CONVERGING THREAT MODELING IN SMART FIREFIGHTING SYSTEMS

Dr. Rajesh Kumar Tiwari

ABSTRACT

This paper delves into security challenges within industrial automation technologies, particularly the realm of the Industrial Internet of Things (IIoT). Despite enhancing efficiency, IIoT introduces notable security risks, especially in smart cyber-physical systems (CPS). The study employs a smart firefighting use case, utilizing the MITRE ATT&CK matrix, and proposes a threat modeling framework for systematic risk analysis. Integrating system requirement collection (SRC) for asset information, the study maps the threat list onto NIST security and privacy controls. This demonstrates the applicability of these controls for mitigating security risks in smart firefighting systems, offering valuable insights for securing critical cyber-physical systems in specific use cases.

Index Terms *Threat modeling, Smart industrial system, Cyber–Physical System (CPS), Smart firefighting system, NIST controls, IoT, IIoT.*

Reference *to this paper should be made as follows**:** Rajesh Kumar Tiwari, (2023), "Converging Threat Modeling In Smart Firefighting Systems: Harmonizing Mitre Att&Ck Matrix With Nist Security Controls" Int. J. Electronics Engineering and Applications, Vol. 11, Issue I, pp. 21-30.*

Biographical notes:

Dr. Rajesh Kumar Tiwari *is Professor and Principal of R.V.S. College of Engineering and Technology,Jamshedpur, Jharkhand. He has completed his PhD form BIT Mesra Ranchi. His research interest includes Data Security, Cloud Computing, Machine Learning and Database Management System. He has Published more than fifty research papers in reputed International Journals.*

1. INTRODUCTION

This research delves into the security challenges inherent in Cyber-Physical Systems (CPS), particularly within the realm of intelligent industrial applications such as smart grids, factories, cities, and homes. CPS, which amalgamates computation with physical elements, presents an innovative approach to real-world device management and Internet of Things (IoT) operations. Despite its numerous advantages, CPS faces heightened vulnerability to a spectrum of cyber and physical security threats, a concern that is further exacerbated by the widespread adoption of the Internet of Things.

The study accentuates the surge in cyberattacks specifically targeting smart CPS, emphasizing the critical importance of implementing robust cybersecurity measures, especially in critical infrastructure sectors. The ongoing COVID-19 pandemic has magnified these concerns, as there has been a notable increase in cyber threats against intelligent industrial systems during this period. This underscores the urgency for the implementation of comprehensive cybersecurity measures to safeguard critical infrastructure from potential disruptions caused by malicious activities.

To address these security challenges, the research advocates for a multi-faceted approach, incorporating measures such as access controls, encryption, and intrusion detection systems. Access controls are essential for restricting unauthorized access to sensitive systems and data, while encryption ensures the confidentiality and integrity of communication within the CPS. Intrusion detection systems play a crucial role in identifying and responding to potential security breaches promptly.

The study zooms in on a specific use case within the domain of intelligent industrial applications: a smart firefighting CPS. By employing the MITRE ATT&CK matrix as a threat modeling framework, the research systematically identifies potential threats that could compromise the security of the smart firefighting CPS. These threats are then meticulously linked to the National Institute of Standards and Technology (NIST) security controls, proposing mitigation tactics to address each identified threat. This approach provides a structured and comprehensive methodology for securing the smart firefighting CPS against a diverse range of cyber threats.

2. LITERATURE SURVEY

The paper explores the fundamental principles of the CIA triad—Confidentiality, Integrity, and Availability—as a robust framework for establishing information security policies within organizations. Recognizing the importance of proactive security measures, the paper underscores the significance of threat modeling during the early phases of system design and operations to identify potential threats comprehensively.

Various existing threat modeling techniques, such as STRIDE and PASTA, are succinctly outlined to provide a comprehensive understanding of their applications in assessing threats to systems, processes, and human resources. By utilizing these techniques, organizations can systematically identify and address potential vulnerabilities, thereby bolstering their overall cybersecurity posture.

Shifting focus to the security challenges posed by smart Cyber-Physical Systems (CPS), the paper delves into notable cyberattacks, including Stuxnet, Mirai, Triton, BlueKeep, and SolarWinds. These examples illustrate the diverse dangers and vulnerabilities that smart CPS can face, emphasizing the need for robust security measures to safeguard against potential threats.

The importance of network segmentation, access control, and regular patching is emphasized as critical security measures for smart CPS. These measures aim to mitigate risks associated with

unauthorized access, data breaches, and exploitation of vulnerabilities, ensuring the confidentiality, integrity, and availability of critical systems.

The paper extends its examination to threat modeling frameworks applied to specific domains, including smart cities, cyber-physical systems, smart grids, homes, and farming. By tailoring threat modeling to the unique characteristics of each domain, organizations can develop targeted strategies to address specific threats and vulnerabilities relevant to their context.

Introducing a novel threat modeling approach for a smart firefighting CPS, the paper leverages NIST security and privacy controls. This innovative approach aims to identify vulnerabilities, threats, and potential attack vectors specific to smart firefighting CPS. By utilizing NIST controls, the research provides a structured framework for developing mitigation strategies, enhancing the overall security and resilience of smart firefighting CPS.

3. SYSTEM MODEL

The research study provides a comprehensive exploration of a smart firefighting system, dissecting its various components into services, networking, and sensor elements. The key aspects discussed across different sections of the study shed light on the intricacies of leveraging Information and Communication Technologies (ICT) to enhance firefighting capabilities, with a specific focus on the roles of firefighters, the integration of IoT technologies, sensor deployment, software applications, communication and networking technologies, and the overarching overview of the smart firefighting system.

1. Services for Firefighters and IoT Technologies (Section 3.1):

In this section, the study details the services crucial for firefighting teams, emphasizing the integration of IoT technologies. Firefighters benefit from real-time data, communication tools, and information-sharing platforms that enhance situational awareness, coordination, and decision-making during emergency incidents.

2. IoT Sensors for Firefighters (Section 3.2):

The study elaborates on the IoT sensors used by firefighters, highlighting their diverse functionalities. Thermal imaging cameras, gas dosimeters, and other sensors are deployed to provide critical information about the environment, enabling firefighters to navigate and respond effectively in hazardous conditions.

3. Integration of Sensors on Firefighter Suit (Section 3.3):

This section describes the seamless integration of sensors into firefighter suits, ensuring that these devices become an integral part of personal protective equipment (PPE). The connectivity with diverse technologies allows for real-time monitoring of vital parameters and environmental conditions.

4. Software Applications, Databases, and Building Systems (Section 3.4):

The focus shifts to software applications, databases, and building systems within the firefighting context. Predictive and analytical models are employed to anticipate fire behavior and optimize response strategies. These tools are crucial for incident commanders to make informed decisions during emergencies.

5. Communication and Networking Technologies (Section 3.5):

In-depth discussions on communication and networking technologies underscore their critical role in facilitating seamless connectivity during emergency response. The creation of a temporary wireless

network connecting personnel and systems enhances coordination and information sharing. Parallels with networking systems employed in autonomous cars highlight the sophistication of the deployed technologies.

6. Smart Firefighting System Overview:

The overall system overview emphasizes the utilization of information, communication, sensor, and simulation technologies. Data integration from databases and sensor networks allows for processing, analysis, and prediction, enabling informed decision-making by leveraging the collected information.

7. Networking System and High-Speed Vehicle Networking (Section 3.5):

The study delves into the creation of a temporary wireless network, drawing parallels with high-speed vehicle networking systems. This innovative approach enhances the agility and responsiveness of the firefighting system, reflecting advancements seen in smart transportation technologies.

8. Sensor Deployment and Information Transmission (Section 3.5):

Diverse sensor technologies, including thermal imaging cameras and gas dosimeters, are deployed strategically. Real-time transmission of critical information to the incident commander ensures swift decision-making, enhancing the overall effectiveness of firefighting operations.

9. Smart Emergency Response Systems (SERS) (Section 3.5):

The study emphasizes the pivotal role of Smart Emergency Response Systems (SERS) in enhancing the capabilities of emergency responders. The combination of communication networks, decision support systems, and advanced sensor technologies forms a holistic approach to optimizing emergency response.

10. Uses of Model Outputs and Predictions (Section 3.5):

Practical applications of model outputs, including real-time 3D visualization, are highlighted. Decision support roles in evacuation planning and patient care underscore the versatility of the smart firefighting system in various emergency scenarios.

11. Roles and Duties of Firefighters (Section 3.1):

An overview of firefighter roles in various teams is provided, with a special focus on the crucial role of the incident commander (IC). This section emphasizes the collaboration and coordination required among team members for effective emergency response.

12. Sensor Technology (Section 3.2):

In-depth discussions on diverse sensor types used in firefighting operations provide insights into the technological advancements aimed at enhancing situational awareness and safety for firefighters. Sensors are deployed in both personal protective equipment (PPE) and carried by firefighters.

13. Integration of Sensors with Analytical Tools (Section 3.3):

The importance of integrating sensor data with analytical tools is emphasized, showcasing the significance of combining real-time sensor information with analytical capabilities. The implementation of standardized grammar semantics and networking protocols ensures seamless integration.

14. Software Application for Incident Commander (Section 3.4):

A detailed description of the software application tailored for the incident commander's use is provided. This application allows access to crucial information from analytical tools, databases, and sensor networks, empowering the incident commander to make informed decisions in real-time.

15. Model-Based Predictions and Decision-Making (Section 3.5):

The study highlights the utilization of computer simulations for predicting fire-related scenarios. The integration of incident storage databases, Ebox access, and machine learning algorithms (Firecast) demonstrates the sophisticated approach to model-based predictions and decision-making in firefighting operations.

This study underscores the imperative of fortifying smart firefighting systems against cyber threats and potential vulnerabilities. The interconnected nature of IoT devices and their pivotal role in emergency response necessitate a robust security framework.

4. METHODOLOGY

The proposed framework for threat modeling in a smart industrial system, with a focus on the smart firefighting CPS as a use case, represents a comprehensive and systematic approach to identifying, analyzing, and mitigating potential threats. The integration of the MITRE ATT&CK matrix, System Requirement Collection (SRC), and NIST controls provides a structured methodology that addresses various layers of security concerns, ensuring the resilience of smart industrial systems.

1. MITRE ATT&CK Matrix Analysis (Section 4.1):

The framework begins with an in-depth analysis of the MITRE ATT&CK matrix, a robust knowledge base for understanding adversarial behaviors. The matrix is organized into three major categories: ATT&CK for enterprise, ATT&CK for mobile, and pre-ATT&CK. Tactics and techniques are systematically laid out in rows and columns, serving as a structured framework for analyzing potential cyber threats. Mitigations associated with specific methods or techniques become key security concepts for thwarting adversarial actions effectively. This section sets the foundation for a comprehensive understanding of potential attacks in the smart firefighting CPS.

2. System Requirement Collection (SRC) (Section 4.2):

The SRC is a critical component of the framework, configuring vulnerabilities by identifying security goals, assets, sensor data, secure network communication, endpoint hardware, and potential threats. This mechanism ensures a holistic and comprehensive understanding of the smart firefighting CPS, mapping out the intricacies of the system's components and their interdependencies. By delineating security goals and identifying potential vulnerabilities, the SRC lays the groundwork for a robust threat modeling process.

3. Threat Identification (Section 4.3):

Building upon the SRC, this section delves into the identification of potential threats. The SRC identifies security goals, assets, sensor data, network communication, and endpoint hardware, providing a rich dataset for threat analysis. Threats are categorized into software, network, and physical layers, allowing for a multi-faceted evaluation of potential risks. The MITRE ATT&CK matrix guides the identification of specific attacks that could target smart firefighting components. This step ensures a comprehensive understanding of the threat landscape, enabling proactive measures to be taken.

4. Mapping of NIST Controls (Section 4.4):

This crucial section involves the mapping of identified threats from the MITRE ATT&CK matrix onto NIST security and privacy controls. Each threat is carefully examined to find relevant NIST controls, and mitigations for each technique or sub-technique are explored. The review, analysis, and tailoring of candidate security controls ensure that they are aligned with specific attacks targeting the smart firefighting CPS. This mapping provides a bridge between the threat identification phase and the implementation of actionable security measures.

5. Threat Mitigation Using NIST Control (Section 4.5):

The final step involves implementing the identified NIST controls to mitigate the threats identified in the smart firefighting CPS. Once threats are mapped to specific NIST controls, their implementation becomes a proactive defense mechanism. These controls ensure continuous defense against various risks, including hostile assaults, human errors, natural disasters, and privacy issues. The adaptable and scalable nature of NIST controls is highlighted, forming a crucial part of an organization-wide risk management strategy.

Integrated Framework Overview:

The integrated framework seamlessly combines the strengths of MITRE ATT&CK, SRC, and NIST controls, offering a holistic approach to threat modeling. The MITRE ATT&CK matrix provides a detailed understanding of potential adversarial actions, while the SRC captures the nuances of the smart firefighting CPS. Mapping threats to NIST controls bridges the gap between theoretical threat identification and actionable security measures.

This framework emphasizes the implementation of NIST controls as a key measure for ongoing defense and effective risk management. NIST controls offer a standardized and widely recognized set of security measures, ensuring that the smart industrial system is fortified against a spectrum of potential threats. The scalability and adaptability of these controls make them well-suited for the dynamic and evolving nature of smart industrial environments.

5. RESULTS AND EVALUATION

5.1. System Requirements Collection (SRC):

5.1.1. Security Goals in Smart Firefighting CPS:

- Confidentiality: Protecting classified and personal information from unauthorized disclosure is paramount in a smart firefighting CPS. This ensures that sensitive data, such as building layouts or personal details, remains inaccessible to unauthorized entities.

- Integrity: Ensuring the accuracy of data is critical to prevent misleading results during firefighting operations. Data integrity safeguards against the manipulation of information that could compromise the effectiveness of response efforts.

- Authorization: Implementing strong authorization systems for resource access guarantees that only authorized personnel can access specific functionalities or data. This safeguards against unauthorized access to critical systems.

- Role-based Access Control: Specifying distinct functions and access levels for authorized users ensures that individuals have access only to the information and functionalities relevant to their roles, minimizing the risk of unauthorized actions.

- Robustness: Including backup systems is essential for prompt reactions to breakdowns. Robustness ensures system resilience, minimizing downtime and enabling continuous functionality during emergencies.

- Availability of Data: Ensuring resilient and responsive access to data at all times is crucial for timely decision-making during firefighting operations. Availability guarantees that critical information is accessible when needed.

- Contractual Integrity: Following contractual definitions for third-party vendors establishes a framework for maintaining the integrity of data and services provided by external entities, contributing to a secure collaborative environment.

5.1.2. Assets in Smart Firefighting CPS:

- Categorized into software, network, and physical layers: The categorization of assets into these layers provides a structured approach to understanding and managing the various components of the smart firefighting CPS.

- Includes various software, hardware, and network components: Assets encompass a wide range of elements detailed in Section 3 of the system model. These include software applications, hardware devices, and network infrastructure critical to firefighting operations.

5.1.3. Sensors Data in Smart Firefighting CPS:

- Sensors categorized as personal protective equipment, mobility, and stationary sensors: Understanding the different categories of sensors aids in tailoring security measures to the specific characteristics and functions of each sensor type.

- Sensor communication methods include IEEE 802.11-based wireless communication: Acknowledging the communication methods ensures that security measures are aligned with the wireless protocols used, addressing potential vulnerabilities associated with wireless communication.

5.1.4. Secure Network Communication in Smart Firefighting CPS:

- Discovery of secure communication mechanisms, including protocols like DTLS, TLS, IPsec, and HIP-DEX: Identifying and implementing secure communication mechanisms using established protocols such as DTLS, TLS, IPsec, and HIP-DEX enhances the overall security of network communication.

- Emphasis on wireless communication and authentication in the network: Prioritizing wireless communication security and robust authentication mechanisms ensures the integrity and confidentiality of data transmitted over the network.

5.1.5. Endpoint Hardware in Smart Firefighting CPS:

- Includes sensors, firefighter personal protective equipment (PPE), IC applications software, and wireless devices: Detailing the endpoint hardware provides a comprehensive view of the physical components that form the foundation of the smart firefighting CPS.

- Detailed structure provided in Section 3 of the system model: Referencing Section 3 of the system model ensures a clear understanding of the specific hardware components involved in the smart firefighting CPS.

5.2. Threats Identification in Smart Firefighting CPS:

- Holistic overview provided by SRC on application, physical, and network layers: The SRC's comprehensive overview ensures that threats are identified across all layers of the smart firefighting CPS, providing a holistic understanding of potential risks.

- MITRE ATT&CK analysis used to generate a threat list (Tables 1-3): Leveraging the MITRE ATT&CK framework for analysis aids in generating a detailed threat list, categorizing potential adversarial behaviors across different attack vectors.

5.3. Mapping of NIST Controls for Smart Firefighting CPS:

- Utilizes the project of the Center for Threat-Informed Defense (CTID) for mapping threats to NIST security and privacy controls 800-53 rev 5: The utilization of the CTID project ensures a standardized and recognized mapping of identified threats to specific NIST controls, facilitating a structured and consistent approach to threat mitigation.

5.4. Threat Mitigation in Smart Firefighting CPS:

- Strategic mechanism used to map threat list to NIST controls: The strategic mapping of the threat list to NIST controls provides a clear roadmap for implementing targeted security measures against identified threats.

- Implementation of mapped controls mitigates specific threats, safeguarding organizational operations and assets: The implementation of NIST controls acts as a proactive defense mechanism, mitigating specific threats and safeguarding the operational integrity of the smart firefighting CPS.

- Security controls are adaptable, customizable, and form part of an organization-wide risk management strategy: The adaptability and customizability of security controls ensure that they can be tailored to the specific needs of the smart firefighting CPS. Furthermore, their inclusion in an organization-wide risk management strategy emphasizes their role in fostering a comprehensive security posture.

In-depth Examples for Threat Mitigation:

- T1040-network sniffing and T1110-brute force: These examples illustrate specific threats identified in the smart firefighting CPS, showcasing how NIST controls effectively address each threat. Multiple controls mapped against each attack highlight the layered approach to security, providing advanced protection.

6. CONCLUSION

In the dynamic landscape of cybersecurity, particularly within the smart industrial sector, the ability to proactively address and mitigate evolving cyber threats is of paramount importance. This study presents a robust approach to tackle this challenge, focusing on the detection and mitigation of potential dangers in smart cyber–physical systems (CPS). Using a smart firefighting CPS as an illustrative example, the study employs a sophisticated threat-modeling technique that combines the MITRE ATT&CK matrix for structured attack analysis and the System Requirement Collection (SRC) for gathering generic asset information.

This synergistic approach results in the creation of a comprehensive threat list that encompasses potential adversarial behaviors across different attack vectors. The identified threats are then systematically mapped onto the National Institute of Standards and Technology (NIST) security and

privacy controls through the Center for Threat-Informed Defense (CTID) project. This mapping ensures a standardized and recognized framework for implementing security controls tailored to the specific threats identified in the smart firefighting CPS.

The proposed framework offers both theoretical insights and practical implications, making it a valuable resource for fortifying the security posture of smart cyber–physical systems. Its applicability extends beyond the realm of smart firefighting CPS to secure various smart industrial systems. By providing security practitioners and professionals with a structured methodology to address cyber threats, the framework contributes to enhancing the resilience of network communication in smart industrial environments. This study thus stands as a significant contribution to the field, offering a proactive and comprehensive approach to cybersecurity that aligns with the evolving nature of threats in the smart industrial sector.

REFERENCES

[1] O.M. Butt, M. Zulqarnain, T.M. Butt, Recent advancement in smart grid technology: Future prospects in the electrical power network, Ain Shams Eng. J. 12 (1) (2021) 687–695.

[2] R.K. Radha, Flexible smart home design: Case study to design future smart home prototypes, Ain Shams Eng. J. 13 (1) (2022) 101513.

[3] OpenID connect basic client implementer's guide 1.0 - draft 42, 2022, https://openid.net/specs/openid-connect-basic-1_0.html.

[4] The OAuth 2.0 authorization framework, 2022, https://datatracker.ietf.org/doc/html/rfc6749.

[5] C. Keßler, R.T.A. de Groot, Trust as a proxy measure for the quality of volunteered geographic information in the case of OpenStreetMap, in: D. Vandenbroucke, B. Bucher, J. Crompvoets (Eds.), Geographic Information Science At the Heart of Europe, Springer International Publishing, Cham, 2013, pp. 21–37.

[6] J. Byabazaire, G. O'Hare, D. Delaney, Using trust as a measure to derive data quality in data shared IoT deployments, in: 2020 29th International Conference on Computer Communications and Networks, ICCCN, 2020, pp. 1–9.

[7] E. Manor, S. Greenberg, Custom hardware inference accelerator for TensorFlow lite for microcontrollers, IEEE Access 10 (2022) 73484–73493.

[8] M. Giordano, N. Baumann, M. Crabolu, R. Fischer, G. Bellusci, M. Magno, Design and performance evaluation of an ultra low-power smart IoT device with embedded TinyML for asset activity monitoring, IEEE Trans. Instrum. Meas. (2022).

[9] Naeem Iqbal, Do Hyeun Kim, et al., Iot task management mechanism based on predictive optimization for efficient energy consumption in smart residential buildings, Energy Build. 257 (2022) 111762.

[10] Imran Jamal, Shabir Ahmad, DoHyeun Kim, Design and implementation of thermal comfort system based on tasks allocation mechanism in smart homes, Sustainability 11 (2019) http://dx.doi.org/10.3390/su11205849.

[11] A. Djenna, D.E. Saïdouni, Cyber attacks classification in IoT-based-healthcare infrastructure, in: 2018 2nd Cyber Security in Networking Conference, CSNet, IEEE, 2018, pp. 1–4.

[12] R. Heartfield, G. Loukas, S. Budimir, A. Bezemskij, J.R. Fontaine, A. Filippoupolitis, E. Roesch, A taxonomy of cyber-physical threats and impact in the smart home, Comput. Secur. 78 (2018) 398–428, Publisher: Elsevier.

[13] T. Domínguez-Bolaño, O. Campos, V. Barral, C.J. Escudero, J.A. García-Naya, An overview of IoT architectures, technologies, and existing open-source projects, Internet Things 20 (2022) 100626, http://dx.doi.org/10.1016/j.iot.2022.100626.

[14] L. Almonte, I. Cantador, E. Guerra, J. de Lara, Towards automating the construction of recommender systems for low-code development platforms, in: Proceedings of the 23rd ACM/IEEE International Conference on Model Driven Engineering Languages and Systems: Companion Proceedings, MODELS '20, Association for Computing Machinery, New York, NY, USA, 2020, pp. 1–10, http://dx.doi.org/10.1145/3417990.3420200.

[15] G. Escalas Rodríguez, Diseño Y Desarrollo De Un Prototipo De Riego Automático Controlado Con Raspberry Pi Y Arduino (B.S. thesis), Universitat Politècnica de Catalunya, 2015.

[16] J. Daly, M. Burchett, F. Torpy, Plants in the Classroom Can Improve Student Performance, National Interior Plantscape Association, 2010, pp. 1–9.