KU Secure Product Lifecycle

Introduction

Winter 2024/2025, 705.071 KU

21.10.2024

Content

- Organizational
- Intro to SDL (Secure Development Lifecycle)
- Intro to Exercises
- Questions

Organizational

- Groups of 3 students
- Registration either done or
  - register yet, by mail; Groupsearch via Discord (#spl-groupsearch).
- 4 exercises in total
- Each exercise needs to be done to achieve a positive mark
- The exercises simulate parts of a typical secure development lifecycle used in enterprises

- Note: Within the exercises we do not judge on the technical correctness of the presentation, the focus is on the process. Each team needs to hand in the required information, needs to argue why it thinks the performed work is correct and sufficient and also need to review the work of another team. Thus, the exercises rebuild the typical flow of a real-life development process in big enterprises.

Intro to typical SDL

- SDL are typically split in phases
  - E.g. Risk and Threat modeling, requirements specification, architecture, development, testing, ….
- Each phase is often closed with a „Gate“ review
- To pass a gate the according requirements need to be fulfilled
- Hand in information -> review information -> Gate meeting -> decision

Exercices

- Perform those exercises based on a fictional product

Topic	Date
Ex 1: Threat modeling and risk assessment	21.10.2024 – 11.11.2024
Ex 2: Security requirements document	11.11.2024 – 09.12.2024
Ex 3: Review of Ex1 and Ex2 of a different team	09.12.2024 – 06.01.2025
Ex 4: Gate review	January 2025

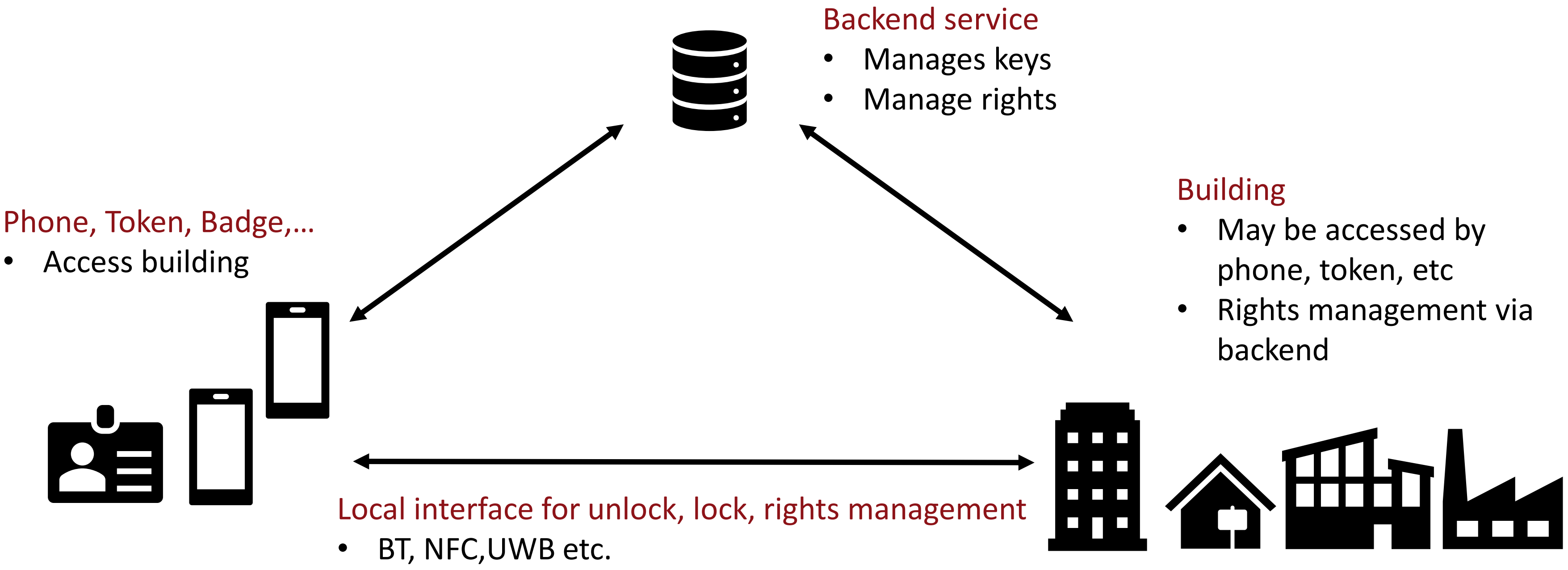
Grading

- 25 points per exercise, 100 max
- Each exercise must be submitted

Points	Grade
89-100	1
76-88	2
63-75	3
50-62	4
0-49	5

Product in scope

- Consider the following setup – Access Control System



Backend service

- Manages keys
- Manage rights

Phone, Token, Badge,…

- Access building

Building

- May be accessed by phone, token, etc
- Rights management via backend

Local interface for unlock, lock, rights management

- BT, NFC,UWB etc.

EXERCISE 1

Overview

- Detail the environment
- Perform a threat and risk analysis of the product in scope
- Create a deliverables of your analysis
  - Paper + Slides
- Argue why you consider this a sound solution

Tasks

- Task 1 (10 points) – Threat modeling
    - Threat modeling
        - Draw data flow diagram (DFD) for the envisioned design / scenario
        - Perform threat modeling based on MS STRIDE
    - Document threat modeling activities
- Task 2 (10 points) – Risk assessment
    - Define a qualitative rating system for likelihood and impact
        - Risk = likelihood x impact
    - Document risk assessment activities
- Task 3 (5 points) – Presentation

Minimum Requirements

Task	Item	Points
Task 1	DFD	4 points
	Argumentation for each combination in the STRIDE matrix (Max 15 threats)	6 points
Task 2	Definition of risk assessment process: • likelihood • impact And risk matrix	4 points
	Risk assessment (min. 2 risks with mitigation controls per component)	6 points
Task 3	Presentation summarizing results	5 points
	Maximum 4 slides	

Submission

- Send to christoph@yagoba.com
  - Paper (.pdf)
  - Presentation (.pdf)
- Send submission before **November 11, 23:59**