TAG

ANALYST REPORT: ADVANTAGES OF SYSTEM LEVEL THREAT MODELING

DR. EDWARD AMOROSO
CHIEF EXECUTIVE OFFICER, TAG

Amenaza®
TECHNOLOGIES LIMITED

ANALYST REPORT: ADVANTAGES OF SYSTEM LEVEL THREAT MODELING

DR. EDWARD AMOROSO, CHIEF EXECUTIVE OFFICER, TAG

This TAG analyst report identifies the practical advantages of system-level threat modeling for cybersecurity engineers. Commercial vendor Amenaza is shown to provide effective functional support in this area.

INTRODUCTION

Most cybersecurity practitioners fully understand the value of performing high-level modeling, investigation, and analysis of the threats, vulnerabilities, and attack scenarios that apply to their systems and infrastructure. The challenge is that the methodologies, platforms, and tools supporting this type of model-based work vary widely.

Military teams, for example, often deploy and use high-level threat modeling tools developed either locally or by system integrators. Commercial banks, however, might not include such investigation, and would depend instead on tools such as their Security Information Event Management (SIEM) or Governance, Risk, and Compliance (GRC) to create high-level views.

Interestingly, the security community has tended to use the term *threat modeling* in a context much different from the need to support high-level system analysis. The term has instead been used in the context of how developers identify threats that emerge during the software process. This is a useful modeling task, but it is different than system level analysis.

Amenaza, a prominent cybersecurity firm, has recognized the significance of threat modeling *at the system level* and has developed its Secur*I*Tree software to support this manner of high-level threat modeling. In this report, we will explain how Amenaza's Secur*I*Tree supports system-level threat modeling and why this is essential for enterprise security and compliance.

SYSTEM-LEVEL THREAT MODELING

The purpose of performing system-level threat modeling is to achieve four main cybersecurity-related objectives for a given product, system, network, or infrastructure component either under development or analysis. The four specific system-level objectives for threat modeling that we will focus on in this report are as follows:

Objective 1: Understanding
The highest-level threat modeling objective involves designers developing a deep functional and operational understanding of the system being constructed or reviewed. This objective might seem obvious, but experienced engineers will acknowledge the challenge of developing accurate insights into how complex systems really operate, including how they are constructed. The interdependencies between components of complex systems are often targeted by adversaries seeking to compromise the system.

Objective 2: Threats
A second major high-level objective is for the threat modeler to consider the specific types of cybersecurity threats that must be addressed for the system under review or construction. This can and should include categorizing and prioritizing these threats in the context of the purpose and mission objective for the system. The origin and source of the threat will also be relevant here.

Objective 3: Consequences
A third objective for system-level threat modeling involves establishing the real impact and consequences that can come from a successful breach or attack. These effects should be demonstrated in the context of the mission in which the system operates. That is, the model should show clearly how an attack can influence the overall purpose of the system.

Objective 4: Mitigation
Finally, the threat modeler should gain deep insights into how a given system might be augmented or redesigned to mitigate the effects of the threats, vulnerabilities, and attack consequences illustrated by the high-level model. This focus on cybersecurity controls is ultimately the most important objective from a practical perspective.

OVERVIEW OF AMENAZA

Located in Calgary and founded back in 2001, cybersecurity vendor Amenaza includes system-level threat modeling as a core component of its security strategy for enterprise and government customers. Amenaza's commercially available Secur*I*Tree platform supports achievement of the four main threat modeling objectives as follows:

Step 1: Systematic Analysis and Understanding
Amenaza's threat modeling process begins with a systematic analysis of the assets and components within the scope of the system. This includes gaining a deep understanding of the system's architecture, data flows, and potential entry points for attackers. The company employs experienced security professionals who collaborate with developers, architects, and stakeholders to ensure a comprehensive understanding of the system's intricacies. This detailed system analysis is foundational for effective threat modeling.[1]

Step 2: Categorizing and Prioritizing Threats

Once the system's structure is understood, Amenaza's threat modeling support team utilizes methodologies such as STRIDE,[2] DREAD,[3] and OWASP's Application Security Verification Standard[4] to categorize and assess potential threats and vulnerabilities. This process enables the team to rate risks and prioritize them based on their potential impact and likelihood. By categorizing and prioritizing threats, organizations can allocate resources efficiently to address the most critical security concerns.

Step 3: Development of Detailed Threat Models

Amenaza then develops detailed threat models that outline potential attack scenarios and vulnerabilities within the system. These models provide a comprehensive overview of the threats and their potential consequences. With a clear understanding of the threats they face, organizations can make informed decisions about security measures and countermeasures to mitigate these risks effectively.

Step 4: Proactive Security Measures

After identifying and prioritizing threats, Amenaza recommends and assists in implementing appropriate security measures and countermeasures. This proactive approach ensures that organizations are well-prepared to defend against known threats and can also proactively address emerging threats. In an ever-evolving cybersecurity landscape, proactive security measures are essential to safeguard sensitive data and maintain the trust of customers and stakeholders.

ADVANTAGES OF USING AMENAZA FOR SYSTEM-LEVEL THREAT MODELING

Amenaza's approach to threat modeling extends beyond reacting to threats. The company believes that cyberattacks can be predicted, and a defender can use that knowledge to prevent attacks and their effects. By using Secur*I*Tree's threat models, organizations can engage in predictive Security Posture Management (SPM), which should allow them to effectively elude adversaries and potential attackers.

In addition, while many organizations enforce cybersecurity with checklists, these lists provide only a basic level of security. Sophisticated adversaries require a more in-depth approach. Organizations with high asset value or those whose systems can impact safety are attractive targets for adversaries. Amenaza's attack tree analysis methodology offers a deeper understanding of an organization's resilience, enabling defenders to view their systems from the perspective of potential attackers and determine which controls are appropriate.

A major advantage is that Secur*I*Tree, Amenaza's software for attack tree-based threat risk analysis, enables analysts to make objective, risk-based security decisions regarding a system's threats. By analyzing thousands of possible attacks against a defender's system, Secur*I*Tree assesses each attack's feasibility, motivation, and probability. This information is then used to calculate the associated risk for each attack scenario.

Secur*I*Tree also allows analysts to evaluate the effectiveness of proposed controls by adding countermeasures to the threat models and observing the reduction in risk achieved. This capability enables organizations to assess the impact of security measures and make informed decisions about their deployment.

An additional benefit of Secur*I*Tree's threat models is that they document what threats and attack vectors were considered by the defender, and the rationale behind whether certain potential attacks were or were not mitigated through controls (based on the projected likelihood and impact). In the event that a serious incident does occur this could be valuable in demonstrating due diligence on the part of the defender.

Obviously, no tool or process is perfect, and the results of any attack tree analysis project will always depend on the accuracy of the model being developed as well as the skill and breadth of thinking of the analyst. Nevertheless, when any analysts use Secur*I*Tree, it should always become easier to determine the broad range of threats and vulnerabilities that apply to a given system under consideration.

Finally, Secur*I*Tree is designed to be user-friendly, running on various operating systems, including Windows-based PCs, Apple Mac-based workstations, and Linux systems. Its graphical user interface makes it easy to create and populate attack trees, associating relevant parameters with tree nodes. Additionally, Secur*I*Tree can handle scenarios involving both random and malicious activities, making it versatile for a wide range of security challenges.

CONCLUDING REMARKS

From a TAG analyst perspective, we view system-level threat modeling as an essential aspect of modern enterprise cybersecurity. Teams focused on addressing requirements in standards such as the NIST Cybersecurity Framework (CSF) often neglect the larger system-level issues inherent in compliance with both the functional specifics and the overall spirit and purpose of enforcing the model. System-level threat modeling is thus highly recommended and is arguably the foundation of a comprehensive security program.

We also fully endorse the approach being taken at Amenaza, recognizing the expertise and experience of the company founder, and acknowledging the importance of decades of relevant application of the Amenaza tool to practical system design and analysis activities. We hope that readers will include Amenaza in their source selection for projects that will benefit from system-level threat modeling.

[1] Amenaza provides in-depth training for customers so that their engineers can take the lead in the threat modeling work.
[2] See https://en.wikipedia.org/wiki/STRIDE_(security).
[3] See https://en.wikipedia.org/wiki/DREAD_(risk_assessment_model).
[4] See https://owasp.org/www-project-application-security-verification-standard/.

ABOUT TAG

TAG is a trusted research and advisory company that provides insights and recommendations in cybersecurity, artificial intelligence, and climate science to thousands of commercial solution providers and Fortune 500 enterprises. Founded in 2016 and headquartered in New York City, TAG bucks the trend of pay-for-play research by offering unbiased and in-depth guidance, market analysis, project consulting, and personalized content—all from a practitioner perspective.

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: Dr. Edward Amoroso

Publisher: TAG Infosphere Inc., 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman at lgoodman@tag-cyber.com to discuss this report. You will receive a prompt response.

Citations: Accredited press and analysts may cite this book in context, including the author's name, author's title, and "TAG Infosphere, Inc.." Non-press and non-analysts require TAG's prior written permission for citations.

Disclaimer: This book is for informational purposes only and may contain technical inaccuracies, omissions, and/or typographical errors. The opinions of TAG's analysts are subject to change without notice and should not be construed as statements of fact. TAG Infosphere, Inc. disclaims all warranties regarding accuracy, completeness, or adequacy and shall not be liable for errors, omissions, or inadequacies.

Disclosures: Amenaza commissioned this book. TAG Infosphere, Inc. provides research, analysis, and advisory services to several cybersecurity firms that may be noted in this paper. No employees at the firm hold any equity positions with the cited companies.

TAG's forecasts and forward-looking statements serve as directional indicators, not precise predictions of future events. Please exercise caution when considering these statements, as they are subject to risks and uncertainties that can affect actual results. Opinions in this book represent our current judgment on the document's publication date only. We have no obligation to revise or publicly update the document in response to new information or future events.