A Comparative Analysis of Threat Modelling Methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN

Nitin Naik[1], Paul Jenkins[2], Paul Grace[1], Dishita Naik[3],
Shaligram Prajapat[4], and Jingping Song[5]

[1] School of Computer Science and Digital Technologies, Aston University, United Kingdom
[2] Cardiff School of Technologies, Cardiff Metropolitan University, United Kingdom
[3] Birmingham City University, United Kingdom
[4] International Institute of Professional Studies, Devi Ahilya University, India
[5] Software College, Northeastern University, China
n.naik1@aston.ac.uk, pjenkins2@cardiffmet.ac.uk,
p.grace@aston.ac.uk, dishita.naik@mail.bcu.ac.uk,
shaligram.prajapat@iips.edu.in, songjp@swc.neu.edu.cn

Abstract. Novel cybersecurity threats are constantly emerging and posing significant security challenges to organisations; therefore, it is important for organisations to proactively analyse existing and emerging cybersecurity threats against their systems. Threat modelling methods are very effective in proactively analysing cybersecurity threats and enhancing organisational security policies and defence mechanisms against these cybersecurity threats. Several threat modelling methods have been proposed, and it is important for security experts to select the appropriate threat modelling method for an organisation according to their specific security challenges and cybersecurity threats. This paper will present a comparative analysis of six threat modelling methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN. It will provide a concise description of all the aforementioned threat modelling methods, and subsequently, a comparative analysis of these six threat modelling methods for highlighting their relative strengths and limitations.

Keywords: Threat Modelling · Threat Models · Cyberattack · Cyberthreat · Cybersecurity Threat · STRIDE Model · DREAD Model · VAST Model · PASTA Model · OCTAVE Model · LINDDUN Model.

1 Introduction

Cybersecurity threats are increasing everyday which is concerning for organisations [16]. Therefore, organisations require to constantly enhance their security policies and defence mechanisms to cope with the existing and emerging cybersecurity threats and ensure the robust security of their systems [15]. Threat modelling methods are very effective in proactively analysing cybersecurity threats and enhancing organisational security policies and defence mechanisms against these cybersecurity threats [19]. Threat

modelling is a process of identifying, analysing, prioritising and mitigating cybersecurity threats and their associated vulnerabilities in a system or network [18]. A cybersecurity threat is a potential or actual event that can adversely affect IT infrastructures, applications and data; and can have negative consequences for individuals or organisations [18].

Threat modelling can be performed in different ways, such as manual analysis or software-based analysis using various popular methods. Several threat modelling methods have been proposed, and it is important for security experts to choose the appropriate threat modelling method for an organisation according to their specific security challenges and cybersecurity threats [17], [20], [21]. Some popular threat modelling methods are available for use depending on the types of threats and systems, such as STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN. Each threat modelling method has a different focus, such as it can be risk-centric, privacy-centric, application-centric, user-centric or organisation-centric. Some of the threat modelling methods may be combined to create a more robust and effective method.

This paper will present a comparative analysis of six threat modelling methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN. It will provide a concise description of all aforementioned threat modelling methods, and subsequently, a comparative analysis of these six threat modelling methods for highlighting their relative strengths and limitations.

This paper is organised into the following sections: Section 2 explains some basic concepts related to threat modelling; Section 3 discusses six popular threat modelling methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN. Section 4 performs a comparative analysis of six threat modelling methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN. Section 5 presents the conclusion and future work.

2 Concepts Related to Threat Modelling

2.1 What is a Cyber Threat?

A cyber threat or cybersecurity threat is a potential or actual event that can adversely affect IT infrastructures, applications and data, which can have negative consequences for individuals or organisations [18]. A cyber threat or cybersecurity threat is a potential security risk that may exploit the vulnerability of a system or asset. The cause of a cyber threat may be internal or external, accidental or intentional, environmental or human failure [18].

2.2 What is Threat Modelling?

Threat modelling is a process of identifying, analysing, prioritising and mitigating cybersecurity threats and their associated vulnerabilities in a system or network [18]. Threat modelling is the process of using theoretical and practical security scenarios, system diagrams, testing methods and tools to assess the security of assets and their potential weaknesses, and suggesting corrective actions and policies. Threat modelling is a structured, proactive and continuous process for addressing existing and emerging cybersecurity threats in a system or network.

2.3 What is Risk Assessment?

Risk assessment is a process of assessing the possibility and severity of the risks due to cybersecurity threats and vulnerabilities in the system or network. This risk could impact the normal working of the system or network, or affect an organisational performance, reputation, finance or compliance. Depending on the level of risk, it can be eliminated, mitigated, avoided or accepted.

3 Types of Threat Modelling Methods

There are several threat models available for use based on the specific requirement of an organisation [6], [7], [22] [27], [30]. This section presents various popular threat models:

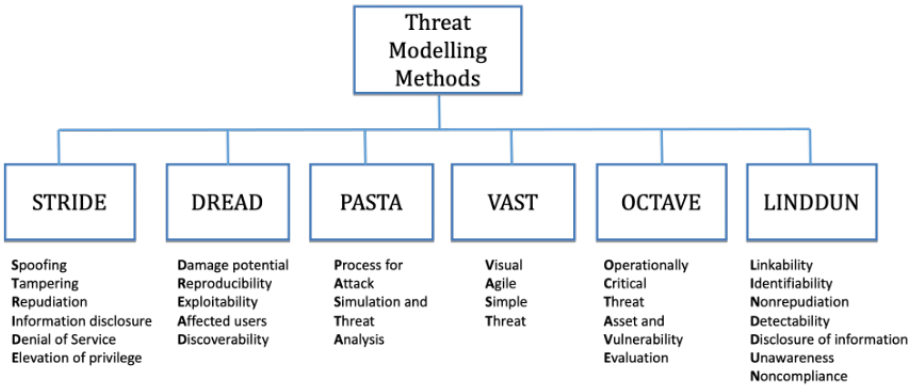

Fig. 1: Types of Threat Modelling Methods

3.1 STRIDE Model

The STRIDE model was developed by Loren Kohnfelder and Praerit Garg at Microsoft in 1999 [9]. This threat model classifies all the cybersecurity threats into six specific threat classes: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. STRIDE is an acronym for all these aforementioned cybersecurity threats, with the model aimed at identifying, analysing, prioritising and mitigating all the threats and vulnerabilities of a one class by using class-specific controls instead of threat-specific controls.

The STRIDE model utilises Data Flow Diagrams (DFDs) for threat modelling and identifying system boundaries, events, and entities. Moreover, the model focuses on security properties of Confidentiality, Integrity, and Availability (CIA), in conjunction with Authorisation, Authentication, and Non-Repudiation; and analyses an application against these properties.

The STRIDE model is mainly used for an application and software security analysis; however, it can be used for other types of systems and networks. Additionally, Microsoft developed some advanced versions of STRIDE, such as STRIDE-per-element and STRIDE-per-interaction. The STRIDE model is not actively maintained by Microsoft; however, it is implemented as part of the Microsoft Security Development Lifecycle (SDL), and available with its Threat Modelling Tool [13], [14].

The description of each threat related to its corresponding letter of STRIDE acronym is as follows:

S - Spoofing: It refers to an attacker impersonating an authentic user or system in order to gain access to the system.

T - Tampering: It refers to an unauthorised modification of data or systems.

R - Repudiation: It refers to denying an event or action by its creator in order to utilise it for malicious purpose.

I - Information Disclosure: It refers to exposing sensitive information to unauthorised users.

D - Denial of Service: It refers to the disruption or blockage caused during an authorised access to systems or resources.

E - Elevation of privilege: It refers to gaining higher privileges in order to perform an unauthorised action.

3.2 DREAD Model

The DREAD model was developed by David LeBlanc and Michael Howard at Microsoft and published in the book *Writing Secure Code 2nd edition* in 2002 [10]. This threat model classifies all the cybersecurity threats into five specific threat classes: Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability. DREAD is an acronym for all these aforementioned cybersecurity threats, and the model is aimed at identifying, analysing, prioritising and mitigating all the threats and vulnerabilities of a class by using class-specific controls instead of threat-specific controls.

This DREAD model assigns a score of 1 to 10 to each of the classes to determine the severity of the potential threat [4]. Later, all the scores are summed to calculate a total score of the threat. The process of severity calculation is somewhat similar to the process of the Common Vulnerability Scoring System (CVSS) method. Some software developers utilise both DREAD and CVSS as a combined threat model when scoring threats and vulnerabilities.

The DREAD model is a quantitative method of calculating the severity of a threat based on the grading system 1 to 10; therefore, a higher scored severity threat can be prioritised and mitigated first [23]. Microsoft stopped using the DREAD model due to its inconsistent scoring and concern about its subjectivity; however, organisations still use it for their threat analysis. Another limitation of the DREAD model was that it was only focused on technical aspects of a potential threat and did not consider other factors that could impact the severity of the potential threat.

The description of each threat related to its corresponding letter of DREAD acronym is as follows:

D - Damage Potential: It refers to the potential impact that a vulnerability could have on the target.

R - Reproducibility: It refers to the ease of reproducing the vulnerability by an attacker.

E - Exploitability: It refers to the ease of exploiting the vulnerability by an attacker.

A - Affected Users: It refers to the total number of users affected by the vulnerability.

D - Discoverability: It refers to the ease of discovering the vulnerability by an attacker.

3.3 VAST Model

The VAST threat model was developed by ThreatModeler, a company founded by Archie Agarwal in 2010 [24], [25]. It is an enterprise level method for identifying, analysing, prioritising and mitigating numerous cybersecurity threats. VAST is an acronym for Visual, Agile, and Simple Threat, thus, the model is aimed at simplified, collaborative, graphical and agile analysis.

It is a highly scalable model that can be scaled across thousands of threats assuming that attackers can perform attacks in an unlimited number of ways. When an enterprise grows, the threats to the enterprise grow, and this model enables a sustainable self-service threat modelling practice driven by the DevOps teams to make proactive security decisions instead of the security team [27].

The VAST model enables the analysis team to analyse the risk of cybersecurity threats from two different perspectives, architectural and operational; and create two types of threat models: application threat model and operational threat model [26]. Application threat models utilise a Process-Flow Diagram (PFD) and are created by the development team to represent the architectural aspect of the threat. Operational threat models utilise a Data-Flow Diagram (DFD) and are created by the infrastructure team to represent the threat from the viewpoint of an attacker [26].

The description of each of the letters of VAST is as follows:

V - Visual: It makes the use of visual aids and diagrams for easy and quick threat identification process.

A - Agile: It can be integrated into an agile environment and provide understandable and actionable outputs for all stakeholders.

ST - Simple Threat: It simplifies the threat analysis at an enterprise level and scale, for example, PFDs are simpler than DFDs, and on the basis of PFDs, the VAST model does not require significant expertise.

3.4 PASTA Model

The PASTA threat model was developed by VerSprite CEO Tony UcedaVélez and security leader Marco M. Morana [28]. It is a comprehensive risk-based method for identifying, analysing, prioritising and mitigating numerous cybersecurity threats [29]. PASTA is an acronym for Process for Attack Simulation and Threat Analysis. The PASTA model is a risk-centric model and is focused on the threats with the highest risks to

the business, thus, enabling the business to invest greater time and resources toward these risks.

The PASTA model is a complex model which requires a high level of expertise and significant time to implement it appropriately; thus, it may not be the preferred choice for smaller organisations with limited resources [8].

It includes a seven-step threat modelling process, where each step comprises multiple activities, and these seven steps are as follows:

Define Objectives: It refers to defining the objectives of the business.

Define Technical Scope: It refers to defining the technical scope of the system.

Decompose the System: It refers to dividing the system into smaller components and analysing each of the component for potential threats.

Analyse the Threat: It refers to analysing and prioritising each threat.

Analyse Weaknesses and Vulnerabilities: It refers to analysing potential vulnerabilities in the system.

Model and Simulate Attack: It refers to modelling and simulating potential attack vectors linked to the identified threats.

Analyse Risk Impact: It refers to analysing the risk associated with each identified threat and prioritise it for its risk mitigation.

3.5 OCTAVE Model

The OCTAVE model was developed by Christopher J. Alberts, Sandra G. Behrens, Richard D. Pethia, and William R. Wilson at Carnegie Mellon University in 1999 [2]. It is a self-directed and enterprise level method for identifying, analysing, prioritising and mitigating numerous cybersecurity threats. OCTAVE is an acronym for Operationally Critical Threat, Asset, and Vulnerability Evaluation.

As a self-directed method, employees assume responsibility for developing the security policy of an organisation instead of only a technical team, because its focus was assessing organisational risks, instead of technological risks. The original version of OCTAVE was aimed at small to medium sized organisations. Later, OCATVE was enhanced in successive versions OCTAVE-S [1], and OCTAVE Allegro [3]. In OCTAVE-S, the threat analysis is performed by an analysis team with extensive knowledge of the organisation; therefore, it does not require training for team members, as they have the knowledge of all assets, security requirements, threats, and security practices of the organisation [1].

The original OCTAVE and OCTAVE-S models consist of three phases, whereas OCTAVE Allegro approach consists of four phases and eight steps [1], [2], [3]. The three phases of OCTAVE and OCTAVE-S models are as follows:

Phase 1 - Identify Assets and Threats: The analysis team identifies all the critical assets in the organisation and possible threats to these assets.

Phase 2 - Technical Analysis of Key Components and Vulnerabilities: The analysis team performs a technical analysis of all the key components of the system and possible vulnerabilities.

Phase 3 - Develop Risk Mitigation Strategies: The analysis team develops risk mitigation strategies for all the identified threats.

3.6 LINDDUN Model

The LINDDUN model was developed by Mina Deng, Kim Wuyts, Riccardo Scandariato, Bart Preneel, and Wouter Joosen at KU Leuven University in 2010 [5]. This threat model is mainly focused on privacy threats and classifies all the privacy related threats into seven specific threat classes: Linkability, Identifiability, Nonrepudiation, Detectability, Disclosure of information, Unawareness, Noncompliance [11]. LINDDUN is an acronym for all these aforementioned privacy threats, and the model is aimed at identifying, analysing, prioritising and mitigating these privacy threats and vulnerabilities [12].

The LINDDUN model utilises DFDs for the analysis of privacy threats of the system, wherein it defines various components of the system, such as data flows, data stores, processes, and external entities using DFDs. This model is useful in assessing privacy regulations and how the system complies with it; however, assessing all technical vulnerabilities using this model may be a difficult task.

The description of the threat related to each of the letters of LINDDUN is as follows:

L - Linkability: It refers to the threat of linking two or more items of interest related to an individual or group by an attacker.

I - Identifiability: It refers to the threat of identifying an individual through leaks, deduction, or inference.

N - Nonrepudiation: It refers to the threat of gathering evidence to counter the claims of the repudiating individual or group.

D - Detectability: It refers to the threat of deducing the involvement of an individual or group through observation.

D - Disclosure of information: It refers to the threat of exposing personal information to unauthorised individuals.

U - Unawareness: It refers to the threat of not having sufficient information to an individual or group about how their personal information is being processed.

N - Noncompliance: It refers to the threat of breaching or deviating from security and privacy policies and regulations by an individual or group.

4 Comparative Analysis of Threat Modelling Methods

This section presents a comparative analysis of six threat modelling methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN. Table 1 shows this comparative analysis of these six threat modelling methods based on various criteria.

5 Conclusion

This paper presented a comparative analysis of six threat modelling methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN. It provided a concise description of all aforementioned threat modelling methods, and subsequently, a comparative analysis of these six threat modelling methods for their relative comparison. This comparative analysis provides a better understanding for choosing the appropriate threat modelling

Table 1: Comparative Analysis of Threat Modelling Methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN

Criteria	**STRIDE**	**DREAD**	**VAST**	**PASTA**	**OCTAVE**	**LINDDUN**
Year	1999	2002	2013	2015	1999	2010
Creator	Kohnfelder and Praerit Garg	David LeBlanc and Michael Howard	Archie Agarwal	Tony UcedaVélez and Marco M. Morana	Christopher J. Alberts, Sandra G. Behrens, Richard D. Pethia, and William R. Wilson	Mina Deng, Kim Wuyts, Riccardo Scandariato, Bart Preneel, and Wouter Joosen
Organisation	Microsoft	Microsoft	ThreatModeler	VerSprite	Carnegie Mellon University	KU Leuven University
Key Feature	It focuses on threat modelling using specific threat classes.	It focuses on threat modelling using specific threat classes and their quantitative risk assessment.	It focuses on threat modelling with collaboration, scalability and sustainability.	It focuses on threat modelling with collaboration, attack simulation and risk assessment.	It focuses on threat modelling with collaboration and organisational risk assessment.	It focuses on threat modelling of privacy threats.
Ease of Use	Easy	Complex	Complex	Complex	Complex	Complex
Scalability	Moderately Scalable	Least Scalable	Highly Scalable	Scalable	Moderately Scalable	Scalable
Application	It can be used for small organisations that are mainly concerned with software security.	It can be used for large organisations that require a structured and quantitative risk assessment method.	It can be used for large organisations that require scalability and sustainability.	It can be used for large organisations that require organisational risk assessment method.	It can be used for organisations that require cross-team collaboration and organisational risk assessment method.	It can be used for organisations that require privacy risk assessment and management.

method for an organisation according to their specific security challenges and cybersecurity threats. In future, all these threat modelling methods may be evaluated using a case study.

References

1. Alberts, C., Dorofee, A., Stevens, J., Woody, C.: OCTAVE-S (2005)
2. Alberts, C.J., Behrens, S.G., Pethia, R.D., Wilson, W.R.: Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework, version 1.0 (1999)
3. Caralli, R.A., Stevens, J.F., Young, L.R., Wilson, W.R.: Introducing OCTAVE Allegro: Improving the information security risk assessment process. Hansom AFB, MA (2007)
4. Cyral.com: Threat modeling with DREAD (2024), https://cyral.com/glossary/threat-modeling-with-dread/
5. Deng, M., Wuyts, K., Scandariato, R., Preneel, B., Joosen, W.: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requirements Engineering **16**(1), 3–32 (2011)
6. Eccouncil.org: Cyber threat modeling (2024), https://www.eccouncil.org/threat-modeling/
7. Gonzalez, C.: Threat modeling: 5 steps, 7 techniques, and tips for success (2023), https://www.exabeam.com/blog/infosec-trends/top-8-threat-modeling-methodologies-and-techniques/
8. Kirtley, N.: PASTA threat modeling (2022), https://threat-modeling.com/pasta-threat-modeling/
9. Kohnfelder, L., Garg, P.: The threats to our products (1999)
10. LeBlanc, D., Howard, M.: Writing secure code. Pearson Education (2002)
11. Linddun.com: LINDDUN privacy threat modelling: Identify privacy threats in software systems (2024), https://linddun.org/threat-types/
12. Linddun.com: LINDDUN: Privacy threat types (2024), https://linddun.org/
13. Microsoft.com: Microsoft threat modeling tool: Mitigations (2022), https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-mitigations
14. Microsoft.com: Microsoft threat modeling tool: Threats (2022), https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats
15. Naik, N., Grace, P., Jenkins, P.: An attack tree based risk analysis method for investigating attacks and facilitating their mitigations in self-sovereign identity. In: IEEE Symposium Series on Computational Intelligence (SSCI). IEEE (2021)
16. Naik, N., Grace, P., Jenkins, P., Naik, K., Song, J.: An evaluation of potential attack surfaces based on attack tree modelling and risk matrix applied to self-sovereign identity. Computers & Security **120**, 102808 (2022)
17. Naik, N., Jenkins, P., Grace, P.: Cyberattack analysis based on attack tree with weighted average probability and risk of attack. In: UK Workshop on Computational Intelligence (UKCI). Springer (2022)
18. Naik, N., Jenkins, P., Grace, P., Naik, D., Prajapat, S., Song, J.: An introduction to threat modelling: Modelling steps, model types, benefits and challenges. In: The International Conference on Computing,Communication,Cybersecurity &AI (The C3AI 2024). Springer (2024)
19. Naik, N., Jenkins, P., Grace, P., Naik, D., Prajapat, S., Song, J., Xu, J., Czekster, R.M.: Analysing cyberattacks using attack tree and fuzzy rules. In: UK Workshop on Computational Intelligence (UKCI). Springer (2023)

20. Naik, N., Jenkins, P., Grace, P., Naik, D., Song, J., Prajapat, S., Mishra, D., Yang, L., Boongoen, T., Iam-On, N.: Fuzzy attack tree: Assessing cyberattack risk using attack tree and fuzzy logic. In: 2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG). pp. 1–9. IEEE (2023)
21. Naik, N., Jenkins, P., Grace, P., Prajapat, S., Naik, D., Song, J., Xu, J., Czekster, R.M.: Cyberattack analysis utilising attack tree with weighted mean probability and risk of attack. In: UK Workshop on Computational Intelligence (UKCI). Springer (2023)
22. Naik, N., Jenkins, P., Grace, P., Song, J.: Comparing Attack Models for IT Systems: Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model. In: 2022 IEEE International Symposium on Systems Engineering (ISSE). IEEE (2022)
23. Satoricyber.com: Threat modeling with microsoft DREAD (2022), https://satoricyber.com/glossary/threat-modeling-with-microsoft-dread/#:~:text=DREAD
24. Threatmodeler.com: The evolution of threat modeling (2016), https://threatmodeler.com/evolution-of-threat-modeling/
25. Threatmodeler.com: Threat modeling methodologies: What is VAST? (2018), https://threatmodeler.com/threat-modeling-methodologies-vast/
26. Threatmodeler.com: Which threat modeling methodology is right for your organization? (2018), https://threatmodeler.com/threat-modeling-methodology/
27. Threatmodeler.com: The ultimate guide to threat modeling (2024), https://threatmodeler.com/the-ultimate-guide-to-threat-modeling/
28. UcedaVlez, T.: What is PASTA threat modeling? why use PASTA? (2021), https://versprite.com/blog/what-is-pasta-threat-modeling/
29. Versprite.com: Risk-based security threat modeling: 7-step process for risk analysis (2024), https://versprite.com/security-resources/risk-based-threat-modeling/
30. Windriver.com: What is threat modeling? (2024), https://www.windriver.com/solutions/learning/threat-modeling