Exercise 08: Threat Modelling

Jan-Matthias Braun

28. of September, 2022

> Threat modelling is an essential tool to guide security considerations from planning over development all the way to deployment. Threat Modelling is a process about mapping potential threats to a specific project, typically in form of a data flow diagram. Please note the parallels to Threat Modelling as part of the assessment during penetration testing. The main difference is that a penetration tester doesn't have the inside view, but pieces the relevant information together by means of research, e.g., active and passive scanning.

Please note that all questions (full lines) marked with † should be answered in the report which you submit as assignment 2. In this specific exercise, please include the flow diagrams and lists or tables of identified threats. Try to find a few examples for every possible threat category.

Pre-Exercise Session Preparations

Read the ACME case (file name '02_Threat_Modelling_-_04_ACME case.pdf') in "Literature/Threat Modelling" in the "Resources" section on itslearning.

In the same folder, also look into the card game (file name '02_Threat_Modelling_-_05_EoP_Card_Game_Images.pdf').

Please download these files to have them available, ideally also before the exercise session.

Exercise 8.1: A simple Data Flow Diagram

Read the ACME case in "Literature" on itslearning. In groups of ≈ 3, develop a data flow diagram for

- An android health-app

- Login using username & password
- The app will be used to manually enter and edit/add/delete, e.g., height, weight, activity, and diet data.
- Data is stored locally
- Use, e.g., inkscape, draw.io, pen & paper ...

Make assumptions as needed, e.g., mobile platform, native framework, ...

Exercise 8.2: Formulate Stride

For the Android App, formulate

- Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
- For each category describe threats
- Use the ACME case & the game cards as a guide

Possible guides

- ACME case & game cards
- CAPEC
- OWASP
- F-Secure
- Exploit-db
- Carnegie Mellon University

Exercise 8.3: Discuss your Data Flow Diagram & STRIDE

Discuss exercises 8.1 & 8.2, ideally with another group. Try to complete your diagram & STRIDE.

† Please include your flow diagram with a description of the essential parts; provide list or table which details your findings using STRIDE.

Exercise 8.4: Update Flow Diagram & STRIDE

Update the data flow diagram & STRIDE for the case that the app becomes more of a fitness tracker

- Collect data from third party devices, e.g., via Bluetooth

- Data includes fitness-related metrics, e.g., steps taken, miles, calories burnt, activities, sleeping times
- The app cleans data and performs necessary computations
- No modification of data by users
- Data is stored on-device and in a cloud

Exercise 8.5: Discuss your Updated Data Flow Diagram & STRIDE

Discuss exercises 8.3, ideally with another group. Try to complete your diagram & STRIDE.

† Please include your updated flow diagram with a description of the essential parts; provide list or table which details your findings using STRIDE.