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

- *V*iew/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.

You will design a Threat Model using the following steps:

Step 1: Identify security objectives:

- What type of data will be published/ held?
- Are there any data regulations? e.g. medical/legal/ financial/ privacy?
- Will the site hold private/ sensitive data?
- Will this generate a large revenue stream?

In other words, what are the issues around *Confidentiality*, *Integrity* and *Availability*

Step 2: Create an application overview

- Draw out a rough sketch of the new subsystem
- Outline the users in the system and their roles
- Identify the technologies (system components – servers, databases, etc.)
- Identify possible security mechanisms

Step 3: Decompose your application

- Identify trust boundaries, entry/ exit points
- Identify data flows and draw a **data flow diagram** (Use MS Threat Model Tool or OWASP Threat Dragon)

Step 4: Identify threats

- Who might be interested in compromising the system? (organised criminals, hacktivists, competitors etc.)
- What are the bad things that can happen? (e.g. stealing customer data)
- What impact would it have on the business?
- Try to decompose the subsystem into components and identify possible threats for each one

Step 5: Identify vulnerabilities

- Look at the system design to identify possible vulnerabilities

Resources:

Microsoft Threat Modelling Tool:

- https://www.microsoft.com/en-ie/download/details.aspx?id=49168

(Older resources but still very relevant)

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/

Microsoft Threat Modelling Tool Tutorial

- See Doc on Brightspace