Secure Programming Lab 1 - Threat Modelling

This lab introduces you to Threat Modelling using Microsoft's Threat Modelling Tool / OWASP Threat Dragon. You are given a fictitious application, and you must use the threat modelling process to determine threats.

Background Scenario

EduPay is a nationwide education services provider that manages payroll and HR services for schools and universities across the country. Management has decided to launch an online payroll portal that allows teachers and staff to view their payslips, manage tax documents, and update personal details (such as addresses and bank account information). This new functionality is implemented as an add-on to EduPay's existing HR system. You are hired to perform a Threat Analysis to identify possible threats and vulnerabilities to the payroll portal. The new portal works like this: - Staff members register using a web interface with personal information (name, email, staff ID, password, bank account details, and tax number). - The system validates the information against the HR database and stores it in a secure payroll database. - Once logged in, users can: * View/download their payslips. * Update personal information (address, bank details). * Access tax forms (e.g., annual income statements). - The web application communicates with the payroll database and HR system to retrieve or update sensitive financial and personal data.

Step 1: Identify Security Objectives

- What type of data will be published/held?
- Are there any data regulations? (e.g. GDPR, financial compliance, payroll laws)?
- Will the site hold private/sensitive data (e.g. banking, salary, tax records)?
- What are the issues around Confidentiality, Integrity, and Availability (CIA triad)?
- Would compromise have financial, reputational, or legal consequences?

Step 2: Create an Application Overview

- Draw out a rough sketch of the new subsystem.
- Outline the users in the system and their roles (e.g., staff, payroll admins, IT support).
- Identify technologies (e.g., web servers, payroll database, HR system, authentication service).
- Identify possible security mechanisms (e.g., encryption, MFA, audit logging).

Step 3: Decompose Your Application

- Identify trust boundaries (e.g., between user browser and web server, between web app and payroll DB).
- Identify entry/exit points (login forms, file downloads, update functions).
- Identify data flows and draw a Data Flow Diagram (DFD) using MS Threat Modelling Tool or OWASP Threat Dragon.

Step 4: Identify Threats

- Who might be interested in compromising the system? (e.g., cybercriminals seeking financial fraud, insider threats, hacktivists).
- What are the bad things that can happen? (e.g., payroll fraud, data leakage, phishing attacks).
- What impact would this have on the business (financial loss, compliance penalties, loss of trust)?
- Decompose the subsystem into components (web app, DB, HR system, user devices, admin accounts) and identify threats for each.

Step 5: Identify Vulnerabilities

- Look at the system design to identify possible vulnerabilities (e.g., weak authentication, insecure storage of banking info, SQL injection, lack of audit logs, poor input validation).

Resources

- Microsoft Threat Modelling Tool: https://www.microsoft.com/en-ie/download/details.aspx?id=49168
- Walkthrough of creating a Threat Model: https://msdn.microsoft.com/en-us/library/ff649749.aspx
- Template: https://msdn.microsoft.com/en-us/library/ff648866.aspx
- Sample Template: https://msdn.microsoft.com/en-us/library/ff649779.aspx
- OWASP Threat Dragon User Guide: https://owasp.org/www-project-threat-dragon/docs-2/getting-started/