ISSN No:-2456-2165

Evaluation of Threat Models

Kelkar Siddhi Suhas, Pursuing BTech in Electronics Engineering – DJSCE
Dr. Neepa Shah, Visiting Faculty - DJSCE

Abstract:- Information system security is the integrity and safety of its resources and activities. In the cyber world, it can be almost impossible to trace sophisticated attacks to their true source. The anonymity enjoyed by the malicious user or cyber attackers pose a grave threat to the global information society.

Cyber threat modelling is an analytical process that is used to identify the potential threats against a system or an organization. It is a core activity and a fundamental practice in the process of building trusted technology. Threat modelling has been identified as one of the best "return on investment" activities in order to identify and address design flaws. Some threat model methods focus on identifying threats and security issues while some methods also perform assessment of the resulting risk.

I. INTRODUCTION

➢ *Threat Modelling*

A threat model is a structured representation of all the information that can affect the security of the system. Identification of security requirement, pointing out security threats potential vulnerabilities, qualifying threat and vulnerability and prioritizing solutions are the objectives of threat modelling. Threat modelling is a process for capturing, organizing, and analysing all of this information. Applied to software, it enables informed decision-making about application security risks. In addition to producing a model, typical threat modelling efforts also produce a prioritized list of security improvements to the concept, requirements, design, or implementation of an application.

Threat modelling works by identifying the types of threat agents that cause harm to an application or computer system. It adopts the perspective of malicious hackers to see how much damage they could do.

Threat modelling technique furnishes security teams and organizations in a way to distinguish potential threats and can be see equivalent balance on a functional level. When conducting threat modelling, organizations perform a thorough analysis of the software architecture, business context, and other artifacts (e.g., functional specifications, user documentation). Generally, developers perform threat modelling in five steps:

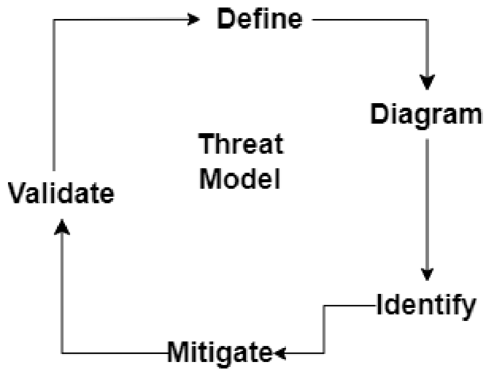

Fig. 1: Steps of threat modelling

➢ *Threat Assessment*

A threat assessment analyses your system to find out what attacks are currently happening or which attacks are being threatened. Threat assessments can gather knowledge on attacks before they happen, which can help determine the extent and danger of a threat and how it might affect an enterprise. It's more of a reactive approach to IT security, and a helpful option for companies who need to know what's going on in their system and what issues need to be resolved right away.

Threat assessments can catch digital threats like:

- Vulnerabilities in applications that can be used to attack your network
- Malware or viruses present
- Current phishing attacks that put your enterprise at risk for a breach
- Misuse of information (especially relevant to financial and health sectors)
- Employee, vendor, and individual risks (detecting anyone with malicious intent)

II. MISCONCEPTIONS OF THREAT MODELLING

Threat modelling is an important practice in the field of information security, but there are some common misconceptions about it. Some of the most common misconceptions include:

- *Threat Modelling is too Complex and Time-Consuming*

While it is true that threat modelling can be a complex process, it doesn't have to be overly time-consuming or difficult. There are many different frameworks and methodologies that can be used to perform threat modelling, and organizations can choose the approach that works best for their needs and resources.

- *Threat Modelling is a One-Time Activity*

Threat modelling is not a one-time activity, but rather an ongoing process that should be integrated into an organization's overall security management program. Threats are constantly evolving, and organizations need to regularly reassess their security posture and adjust their strategies accordingly.

- *Threat Modelling is Only for Technical Experts*

While technical expertise can certainly be helpful in performing threat modelling, it is not necessary for everyone involved in the process. Threat modelling can involve a range of stakeholders, including business managers, risk management professionals, and other non-technical experts.

III. TYPES OF THREAT MODELS

Almost all software systems or organizations today face a variety of threats, and more are being added constantly as there is change in technology. These threats can come from outside or within organizations, and their impact has the potential to be devastating. Systems could be prevented from working entirely or sensitive information could be leaked, which would impact consumer trust in the system provider. To prevent threats from taking advantage of system flaws, threat modelling methods can be used to think defensively.

Threat modelling methods are used to create an abstraction of the system; profiles of potential attackers, including their goals and methods; and a catalogue of potential threats that may arise. Some threat modelling methods discussed in this paper come from variety of sources and target different parts of the process:

A. STRIDE (Developer Focused):

It is the oldest methodology developed by Microsoft. Currently STRIDE is the most mature threat modelling method. It includes full breakdown of processes, data stores, data flows and trust boundaries. Its goal is to get an application to meet the security properties of Confidentiality, Integrity and Availability (CIA), along with Authorization, Authentication and Non-Repudiation. This is an easy method to adopt but it can be time consuming. Its main issue is that as the system complexity increases the number of threats can grow rapidly. STRIDE is an acronym for the types of threat it addresses.

Table 1. STRIDE Threat Categories

Types of Threat	**What was violated?**	**How was it violated?**
Spoofing	Authenticity	Pretending to be someone you are not. Unauthorized user.
Tampering	Integrity	Manipulating the data to achieve malicious goals.
Repudiation	Non-repudiation	Claiming not to be responsible for an action.
Information disclosure	Confidentiality	Leaking protected credential to unauthorized entities.
Denial of Service (DoS)	Availability	Denying access to resources needed to provide service.
Elevation of Privilege	Authorization	Allowing someone to do something they are not authorized to do.

B. OCTAVE (Practiced Focused):

The OCTAVE method (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a security framework for determining risk level and planning defence against cyber assaults. It is a risk based strategic assessment and planning technique developed by Computer Emergency Response Team (CERT). OCTAVE is self-directed approach, meaning that people from an organization assume responsibility for setting the organization's security strategy.

Octave method focuses on three phases:

- **Phase 1:** Identifying critical assets of the organization and the threats to those assets.
- **Phase 2:** Identifying the vulnerabilities, both organizational and technological, identifying risk to the organization.
- **Phase 3:** Developing a practiced based protection strategy and risk mitigation plans.

The framework has gone through several evolutionary phases, but the basic principles and goals have remained the same.

Two versions exist:

- **OCTAVE-S**, a simplified methodology for smaller organizations or those with single level structures.
- **OCTAVE Allegro**, a more comprehensive version for large organizations or those with multilevel structures.

Though OCTAVE threat model method provides a robust, asset-centric view, and organizational risk awareness, the documentation can become voluminous. OCTAVE lacks scalability – as technological systems add users, applications, and functionality, a manual process can quickly become unmanageable.

This method is most useful when creating a risk-aware corporate culture. The method is highly customizable to an organization's specific security objectives and risk environment.

C. P.A.S.T.A. (Attacker Focused):

PASTA stands for Process for Attack Simulation and Threat Analysis. PASTA threat models have some qualities, first of all it is risk centric. That is threat model is performed with the aim of identifying risks, classifying risks and focusing on the highest risks for the organization. Then it is capable of simulations that means simulations can be performed using identified threats, collected evidences, etc. PASTA has seven different stages. Each stage adds information known about the object in scope, its technical environment.

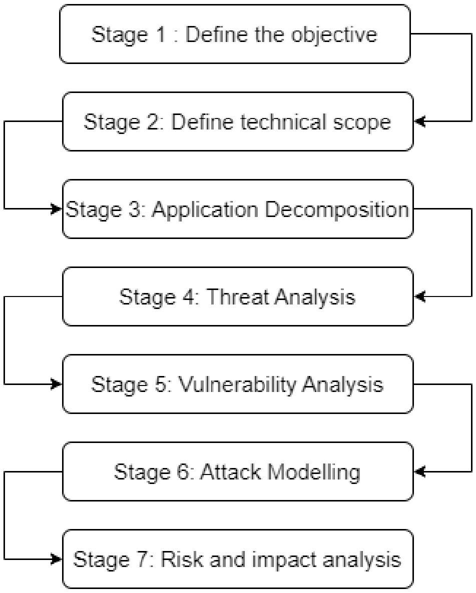
Stage 1 : Define the objective
Stage 2: Define technical scope
Stage 3: Application Decomposition
Stage 4: Threat Analysis
Stage 5: Vulnerability Analysis
Stage 6: Attack Modelling
Stage 7: Risk and impact analysis

Fig 2: Pasta threat modelling stages

The output of each stage acts as the input of the next stage.

D. TRIKE (Acceptable Risk Focused):

TRIKE is an open-source threat modelling methodology. It is an improved version of STRIDE and it is mainly used when security auditing is the concern from a risk management perspective. It is the combination of two models namely – Requirement model and implementation model. The Requirement model is the base of the TRIKE model that the security characteristics and assigns acceptable risk to each asset. It also co-ordinates among different security teams. Whereas, in Implementation model a Data flow Diagram (DFD) is created which illustrates the of data and the user performs actions within a system. TRIKE differs from other threat models because it uses risk-based approach with distinct implementation, threat and risk models.

Beyond its more systematic methodology, TRIKE is different from other existing approaches to threat modelling in that it focuses on modelling threats from a defensive perspective, not that of an attacker. It has automated components to implement. It has vague, insufficient documentation. It also has built-in prioritization of mitigation.

E. LINDDUN (Privacy Focused):

LINDDUN was created to provide support for a thorough, systematic privacy threat assessment. It has helped the user through each step and ensures exhaustive coverage and documentation of the privacy threat modelling process, and includes an extensive knowledge base of potential privacy threats. The LINDDUN privacy framework enables organizations to analyse privacy threats based on 7 threat categories. These categories from its acronym:

➢ *Likability:*

An unauthorized user can link two items of interest even if they do not know the authorized user's identity.

➢ *Identity:*

Through an item of interest, an unauthorized user can identify a particular data subject from a set.

➢ *Non-repudiation:*

The data subject cannot deny a particular claim.

➢ *Detectability:*

An unauthorized user can detect data subject and distinguish whether an item of interest about that subject exists.

➢ *Disclosure of information:*

An unauthorized user can learn the contents of an it of interest.

➢ *Unawareness:*

The authorized user is unaware that their personal data is being collected, processed, stored or shared.

➢ *Non-compliance:*

The handling or storage of personal data does not comply with relevant laws or policies.

The LINDDUN methodology consists of 3 main steps:

- Model the system.

- Elicit threats.

✓ Map DFD elements to threat categories
✓ Elicit and document threats
✓ Document threats

- Manage threats

✓ Prioritize threats
✓ Select suitable mitigation strategy

✓ Select privacy enhancing solution

In the example below, the high-level DFD of a simplistic social networking system is shown. In the Data Flow Diagram, the user is represented as an entity to interact with the system. The social network application contains two processes that is the portal and the service and one data store that contains all the personal information of the users.

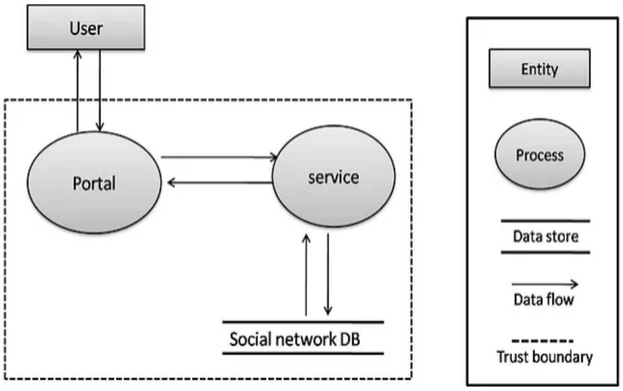

Fig 3: Data Flow Diagram (DFD) of a simple social networking application

IV. EVALUATION CRITERIA

The first criteria is Strengths and Weaknesses. Although there are many threat model methods, there is no perfect method. Each method was developed with different perspective and each has different priorities. Some methods focus on assets whereas some focus on attackers or on risks. Each method has its own strengths and weaknesses.

Table 2. Strengths and weaknesses

	Perspective	**Mitigation**	**Consistent Result**
STRIDE	Defender	Yes	No
OCTAVE	Risk	Yes	Yes
PASTA	Risk	Yes	Not clear
TRIKE	Risk	Yes	No
LINDDUN	Assets	Yes	No

The second criteria is Adoptability. Availability of or absence of good documentation and support can be critical for successful adapting a method.

Table 3. Adaptability

	Easy to learn	**Easy to use**	**Documentation**
STRIDE	Medium	Medium	Very good
OCTAVE	No	No	Good
PASTA	No	No	Very good
TRIKE	Medium	Medium	Good for v1
LINDDUN	Medium	No	Good

The third criteria is Applicability. Methods must be able to be applied recursively and account for the relationship among sub systems. They must also address hardware-software dependencies and safety-security interdependencies.

V. CONCLUSION

Threat modelling can help to make organization more secure and trustworthy. Desired output should govern an organization's choice of threat model method. While all threat model methods, maybe capable of identifying potential threat and the type of threats identified vary significantly. This paper consists of five threat model methods. Some can be used alone while some can be used in conjunction with others.

PASTA modelling method can be used in the basis of framework. Whereas the components STRIDE and LINDDUN can be used. PASTA also mitigates the threat explosion weakness of STRIDE and LINDDUN by utilizing risk and impact analysis. PASTA also uses Attack Tree and CVSS (Common Vulnerability Scoring system). Choosing what method is best for a project depends upon the specific areas where the user wants to target that target can be risk, security or privacy or how long the user can perform threat model, how much experience the user has with threat model.

REFERENCES

[1]. N. Shevchenko, B. Frye, C. Woody, "THREAT MODELING: EVALUATION AND RECOMMENDATIONS", September 2018

[2]. J. Brown-White, L. Cobb, J. DelGrosso, E. Foroughi, A. Ganjali, S. Moghnie, N. Ozmore, R. Padmanabhan, B. Schoenfield, I. Taradach, "Tactical Threat Modeling", SAFECode, 2017

[3]. McGraw, Gary, and John Viega. Building Secure Software: How to Avoid Security Problems the Right Way. San Francisco: Addison-Wesley, 2002, 0-201-72152-X.

[4]. Swiderski, Frank and Window Snyder. Threat Modeling. Redmond, WA: Microsoft Press, 2004, 0-7356-1991-3

[5]. Alberts, Christopher J. and Audrey J. Dorofee. OCTAVESM Criteria, Version 2.0. Pittsburgh, PA: Carnegie Mellon Software Engineering Institute, 2001, http://www.cert.org/archive/pdf/01tr016.pdf.

[6]. Common Criteria Development Board. Common Criteria for Information Technology Security Evaluatio2005, http://www.commoncriteriaportal.org/public/expert/index.php?menu=3.

[7]. Threatmodeler, "Security threat modeling methodologies: Comparing stride, vast &amp; more," ThreatModeler, 24-Aug-2022. [Online]. Available: https://threatmodeler.com/threat-modeling-methodologies-overview-for-your-business/. [Accessed: 25-Feb-2023].

[8]. (PDF) threat modeling methodologies for network security Available at: https://www.researchgate.net/publication/350891779_Threat_Modeling_Methodologies_for_Network_Security (Accessed: February 25, 2023).

[9]. Omar A. Turner, C.I.S.S.P. Privacy threat modeling with the linddun framework, LinkedIn. Available at: https://www.linkedin.com/pulse/privacythreat-modeling-linddun-framework-omar/ (Accessed: February 25, 2023).

[10]. Linddun LINDDUN. Available at: https://www.linddun.org/linddun (Accessed: February 25, 2023)