UNIVERSITÄT BONN

Secure Software Engineering

Exercise Sheet 3, Winterterm 25/26

Discussion Week: Tue 11.11.25 to Fri 14.11.25

We highly encourage you to do the assignments yourselves, as all the exercises are relevant for the exam. It is also recommended to visit the tutorial, as there will be a discussion about the exercises, not just the solutions. For the *Vulnerability of the Day* exercises, we recommend looking into the code snippets, if you find any, while doing research. Keep in mind, the entirety of the lecture is relevant for the exam. If a topic or some details are not specifically talked about or mentioned in the exercises, that does **not** mean that it will not be part of the exam!

If you have any questions, please do not hesitate to ask your tutor Aura, Kati or Lukas. (Hint: the mails are embedded in the names.)

Good luck and have fun! :)

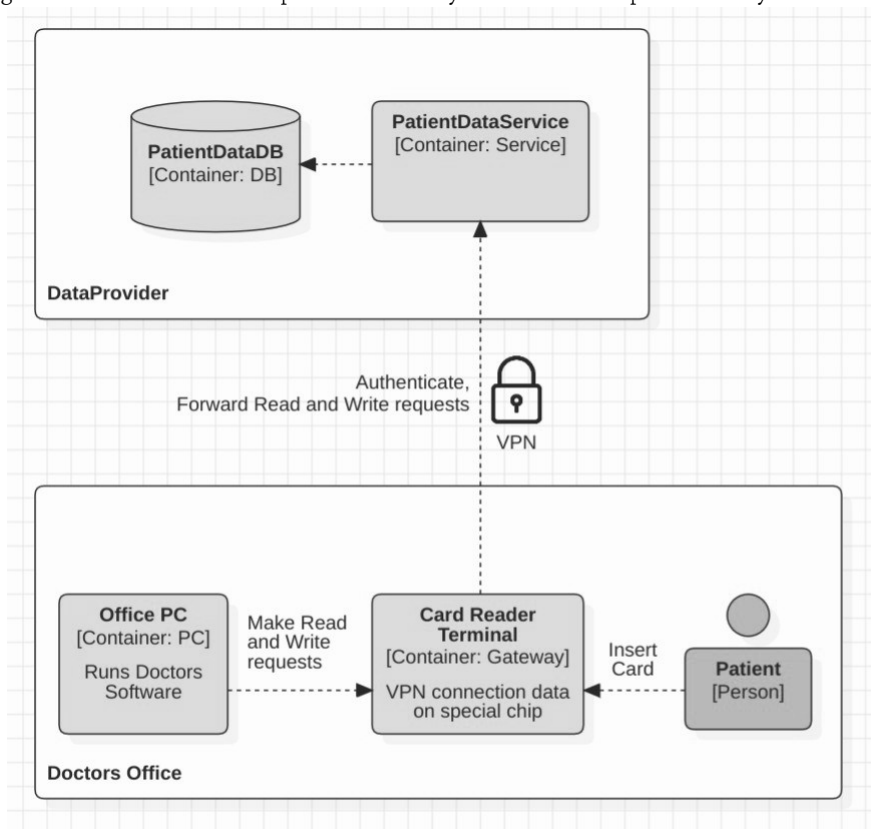
Ex. 1 - Risk Analysis

Answer the following sub-tasks:

a) What should you keep in mind when it comes to architectural risk analysis? Name at least 4 things.

b) Name the three sections of threat modeling.

c) This scenario is inspired by the German *Elektronische Patientenakte* (ePA, electronic patient files) but is neither dependent on nor directly related to it. In this exam, you are tasked with developing the *Sichere elektronische Patienten Akte-Software* (SePA, Secure Electronic Patient Files) following the secure software development lifecycle steps. The diagram below shows the components of this system. Think of a place where you would set boundaries and why?



Workflow Overview

1. Patient Arrival When a patient arrives at the doctor's office, they present their insurance card. The card is inserted into a terminal connected to the doctor's PC. This authorizes the doctor to access the patient's data for 30 days.
2. Data Retrieval The doctor uses their software to request the patient's data from the PatientDataService.
3. Data Update At the end of the visit, the doctor updates the patient's information and sends these changes to the PatientDataService.
4. Data Persistence The PatientDataService then persists the updated data in the PatientDataDB.

System Conditions

- Patient Insurance Card: The card contains the patient's information (e.g., PatientID), a private key used to sign requests, and additional health information (e.g., allergies, blood type, organ donor status).
- Doctor's Chip Card: The terminal also contains a chip card unique to each doctor, which establishes a secure connection to the SePA-VPN.
- Secure Gateway: All requests from the doctor's software pass through the terminal, which acts as a secure gateway to the SePA-VPN.
- Restricted Access:
  - The PatientDataService is only accessible through the SePA-VPN.
  - The PatientDataDB is only reachable by the PatientDataService (i.e., not directly by clients).

d) Why are threat models and architectures different?

Ex. 2 -Distrustful Decomposition

What are the aspects of *Distrustful Decomposition*? Why is it important to uphold them? Explain each aspect.

Ex. 3 - Vulnerability of the Day

In the lecture, we talked about *Cross-Site Scripting (XSS)*. Research an example of this that was not discussed and explain what happened, how it happened, and how it was dealt with. In addition to that, explain which of the CIA properties were affected.