STRIDE Framework

The STRIDE framework is **a threat modeling approach developed by Microsoft that helps identify potential security threats in a system**. It categorizes threats based on the types of attacks or vulnerabilities that could be exploited, providing a structured way to assess and mitigate risks. STRIDE stands for **Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege**. Each category represents a specific type of threat.

Components of STRIDE:

1. **Spoofing**:

- Definition: Spoofing occurs when an **attacker impersonates another user or device**, usually by falsifying identity credentials, such as usernames, passwords, or IP addresses.
- Example: An attacker uses stolen credentials to log in to a system as an authorized user, gaining access to restricted resources.
- Mitigation: Implement **strong authentication mechanisms** (e.g., multi-factor authentication), secure password policies, and digital certificates to verify identity.

2. **Tampering**:

- Definition: Tampering involves **maliciously modifying data or code**. This can **occur in transit, at rest, or even within an application**, compromising data integrity and potentially leading to unauthorized actions.
- Example: An attacker intercepts and modifies network traffic to inject malicious commands or modify data in a database.
- Mitigation: **Use encryption** to protect data in transit, **implement integrity checks** (e.g., digital signatures or checksums), and control file permissions to **restrict data access**.

3. **Repudiation**:

- Definition: Repudiation refers to the ability of **users or attackers to deny actions they have performed**. Without proper logging and accountability, it can be difficult to trace activities back to the responsible party.
- Example: A user performs a transaction but later denies it, and there is no log or evidence to prove the action.
- Mitigation: **Implement audit logs with timestamps and user identifiers to track actions**. Ensure logs are **secure and tamper-resistant for accountability**.

4. **Information Disclosure**:

- Definition: Information disclosure involves **unauthorized access to sensitive information, exposing it to unintended recipients**. This compromises confidentiality.
- Example: Sensitive data like personally identifiable information (PII) is accidentally exposed via an unsecured API endpoint or a public-facing server.
- Mitigation: **Use encryption** for data storage and transmission, control access with **role-based permissions**, and **conduct regular audits to detect potential data leaks**.

5. **Denial of Service (DoS)**:

- Definition: Denial of Service occurs when **an attacker overwhelms a system, network, or application, causing it to become unavailable to legitimate users**.
- Example: An attacker sends a massive number of requests to a server, exhausting its resources and making it inaccessible to other users.
- Mitigation: **Implement rate limiting, load balancing, and redundancy**. Employ DDoS protection measures, such as web application firewalls (WAFs) and traffic filtering.

6. **Elevation of Privilege**:

- Definition: Elevation of privilege occurs when **an attacker gains higher access levels than intended**, allowing them to perform actions beyond their normal permissions.
- Example: A regular user exploits a vulnerability to gain administrator access and modify system configurations.
- Mitigation: Use the principle of **least privilege**, regularly **patch** systems to fix vulnerabilities, and implement **strict access control** policies.

Summary of STRIDE:

Threat Type	Definition	Example	Mitigation
Spoofing	Impersonating another user or system	Using stolen credentials	Multi-factor authentication, secure passwords
Tampering	Modifying data or code maliciously	Modifying database entries	Encryption, integrity checks
Repudiation	Denying an action or transaction	Denying a transaction with no audit log	Secure audit logging
Information Disclosure	Unauthorized access to sensitive information	Exposing PII via unsecured API	Encryption, access control
Denial of Service	Making a system or service unavailable by overwhelming it	Sending excessive requests to exhaust server resources	Rate limiting, redundancy, DDoS protection
Elevation of Privilege	Gaining unauthorized access to higher privileges	Exploiting a vulnerability to gain admin rights	Least privilege, regular patching

Purpose of STRIDE in Threat Modeling:

The STRIDE framework helps security teams systematically identify potential threats and vulnerabilities, enabling them to develop countermeasures for each specific threat type. It is often used during system design to assess security risks and ensure that appropriate protections are in place to defend against different types of attacks.