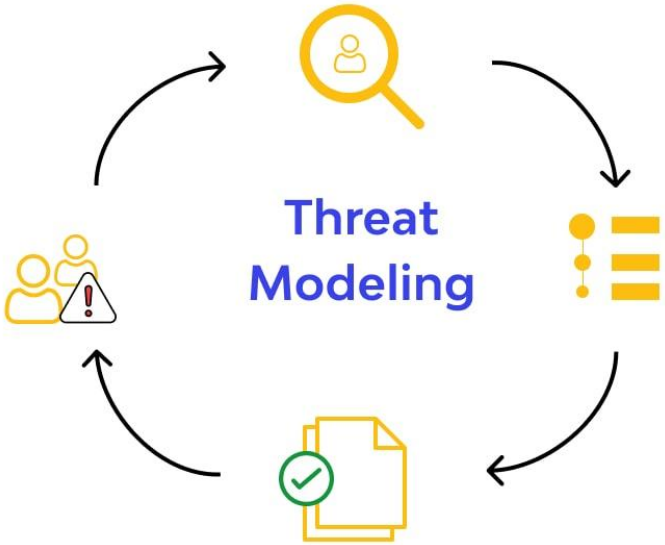

University Financial System Threat Model Design Documentation

Developed by Abdelaziz El-Sheikh

@aelsheikh04

1. Introduction

Project Overview

The project involves developing a secure financial system for a university, which includes a new web-based portal for students to access financial services. This portal enables students to view their current balances, payment history, set up payment accounts, make one-time payments, and configure automatic payments. The system integrates with the university's existing financial infrastructure, emphasizing robust security measures.

Objectives

1. Perform threat modeling to identify and mitigate potential security risks.
2. Create a detailed threat model report using Microsoft Threat Modeling Tool (TMT).
3. Develop an attack tree for VPN Spoofing.
4. Propose a defense tree to mitigate VPN Spoofing.
5. Document the processes and steps taken to achieve the above goals.

Tools Used

- **Microsoft Threat Modeling Tool (TMT) 2016**: To generate the threat model report and Data Flow Diagram (DFD).
- **Microsoft Visio**: For creating attack and defense trees.
- **Documentation Software**: Microsoft Word and PDF tools for report creation.

---

2. Threat Modeling Process

Data Flow Diagram Creation

A Data Flow Diagram (DFD) of the university financial system was developed to visualize:

- Data exchange between entities (students, staff, servers).
- Trust boundaries (DMZ, internal network).
- Key components (Web Portal, AD Domain Controllers, Database Servers).

Threat Identification

Using TMT 2016, threats were identified across the system. Categories included:

- Spoofing
- Tampering
- Information Disclosure
- Denial of Service (DoS)
- Elevation of Privilege (EoP)

Threat Categorization

Threats were prioritized based on their likelihood and impact:

- High Priority: Tampering with data flows, weak credential storage, and VPN Spoofing.
- Medium Priority: Excessive resource consumption and insufficient audit mechanisms.
- Low Priority: Minimal elevation of privilege scenarios.

Mitigation Measures

Mitigation strategies implemented include:

- Enforcing HTTPS for all connections.
- Strengthening authentication with Active Directory policies.
- Securing logs and sensitive data with encryption.
- Introducing resource consumption controls to prevent DoS attacks.

---

3. VPN Spoofing Analysis

Attack Tree

The attack tree for VPN Spoofing was developed to explore potential attack vectors and their preconditions:

- **Root Node**: Compromise VPN to access the system.
    - **First Level**:
        - Exploit weak authentication mechanisms.
        - Utilize stolen credentials.
        - Perform man-in-the-middle attacks.
    - **Second Level**:
        - Crack poorly encrypted VPN configurations.
        - Intercept network traffic.

Defense Tree

The defense tree outlines strategies to prevent VPN Spoofing:

- **Root Node**: Prevent VPN Spoofing.
    - **First Level**:
        - Implement multi-factor authentication (MFA).
        - Use robust encryption protocols (e.g., AES-256).
        - Regularly update VPN software and configurations.
    - **Second Level**:
        - Conduct routine security audits.
        - Train staff on phishing and credential protection.
        - Deploy intrusion detection systems (IDS).

Key Insights

- Weak credentials and outdated VPN protocols are primary vulnerabilities.
- Multi-layered defenses significantly reduce the risk of successful spoofing attempts.

---

4. Documentation of Steps

TMT 2016 Utilization

1. Created the DFD to map system interactions.
2. Identified threats using STRIDE methodology.
3. Documented mitigation strategies directly in the tool.
4. Generated a comprehensive report summarizing findings and actions.

Collaboration and Review

- Team members contributed to diagram creation, threat identification, and review.
- Regular discussions ensured accurate and realistic modeling.

Challenges Faced

- Balancing system usability with stringent security requirements.
- Adapting to TMT 2016's limitations in visual representation.
- Ensuring thorough documentation of all identified threats and mitigations.

---

5. Conclusion

Summary of Work

This project successfully:

1. Modeled threats to the university financial system using Microsoft TMT.
2. Identified and mitigated most potential risks.
3. Developed comprehensive attack and defense trees for VPN Spoofing.

Recommendations

- Continuously monitor the system for emerging threats.
- Conduct regular training sessions for users and administrators.
- Periodically review and update the threat model to adapt to new vulnerabilities.

---

6. Appendices

Threat Model Report Excerpts

Refer to the provided report for a detailed list of threats and mitigations.

Visuals

1. Data Flow Diagram
2. UFS Threat Model Report
3. VPN Spoofing Attack Tree
4. VPN Spoofing Defense Tree

References

1. Microsoft Threat Modeling Tool Documentation.
2. Industry best practices for VPN security.
