Enhancing IoRT Security: A Unified Approach to Threat Identification, Prioritization, and Mitigation

Neha Koul[1], Neerendra Kumar[2,*], Arvind Selwal[3], Narinder Verma[4,*]

[1] Research Scholar, Department of Professional Studies, Christ (Deemed to be University), Bengaluru, India.
[2] Department of Professional Studies, Christ (Deemed to be University), Bengaluru, India
litty.sylus@res.christuniversity.in

Abstract. The Internet of Robotic Things (IoRT) is an anticipated integration of robotic systems with interconnected communications that enable independent and intelligent exchange in multiple domains. Such interconnectivity, however, also has serious concerns related to cybersecurity, necessitating advanced approaches to threat modeling. Such a hybrid method tailored for IoRT, appropriate for systematic identification of threats through STRIDE, threat prioritization based on the severity of impact through DREAD, and subsequent organized mitigation using attack trees along with attack-defense trees, is adopted in the present paper. By employing this hybrid methodology, we establish a robust framework that addresses security at multiple levels. This process includes identifying potential threats, prioritizing them according to their severity, and devising effective defenses. Our findings suggest that this approach offers a more comprehensive assessment of vulnerabilities and stronger mitigation strategies compared to traditional single-method approaches. This extensive methodology is designed to enhance the security of Robotic systems and their applications across various fields, ensuring the resilient and secure deployment of robotic systems within interconnected environments.

Keywords: Robotic security, Threat Modeling, STRIDE, DREAD, Threat Mitigation.

1 Introduction

The Internet of Robotic Things (IoRT) has emerged as a seminal technological development that has merged robotic systems with networked intelligence toward self-governing and interactive undertakings in all walks of life such as healthcare, manufacturing, environmental observation, and logistics. IoRT has become an integral part of different spheres [1]. For instance, we recurrently make use of robotic vacuum cleaners in our households and homes, Amazon Prime Air drones deliver diverse amenities (such as pizza delivery). Robotic systems are being utilized in manufacturing for assembly (e.g., auto-vehicles) and healthcare, and now, more recently, self-driving automobiles have been permitted in several States in the United States, such as Uber's autonomous vehicles operational in Pittsburgh, Arizona, and California [2]. Also, the forthcoming era of semi or fully-autonomous robotics in private citizen, commerce, and military fields, and in nearly all fields present in our environs can resolve many hitches and save time, power, and human lives [3]. For example, unmanned robotics devices (such as drones, robot dogs, and underwater bots) used in the military are both aerial and terrestrial operations [4].

M. Sharma et al. (eds.), *Proceedings of the Third International Conference on Recent Advances in Computing Sciences (RACS 2025)*, Advances in Intelligent Systems Research 212,
https://doi.org/10.2991/978-94-6239-768-2_10

Therefore, safeguarding security and privacy, commonly referred to as cybersecurity, for robotic system platforms is of paramount importance, as catastrophes and outbreaks may lead to disastrous results. IoRT frameworks leverage actuators, sensors, and innovative communication protocols that empower robots to detect and scrutinize elusive environmental signals proactively. However, such connectivity increases the capabilities of robotic systems and brings with them crucial risks regarding cybersecurity. Potentially, attackers may cause disturbances or even leaks in the data together with physical harm through damage or exploitation vulnerabilities in the communication channels, modules processing data, or any physical components in the framework of IoRT systems. According to the National Institute of Science and Technology (NIST) [5], robots that have been compromised can pose both digital and physical risks to their operating environment. Such vulnerability calls for more stringent cybersecurity measures. To evaluate the cybersecurity robustness of a robotic system, the following procedures are commonly applied [6]:

- Identification of Privacy and Security Threats: Recognizing potential threats across different robotic systems.
- Systematic Impact Evaluation: Assessing the potential impression of acknowledged threats in a structured method.
- Threat Inhibition and Mitigation: Implementing measures to prevent and reduce the risks associated with these threats.

These procedures mentioned above altogether pave the way to the threat modeling of the robotic systems to protect them from cyber-attacks. Threat modeling is a method for identifying and quantifying security risks. It can be difficult to do a security evaluation for intricate IoRT systems. Furthermore, contemporary robotic systems have a greater attack surface as a result of having internet connectivity. Therefore, a threat model to counteract or lessen the potential threats might be developed by assessing the possible risks associated with the robotic systems [7]. A generic threat model takes into account any element and method that could jeopardize security. Threat analysis explains the possible attackers, the reasons behind their attacks, and the system components that are under threat [8].

Difficulties Associated with Conventional Threat Modeling Methodologies: Traditional threat modeling approaches are valuable but lack comprehensive support for the layered and interconnected nature of IoRT systems[9]. Categorization models, such as STRIDE-Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege-and DREAD-Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability-help with identification and prioritization of threats, respectively. When used alone, they are limited in terms of depth of analysis. Whereas STRIDE can only identify threats, but not rank them by impact level, DREAD ranks threats but lacks a deep structure for mitigation. Lastly, whereas classical attack trees detail possible paths for the attacks, they may fall short without a corresponding defense strategy. Some hybrid threat models do exist, each with some or the other restrictions or limitations. The authors of this article have tried their best to improve and overcome the existing limitations.

Towards a Hybrid Approach to Threat Modeling for IoRT Security: To tackle the above-mentioned issues, the introduction of a thorough hybrid threat modeling methodology that utilizes the advantages of STRIDE, DREAD, and attack trees,

enhanced by the incorporation of attack-defense trees, to provide a resilient framework for IoRT threat modeling. Within this integrated methodology, STRIDE methodically detects possible threats present in IoRT system components, while DREAD assesses and prioritizes these threats according to their severity, and attack trees delineate various potential attack vectors. Attack-defense trees augment the methodology by delineating defensive strategies corresponding to each stage of an attack, thereby establishing a systematic framework for efficient threat alleviation.

Aims and Contribution: The goal of this paper is to advance IoRT security by presenting a hybrid methodology that encompasses threat identification, prioritization, and mitigation. Specifically, this article:

1. Present a unifying approach integrating STRIDE, DREAD, and attack-defense trees customized for IoRT applications.

2. Illustrate such an approach through a generic case study of an IoRT system to provide a template to deal with complex cybersecurity threats.

3. Illustrate how the hybrid approach supports a better understanding of vulnerabilities and offers a structured framework for carrying out security measures. The proposed hybrid threat modeling methodology presents a scalable and adaptable framework aimed at improving the security of IoRT systems, thereby establishing a route towards resilient and secure IoRT implementations across diverse domains.

The layout of the paper is as follows. The related work is provided in Section 2. Section 3 presents the proposed threat modeling methodology. The discussion and future work is presented in Section 4. Conclusions are summarized in Section 5.

2 Related work

For IoRT systems, threat modeling must account for the unique combination of hardware (robotic components), software (control algorithms), and networking (data communication protocols). Several methodologies have been developed for threat modeling, each addressing specific aspects of system security.

[10] presented a new threat model for cyber-physical systems that take into consideration the physical, cyber, and human aspects. This model showcases the relation of components in the system as well as its security aspects. A method for threat analysis is also proposed for the understanding of the security perspective of the system modules. The automation tool used is TAMELESS.

[9] has developed a threat model that combines STRIDE, attack trees, and attack libraries for modeling threats. This model adopts a structural approach that provides readability and optimum details for successful threat modeling.

The researchers in [11] have given a framework named modeling threats with hybrid techniques (MOTH) to help secure the software assets of robotic systems from attackers so that the prevention of SQL injection attacks can be done. Here the authors focused only on conventional threat modeling using attack trees.

In [12], authors designed a model for modeling threats that combines the best features of STRIDE, security cards, and persona non grata in their framework for threat

modeling. Their model identifies threats and performs the risk assessment to secure the smart systems in IoRT.

The authors of [13] in their work have created a hybrid vehicular model based on STRIDE and attack trees and have named it SAVTA (Software-Asset-Vulnerability-Threat-Attackers). This identifies the threats using the traditional STRIDE model and develops the attack trees to represent the attack vectors that pose a danger to a specific vehicle asset.

Authors in [14] have done the threat modeling of water and waste-water systems (WWS) to minimize the risk of cyber threats that are postured by malevolent cyber threat actors. The authors here used the two existing threat models (STRIDE and DREAD) for threat recognition and their prioritization.

Table 1. A comparative analysis of the proposed Unified Threat Model with existing Threat Models**.**

Feature	Identify Threats (STRIDE)	Score Threats (DREAD)	Mitigation (Attack Trees)	Mitigation (Attack-Defense Trees)	Comprehensive
[10] TAMELESS	✓	✗	✗	✗	✗
[9] STRIDE + Attack Trees	✓	✗	✓	✗	✗
[11] MOTH	✓	✗	✓	✗	✗
[12] STRIDE + Cards	✓	✗	✗	✗	✗
[13] SAVTA	✓	✗	✓	✗	✗
[14] STRIDE + DREAD	✓	✓	✗	✗	✗
Proposed Hybrid Model	✓	✓	✓	✓	✓

3 Proposed Unified Threat Modelling Methodology

The proposed hybrid methodology integrates three established models: 1) STRIDE, 2) DREAD, and 3) attack trees into a unified framework for identifying, prioritising, and mitigating threats in IoRT systems. This section outlines the methodology and explains its application to address the unique security challenges of IoRT systems. Fig. 1 presents the Proposed Hybrid Threat Model for Security Attacks on the IoRT System. The proposed model is divided into three modules. The first one deals with the identification of threats in the robotic system using the STRIDE model. The identification and analysis of threats can be performed manually through brainstorming sessions or by making use of the threat modeling tool given by Microsoft. The second module performs the risk assessment by scoring the threats. Based on this scoring the threats can be prioritized, and the severity of the threat can be analyzed. Third and the last one deals with the countermeasures of the threats identified and prioritized by the

first two consecutive modules. The complete proposed model is explained below in detail defining the STRIDE, DREAD, Attack Trees, and Attack Defense Trees individually. The attributes and description of STRIDE and DREAD, and example basic structure of Attack Trees and Attack Defense Trees are also presented.

3.1 STRIDE Model for Threat Identification

The STRIDE model systematically identifies potential threats by categorizing them into six types: 1) Spoofing (S), 2) Tampering (T), 3) Repudiation (R), 4) Information Disclosure (I), 5) Denial of Service (D), and 6) Elevation of Privilege (E) [15][16], as shown in Fig. 2.

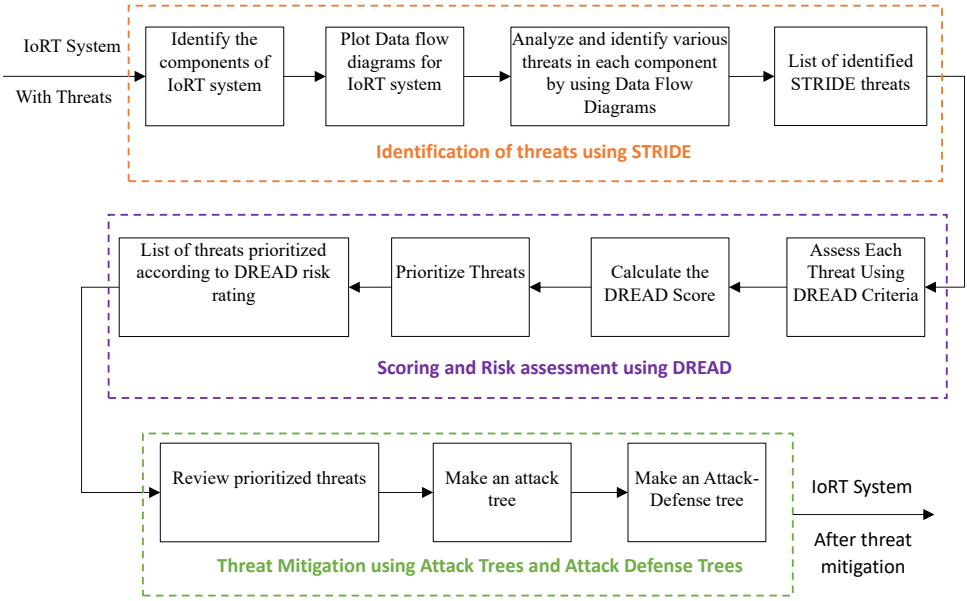


Fig. 1. The Proposed Hybrid Threat Model for Security Attacks on IoRT System.

For IoRT systems, STRIDE is applied across all critical components, such as:

1. Sensors: Vulnerabilities in spoofing or tampering with sensor data.
2. Actuators: Risks from tampering or denial-of-service attacks that could disrupt robotic movements.

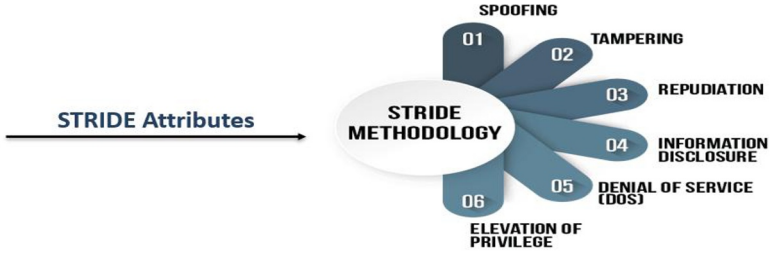
3. Communication Channels: Potential for information disclosure and spoofing during data transmission.
4. Cloud/Server Systems: Threats from privilege escalation or tampering with stored data.

This systematic categorization ensures the comprehensive identification of threats, providing a foundation for further analysis. After identifying threats, we can also define a coverage ratio to quantify STRIDE's comprehensiveness as shown in Equation 1:

$$\text{Coverage} = \frac{T_{identified}}{T_{total}} . 100 \qquad (1)$$

Where:

$T_{identified}$: Number of threats identified by STRIDE
T_{total}: Total possible threats (based on domain knowledge or attack databases)



Category	Description	Controls
Spoofing	Pretending to be someone else	Authentication
Tampering	Changing data to be inaccurate	Integrity controls
Repudiation	Denying that you did a thing you did	Accountability controls
Information Disclosure	Revealing information that should not be otherwise accessible	Confidentiality controls
Denial of Service	Trying to stop someone else from using a system	Availability controls
Elevation of Privilege	Trying to get a higher level of access than you are currently assigned	Authorization controls

Description & Control

Fig. 2. STRIDE Model attributes and description.

Table 2. Potential STRIDE Threats and Descriptions in a Robotic System

Parameters	Attacks	Violation	Threat Description
Spoofing Identity	Manipulation of authentication protocols, impersonation of authorized users	Compromised access tokens	Attackers gain access to the robotic system by spoofing their identity and posing as authorized users.
Tampering	Injection of malicious code, unauthorized modifications to software or firmware	Compromised software	Malicious software alters the functionality of the robotic system or modifies critical settings.
Repudiation	Denial of executed commands, falsification of system logs	Insider credentials	Insider denies executing commands or alters system logs to hide unauthorized actions.
Information Disclosure	Eavesdropping on communication channels, unauthorized access to data repositories	Intercepted communication data	Attackers eavesdrop on communications or gain unauthorized access to sensitive data stored within the robotic system.
Denial of Service	Overloading system resources, network flooding attacks	Botnet access	Attackers flood the robotic system with traffic to overwhelm resources, rendering it unresponsive.
Elevation of Privilege	Exploitation of software vulnerabilities, unauthorized escalation of user privileges	Software exploits	Attackers exploit vulnerabilities in the robotic system to gain escalated privileges, potentially taking full control.

3.2 DREAD Model for Threat Prioritization

After identifying threats using STRIDE, the DREAD model is employed to prioritize them based on their severity and impact. In DREAD, D stands for Damage potential, R for reproducibility, E for exploitability, A for affected users, and D for discoverability. Microsoft created this asset-centric threat modeling technique. DREAD applies a qualitative risk assessment of 3, 2, and 1 following the conventional qualitative risk rating system (HIGH, MEDIUM, LOW). High-priority threats are addressed first, ensuring the most critical vulnerabilities are mitigated promptly.

Generally speaking, the DREAD threat modeling approach determines the likelihood of occurrence for each of the indicated regions of the asset under threat modeling using a scoring system.

The DREAD threat modeling approach predicts the likelihood of each danger found during the threat modeling process by combining the risk rating values acquired [17].

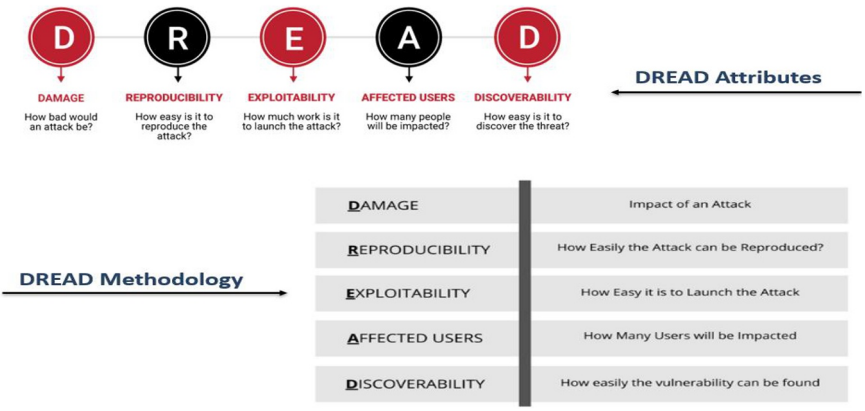


Fig. 3. DREAD Attributes and Methodology

In general, for a robotic system:

- A denial-of-service attack on a robotic control system might score high in Damage Potential and Affected Users, making it a top priority for mitigation.
- Spoofing a sensor might score lower due to limited immediate impact, ranking it as a medium-priority threat.

The DREAD score is calculated for various threats identified by STRIDE as follows in equation 2:

$$DREAD\_SCORE(T) = Da_T + R_T + E_T + A_T + Di_T \quad (2)$$

Where:

Da_T = Damage potential
R_T = Reproducibility
E_T = Exploitability
A_T = Affected users
Di_T = Discoverability

The ranking and prioritizing of threats is done by their DREAD_SCORE(T), with higher scores indicating higher risk. For no risk, the DREAD score can be set to 0. So, the total score ranges from 0 for no risk and 1 (minimum risk) to 15 (maximum risk).

Table 3. Criteria for Scoring in the DREAD Threat Model

Symbol	Attribute	Low Risk (1)	Medium Risk (2)	High Risk (3)
D	Damage Potential	Disclosing trivial information	Sensitive information disclosure	Potential indemnities by receiving full authorization and can overthrow the security.
R	Reproducibility	Difficult to reproduce the attack	The attack could be regenerated with the specified requirements and time interval.	The attack can take place without any specific time-bound or other requirements.
E	Exploitability	The requirement of great proficiency and knowledge to perform an attack	Moderately skilled programmers can perform the attack	A greenhorn programmer or even a scripted cyberpunk can execute the attack
A	Affected Users	A small number of anonymous users are pretentious by the attack	Only a few users are affected by the attacks	The attack affects all users
D	Discoverability	No statistics exist about the attack (like, a zero-day attack)	Less information is obtainable about the attack and also all users don't get to know about it	Information about the process of implementing an attack is easily obtainable

3.3 Attack Trees and Attack-Defense Trees for Threat Mitigation

1) Attack trees: One of the earliest and most popular methods for modeling threats on only cyber systems, physical systems, and cyber-physical systems is the use of attack trees. Created by Bruce Schneider in 1999, it was first used as a stand-alone technique before being integrated with other frameworks and techniques. In essence, attack trees are diagrams that show system attacks in the shape of a tree. The attack's target is the tree root, and the leaves serve as a means of getting there [15].

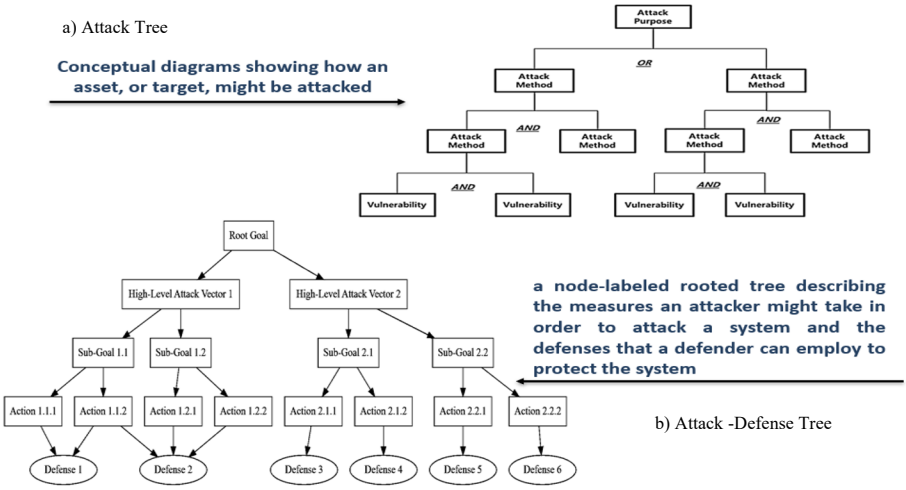


Fig. 4. Basic structure of a) Attack tree and b) Attack-Defense Tree

A distinct tree is utilized to epitomize each goal. Consequently, a collection of attack trees is generated by the system threat analysis. For IoRT systems, attack trees help model threats such as:

- Goal: Disrupt robotic control during an operation.
  - Step 1: Gain unauthorized network access.
    - Sub-step: Exploit weak credentials.
    - Sub-step: Intercept communication.
  - Step 2: Inject malicious commands.

Attack trees provide a clear understanding of how threats can materialize, aiding in the design of specific mitigation strategies. Formally, an attack tree may be defined as equation 3:

$$\text{Attack\_tree} = \{N,E,N_R,R\} \quad (3)$$

Where N is a set of nodes, E is a set of edges, N_R is the root node and R is the set of relations between the nodes of the attack tree. In an attack tree, the root node is the aim of the attacker. So, to exploit the root node an attacker has to follow a particular path starting from a leaf node to the root node. There may be more than one path to perform an attack consisting of two logical operations (AND, OR).

2) Attack Defense Trees: An expansion of the Attack Trees is the Attack-Defense Trees. They consist of a root node, a list of potential attacks on a system, and a list of defense strategies the defender can use. The assault and defend nodes are the two types of nodes that can be further subdivided into sub-goals on the assault-defense Trees. Additionally, each node may contain a sub-node known as a countermeasure, which is a child of the opposite type[18]. This dual representation enables simultaneous visualization of attack pathways and countermeasures. For instance:

- Goal: Disrupt robotic control during an operation.
  - Defense 1: Use strong encryption for network communication (to prevent unauthorized access).
  - Defense 2: Implement anomaly detection systems (to identify malicious commands).

By mapping defenses directly to attack steps, attack-defense trees offer actionable insights into securing IoRT systems, ensuring that mitigation strategies are comprehensive and targeted.

4 Discussion and Future Work

To handle the complex security issues of Internet of Robotic Things (IoRT) systems, the suggested hybrid threat modeling methodology combines STRIDE, DREAD, attack trees, and attack-defense trees. The framework guarantees a thorough and organized approach to cybersecurity by fusing quantitative prioritization, systematic threat detection, and visual portrayal of attack and defense tactics. Nevertheless, there is still room for improvement. The methodology's primary focus on cybersecurity risks fails to fully account for interrelated cyber-physical threats, and its reliance on precise probability and impact estimations in DREAD grading introduces subjectivity. Furthermore, difficulties with automation and scalability may prevent it from being applied to extremely complicated IoRT systems. Future studies will concentrate on the following to improve the framework:

1. AI-Driven Threat Prediction: Using AI to improve threat probabilities and dynamically detect new threats.
2. Cyber-Physical Integration: broadening the focus to encompass cross-domain vulnerabilities and physical safety.

3. Wider Uses: Validating the approach in a variety of IoRT fields, including industrial robotics and autonomous automobiles.
4. Defence Optimisation: Developing metrics to measure cost-effectiveness and maximize the use of available resources.
A fundamental framework for protecting IoRT systems is offered by this work. Its relevance and effectiveness against changing threats will be strengthened by future developments in automation, transdisciplinary approaches, and domain-specific modifications.

5 Conclusion

As IoRT technologies continue to evolve and become more integrated into critical infrastructure, the importance of securing these systems becomes increasingly critical. This paper has introduced a unified approach to enhancing the security of Internet of Robotic Things (IoRT) systems, integrating threat identification, prioritization, and mitigation into a comprehensive framework. The proposed methodology combines STRIDE for systematic threat identification, DREAD for prioritizing those threats based on their potential impact, and attack-defense trees for modeling both attack scenarios and corresponding defense strategies. By bringing together these established threat modeling techniques, the approach provides a structured and effective way to address the unique security challenges posed by IoRT systems. This unified strategy's strength is its comprehensive approach to IoRT system security. A balanced evaluation of risk and security measures is made possible by the methodology's consideration of both offensive and defensive components within a single framework. Based on the type and importance of the threats, it assists organizations and researchers in identifying weaknesses, evaluating the performance of current defenses, and putting targeted mitigation plans into action.

References

[1] N. Koul, N. Kumar, A. Sayeed, C. Verma, and M. S. Raboaca, “Data Exchange Techniques for Internet of Robotic Things: Recent Developments,” IEEE Access, vol. 10, pp. 102087–102106, 2022, doi: 10.1109/ACCESS.2022.3209376.

[2] S. E. Shladover and C. Nowakowski, “Regulatory challenges for road vehicle automation: Lessons from the California experience,” Transp Res Part A Policy Pract, vol. 122, pp. 125–133, Apr. 2019, doi: 10.1016/J.TRA.2017.10.006.

[3] I. Priyadarshini, “Cyber security risks in robotics,” in Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, IGI Global, 2018, pp. 1235–1250. doi: 10.4018/978-1-5225-5634-3.ch061.

[4] K. M. Ahmad Yousef, A. AlMajali, S. A. Ghalyon, W. Dweik, and B. J. Mohd, “Analyzing cyber-physical threats on robotic platforms,” Sensors (Switzerland), vol. 18, no. 5, May 2018, doi: 10.3390/s18051643.

[5] T. A. Zimmerman, “Metrics and key performance indicators for robotic cybersecurity performance analysis,” Gaithersburg, MD, Apr. 2017. doi: 10.6028/NIST.IR.8177.

[6] G. Lacava et al., "Cybsersecurity issues in robotics," J Wirel Mob Netw Ubiquitous Comput Dependable Appl, vol. 12, no. 3, pp. 1–28, Sep. 2021, doi: 10.22667/JOWUA.2021.09.30.001.
[7] L. O. Nweke and S. D. Wolthusen, "A review of asset-centric threat modelling approaches," International Journal of Advanced Computer Science and Applications, no. 2, pp. 1–6, 2020, doi: 10.14569/ijacsa.2020.0110201.
[8] S. P. Rao, H. Y. Chen, and T. Aura, "Threat modeling framework for mobile communication systems," Comput Secur, vol. 125, Feb. 2023, doi: 10.1016/j.cose.2022.103047.
[9] S. Krishnan, "A Hybrid Approach to Threat Modelling A Hybrid Approach to Threat Modelling A Hybrid Approach to Threat Modelling," 2017, doi: 10.13140/RG.2.2.33303.88486.
[10] F. Valenza, E. Karafili, R. V. Steiner, and E. C. Lupu, "A Hybrid Threat Model for Smart Systems," IEEE Trans Dependable Secure Comput, vol. 20, no. 5, pp. 4403–4417, Sep. 2023, doi: 10.1109/TDSC.2022.3213577.
[11] H. Omotunde and R. Ibrahim, "A Hybrid Threat Model for Software Security Requirement Specification," ICISS 2016 - 2016 International Conference on Information Science and Security, Mar. 2017, doi: 10.1109/ICISSEC.2016.7885836.
[12] "A Hybrid Threat Modeling Method." Accessed: Nov. 17, 2024. [Online]. Available: https://insights.sei.cmu.edu/library/a-hybrid-threat-modeling-method/
[13] M. Hamad and V. Prevelakis, "SAVTA: A Hybrid Vehicular Threat Model: Overview and Case Study," Information 2020, Vol. 11, Page 273, vol. 11, no. 5, p. 273, May 2020, doi: 10.3390/INFO11050273.
[14] R. Davis and O. F. Keskin, "Cyber Threat Modeling for Water and Wastewater Systems: Contextualizing STRIDE and DREAD with the Current Cyber Threat Landscape," 2024 Systems and Information Engineering Design Symposium, SIEDS 2024, pp. 301–306, 2024, doi: 10.1109/SIEDS61124.2024.10534706.
[15] N. Shevchenko, T. A. Chick, P. O'riordan, T. P. Scanlon, and C. Woody, "THREAT MODELING: A SUMMARY OF AVAILABLE METHODS," 2018.
[16] Z. Abuabed, A. Alsadeh, and A. Taweel, "STRIDE threat model-based framework for assessing the vulnerabilities of modern vehicles," Comput Secur, vol. 133, p. 103391, Oct. 2023, doi: 10.1016/J.COSE.2023.103391.
[17] L. O. Nweke and S. D. Wolthusen, "A review of asset-centric threat modelling approaches," International Journal of Advanced Computer Science and Applications, no. 2, pp. 1–6, 2020, doi: 10.14569/ijacsa.2020.0110201.
[18] A. M. Konsta, A. Lluch Lafuente, B. Spiga, and N. Dragoni, "Survey: Automatic generation of attack trees and attack graphs," Comput Secur, vol. 137, p. 103602, Feb. 2024, doi: 10.1016/J.COSE.2023.103602.