STRIDE Analysis Challenge for CycleSwift

Supporting materials for the O'Reilly training Threat Modeling Fundamentals - Debug Your Security Design through Whiteboard Hacking by Sebastien Deleersnyder, Toreon.

To learn more on threat modeling, visit https://www.toreon.com/threat-modeling-training/

Exercise Input:

Objective: Identify potential security threats to the CycleSwift E-Bike Rental App using the STRIDE methodology.

1. Spoofing Identity
    - **Challenge:** Consider the user registration and authentication process managed by Amazon Cognito. How could an attacker potentially spoof a user's identity to gain unauthorized access to the app? Consider the implications of weak authentication mechanisms or social engineering attacks.
2. Tampering with Data
    - **Challenge:** Analyze the real-time tracking of e-bike locations and availability, which relies on AWS IoT Core, Amazon Location Service, and Amazon DynamoDB. How might an attacker tamper with the e-bike data, such as location or availability status? What would be the potential impact of such tampering on users and the company.
3. Repudiation
    - **Challenge:** With regard to payment processing that involves AWS Lambda, API Gateway, and Amazon RDS/Aurora, identify how an attacker could perform actions without the ability to trace those actions back to them. How can the system ensure non-repudiation, so users or attackers cannot deny their transactions?
4. Information Disclosure
    - **Challenge:** Given the use of Amazon S3 for data storage in data analytics, explore how sensitive information, such as usage patterns or user data, might be unintentionally disclosed. Consider the consequences of such disclosures for users and city planners.
5. Denial of Service (DoS)
    - **Challenge:** Evaluate the potential for DoS attacks against the CycleSwift app's reservation functionality. Discuss how an attacker might attempt to overload or manipulate the e-bike reservation services and the impact on the CycleSwift availability.
6. Elevation of Privilege
    - **Challenge:** Considering the app's backend services and AWS environment, how might an attacker exploit vulnerabilities to elevate privileges beyond their intended level? Focus on areas like AWS IAM roles and policies, and the interaction between different AWS services.

Challenge:

- For each STRIDE component, identify and list potential threats specific to the CycleSwift app and its AWS environment.