KU Secure Product Lifecycle

Introduction

Winter 2024/2025, 705.071 KU

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

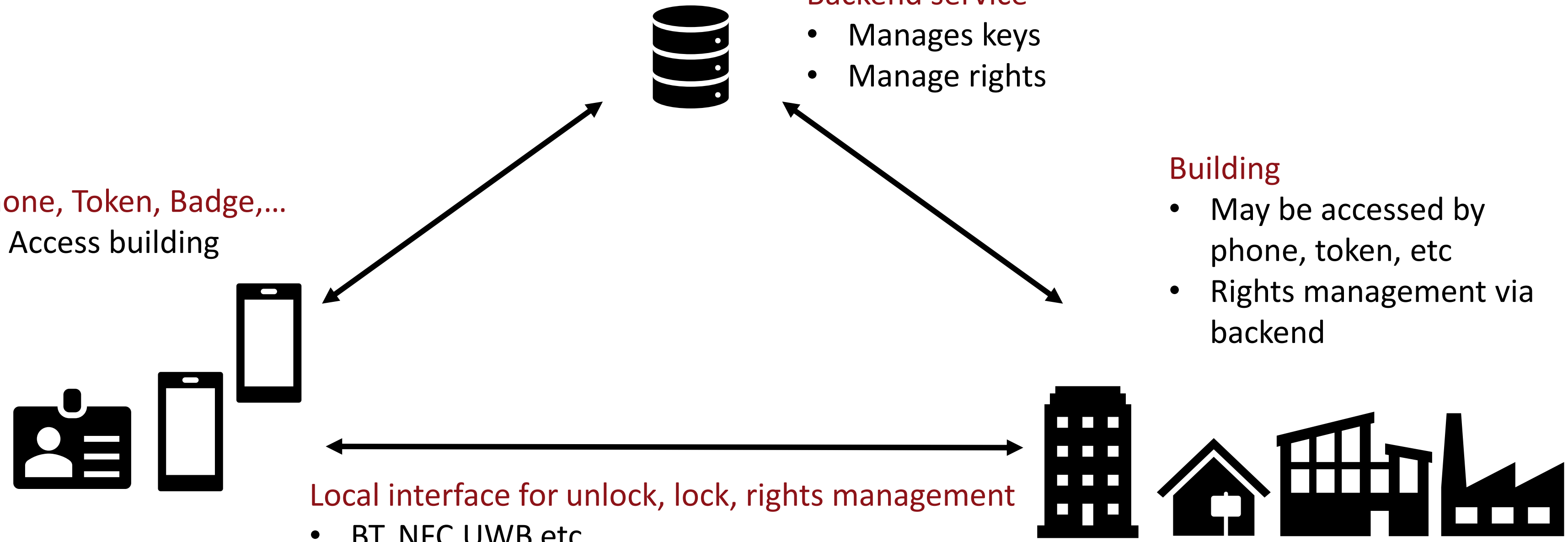
Grading

- 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 2

Overview

- Based on your threat and risk analysis deliver a security requirements specification
- Including
  - Security requirements
  - Verification requirements
  - Requirements for the usage

Tasks

- Task 1 (8 points) – Security requirements
  - Describe the security requirements of each component (Phone, Backend, Building)
  - Including the communication between them
- Task 2 (9 points) – Verification requirements
  - Describe how you would verify the security requirements
- Task 3 (3 points) – Requirements for the usage
  - Provide guidance how to securely use the solution
- Task 4 (5 points) – Presentation

Minimum Requirements

Task	Item	Points
Task 1	Security requirements for App	2
	Security requirements for Backend	3
	Security requirements for Building	3
Task 2	Verification requirements for App	2
	Verification requirements for Backend	3
	Verification requirements for Building	3
	Mapping from verification to security requirements	1
Task 3	User guidance	3
Task 4	Presentation summarizing results	5
	Maximum 6 slides	

Submission

- Send to christoph@yagoba.com
  - Paper (.pdf)
  - Presentation (.pdf)
- Send submission before **December 09, 23:59**

EXERCISE 3

Exercise 3

- You will get the deliverables of Ex1 and Ex2 of another group and do a thorough review of the deliverables
- Write a review report
  - Review the completeness of the threat model and risk analysis
  - Review the completeness of security and verification requirements
  - Review sufficiency of user guidance

Tasks

- Task 1 (8 points) – Review Threat Model and Risk Analysis
  - Provide a comment for each risk
  - Define additional risks
- Task 2 (8 points) – Review Requirements
  - Provide a comment for each security and verification requirement
  - Define additional requirements
- Task 3 (4 points) – Review User Guidance
  - Provide a comment for the guidance
- Task 4 (5 points) – Presentation

Note: valid comments are

- passed,
- needs improvement – including a description of it
- fail - with argument why

Minimum Requirements

Task	Item	Points
Task 1	Provide a comment for each risk	6
	Provide at least 1 additional risk	2
Task 2	Provide a comment for each security requirement	3
	Provide a comment for each verification requirement	3
	Provide at least 1 additional security and verification requirement	2
Task 3	Provide a comment for the guidance	4
Task 4	Presentation summarizing results	5
	Maximum 3 slides	

Submission

- Send to christoph@yagoba.com
  - Paper (.pdf)
  - Presentation (.pdf)
- Send submission before **January 06, 23:59**

EXERICSE 4

Exercise 4

- You will be invited to a “Gate meeting” together with the other group which is your counter part
- Presentation of Ex1 and Ex2
- Presentation of your Ex3 including a recommendation for passing a gate or not. If not: argue why.

Tasks

- Task 1 (10 points) – Presentation Ex1 and Ex2
  - Summary of your results
- Task 2 (10 points) – Presentation Review Ex3
  - Summary of your review results
- Task 3 (5 points) – Discussions and Q&A

Dates

- Date of gate review will be determined via Doodle and Discord, starting January 9th, 2025