LECTURE # 2

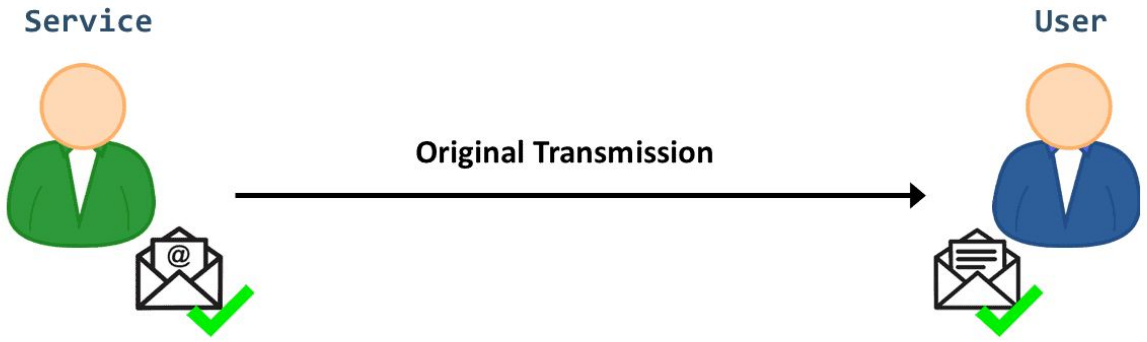
Attack and Vulnerabilities Models

ATTACK AND VULNERABILITY MODELS

- **Attack models**: Methods used by attackers to compromise systems or networks
- **Vulnerabilities models**: Weaknesses or flaws in systems that can be exploited by attack models.
- **Importance**: Understanding attack models and vulnerabilities helps identify, mitigate, and prevent potential threats in cybersecurity.

Normal Communication

- Normal communication refers to the exchange of data or information between two or more parties over a network without any interference, manipulation, or unauthorized access.
- The integrity, confidentiality, and availability of the data are preserved.
- Typical Flow:
    1. Sender
    2. Channel
    3. Receiver



ATTACK MODELS

An **attack model** is a systematic representation of the different ways an attacker can compromise the security of a system. It helps identify potential threats and vulnerabilities to guide defensive measures.

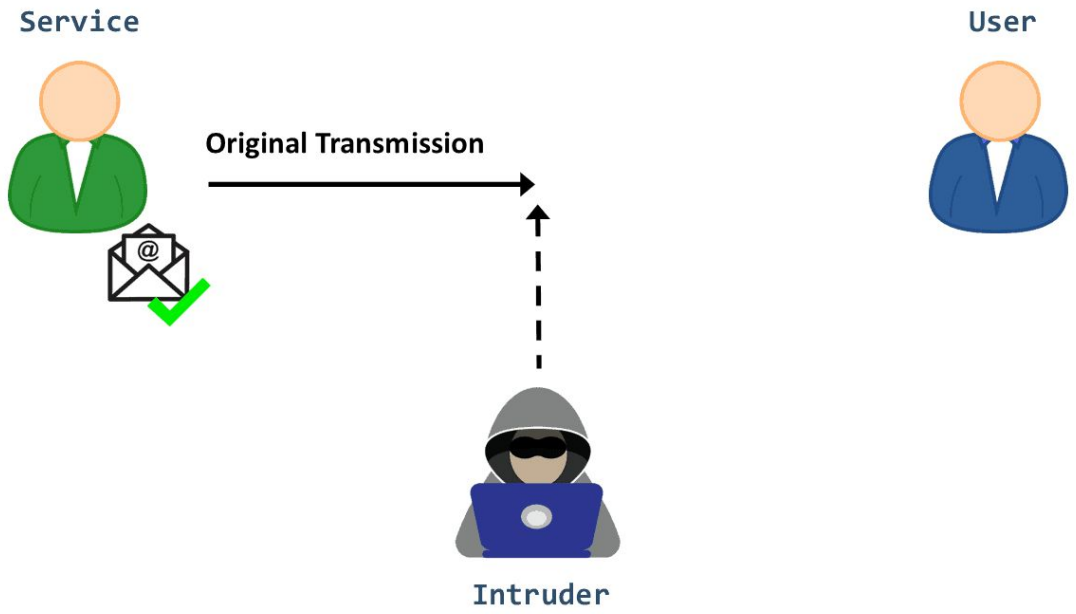
Purpose:
Attack models are used to:

- Understand how attackers operate.
- Identify potential entry points and weaknesses.
- Evaluate security mechanisms to protect against attacks.

ATTACK MODELS

Interruption

An attack that **disrupts** services or the normal functioning of a system, causing legitimate users to be unable to access resources (violates the **Availability)**



ATTACK MODELS

Interruption

Examples:

- **Denial of Service (DoS)**: Flooding a server with traffic to make it unavailable.
- **Distributed Denial of Service (DDoS)**: Same as DoS but involves multiple machines (botnet).

Impacts:

- Business downtime, financial losses, and damaged reputation

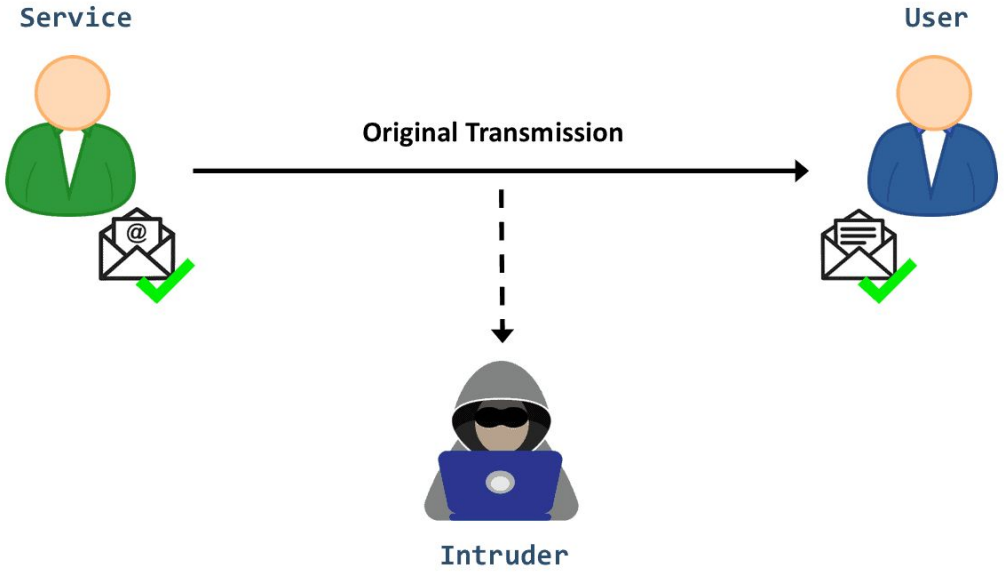
Mitigation:

- Use of load balancers and Intrusion Prevention Systems (IPS).
- Implement redundancy and failover systems

ATTACK MODELS

Interception

Unauthorized access to data or resources, often involving eavesdropping or network sniffing to capture sensitive information. (Compromises **Confidentiality)**



ATTACK MODELS

Interception

Examples:

- **Man-in-the-Middle (MitM) Attack**: Attacker secretly intercepts communication between two parties.
- **Packet Sniffing**: Capturing data packets traveling over a network to extract sensitive information (e.g., login credentials).

Impacts:

- Loss of confidentiality and sensitive data exposure

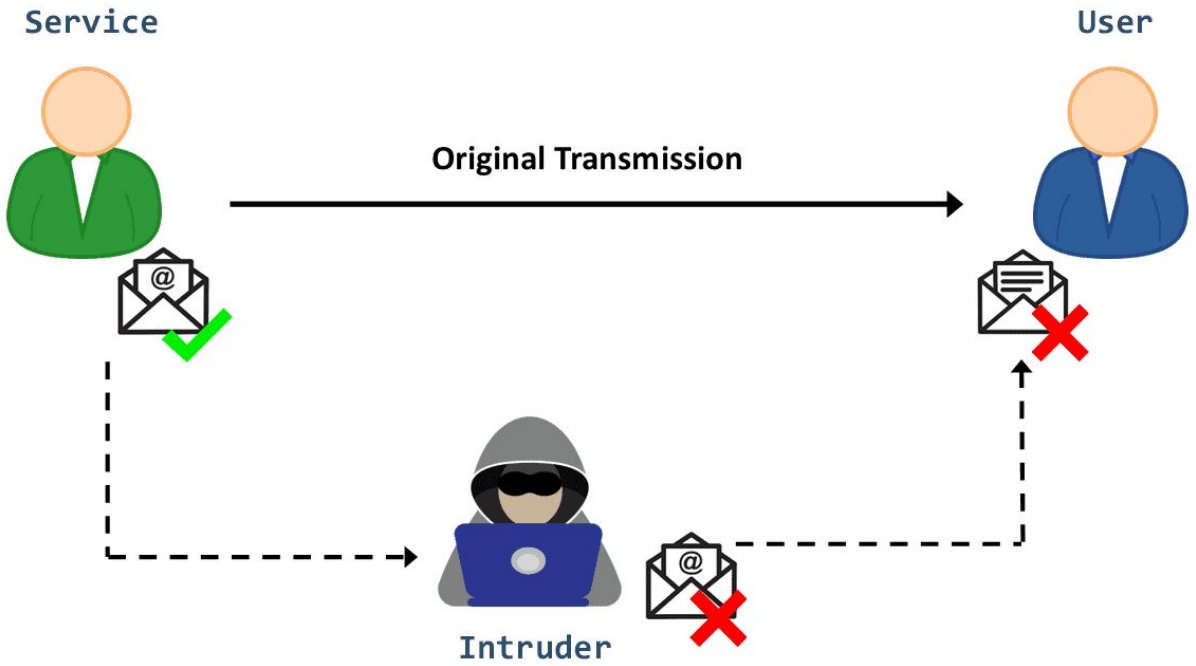
Mitigation:

- **Encryption** (e.g., SSL/TLS for secure communication).
- **VPNs** to secure network traffic

ATTACK MODELS

Modification

Tampering with data or system resources to alter them maliciously. Attackers modify information without authorization. (Violates **Integrity**.)



ATTACK MODELS

Modification

Examples:

- **SQL Injection**: Modifying SQL queries to manipulate database contents.
- **DNS Spoofing**: Altering DNS records to redirect traffic to malicious sites.

Impacts:

- Data corruption, misleading information, or unauthorized actions taken by a system

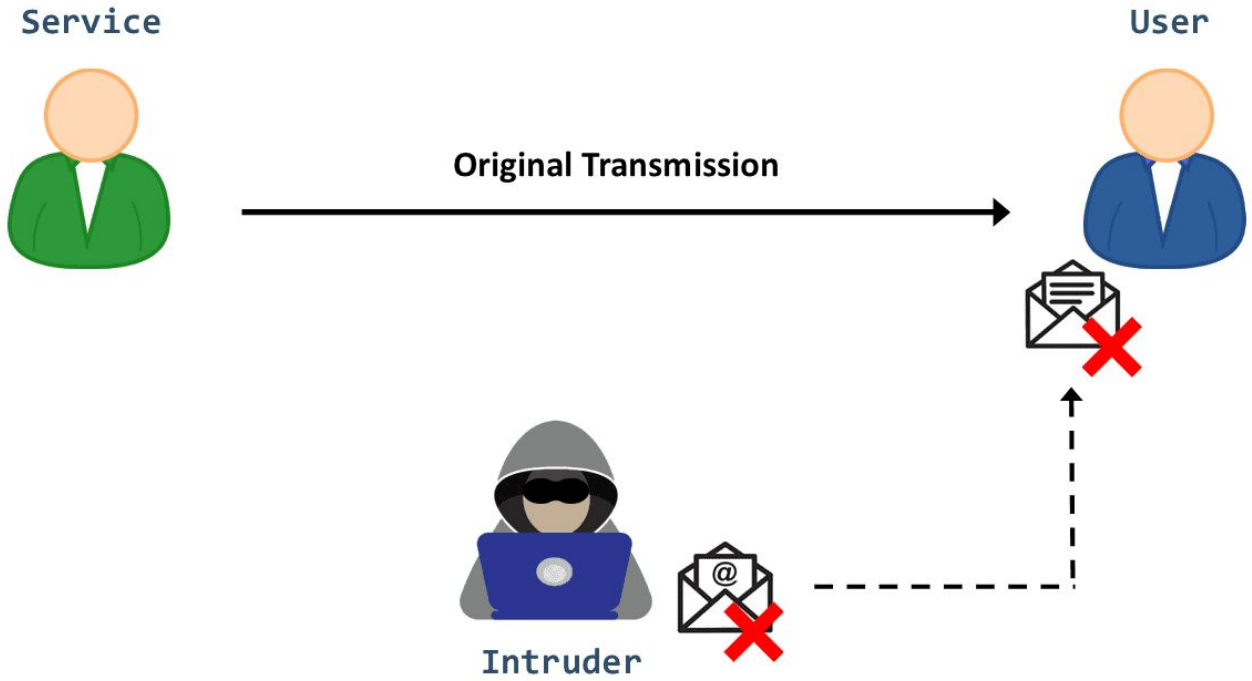
Mitigation:

- Input validation and sanitization. (Prevent SQL injection)
- Use **firewalls** and Intrusion Detection Systems (IDS)

ATTACK MODELS

Fabrication

Attackers create false information, messages, or data that never existed within the system.(Violates **Authenticity** and sometimes **Integrity**.)



ATTACK MODELS

Fabrication

Examples:

- **Email Spoofing**: Falsifying email headers to send fraudulent messages that appear to be from trusted sources.
- **Counterfeit Websites**: Creating fake websites that mimic legitimate ones to deceive users

Impacts:

- Fraud, identity theft, and reputational damage to the original service provider

Mitigation:

- Implement email authentication protocols (SPF, DKIM, DMARC).
- Encourage users to check URL authenticity and security certificates

ATTACK MODELS

Disclosure

Unauthorized access or exposure of sensitive, confidential information to individuals who should not have access.

ATTACK MODELS

Disclosure

Examples:

- **Data Breaches**: Exposure of user data (e.g., credit card numbers, passwords) through hacking.
- **Internal Threats**: Employees leaking confidential information to external parties

Impacts:

- Legal liabilities, financial losses, and customer distrust

Mitigation:

- Encrypt sensitive data both at rest and in transit.
- Employ **data access controls** and **user monitoring**

ATTACK MODELS

Deception

Misleading or tricking users or systems into making incorrect decisions that benefit the attacker.

ATTACK MODELS

Deception

Examples:

- **Phishing Attacks**: Attackers send fake emails posing as banks or services, tricking users into sharing passwords or financial data.
- **Social Engineering**: A caller pretends to be IT support and deceives an employee into giving login credentials.

Impacts:

- Data theft, fraud, and unauthorized system access

Mitigation:

- Educate users on **phishing awareness**.
- Implement **anti-phishing tools** and filters

ATTACK MODELS

Usurpation

Unauthorized control or takeover of a system, network, or data.

ATTACK MODELS

Usurpation

Examples:

- **Rootkits**: Malware that allows attackers to gain privileged access to a system.
- **Privilege Escalation**: Exploiting vulnerabilities to gain higher-level access than intended.(e.g., a normal user gaining admin rights)

Impacts:

- Complete control of systems by the attacker, leading to data theft, tampering, or sabotage.

Mitigation:

- Apply **least privilege** principles for user access.
- Implement strong **authentication** mechanisms (e.g., MFA).

VULNERABILITY MODELS

Information Leakage

Systems that **leak information** unintentionally, potentially exposing sensitive data to unauthorized individuals.

VULNERABILITY MODELS

Information Leakage

Examples:

- **Insecure APIs**: Poorly designed APIs that expose internal details or sensitive data.
- **Side-channel Attacks**: Exploiting hardware weaknesses to gather data (e.g., Spectre and Meltdown vulnerabilities).

Impacts:

- Exposure of private data, leading to identity theft or unauthorized access.

Mitigation:

- Secure API development with proper authentication and data handling.
- Regularly update and patch systems to protect against side-channel attacks.

VULNERABILITY MODELS

Corruption

Systems or data that can be easily **corrupted** due to weaknesses, either intentionally (by attackers) or unintentionally (due to bugs or failures).

VULNERABILITY MODELS

Corruption

Examples:

- **Buffer Overflows**: Attackers exploit poorly written code to overwrite system memory and cause crashes or unauthorized code execution.
- **Data Corruption**: File system errors or malware leading to corrupted files.

Impacts:

- System crashes, loss of data integrity, and compromised security.

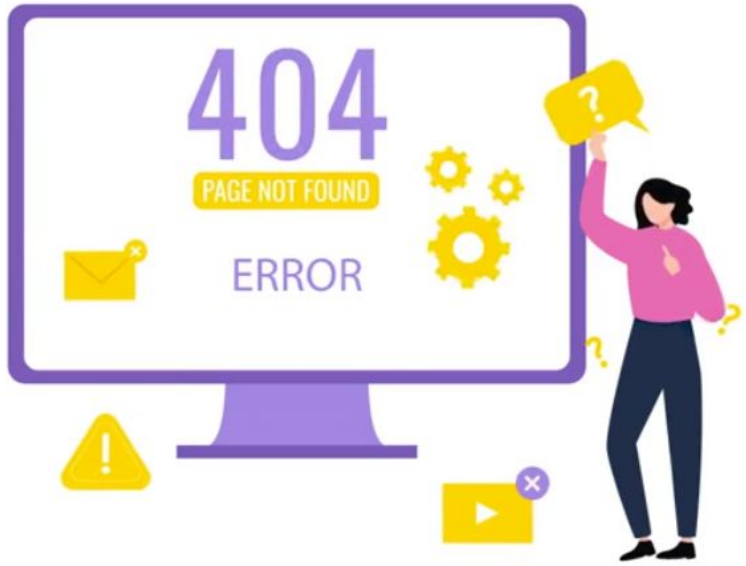
Mitigation:

- Use **secure coding practices** to avoid vulnerabilities like buffer overflows
- Implement regular system checks and backups

VULNERABILITY MODELS

Unavailability

Systems that are vulnerable to becoming **unavailable**, either through attacks or system failures.



VULNERABILITY MODELS

Unavailability

Examples:

- **Ransomware**: Encrypting user data and making systems unavailable until a ransom is paid.
- **Hardware Failures**: System outages due to server crashes or network issues.

Impacts:

- Service unavailability, leading to financial loss and productivity decline.

Mitigation:

- **Disaster Recovery Plans**: Develop strategies to restore systems after failure.
- Implement **redundant systems** to ensure high availability

CASE STUDIES

Case Study 3: SolarWinds Attack (Usurpation and Interception)

- **Incident**: In 2020, hackers compromised SolarWinds' software, giving them access to the networks of numerous high-profile organizations.
- **Attack Types**: Usurpation (attackers gained control of systems), Interception (they accessed sensitive data).
- **Lessons Learned**: The importance of securing supply chains and monitoring third-party software.

THANK YOU