# Threat Modeling Framework

**Threat Modeling** is a security-focused process used to identify, assess, and address potential security risks in a system. It provides a structured approach to understanding possible attack vectors and vulnerabilities and helps prioritize mitigations based on risk severity.

## Purpose of Threat Modeling

- Identify possible security threats to the system
- Evaluate vulnerabilities that could be exploited
- Design defensive mechanisms to mitigate risks
- Prioritize risk mitigation based on potential impact

## Key Elements of Threat Modeling

1. **Assets** – What are you protecting (e.g., data, systems, hardware)?
2. **Threat Actors** – Who might attack the system (e.g., hackers, malicious insiders)?
3. **Entry Points** – How can attackers access the system (e.g., APIs, login forms)?
4. **Threats** – What are the possible attacks (e.g., SQL injection, DDoS)?
5. **Security Controls** – What mitigations are in place (e.g., encryption, firewalls)?

## Common Threat Modeling Frameworks

### 1. STRIDE

Developed by Microsoft, STRIDE helps identify threats based on six categories:

- **S**poofing: Impersonating another user/system.
- **T**ampering: Unauthorized data modification.
- **R**epudiation: Denying actions performed.
- **I**nformation Disclosure: Leaking sensitive information.
- **D**enial of Service: Disrupting service availability.

- **E**levation of Privilege: Gaining unauthorized privileges.

**2. DREAD**

DREAD is a risk assessment framework that evaluates each threat based on five factors:

- **D**amage potential: How much damage could the attack cause?
- **R**eproducibility: How easy is it to reproduce the attack?
- **E**xploitability: How easy is it to exploit the vulnerability?
- **A**ffected users: How many users are affected?
- **D**iscoverability: How easily can the vulnerability be discovered?

**3. PASTA (Process for Attack Simulation and Threat Analysis)**

PASTA is a seven-step risk-centric threat modeling framework, focusing on business impact and simulating real-world attacks. The stages include:

1. Definition of Objectives
2. Definition of Technical Scope
3. Application Decomposition
4. Threat Analysis
5. Vulnerability & Weakness Analysis
6. Attack Modeling & Simulation
7. Risk & Impact Analysis

**4. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)**

OCTAVE is a self-directed threat modeling methodology focusing on organizational risk. It includes three main phases:

1. Identify key information assets.
2. Identify threats to those assets.
3. Evaluate the organization’s security posture.

**5. VAST (Visual, Agile, and Simple Threat)**

VAST integrates threat modeling into the Agile development lifecycle, making it more scalable across larger enterprises. It provides two models:

- **Application Threat Model** for individual applications
- **Operational Threat Model** for infrastructure

## Steps in the Threat Modeling Process

- **Identify Assets**

  Determine what critical assets (e.g., data, systems) you need to protect.

- **Create an Architecture Diagram**

  Model the system's architecture, including components, data flow, entry points, and trust boundaries.

- **Identify Threats**

  Use frameworks like STRIDE or DREAD to identify potential threats that could exploit vulnerabilities.

- **Mitigation**

  Propose security controls to address each identified threat (e.g., firewalls, encryption, authentication).

- **Prioritize Threats**

  Use a risk assessment framework (e.g., DREAD) to prioritize threats based on their severity and potential impact.

- **Document the Process**

  Maintain a detailed record of the identified threats, security controls, and decisions made throughout the process.

## Benefits of Threat Modeling

- **Proactive Risk Management**: Identifies potential vulnerabilities before attackers exploit them.
- **Improved Security Posture**: Ensures a more secure design and better prioritization of security efforts.
- **Cost Efficiency**: Reduces the cost of fixing security issues by addressing them early in the development process.
- **Continuous Improvement**: Enables ongoing refinement and optimization of security measures as the system evolves.

**Tools for Threat Modeling**

- **Microsoft Threat Modeling Tool**: Helps to apply the STRIDE model and visualize potential threats.
- **OWASP Threat Dragon**: An open-source tool to model threats and develop mitigation strategies.
- **IriusRisk**: A platform for threat modeling and risk management.
- **ThreatModeler**: An automated tool for performing enterprise-level threat modeling.

## Conclusion

Threat modeling is an essential part of the security development lifecycle, providing a structured way to identify, assess, and mitigate risks before they can be exploited. Whether using STRIDE, DREAD, PASTA, or other methodologies, threat modeling ensures that systems are designed with security in mind from the outset.