Threat Modeling Report

Rohan Shah

9/18/2024

1. Executive Summary

This report provides an in-depth threat modeling exercise for MAISON’s digital-first hotel system. The analysis focuses on key assets such as customer data, the custom CRM, and smart IoT devices. Through the STRIDE framework, several threats and vulnerabilities were identified, including spoofing, tampering, and elevation of privilege attacks. Mitigation strategies are recommended, focusing on robust encryption, access controls, and monitoring to safeguard the system.

2. Introduction

System Description:

MAISON operates a cloud-based hotel system with no centralized headquarters, relying heavily on a custom CRM and smart devices to manage guest interactions, bookings, and services. The system includes components like a mobile app for booking, an AI concierge, and cloud servers hosting sensitive customer data.

Objective:

The primary objective of this threat modeling exercise is to identify potential threats across MAISON’s digital ecosystem, evaluate vulnerabilities, and recommend mitigation strategies to strengthen cybersecurity.

Scope:

This exercise covers the guest booking process, the digital check-in system, and third-party integrations such as rental car booking and the AI concierge.

3. Threats and Vulnerabilities

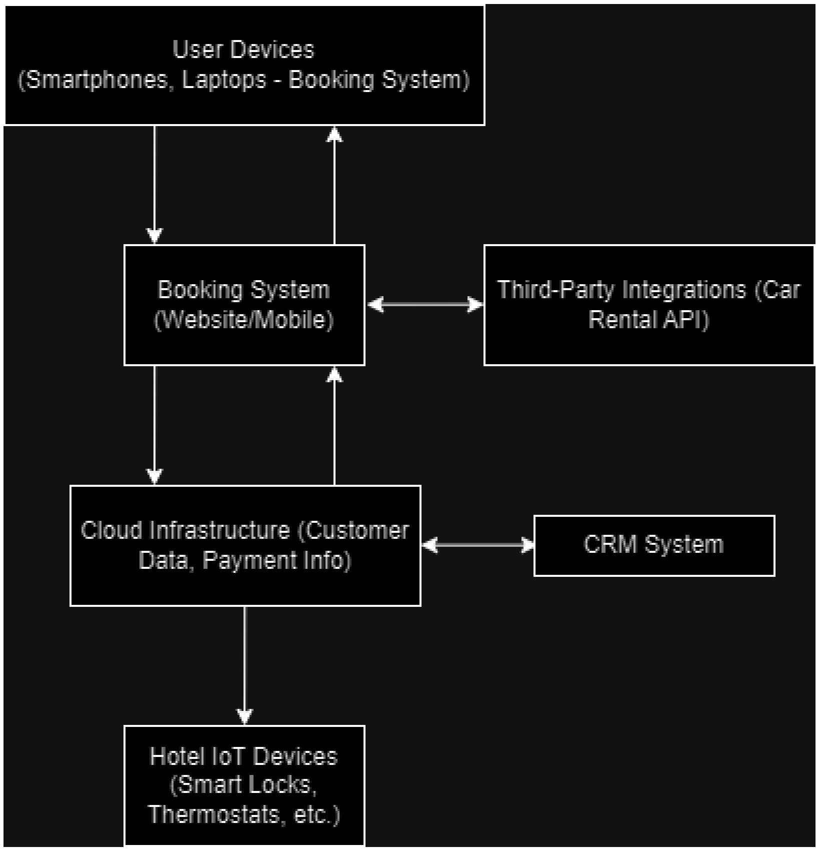
Using the **STRIDE** methodology, we identified the following threats and vulnerabilities:

Threat	Description	Impact	Likelihood	Mitigation

Spoofing	Attackers impersonate users to gain access to customer data	High	Medium	Multi-factor authentication (MFA), OAuth2
Tampering	Data manipulation during booking or check-in processes	High	Medium	Digital signatures, integrity checks
Repudiation	Users deny bookings or financial transactions	Moderate	Medium	Non-repudiation techniques using logs, digital signatures
Information Disclosure	Unauthorized access to customer data due to API vulnerabilities	Severe	Medium	Role-based access control, encryption at rest
Denial of Service (DoS)	Overloading the booking system to disrupt operations	Moderate	High	Rate limiting, firewalls
Elevation of Privilege	Gaining administrative access to modify room bookings or hotel systems	Critical	Medium	Least privilege principle, security monitoring

4. Threat Model

Visual Representation: A visual threat model diagram represents the interactions between the app, cloud infrastructure, and third-party services. This will highlight areas where threats, such as tampering and elevation of privilege, can be exploited.



Highlighted Risks:

- Spoofing: Impersonating user identity in the Booking System.

- Tampering: Modifying booking or payment data during transmission.

- Information Disclosure: Leaks through API vulnerabilities in 3rd-party integrations.

- Elevation of Privilege: Unauthorized admin access via CRM or Booking System.

Context:

- **Spoofing**: Guests may attempt to fake their identities by manipulating the booking system or forging digital credentials.
- **Tampering**: An attacker could modify booking data or interfere with communication between the app and the server.
- **Information Disclosure**: Guest data could be exposed through weak API protection, particularly during communication with external services like rental car companies.
- **Elevation of Privilege**: A hacker could exploit vulnerabilities in the CRM to gain access to privileged functions and modify bookings or access guest information.

5. Mitigation Strategies

Spoofing:

- Use **OAuth2.0** for secure API authentication.
- Implement **MFA** for critical operations such as check-ins, room access, and account management.

Tampering:

- Employ **message integrity checks** and **digital signatures** to detect any unauthorized changes to data.
- Ensure **TLS 1.3** is used for all communications to prevent tampering in transit.

Information Disclosure:

- **Encrypt sensitive data** at rest using AES-256.
- Implement **role-based access control (RBAC)** to limit who can access sensitive data.

Denial of Service (DoS):

- Set up **rate limiting** and **firewall rules** to prevent overwhelming the booking system.
- Use **load balancing** and **redundancy** in cloud infrastructure to handle peak loads.

Elevation of Privilege:

- Implement the **principle of least privilege (PoLP)** for all users and employees.
- Use **security monitoring** to log and detect any suspicious privilege escalation attempts.

6. Conclusion

The STRIDE threat modeling exercise revealed several potential vulnerabilities within MAISON’s digital-first hotel system. Key threats include spoofing, tampering, and elevation of privilege, all of which could lead to critical data breaches or disruptions in service. The recommended mitigation strategies—focusing on encryption, access control, and real-time monitoring—will reduce the likelihood and impact of these threats, thereby strengthening the overall security posture of MAISON.

7. References

- OWASP API Security Guidelines
- NIST Cybersecurity Framework
- Cloud Security Alliance (CSA) Best Practices