Chapter 18
Unified Threat Modeling: Strategies for Comprehensive Risk Assessment in Modern Systems

Rasmita Kumari Mohanty
https://orcid.org/0000-0002-5828-5649
Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering and Technology, India

Chinimilli Venkata Rama Padmaja
Institute of Aeronautical Engineering, India

Suresh Kumar Kanaparthi
https://orcid.org/0000-0003-4945-6554
SRM University, India

Anusha Rajan
Mallareddy University, India

ABSTRACT

Today, in the digital world, the security of systems is crucial because, with continuous information exchange and huge quantities of data being processed, the protection of operation processes and data assets becomes paramount. Threat modeling is an important part of cybersecurity management methodology that looks for any possible threats or weaknesses that can break the system or endanger the environment. This paper is an attempt to analyze all the models of threat modeling by taking STRIDE, PASTA, DREAD, TREK, VAST and Attack Trees as references. An integrated model is suggested that combines the benefits of existing approaches, which includes the adoption of a comprehensive frame to deal with cyber threats. This methodology emphasizes iterative refinement and rigorous testing to ensure the effectiveness of threat mitigation strategies. By incorporating user-friendly web portals and the

DOI: 10.4018/979-8-3693-6745-2.ch018

integration of new technologies, this framework enhances usability and addresses emerging threats.

1. INTRODUCTION

As it is today, making the systems, computers, and data safe from hackers and such threats is a matter of great importance since they are preventing interruptions and protecting data that has a huge value. Against the backdrop of the threat and being armed with an arsenal of sophisticated tools and techniques, organizations in different sectors face such critical challenges. While these entities are not the same and face other threats, each one should develop purposeful defense strategies. Achieving the necessary environment of anticipating and handling these threats is an essence for effective cyber security, and therefore threat modeling is a critical part of this quest. Threat modeling implicates a methodical procedure of studying and analyzing threats, vulnerabilities, and risks in a certain system or environment. By looking at the assets, the associated weaknesses, and the possible intrusion paths, organizations will be able to start addressing these security concerns and will also strengthen their defenses. The strategic planning model which falls within the framework comprises such steps as scoping and goal definition, threat identification, environment characterization, threat evaluation, their selection, and implementing evaluated solutions. Many legacy threat modeling frameworks combine structure methodologies into one to make sure that the threat analyses performed in certain contexts are complete. STRIDE, for instance, categorizes threats into six distinct types: the types of attacks that cause spoofing, result in tampering, service DoS, denial of service, data exhilaration, and escalation. By delineating these threat categories, STRIDE provides valuable insights into potential attack vectors, aiding organizations in identifying and prioritizing security measures effectively.

As opposed to this PASTA a risk-based strategy takes up a direction that enhances the Know- how crashing business operations. Such a strategy paves the way for organizations to ensure that resources are distributed effectively by primarily concentrating on minimizing the effects of those risks that will probably cause the greatest disruption to the continuity of their operations. On the other hand, DREAD sticks to both a novel grading scenario and offers an evaluative framework that assesses threats according to Damage, Reproducibility, Exploitability, Affected users, and Discoverability. Threat modeling gains strength through digitalization with visualization techniques. VAST (Visualization and Sensory Training) improves comprehension and communication of threats and vulnerabilities. Ultimately, TRIKE brings together the aspects of attack trees with passengers under the general classification of transportation. Connecting these models into one form, there is a