

Objective Threat Model (OTM)

Compare and Contrast with STRIDE and MITRE ATT&CK[®]

by ChatGPT 4o 2024-12-22

STRIDE

STRIDE is a threat modeling framework that categorizes security threats into six distinct types, each focusing on a specific aspect of system vulnerabilities. Its name is an acronym derived from these categories:

1. Spoofing: Impersonating a trusted identity (e.g., user, process, or device) to gain unauthorized access.
2. Tampering: Unauthorized modification of data, code, or system components.
3. Repudiation: The ability of users or entities to deny their actions, often due to a lack of proper logging or auditing.
4. Information Disclosure: Unauthorized exposure or access to sensitive information, such as personal data or system details.
5. Denial of Service (DoS): Actions that disrupt or degrade system availability, preventing legitimate users from accessing resources.
6. Elevation of Privilege: Exploiting vulnerabilities to gain higher levels of access or permissions than authorized.

Each category helps identify potential security risks, enabling targeted mitigations to strengthen a system's defenses. STRIDE is commonly used in the context of designing secure systems and evaluating existing architectures.

MITRE ATT&CK[®]

MITRE ATT&CK[®] (Adversarial Tactics, Techniques, and Common Knowledge) is a comprehensive framework that categorizes and documents the behaviors, tactics, and techniques used by cyber adversaries across various stages of an attack. It provides a structured approach for understanding and countering threats. Key aspects include:

1. Tactics: High-level objectives that attackers aim to achieve, such as initial access, persistence, or data exfiltration.

2. Techniques: Specific methods adversaries use to achieve these objectives, such as phishing, privilege escalation, or command and control.
3. Sub-techniques: More granular descriptions of techniques, detailing variations in how they are executed.
4. Procedures: Real-world examples of how threat actors implement techniques, tied to specific campaigns or groups.
5. Knowledge Base: A constantly updated repository of adversarial behaviors, mapped to known threat actors and their methods.

MITRE ATT&CK supports security teams in threat modeling, detection, and response by providing a detailed map of potential attack vectors and behaviors. It is widely adopted for improving cybersecurity strategies and aligning defenses to specific adversarial tactics and techniques.

Objective Threat Model (OTM)

The Objective Threat Model (OTM) is a modern threat modeling framework that focuses on the objectives and outcomes of threat actors rather than just technical attack mechanisms. By prioritizing the impact of threats, OTM broadens its applicability across technical, operational, and psychological domains. Key aspects include:

Core Concept:

- Outcome-Centric Approach: Highlights the goals and impacts of threats, such as operational disruption, reputational harm, or manipulation, instead of focusing solely on how attacks are executed.

Threat Types:

1. Increased Overhead: Adds burdens like costs, time, cognitive load, or administrative demands.
2. Degraded Capability: Reduces the ability to perform desired actions, such as through service denial or communication blocks.
3. Manipulation: Alters behaviors or decisions via misinformation, targeting, or exploitation.
4. Reputation Attack: Damages trust or credibility through fabricated information, leaks, or degraded experiences.
5. Vessel or Vehicle for Attack: Exploits devices or systems as attack platforms or for payload delivery.
6. Longitudinal Risk: Sustains or escalates risk over time through latent threats, cascading failures, or adaptive evolution.
7. Device Dependency: Creates reliance on specific ecosystems, reducing autonomy or flexibility.

Applications:

- **Interdisciplinary Relevance:** Extends beyond technical systems to encompass psychological operations, business strategy, and information warfare.
- **Operational Focus:** Provides actionable insights into how threats affect business processes, user trust, and long-term resilience.

Key Question Framework:

Each threat type includes guiding questions (e.g., "Am I being manipulated?" or "Could this harm someone's reputation?") to ensure comprehensive evaluation of potential impacts.

The OTM framework is designed to adapt to dynamic and evolving threat landscapes, offering a versatile tool for threat modeling across diverse contexts. It is particularly effective for aligning strategic, operational, and technical perspectives in risk assessment and mitigation.

Compare, Contrast, Combine

Prompt: Compare and contrast STRIDE, MITRE ATT&CK, and OTM. Then, consider ways the models can be used together.

Comparison and Contrast: STRIDE, MITRE ATT&CK, and OTM

Aspect	STRIDE	MITRE ATT&CK	Objective Threat Model (OTM)
Primary Focus	Identifying system vulnerabilities	Documenting adversary behaviors and methods	Understanding threat actors' objectives and impacts
Scope	Technical and architectural threats	Detailed adversarial tactics and techniques	Broader, outcome-driven threats, including operational and psychological factors
Granularity	High-level threat categories	Very granular, includes sub-techniques and real-world examples	Abstract and strategic, focusing on high-level impacts and objectives
Audience	Security architects and engineers	Threat hunters, SOC analysts, and red teams	Strategists, risk managers, and cross-disciplinary teams
Use Case	Secure system design	Threat detection, response, and emulation	Operational and strategic risk assessment

Structure	Categorization framework	Taxonomy and knowledge base	Contextualized threat analysis framework
Examples	Focus on spoofing, tampering, etc.	Phishing, lateral movement, command-and-control	Reputation attacks, increased overhead, manipulation
Adaptability	Less flexible, tied to system vulnerabilities	Highly detailed and precise for cybersecurity	Flexible, extends beyond technical to operational and psychological domains

How They Work Together

By integrating **STRIDE**, **MITRE ATT&CK**, and **OTM**, organizations can create a comprehensive and multi-dimensional approach to threat modeling, detection, and mitigation. Here's how the models complement each other:

1. Design and Architecture (STRIDE):

- Use STRIDE during system design to identify vulnerabilities at the architectural level, ensuring robust security foundations.
- Focus on mitigating technical risks like spoofing or information disclosure.

2. Operational and Tactical Awareness (MITRE ATT&CK):

- Leverage ATT&CK to understand real-world adversarial behaviors and tactics that exploit vulnerabilities identified using STRIDE.
- Apply it for threat detection, incident response, and adversary emulation during penetration testing.

3. Strategic and Objective-Level Thinking (OTM):

- Incorporate OTM to assess how threats align with broader operational impacts, such as reputational harm, long-term risks, or manipulation.
- Use it to inform business strategy, psychological operations, and communication planning.

Integration Framework

1. Threat Modeling Workflow:

- **Start with STRIDE:** Identify core vulnerabilities during system design.
- **Map to MITRE ATT&CK:** Determine tactics and techniques that adversaries might use to exploit those vulnerabilities.
- **Apply OTM:** Analyze the broader impact of these threats on business operations, reputation, and user trust.

2. Detection and Mitigation:

- Use **MITRE ATT&CK** to develop detection mechanisms and monitoring for adversary behaviors.
- Ensure architectural defenses address STRIDE threats.
- Evaluate mitigation efforts against OTM objectives to ensure they reduce operational, psychological, and long-term risks.

3. Risk Communication:

- Present **OTM findings** to leadership for high-level risk awareness.
- Use **MITRE ATT&CK examples** to demonstrate real-world relevance.
- Integrate **STRIDE categories** to explain the technical origins of risks.

4. Continuous Improvement:

- Refine system designs with **STRIDE**.
- Update detection rules with new techniques from **MITRE ATT&CK**.
- Reassess business and operational impacts using **OTM** as threats evolve.

Conclusion

By combining **STRIDE**, **MITRE ATT&CK**, and **OTM**, organizations benefit from:

- **Comprehensive Coverage:** Address technical, tactical, and strategic dimensions of threats.
- **Layered Defense:** Align secure design, active detection, and impact-driven mitigation.
- **Cross-Disciplinary Insights:** Bridge technical teams with leadership and operational stakeholders.

This integration ensures a holistic approach to security, emphasizing both prevention and preparedness for evolving threat landscapes.