American Journal Of Applied Science And Technology
(ISSN – 2771-2745)
VOLUME 04 ISSUE 10 Pages: 87-94
OCLC – 1121105677

Publisher: Oscar Publishing Services

Journal Website: https://theusajournals.com/index.php/ajast

Research Article

THREAT MODEL FOR PAYMENT SYSTEMS

Submission Date: October 15, 2024, Accepted Date: October 20, 2024,
Published Date: October 25, 2024
Crossref doi: https://doi.org/10.37547/ajast/Volume04Issue10-13

Agzamova Mohinabonu
PhD Student Of Tashkent University Of Information Technologies Named After Muhammad Al-Khwarizmi, Tashkent, Uzbekistan

ABSTRACT

Payment systems are the backbone of modern economies, and their security is a critical aspect of maintaining user trust and safeguarding financial data. In this context, the development of threat models plays a central role in ensuring the protection of these systems from attacks. One of the most effective methodologies for threat modeling is STRIDE, which helps to structure and systematize the analysis of risks and threats. By utilizing the STRIDE model and incorporating a customized threat model for payment systems, the security of authentication processes and transaction handling can be significantly enhanced.

KEYWORDS

Payment systems, threat modeling, STRIDE, authentication, data security, spoofing, tampering, information disclosure, denial of service, privilege escalation.

INTRODUCTION

Payment systems are the cornerstone of modern economies, enabling the secure transfer of funds and facilitating transactions across various sectors. With the rapid growth of digital and mobile payment platforms, the need for robust security measures has become more critical than ever. As these systems evolve, so do the methods of attack employed by cybercriminals, who seek to exploit vulnerabilities for financial gain. The increasing frequency of cyberattacks targeting payment systems poses a significant threat to both individual users and the global financial infrastructure [1].

This paper aims to explore the application of the STRIDE threat model in the context of payment systems, analyzing common vulnerabilities and proposing strategies to mitigate them. In addition to applying the STRIDE model, the paper introduces a detailed threat model specific to payment systems, highlighting the unique challenges associated with authentication, data management, and transaction processing. By understanding the nature of these threats and implementing multi-layered security measures, payment systems can enhance their defenses against a wide range of cyberattacks, ensuring the safety and integrity of financial transactions.

1. The STRIDE Model: core threats to payment systems

The STRIDE model (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) classifies potential threats and helps identify corresponding protective measures. Below is a breakdown of each threat in the context of payment systems (fig.1).

1.1 Spoofing (identity impersonation)

Spoofing involves a malicious actor impersonating a legitimate user to gain unauthorized access to a system or execute fraudulent transactions. An example is when an attacker intercepts a user's authentication session over an insecure network [2].

- Protection Measures: Multi-factor authentication (MFA), session data encryption, enhanced verification through cryptographic tokens.

1.2 Tampering (Data Manipulation)

Tampering occurs when data is altered during transmission or processing without authorization. In payment systems, this could involve modifying transaction amounts or recipient details [3].

- Protection Measures: Data encryption in transit, digital signatures to verify data integrity, routine database integrity checks.

1.3 Repudiation (Denial of Actions)

Repudiation happens when an individual denies performing a transaction or action, making it difficult to prove the authenticity of their involvement without proper logging mechanisms.

- Protection Measures: Reliable audit logs with immutable records, timestamps, digital signatures, and user activity tracking systems.

1.4 Information Disclosure (Data Breach)

Information disclosure involves the leakage of sensitive data, such as user information or credit card details, due to vulnerabilities in APIs or unprotected databases.

- Protection Measures: Data encryption at all levels, strict access control policies, regular security audits, and vulnerability assessments[4].

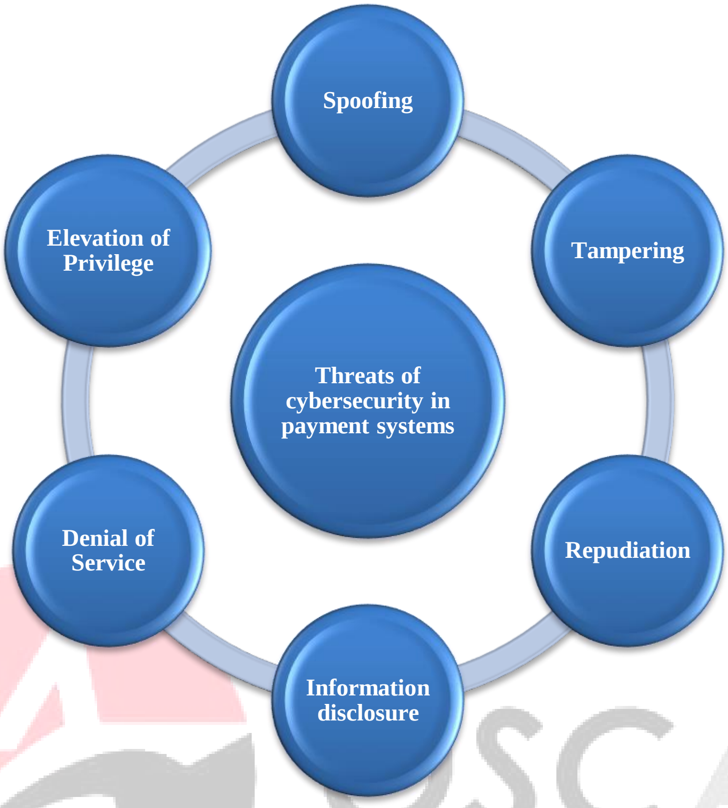

Figure 1. Threats of cybersecurity in payment systems

1.5 Denial of Service (DoS)

DoS attacks aim to overwhelm system resources, making the system unavailable to legitimate users. In payment systems, this could prevent the completion of transactions, leading to financial losses and reputational damage.

- Protection Measures: DDoS protection, request rate limiting, web application firewalls (WAF), and resource distribution for handling request surges [5].

1.6 Elevation of Privilege

Elevation of privilege occurs when an attacker gains access to system functions or data that they are not authorized to use. This could involve accessing confidential information or administrative functions within the payment system.

- Protection Measures: Principle of least privilege, role-based access control (RBAC), regular system vulnerability testing.

2. Proposed threat model for payment systems

In addition to applying the STRIDE model, the proposed threat model specifies the unique aspects of attacks related to authentication, access control, and data management processes. This model, depicted in Figure 2, outlines different threat states, from secure operation to specific malicious activities such as unauthorized access or manipulation of authentication data [6].

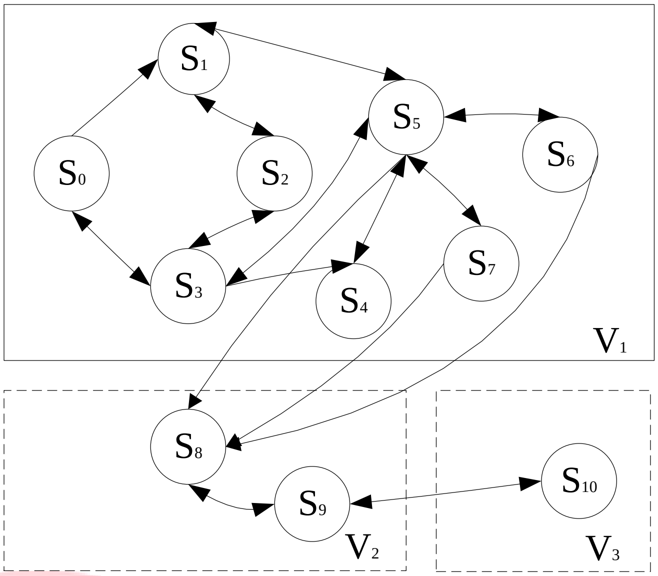

Figure 2. Proposed threat model for payment systems

2.1 Threat States

- S0 – Initial secure state of the authentication system where all processes are functioning correctly, and the system is protected from external attacks.

- S1 – Interaction with the authentication system begins the user verification process. Vulnerabilities related to authentication may arise at this stage.

- S2 – Unauthorized modification or copying of authentication data. Here, an attacker may manipulate credentials, such as passwords or access keys.

- S3 – Password cracking or breaching other authentication methods, including biometrics, leading to unauthorized access to the payment system.

- S4 – Theft of sensitive authentication data, which can be used for further attacks or sold on the black market.

- S5 – Unauthorized access and privilege escalation in the payment system, allowing the attacker to perform transactions or modify data on behalf of a legitimate user.

- S6 – Creation of illegitimate users in the system, giving attackers the ability to act through fake accounts.

- S7 – Introduction of malicious software or code into the authentication system, manipulating processes to gain illegal access.

- S8 – Disruption of the payment system's operation through a Denial of Service (DoS) attack.

- S9 – Maintaining unauthorized access by bypassing standard security measures, which may go unnoticed for extended periods.

- S10 – Hiding traces of the attack and ensuring continued access by erasing logs and creating backdoors for future intrusions.

2.2 Attack Stages

Threats can be divided into three main stages:

- V1 – Reconnaissance and Preparation:

The attacker conducts reconnaissance of the payment system's network, identifying key nodes and vulnerabilities. This may involve port scanning, analyzing active services, and studying the system structure to plan an intrusion.

- V2 – Attack Implementation:

The attacker executes the attack, exploiting vulnerabilities in the authentication system through methods such as phishing, social engineering, or exploiting technical vulnerabilities like API weaknesses.

- V3 – Access Maintenance and Trace Concealment:

The attacker takes steps to maintain unauthorized access to the system, which may include log wiping, obfuscation methods, and other measures to conceal their actions.

The final state is S10, where the attacker ensures a way to regain access to the system by leaving backdoors or other vulnerabilities [7].

2.3 External Factors Affecting the Threat Model

The threat model also considers external factors that may influence the likelihood of a successful attack. These include:

- Attacker Skill Level:

Attackers may possess advanced technical knowledge, using sophisticated tools to bypass security systems. Such tools may include network scanners, exploits, and specialized software products for analyzing payment systems.

- Social Engineering and Psychological Techniques:

Social engineering plays a significant role in gaining access to payment systems. By manipulating employees or users, an attacker can obtain access to accounts or critical information.

3. Components of payment systems and their vulnerabilities

Each payment system is composed of various components that are exposed to different types of threats. Below is an analysis of key system components and their potential vulnerabilities (Figure 3).

3.1 Authentication component

This is the core security element of the system, responsible for verifying user identities. Vulnerabilities in authentication can lead to spoofing and elevation of privilege attacks. Advanced authentication methods such as neural networks and biometrics can significantly reduce the likelihood of such attacks [8].

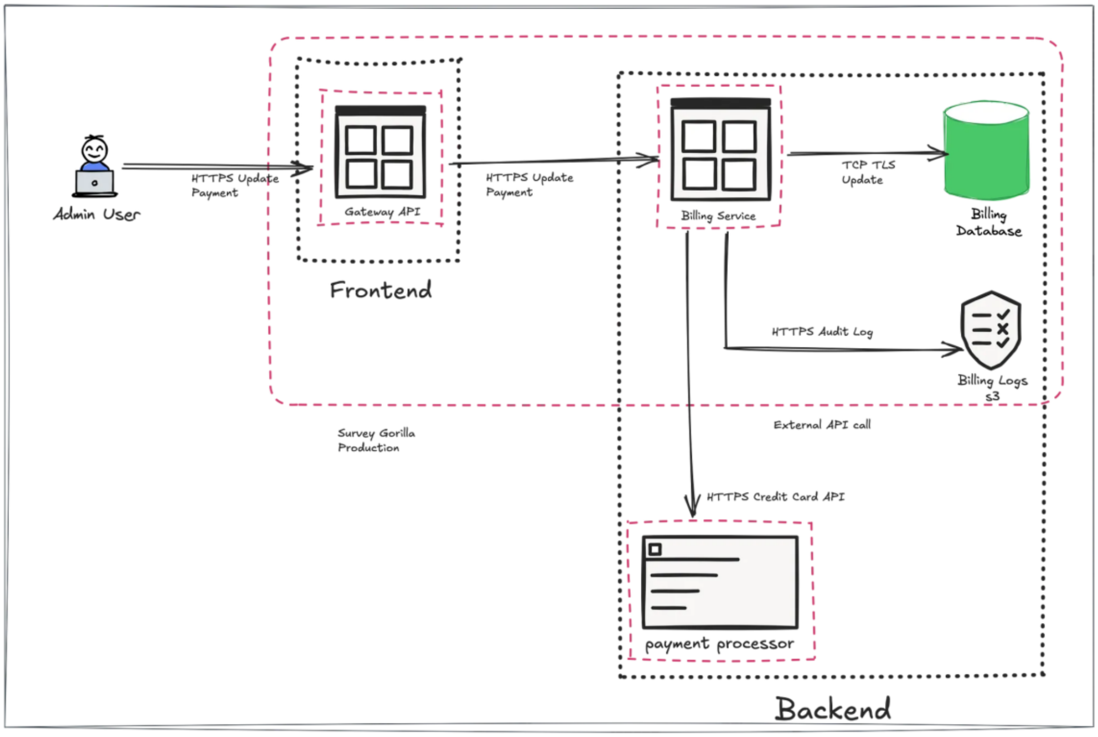

Figure 3. Key system components and their potential vulnerabilities

3.2 Payment gateway (Gateway API)

This component processes payment requests. Vulnerabilities may allow attackers to manipulate transaction data (tampering) or overload the system through DoS attacks [9].

3.3 Billing database

The billing database contains sensitive information such as credit card data, making it a target for information disclosure or tampering attacks. Encryption and strict access control measures are critical for protection.

3.4 Transaction logs

Transaction logs are essential for auditing and investigating incidents. Vulnerabilities in logs may lead to repudiation if attackers can alter or delete records.

3.5 Access management system

This system governs user rights and access control. Attacks on this component can lead to privilege escalation, granting unauthorized access to sensitive data and system resources.

4. Applying STRIDE to secure payment systems

The STRIDE model provides a structured approach to protecting payment systems by identifying threats and developing measures to counteract each category. For example, to mitigate spoofing risks, multi-factor authentication and data encryption should be implemented. Similarly, to prevent data leakage (information disclosure), it is essential to encrypt data at all levels and regularly conduct vulnerability tests and configuration reviews [10-12].

5. Mathematical modeling of threat probability

The probability of a system threat state at any given time is described using a mathematical model that accounts for random changes in the system's state. The probability of a system being in a specific threat state, P_i (t), at time t is defined as:

$$P_i(t) = P(S(t) = s_i)$$

Where $S(t)$ is the random state of the system at time t, and i=1, 2, 3,..,n represents the threat states. The transition probability between states is expressed as:

$$P_{ij}(t) = P\big(S(k) = s_j \big| S\,(k-1) = s_j\big)$$

Using the total probability formula and transitioning from step (k-1) to step k, the unconditional probability of the system being in a specific threat state at step k is calculated as:

$P_j(k) = \sum_{i=1}^{n} P_i(k-1)P_{il}$Using the total probability formula and transitioning from step (k-1) to step k, the unconditional probability of the system being in a specific threat state at step k is calculated as:

P_j (k)=∑_(i=1)^n▒〖P_i (k-1)P_il 〗

For an effective defense against a stream of attacks with such intensity, the system must utilize neural network methods for timely threat classification and identification [13].

CONCLUSION

The development and application of threat models for payment systems, such as the STRIDE model, allow for effective identification and classification of threats across all levels of the system, including authentication processes and access management. The incorporation of multi-layered security systems such as encryption, data integrity controls, and access control policies helps minimize risks and improve overall system resilience against attacks.

By systematically addressing each threat and implementing tailored security measures, payment systems can maintain high levels of security, protecting users' financial data and maintaining trust in an ever-evolving cyber threat landscape.

REFERENCES

1. Chenqian Yan, Yuge Zhang, Quanlu Zhang, Yaming Yang, Xinyang Jiang, Yuqing Yang, Baoyuan Wang. Privacy-preserving Online AutoML for Domain-Specific Face Detection. URL: https://openaccess.thecvf.com/content/CVPR2022/papers/Yan_Privacy-Preserving_Online_AutoML_for_Domain-Specific_Face_Detection_CVPR_2022_paper.pdf
2. Yang Liu, Fei Wang, Jiankang Deng, Zhipeng Zhou, Baigui Sun, Hao Li. MogFace: Towards a Deeper Appreciation on Face Detection. URL: https://openaccess.thecvf.com/content/CVPR2022/papers/Liu_MogFace_Towards_a_Deeper_Appreciation_on_Face_Detection_CVPR_2022_paper.pdf
3. Roberto Pecoraro, Valerio Basile, Viviana Bono, Sara Gallo. Local Multi-Head Channel Self-Attention for Facial Expression Recognition. URL: https://arxiv.org/pdf/2111.07224v2.pdf
4. Kai Wang, Xiaojiang Peng, Jianfei Yang, Debin Meng, Yu Qiao. Region Attention Networks for Pose and Occlusion Robust Facial Expression Recognition. URL: https://arxiv.org/pdf/1905.04075v2.pdf
5. Andrey V. Savchenko. Facial expression and attributes recognition based on multi-task learning of lightweight neural networks. URL:

https://ieeexplore.ieee.org/abstract/document/9582508/authors#authors

6. Minchul Kim, Anil K. Jain, Xiaoming Liu. AdaFace: Quality Adaptive Margin for Face Recognition. URL: https://arxiv.org/pdf/2204.00964.pdf
7. M.Sh.Agzamova, A.G.Nuriddionova., Sh.R.Gulomov: Settings firewalls to implement special filtering mode. XIII INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE «INTERNATIONAL SCIENTIFIC REVIEW OF THE PROBLEMS AND PROSPECTS OF MODERN SCIENCE AND EDUCATION» Chicago. USA 21-22 APRIL 2016. № 5 (15), p.34-39
8. M.Sh.Agzamova, A.G.Nuriddionova., A.Mamathanov: Mechanisms of provision of information security as a factor of economic security of small and private business. International Scientific and Practical Conference "WORLD SCIENCE" Proceedings of the IInd International Scientific and Practical Conference Dubai, UAE "Topical researches of the World Science № 7(11), Vol.1, July 2016 p.33-34.
9. Tashev, K., Durdona, I., Mokhinabonu, A./Comparative performance analysis the Aho-Corasick algorithm for developing a network detection system// 2022 International Conference on Information Science and Communications Technologies, ICISCT 2022
10. M.Sh.Agzamova, S.G.Svetunkov, A.G.Nuriddionova.: Big Data Simulation for Demand Forecasting in Retail Logistics. Algorithms and Solutions Based on Computer Technology. Lecture Notes in Networks and Systems, vol 387. Springer, Cham. Conference paper, First Online: 04 May 2022, pp 137–147 https://doi.org/10.1007/978-3-030-93872-7_12
11. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
12. Taigman, Y., Yang, M., Ranzato, M. A., & Wolf, L. (2014). DeepFace: Closing the Gap to Human-Level Performance in Face Verification. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 1701-1708).
13. Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 815-823).