THE ROLE OF CYBER THREAT MODELING IN ENSURING INFORMATION SECURITY IN A DIGITAL ENGINEERING ENVIRONMENT.

Omonov Odiljon Mirzaulug'bek o'g'li
Sharda university uzbekistan faculty of engineering & technology (cybersecurity direction) mtech-2501 (2 courses)

Abstract. *The increasing digitization of engineering environments has heightened exposure to complex and evolving cyber threats. Digital engineering systems, including industrial control systems, cloud-based platforms, and Internet of Things infrastructures, require proactive security strategies beyond traditional reactive measures. Cyber threat modeling is a structured methodology for identifying, analyzing, and prioritizing potential threats, enabling early implementation of effective security controls. This study examines the role of threat modeling in digital engineering environments and demonstrates how systematic threat assessment enhances the resilience and security of critical engineering infrastructures. The findings emphasize that integrating threat modeling into cybersecurity strategies improves risk management, reduces vulnerabilities, and strengthens overall system protection.*

Keywords: *Cybersecurity, Threat Modeling, Digital Engineering, Information Security, Risk Assessment, Engineering Systems.*

Introduction

Digital transformation in engineering systems has brought significant efficiency and automation advantages but has also increased the risk of cyberattacks [1, 2]. Industrial control systems, smart manufacturing, cloud platforms, and IoT infrastructures are interconnected and exchange large volumes of data, making them attractive targets for malicious actors [3]. Traditional security mechanisms, primarily based on predefined rules and signature detection, are insufficient to address sophisticated threats, such as zero-day attacks, polymorphic malware, and advanced persistent threats [4].

Cyber threat modeling provides a proactive approach to information security. It involves systematically analyzing system components, data flows, and potential attack vectors to identify vulnerabilities and prioritize risks [5]. By anticipating threats during system design and deployment, organizations can implement effective preventive measures, enhance resilience, and reduce potential economic and operational consequences [6]. This study focuses on the significance of cyber threat modeling for ensuring information security in digital engineering environments and examines its practical application in enhancing system protection.

Main Part

Cyber threat modeling typically follows structured methodologies such as STRIDE, PASTA, and Attack Trees [7, 8]. These frameworks enable the systematic identification of threats based on system architecture, data sensitivity, and attack likelihood. For example,

STRIDE categorizes threats into Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege, providing a comprehensive framework for evaluating vulnerabilities [9]. PASTA (Process for Attack Simulation and Threat Analysis) focuses on risk-centric modeling, integrating business impact, threat intelligence, and attack simulations [10].

In digital engineering environments, threat modeling involves several key steps:

1. **System Characterization** – Mapping system components, interfaces, and data flows.
2. **Threat Identification** – Recognizing potential threats based on known attack patterns and emerging threats.
3. **Vulnerability Assessment** – Evaluating system weaknesses that could be exploited.
4. **Risk Analysis and Prioritization** – Estimating potential impacts and likelihood of attacks to focus resources on critical areas.
5. **Mitigation Planning** – Designing preventive and detective controls to reduce identified risks [11].

Application of threat modeling in engineering systems has been shown to reduce vulnerabilities, improve security awareness, and support compliance with international standards such as ISO/IEC 27001 [12]. By integrating modeling with continuous monitoring, organizations can dynamically adapt to evolving cyber threats and improve overall resilience. Additionally, threat modeling facilitates collaboration between engineering, IT, and security teams, ensuring a holistic approach to information protection [13].

Conclusion

Cyber threat modeling plays a pivotal role in ensuring information security in digital engineering environments. Structured methodologies enable early identification of vulnerabilities, risk prioritization, and implementation of effective security measures. This proactive approach not only mitigates potential cyber threats but also enhances system resilience and operational continuity. Integrating threat modeling into cybersecurity strategies is essential for sustainable and secure operation of modern engineering systems. Future research should focus on automating threat modeling processes, improving predictive capabilities, and adapting methodologies for emerging engineering technologies such as Industry 4.0 and IoT-enabled infrastructures.

References

1. Russell S., Norvig P. *Artificial Intelligence: A Modern Approach*. – 4th ed. – New York: Pearson, 2021. – 1136 p.
2. Stallings W. *Cryptography and Network Security: Principles and Practice*. – 8th ed. – Boston: Pearson, 2023. – 864 p.
3. Conti M., Dehghantanha A., Franke K., Watson S. Internet of Things Security and Forensics: Challenges and Opportunities // *Future Generation Computer Systems*. – 2018. – Vol. 78. – P. 544–546.
4. Behl A., Behl K. *Cyberwar: The Next Threat to National Security and What to Do About It*. – Oxford: Oxford University Press, 2017. – 256 p.

5. Howard M., LeBlanc D. *Writing Secure Code*. – 2nd ed. – Redmond: Microsoft Press, 2003. – 720 p.

6. Chen T., Zhao J., Zhang Y. Cyber Threat Modeling for Industrial Control Systems // *Journal of Information Security and Applications*. – 2020. – Vol. 55. – Article 102595.

7. Shostack A. *Threat Modeling: Designing for Security*. – Hoboken: Wiley, 2014. – 336 p.

8. UcedaVelez T., Morana M. *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. – Waltham: Elsevier, 2015. – 320 p.

9. Microsoft. STRIDE Threat Model. – Microsoft Docs, 2023. Available at: https://learn.microsoft.com/en-us/security/engineering/stride

10. Open Web Application Security Project (OWASP). Threat Modeling. – 2022. Available at: https://owasp.org/www-community/Threat_Modeling

11. ISO/IEC 27001:2022. *Information Security Management Systems – Requirements*. – Geneva: ISO, 2022.

12. Kim G., Lee S., Kim S. A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection // *Expert Systems with Applications*. – 2014. – Vol. 41, No. 4. – P. 1690–1700.