Its primary purpose is to establish a barrier between a trusted internal network and untrusted external networks, such as the internet, to prevent unauthorized access and protect data integrity and confidentiality.

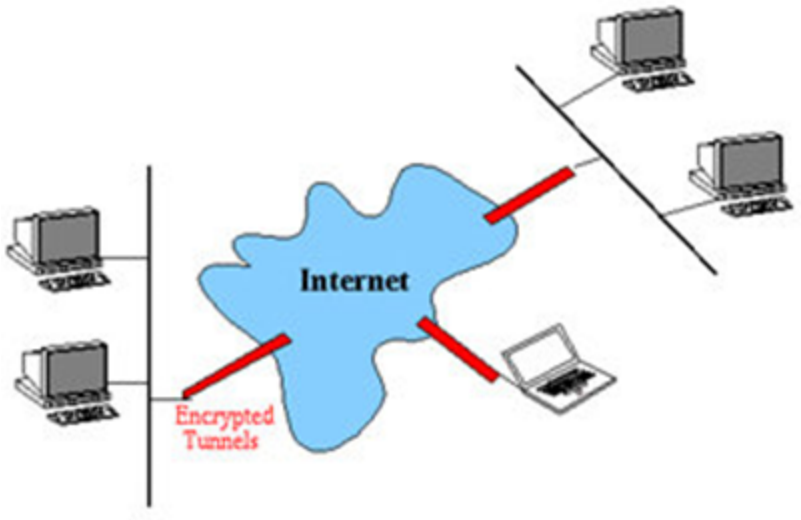
Types of Firewalls

1. **Packet-Filtering Firewalls:**
    - **Description:** These firewalls inspect packets at a low level (IP layer) and make decisions based on the source and destination addresses, ports, and protocols.
    - **Pros:** Simple and efficient for basic filtering tasks.
    - **Cons:** Limited in-depth inspection, vulnerable to certain types of attacks.
2. **Stateful Inspection Firewalls:**
    - **Description:** Also known as dynamic packet filtering, these firewalls track the state of active connections and make decisions based on the context of traffic.
    - **Pros:** More secure than packet-filtering firewalls as they track the state of connections.
    - **Cons:** More complex and resource-intensive.
3. **Proxy Firewalls:**
    - **Description:** These firewalls act as intermediaries between users and the services they access. They make requests on behalf of the client and relay responses back to the client.
    - **Pros:** Can perform deep packet inspection and provide anonymity.
    - **Cons:** Can be slower due to the additional processing required.
4. **Next-Generation Firewalls (NGFW):**
    - **Description:** NGFWs combine traditional firewall features with advanced functionalities like deep packet inspection, intrusion prevention, and application awareness.
    - **Pros:** Comprehensive protection against a wide range of threats.
    - **Cons:** More expensive and complex to manage.

5. **Unified Threat Management (UTM) Firewalls:**
    - **Description:** These firewalls integrate multiple security features, such as antivirus, anti-spam, content filtering, and intrusion detection, into a single appliance.
    - **Pros:** Simplifies management by consolidating security features.
    - **Cons:** Can become a single point of failure and may impact performance.
6. **Cloud Firewalls:**
    - **Description:** Also known as firewall-as-a-service, these are hosted in the cloud and protect cloud infrastructure and applications.
    - **Pros:** Scalable and easy to deploy for cloud environments.
    - **Cons:** Dependence on internet connectivity and provider reliability.
7. **Network Address Translation (NAT) Firewalls:**
    - **Description:** These firewalls modify network address information in packet headers while in transit, effectively hiding internal network addresses.
    - **Pros:** Enhances security by obscuring internal IP addresses.
    - **Cons:** May complicate certain types of traffic, such as peer-to-peer applications.
8. **Web Application Firewalls (WAF):**
    - **Description:** Specifically designed to protect web applications by filtering and monitoring HTTP/HTTPS traffic and preventing attacks like SQL injection and cross-site scripting (XSS).
    - **Pros:** Provides specialized protection for web applications.
    - **Cons:** Limited scope, focusing only on web traffic.

Virtual Private Network

VPN stands for Virtual Private Network. It refers to a safe and encrypted network that allows you to use network resources in a remote manner. Using VPN, you can create a safe connection over a less secure network, e.g. internet. It is a secure network as it is completely isolated from rest of the internet. The government, businesses, military can use this network to use network resources securely.



VPN is free to use and it uses site-to-site and remote access methods to work. It uses an arrangement of encryption services to establish a secure connection. It is an ideal tool for encryption; it provides you strong AES256 encryption with an 8192bit key.

VPN works by creating a secure tunnel using powerful VPN protocols. It hides your IP address behind its own IP address that encrypts all your communication. Thus, your communication passes through a secure tunnel that allows you use network resources freely and secretly.

VPN protocols

There are several different VPN protocols that are used to create secure networks. Some of such protocols are given below;

- IP security (IPsec)
- Point to Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

System Security:

System security refers to the practices and measures implemented to protect computer systems from threats and unauthorized access. It involves ensuring the availability, confidentiality, and integrity of systems and the data they handle. Key components of system security include:

1. **Threat Identification and Prevention**:
    - Identifying potential threats like viruses, malware, and unauthorized users.
    - Implementing measures such as antivirus software, firewalls, and intrusion detection systems to prevent these threats.
2. **Access Control**:
    - Restricting access to system resources to authorized users only.

- Using methods such as passwords, biometrics, and multi-factor authentication to ensure only authorized individuals can access sensitive information.

3. **Data Protection**:
    - Ensuring the confidentiality and integrity of data by using encryption for data at rest and in transit.
    - Regularly backing up data to prevent loss from accidental or malicious events.
4. **System Monitoring and Maintenance**:
    - Continuously monitoring systems for signs of suspicious activity.
    - Regularly updating software and applying security patches to address vulnerabilities.
5. **Security Policies and Procedures**:
    - Developing and enforcing security policies that define acceptable use and access controls.
    - Conducting regular security audits and training for employees to recognize and avoid security threats.
6. **Incident Response and Recovery**:
    - Establishing protocols for responding to security breaches, including containment, eradication, and recovery steps.
    - Analyzing incidents to improve future security measures and prevent recurrence.
7. **Physical Security**:
    - Protecting the physical components of the system, such as servers and network equipment, from theft, damage, or unauthorized access.

o

Email, Web and Database Security:

Securing email, web applications, and databases is critical for maintaining the confidentiality, integrity, and availability of information. Here's a breakdown of the security measures for each:

Email Security

1. **Encryption**:
    - **Transport Layer Security (TLS)**: Ensure emails are encrypted during transmission.
    - **End-to-End Encryption**: Use encryption protocols like PGP or S/MIME for end-to-end security.
2. **Authentication**:
    - **Multi-Factor Authentication (MFA)**: Require multiple forms of verification.
    - **SPF, DKIM, and DMARC**: Implement these protocols to verify the sender's identity and protect against spoofing.
3. **Anti-Phishing Measures**:

- **Training and Awareness**: Regularly train users to recognize phishing attempts.
- **Phishing Filters**: Use advanced spam and phishing detection filters.

4. **Malware Protection**:
   - **Anti-Virus and Anti-Malware Software**: Regularly update and scan emails for malicious attachments or links.
5. **Access Control**:
   - **Least Privilege**: Ensure users have the minimum necessary access.
   - **Regular Audits**: Perform regular audits of email account activities.

Web Security

1. **Secure Development Practices**:
   - **Input Validation**: Validate all inputs to prevent SQL injection, XSS, and other attacks.
   - **Secure Coding Guidelines**: Follow OWASP guidelines for secure coding.
2. **Authentication and Authorization**:
   - **Strong Password Policies**: Enforce strong, complex passwords.
   - **Role-Based Access Control (RBAC)**: Implement RBAC to restrict access based on user roles.
3. **Encryption**:
   - **HTTPS**: Use HTTPS to encrypt data in transit.
   - **TLS/SSL Certificates**: Regularly update and manage SSL certificates.
4. **Security Testing**:
   - **Penetration Testing**: Regularly conduct penetration testing to identify vulnerabilities.
   - **Vulnerability Scanning**: Use automated tools to scan for vulnerabilities.
5. **Content Security Policy (CSP)**:
   - **CSP Headers**: Implement CSP headers to mitigate XSS and data injection attacks.
6. **Web Application Firewalls (WAF)**:
   - **WAF Deployment**: Use WAFs to filter and monitor HTTP traffic.

Database Security

1. **Access Control**:
   - **User Permissions**: Use granular permissions to restrict access.
   - **Least Privilege Principle**: Ensure users have only the access they need.
2. **Encryption**:
   - **Data-at-Rest Encryption**: Encrypt sensitive data stored in the database.
   - **Data-in-Transit Encryption**: Use TLS/SSL to encrypt data transmitted to and from the database.
3. **Regular Updates and Patching**:
   - **Patch Management**: Regularly update database software to fix vulnerabilities.
4. **Backup and Recovery**:

- **Regular Backups**: Ensure regular backups of the database.
- **Disaster Recovery Plan**: Have a plan in place for data recovery.

5. **Monitoring and Logging**:
    - **Audit Logs**: Maintain and regularly review audit logs of database activities.
    - **Intrusion Detection Systems (IDS)**: Use IDS to detect and respond to suspicious activities.
6. **SQL Injection Prevention**:
    - **Prepared Statements**: Use prepared statements to prevent SQL injection.
    - **Stored Procedures**: Implement stored procedures for database queries.

4.6User Security

Access

User access security authorization is the process of granting someone permission to carry out a task. It explains how to find out if a user is authorised to use a resource or not. It may represent data and information to which a user has access.
Another name for it is AuthZ. In general, authorization works in conjunction with authentication to allow the system to determine who is accessing the information. A security framework called **authorization** is used to determine the level of access that a user or client has to certain system resources, like software, files, services, data, and application features. Authentication is typically required before authorization in order to verify the identity of the customer. Generally, system administrators (SA) give access rights to certain customers and system resources.

A system verifies an authenticated user's access rules during authorization and decides whether to grant or deny them access to resources. In order to facilitate the deployment and management of applications, modern, multiuser operating systems rely on well-designed authorization processes.
Verification is necessary for important elements including user type, quantity, and credentials, as well as associated roles and actions. Role-based authorization, for example, can be assigned to user groups that require specific user resource tracking rights.
Moreover, authorization can be based on an enterprise authentication structure such as Active Directory (AD) for seamless integration with security policies. For instance, by connecting with Microsoft Windows and the Internet Information Server (IIS), ASP.NET provides authorization and authentication services for web-based.NET applications.
For certain resources, Windows supports Access Control Lists (ACL) via the New Technology File System (NTFS). The final authority on resource access is held by the ACL. For authorization support, the.NET Framework provides an alternative role-based security mechanism.
Similar to code access security checks, role-based security is a dynamic method that works well with server applications. Authorized application users are determined based on their responsibilities.

Files and Devices:

File and device security is essential for protecting sensitive information, preventing unauthorized access, and maintaining the integrity of data within an organization. Here's a comprehensive approach to securing files and devices:

File Security

1. **Encryption**
    - **Data-at-Rest Encryption**: Encrypt sensitive files stored on devices or servers to prevent unauthorized access if the storage medium is compromised.
    - **Data-in-Transit Encryption**: Use secure communication protocols (e.g., TLS/SSL) to encrypt data transmitted over networks, preventing interception by unauthorized parties.
2. **Access Control**
    - **File Permissions**: Implement granular access controls based on the principle of least privilege, ensuring users have access only to files necessary for their roles.
    - **Role-Based Access Control (RBAC)**: Assign permissions based on predefined roles within the organization to streamline access management and minimize errors.
3. **Backup and Recovery**
    - **Regular Backups**: Schedule regular backups of critical files to ensure data availability in case of accidental deletion, hardware failure, or ransomware attacks.
    - **Secure Backup Storage**: Store backups securely, preferably offline or in a separate location, to protect against data loss due to cyberattacks or disasters.
4. **Data Loss Prevention (DLP)**
    - **Content Discovery**: Implement DLP solutions to identify and classify sensitive information within files, such as personally identifiable information (PII) or intellectual property.

- **Monitoring and Blocking**: Monitor data flows and block unauthorized transfers of sensitive files outside the organization's network.

5. **File Integrity Monitoring (FIM)**
    - **Continuous Monitoring**: Deploy FIM tools to detect unauthorized changes or modifications to files, alerting administrators to potential security incidents or compliance violations.
6. **Audit Trails**
    - **Logging and Auditing**: Maintain audit logs of file access and modifications to track user activities and ensure compliance with security policies and regulations.
    - **Regular Review**: Periodically review audit logs to detect suspicious behavior and investigate potential security breaches promptly.

Device Security

1. **Endpoint Protection**
    - **Anti-Virus and Anti-Malware**: Install and regularly update endpoint security software to detect and remove malicious software that could compromise device security.
    - **Host-Based Intrusion Detection/Prevention Systems (HIDS/HIPS)**: Implement HIDS/HIPS to monitor and respond to suspicious activities on individual devices.
2. **Device Encryption**
    - **Full Disk Encryption**: Encrypt entire storage devices (e.g., hard drives, SSDs) to protect data-at-rest against unauthorized access in case of theft or loss.
    - **Removable Media Encryption**: Encrypt USB drives and other removable media to prevent data leakage if devices are lost or stolen.
3. **Patch Management**
    - **Regular Updates**: Apply security patches and updates promptly to operating systems, applications, and firmware to mitigate vulnerabilities exploited by cyber threats.
    - **Automated Patching**: Use automated tools to streamline patch management processes and reduce the risk of human error.
4. **Network Access Control (NAC)**
    - **Device Authentication**: Implement NAC solutions to authenticate devices before allowing them to connect to the network, enforcing security policies based on device health and compliance.
5. **Mobile Device Management (MDM)**
    - **Policy Enforcement**: Use MDM solutions to enforce security policies on mobile devices, including password requirements, encryption settings, and app installation restrictions.
    - **Remote Wipe**: Enable remote wiping capabilities to erase sensitive data from lost or stolen devices to prevent unauthorized access.

Electronic Communications

Electronic communications security (eComm security) refers to the measures and practices designed to protect the confidentiality, integrity, and availability of electronic communications. This field encompasses a wide range of technologies, protocols, and strategies aimed at securing

various forms of electronic communication, including email, instant messaging, VoIP (Voice over Internet Protocol), video conferencing, and more.

Key aspects of electronic communications security include:

1. **Encryption**: Encryption is fundamental to eComm security. It involves encoding information so that only authorized parties can access and understand it. This prevents unauthorized interception and eavesdropping. Strong encryption algorithms and protocols are essential for securing sensitive communications.
2. **Authentication**: Authentication ensures that communicating parties are who they claim to be. This can involve passwords, digital certificates, biometrics, or other methods to verify identities and prevent impersonation.
3. **Integrity**: Integrity ensures that data transmitted is not altered or tampered with during transmission. Hash functions and digital signatures are commonly used to verify data integrity.
4. **Access Control**: Limiting access to electronic communications to authorized users and devices helps prevent unauthorized access and misuse. Access control mechanisms include firewalls, VPNs (Virtual Private Networks), and role-based access controls.
5. **Network Security**: Protecting the underlying networks that transmit electronic communications is crucial. This includes securing routers, switches, and other network infrastructure components from attacks and vulnerabilities.

Program Security

Program security, also known as software security, refers to the measures and practices designed to protect computer programs and software systems from vulnerabilities and attacks that could compromise their integrity, confidentiality, and availability. It involves a range of techniques and strategies aimed at identifying, mitigating, and preventing security risks throughout the software development lifecycle and during program execution.

Key aspects of program security include:

1. **Secure Design**: Building security into software from the initial design phase, considering potential threats and risks, and implementing appropriate security controls.
2. **Secure Coding Practices**: Following coding standards and best practices to minimize vulnerabilities such as buffer overflows, injection flaws (e.g., SQL injection, XSS), and other common software weaknesses.
3. **Authentication and Authorization**: Implementing mechanisms to verify the identities of users and ensure they have appropriate permissions to access resources within the program.
4. **Encryption**: Utilizing strong encryption algorithms and protocols to protect sensitive data at rest and in transit within the program.
5. **Input Validation**: Validating and sanitizing input from users and external sources to prevent injection attacks and other forms of malicious input.

4.6.1 Common Security-Related Programming Problems

Common security-related programming problems include:

1. **Injection Flaws**: This occurs when untrusted data is sent to an interpreter as part of a command or query. Examples include SQL injection, LDAP injection, and OS command injection.
2. **Cross-Site Scripting (XSS)**: This happens when untrusted data is sent to a web browser without proper validation or escaping, allowing attackers to execute scripts in the victim's browser.
3. **Broken Authentication**: Issues like improper session handling, weak passwords, or not implementing multi-factor authentication can lead to compromised user accounts.
4. **Sensitive Data Exposure**: Storing sensitive information (like passwords or credit card details) without encryption or using weak encryption methods can expose data to unauthorized access.
5. **Security Misconfiguration**: Failure to implement security best practices such as unnecessary open ports, default passwords, or leaving debugging information in production can lead to vulnerabilities.