Cyber Security Threat Modelling:Classical Approaches Survey – An Insight

Naveen Watson
Department of Information Technology
University of Technology and Applied Sciences,Oman
naveentester07@gmail.com

Prof.Dr.G.Shanmuga Rathinam
Department of Information Technology
Presidency University,Bengaluru
shanmugarathinam@presidencyuniversity.in

Angelin Gladys Jesudoss
Department of Information Technology
University of Technology and Applied Sciences,Oman
kuttijag@gmail.com

***Abstract*— Threat modeling provides a systematic way to identify cybersecurity threats. It is an essential part of the Cybersecurity Risk Management Process. It defines countermeasures to prevent or mitigate the effects of threats to the system. Every software system today faces a range of threats, and it is increasing constantly as technology rapidly changes. Increasing use of mobiles and IoT devices also increases the threat landscape. Threats can emanate from inside/outside of organizations, and their impact has the potential to be devastating. Systems could be stopped from working entirely or sensitive information could be leaked, which would impact consumer faith. To avoid threats from taking benefit of system flaws, threat modeling methods can be used to think defensively. Though there are numerous types of frameworks for security architectures available, not a single framework is complete and totally secure. In this paper we analyzed some of the commonly used thereat modelling approaches.**

Keywords—Risk, threat modelling, mitigation

1.INTRODUCTION

Threat modeling techniques are used to create an abstraction of the system; profiles of probable attackers, including their objectives and methods; and a collection of potential threats that may arise. Many threat modeling methods are developed over the period of time. Some of them are comprehensive and broad; Some methods focus specifically on risk or privacy concerns.

Threat modeling methods can be combined to create a more robust and well-rounded view of potential threats. Software systems are progressively being integrated into physical infrastructures. These hybrids are often referred to as cyber-physical systems; this term accounts for their multiple components. While innovative, cyber-physical systems are vulnerable to threats that manufacturers of traditional physical infrastructures may not consider.

Performing threat modeling on cyber-physical systems with a variety of participants can help catch threats across a wide spectrum of threat types. To best use threat modeling, it should be performed early in the development cycle.

The classical threat modeling methods discussed in this paper are from a variety of sources and aims at different parts of the process.

Threat modelling methods are very much useful in creating,

- an abstraction of the system
- profiles of potential attackers, including their goals and methods
- a catalog of potential threats that may arise

Numerous threat-modeling approaches have been developed. They can be combined to create a more robust and a matured view of potential threats. Not all of them are comprehensive; some are abstract and others are people-centric. Some methods focus specifically on risk or privacy concerns.

The Lexicon of the known and approved Threat Models' abbreviations:

Model	Abbreviation Description
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) and Associated Derivations
PASTA	The Process for Attack Simulation and Threat Analysis
LINDDUN	Linkability, Identifiability, Nonrepudiation, Detectability, Disclosure of information, Unawareness, Noncompliance) method
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
VAST	Visual, Agile, and Simple Threat Modeling
hTMM	Hybrid Threat Modeling Method

qTMM	Quantitative Threat Modeling Method
TRIKE	Abbreviation is unknown, unified conceptual framework for security auditing automated concept from a risk management perspective
Trees	Attack Trees
PnG	Persona non Grata

Table 1:1

The 10 threat-modeling methods shown above are from a variety of sources and target different parts of the process. No one threat-modeling method is endorsed over another; organizations should choose which method to use based on the specific requirements of their project.

2.Threat Modelling Techniques

a) STRIDE

Developed in 1999 and adopted by Microsoft in 2002, STRIDE is currently the most mature threat-modeling method. STRIDE has evolved over time to include new threat-specific tables and the variants STRIDE-per-Element and STRIDE-per-Interaction.
STRIDE is a free tool that will produce DFDs and analyze threats. It models the in-place system. By building data-flow diagrams (DFDs), STRIDE is used to identify system entities, events, and the boundaries of the system. STRIDE applies a general set of known threats based on its name, which is a mnemonic, as shown in the following table:

	Threat	Property violated
S	Spoofing Identity	Authentication
T	Tampering with data	Integrity
R	Repudiation	Non-repudiation
I	Information disclosure	Confidentiality
D	Denial of Service	Availability
E	Elevation of privileges	Authorization

Table 2.1

DREAD threat modeling:

DREAD was conceived of as an add-on to the STRIDE model that allows modelers to rank threats once they've been identified. DREAD stands for six questions you would ask about each potential threat:

Damage potential: How great is the damage if the vulnerability is exploited?
Reproducibility: How easy is it to reproduce the attack?
Exploitability: How easy is it to launch an attack?
Affected users: As a rough percentage, how many users are affected?
Discoverability: How easy is it to find the vulnerability?
Each of these questions is answered with a rating between one and three.

Pros and Cons of STRIDE:

Pros:

- Easy to understand and easy to teach – which helps to adopt STRIDE among non-security and non-technical team members.
- Swiftly identify high-level threats that may impact the system which are to be modelled.
- Relatively quick to perform.

Cons:

- May miss many potential threats.
- Does not include a mechanism to take standard frameworks into account (like NIST CSF, application requirements, etc.).

b) **PASTA**

The Process for Attack Simulation and Threat Analysis (P.A.S.T.A) is a risk-centric threat modeling framework developed in 2012 by Tony UcedaVélez. It contains seven stages, each stage adds to the information known about the object in scope, its business/technical environment, potential threats involved, and its risks (and feeds into the overall threat model).
The seven stages of PASTA threat modeling:

1. Define the Objectives
2. Define the Technical Scope
3. Decompose the Application
4. Analyze the Threats
5. Vulnerability Analysis
6. Attack Analysis
7. Risk and Impact Analysis

The big advantage of using PASTA threat modeling is the method's end-to-end nature, including the inclusion of risk to the business.

Some of the benefits of PASTA threat modelling include:

- Put security at the centre of the entire business. PASTA threat modelling is an opportunity to involve stakeholders from across the organisation to understand how their goals are impacted by cybersecurity threats, and how in turn their goals influence the cybersecurity decisions the organisation makes.

- Get a full picture of the threats an organisation may face. This includes the risks of those threats becoming attacks, and the goals those threats impact. Your security team can then prioritise

threats to mitigate, ensuring that resources and attention are distributed effectively.

- Understanding of the evolving cyber threat landscape. PASTA threat modelling is not a static, one-time assessment. Built into the process (at stage 4) is understanding of the current threats that your organisation may face. Cybersecurity threats are constantly evolving, and PASTA threat modelling encourages you to put time into understanding those threats rather than relying on old data or intelligence.

- Informed decision making. PASTA threat modelling on new products allows your company to see whether existing protections are appropriate for the new product. It also helps make the decision whether to utilize a new tool or product from a supplier.

c) LINDDUN

The LINDDUN framework focuses on analysis of privacy threats, based on the categories that form its acronym: linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness, and non-compliance. It uses threat trees to help users choose the relevant privacy controls to apply.

LINDDUN starts with a DFD of the system that defines the system's data flows, data stores, processes, and external entities. By systematically iterating over all model elements and analyzing them from the point of view of threat categories, LINDDUN users identify a threat's applicability to the system and build threat trees.

One of the strong features of the LINDDUN method is its extensive privacy knowledgebase and documentation. The LINDDUN method is labor intensive and time consuming. It suffers from the same issues as STRIDE—the number of threats can grow rapidly as a system increases in complexity.

d) OCTAVE

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method is a risk-based strategic assessment and planning method for cybersecurity. It was created by the CERT Division of the SEI in 2003 and refined in 2005. OCTAVE focuses on assessing organizational risks and does not address technological risks. Its main aspects are operational risk, security practices, and technology.

OCTAVE has three phases:

1.Build asset-based threat profiles. (This is an organizational evaluation.)

2.Identify infrastructure vulnerability. (This is an evaluation of the information infrastructure.)

3.Develop a security strategy and plans. (This is an identification of risks to the organization's critical assets and decision making.)

e) VAST

VAST stands for Visual, Agile Threat Modeling. This model underlies Threat Modeler, an automated threat modeling platform that distinguishes between application and operational threat models. It scales threat modeling process across infrastructure & is focused on attacker.VAST is designed specifically to integrate into workflows built around the devops philosophy.

The fundamental value of the method is the scalability and usability that allow it to be adopted in large organizations throughout the entire infrastructure to produce actionable and reliable results for different stakeholders.

Recognizing differences in operations and concerns among development and infrastructure teams,VAST requires creating two types of models: application threat models and operational threat models.

Application threat models use process flow diagrams, representing the architectural point of view. Operational threat models are created with an attacker point of view in mind based on DFDs.

f) hTMM:

The Hybrid Threat Modeling Method (hTMM) was developed by the Software Engineering Institute in 2018. It consists of a combination of SQUARE (Security Quality Requirements Engineering Method), Security Cards, and PnG activities. The targeted characteristics of the method include no false positives, no overlooked threats, a consistent result regardless of who is doing the threat modeling, and cost-effectiveness

The following are the main steps of the method:

1. Identify the system to be threat-modeled.
2. Apply Security Cards based on developer suggestions.
3. Remove unlikely PnGs (i.e., there are no realistic attack vectors).
4. Summarize the results using tool support.
5. Continue with a formal risk assessment method

g) qTMM:

A quantitative type threat model which is focused on Attacker/Defender models, melds features of Attack Trees, STRIDE, and CVSS.

The first step of the Quantitative Threat Modeling Method (Quantitative TMM) is to build component attack trees for the five threat categories of STRIDE. This activity

shows the dependencies among attack categories and low-level component attributes. After that, the CVSS method is applied and scores are calculated for the components in the tree.

An additional goal for the method is to generate attack ports for individual components. These attack ports (effectively root nodes for the component attack trees) illustrate activities that can pass risk to the connected components.

h) TRIKE:

An open-source tool available as a spreadsheet template or stand-alone program, Trike consists of a matrix combining assets, actors, actions, and rules. When parameters and data are entered in this matrix, the program produces a score-based analysis of risks and probabilities.

As with many other methods, Trike starts with defining a system. The analyst builds a requirement model by enumerating and understanding the system's actors, assets, intended actions, and rules. This step creates an actor-asset-action matrix in which the columns represent assets and the rows represent actors.

Each cell of the matrix is divided into four parts, one for each action of CRUD (creating, reading, updating, and deleting). In these cells, the analyst assigns one of three values: allowed action, disallowed action, or action with rules. A rule tree is attached to each cell.

After defining requirements, a data flow diagram (DFD) is built. Each element is mapped to a selection of actors and assets. Iterating through the DFD, the analyst identifies threats, which fall into one of two categories: elevations of privilege or denials of service. Each discovered threat becomes a root node in an attack tree.

To assess the risk of attacks that may affect assets through CRUD, Trike uses a five-point scale for each action, based on its probability. Actors are rated on five-point scales for the risks they are assumed to present (lower number = higher risk) to the asset. Also, actors are evaluated on a three-dimensional scale (always, sometimes, never) for each action they may perform on each asset.

i) TREE:

Attack trees are a graphic representation of systems and possible vulnerabilities. The trunk of the attack tree is the asset, while entry points and threats are branches or roots. Attack trees are often combined with other methods.

In the case of a complex system, attack trees can be built for each component instead of for the whole system. Administrators can build attack trees and use them to inform security decisions, to determine whether the systems are vulnerable to an attack, and to evaluate a specific type of attack.

Attack trees are easy to comprehend and adopt but are only useful when the system and security concerns are well understood. The method assumes that analysts have high cybersecurity knowledge and thus does not provide guidelines for measuring sub-goals, attacks, or risks

In recent years, this method has often been used in combination with other techniques and within frameworks such as STRIDE, CVSS, and PASTA.

j) PnG:

Persona non Grata (PnG) focuses on the motivations and skills of human attackers. It characterizes users as archetypes that can misuse the system and forces analysts to view the system from an unintended-use point of view.

This method is similar to criminal profiling in law enforcement. To anticipate attacks in more detail, brainstorming exercises are performed to create a detailed picture of a hypothetical attacker, including their psychology, motivations, goals, and capabilities.

PnG can help visualize threats from the counterpart side, which can be helpful in the early stages of the threat modeling. The idea is to introduce a technical expert to a potential attacker of the system and examine the attacker's skills, motivations, and goals. This analysis helps the expert understand the system's vulnerabilities from the point of view of an attacker.

PnG fits well into the Agile approach, which uses personas.

Overview of Threat Classification Techniques:

Methods discussed above can be divided into subgroups, in which they:

- Are used independently from everyone;
- Are used in blend with others;
- Are examples for merging different methods.

To select the best method for a project, we need to think about particular areas in which the goal needs to be decided, such as risk, security or privacy, how much time there is for threat modeling, what experience of threat modeling is available, stakeholders’degree of involvement, etc.

It can be seen from the above discussion that all methods are same in some parameters, but that they are still different from each other. To comprehend how exactly they differ and where they are used, it is necessary to refer to the publications of various authors who consider these methods.

The different creations of objects of protection and methods of threat grouping, covered by the studied methodologies, are caused by the fact that each organization attempts to implement its private model of the system and the model of

threats aimed at it for further use, since there is no single formally described model that would fit any organization.

Thus, it can be concluded that, due to the lack of a general system model and a threat model aimed at the system, many organizations disregard the protection of information, and, therefore, lose confidential data. If not handled with care, the direct application of incomplete methodologies can result in a failure to fully comply and demonstrate compliance, leading to large fines and losses.

The description of a unified and comprehensive structure for describing a system model opens up new opportunities for research and use by many organizations. First, it will help organizations better configure and use their system. Secondly, this model will help prevent the leakage of confidential data.

The above findings do not only relate to IT systems, but also to systems engineering in general. This formulation can be summarized in two aspects. First, IT systems use software intensively. Secondly all systems correspond to the definition of the system as a whole, that is, there are artificial solutions with equipment, software, data, people, processes, procedures, means, materials and natural objects.

Conclusions:

Information security is a serious problem for people and organizations because it leads to excessive monetary losses. In this paper we analyzed popular threat modelling techniques and methodologies in order to find a generic and flexible model that allows enhanced understanding of the nature of threats in order to develop suitable strategies and information security decisions to prevent or mitigate their effects.

After the analysis of various methodologies and publications in the relevant area, a thorough inference was made that, currently, there is no single formally defined model of the system and the model of threats aimed at this system.

The existing approaches in threat modelling cannot be classified into any openly defined categories that would focus on the confidentiality and integrity of the system. The nonexistence of these categories does not lead to specific confidentiality and integrity issues being addressed in the system development process.

References:

1) Nataliya Shevchenko, Timothy A. Chick, Paige O'Riordan, Thomas Patrick Scanlon, PhD, & Carol Woody, PhD July 2018-"THREAT MODELING: A SUMMARY OF AVAILABLE METHODS"- SOFTWARE ENGINEERING INSTITUTE | CARNEGIE MELLON UNIVERSITY REV-03.18.2016.0

2) Josh Fruhlinger-"Understanding the frameworks, methodologies and tools to help you identify, quantify and prioritize the threats you face"

3) Simon Yusuf Enoch, Mengmeng Ge,Jin B. Hong,Dong Seong Kim –"Model-based Cybersecurity Analysis: Past Work and Future Directions" - 67th Annual Reliability and Maintainability Symposium (RAMS) . IEEE 2021

4) David, N.; David, A.; Hansen, R. R.; Larsen, K. G.; Legay, A.; Olesen, M. C.; & Probst, C. W.Modelling Social-Technical Attacks with Timed Automata. Pages 21-28. In Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats. Conference on Computer and Communications Security. October 2015. DOI 10.1145/2808783.2808787.

5) Mouna Jouinia, Latifa Ben Arfa Rabaia, Anis Ben Aissab-Classification of security threats in information systems-1877-0509 © 2014 Published by Elsevier B.V. Open access under CC BY-NC-ND license.Selection and Peer-review under responsibility of the Program Chairs.

6) Lindqvist U, Jonsson E. How to systematically classify computer security intrusions. IEEE Symposium on Security and Privacy; 1997. 154-163.

7) Tang J, Wang D, Ming L, Li X. A Scalable Architecture for Classifying Network Security Threats. Science and Technology on Information System Security Laboratory; 2012.

8) Anton Konev , Alexander Shelupanov, Mikhail Kataev , Valeriya Ageeva and Alina Nabieva - A Survey on Threat-Modeling Techniques: Protected Objects and Classification of Threats - Symmetry 2022, 14, 549. https://doi.org/10.3390/sym14030549

Direct References:

https://wiki.owasp.org/index.php/Category:Threat_Modeling

https://www.first.org/global/sigs/cti/curriculum/threat-modelling#:~:text=Modeling%20%2D%20Generic%20Steps Threat%20Modeling%3A%2012%20Available%20Methods ,-Threat%20Modeling%3A%20Designing

https://insights.sei.cmu.edu/blog/threat-modeling-12available-methods/