TDDE49 2024

Assignment 4 – Information Security Modeling

Background Reading

Read the introduction to CORAS by den Braber et al.:
https://link.springer.com/content/pdf/10.1007/s10550-007-0013-9.pdf

Introduction

Your task is to analyze the potential security and safety risks of a (hypothetical) remotely managed pacemaker system. The pacemaker contains sensors that monitor the heart activity of the patient, and sends periodic measurement reports to the patient's cardiologist. After reviewing the report, the cardiologist can remotely update configuration parameters of the pacemaker to accommodate for any changes in the patient's heart condition.

Communication with the pacemaker is done via an app in the patient's smartphone. The app connects to the pacemaker using Bluetooth to retrieve measurement reports. The reports are then forwarded to the servers of the pacemaker manufacturer, which in turn forward the report the patient's cardiologist. For convenience, the report is sent as an email to the physician's registered email address (so that the physician doesn't have to remember to log in to a special system every day to check reports.)

During Bluetooth connection, the phone/app authenticates to the pacemaker with a fixed password that is unique to each pacemaker device. (The app must be configured with the correct password the first time the phone and pacemaker are paired.)

If the cardiologist wishes to update the pacemaker configuration, he/she needs to log in to a special system (provided by the pacemaker manufacturer). The configuration is then pushed to the patient's phone, and the app will connect to the pacemaker and transmit the configuration update. If the phone is not connected to the internet, the server will temporarily store the configuration, and push it to the phone as soon as it becomes available.

The pacemaker has a surgically inserted battery pack that needs to be recharged once per week using a contactless charger that is placed onto the patient's chest. Since any communication over Bluetooth draws a lot of power from the battery, the Bluetooth interface is not continuously connected. Instead, the app will connect to the pacemaker only once per day (since every connection attempt also draws significant battery power) to download recorded data, and then shut down the connection again. (The pacemaker can store up to 3 days of data internally.)

Tasks

Your task is to perform a security analysis of the system described above. You don't need to delve into deep technical details of attacks against, e.g., the Bluetooth protocol (there are many). Instead, perform a high-level analysis, using what you have learnt during the information security part of the course, and the above description.

Your analysis should be based on the overall CORAS workflow. However, you don't need to perform every part of CORAS. Moreover, some parts of the analysis are already provided in order to make the task more manageable within the given time frame. Below is a description of the CORAS workflow and the three specific tasks you should complete.

CORAS Step 1: Analysis overview. This can be considered covered by the problem description.

CORAS Step 2: Identify assets. In this exercise we will consider four assets, where "Patient's health" is an indirect asset, while the other three are direct assets. You should only consider the assets below during the assignment (i.e., you don't need to come up with additional assets on your own).

- **Pacemaker functionality** → *Patient's health*
- **On-device recorded data**
- **Centrally-stored patient data**

CORAS Step 3: Scales and risk evaluation matrices. During this step the assets should be r*anked* and *consequence scales* should be created for each of them. The same consequence *categories* should be used for all assets, but the definition of categories will be different for each asset. We already provide a consequence scale for the asset **Pacemaker functionality**.

Pacemaker functionality		
Consequence	**Description**	**Motivation**
Catastrophic	Stops working	May result in patient death
Major	Degraded function	May negatively affect patient's health
Moderate	-	
Minor	-	
Insignificant	-	

Task 1

- Create *consequence scales* for the assets **On-device recorded data** and **Centrally-stored patient data**.
- Create *one* common *likelihood scale*.
- Create *risk evaluation matrices* for each of the three assets.

For each of the above, motivate your choices.

Note that the definition of consequence can be based either on a quantitative measure (like the number of affected patient records in the CORAS paper) or a qualitative measure (like the consequences for **Pacemaker functionality** used here). Also note that for some assets, only some of the consequence categories might be used (as is the case for **Pacemaker functionality**).

When designing consequence scales, it might be helpful to keep the C-I-A properties in mind. For example, how would you rank the respective consequences of compromised confidentiality, integrity or availability of **On-device recorded data**?

CORAS Step 4: Brainstorming about threats.

Task 2

- Create an *attack tree* for the attacker goal "degrade pacemaker function". (This can encompass both making the pacemaker perform sub-optimally or making it stop working altogether.) Remember that an attack tree should only consider deliberate malicious actions, not that things break by accident. Annotate the tree with *likelihood estimates* to aid in the risk analysis.
- Come up with potential threats against the assets in Step 2. You don't need to draw CORAS threat diagrams (although this might help to get an overview of risks), but for each identified threat, the following must be clearly stated: *threat actor* (accidental, deliberate, non-

human), *vulnerability*, *threat scenario*, *unwanted incident* (i.e., consequence), and the affected *asset*. Your solution **should contain at least one threat from each type** (accidental, deliberate, non-human). You should include threats identified during the attack tree analysis here, but note that there are other threats to consider as well (e.g., accidental and non-human threats, and other assets).

Important: Keep in mind that the purpose of the analysis is to identify concrete security risks, in order to help the provider to mitigate security problems in *their* product and associated services. Your focus in this step should therefore be on vulnerabilities in the technical design or intended operation of the pacemaker system, rather than security problems outside the control of the provider.

For example, the threat "*Hackers install spyware on the cardiologist's workstation, allowing them to monitor everything he/she does with the computer*" would obviously be a serious threat against the confidentiality of sensitive patient data. However, there is virtually nothing the provider could do to avoid this threat, regardless of how they design their solution, since they have no control over the management of IT systems at an individual hospital.

Instead of focusing on generic and unspecific attacks like in the example above, make sure to *carefully read the technical description of the system several times*, try to think from the attacker's point of view, and be creative. Also make sure to keep the "C-I-A" properties and the STRIDE keywords in mind. What are possible ways you would be able to cause harm against one of the assets, just given the information about the system provided in this assignment? What are plausible ways in which harm can come to assets by human mistakes or non-human threats?

CORAS Steps 5 – 7: Analysis and mitigation of identified threats.

Task 3

- Estimate risks by assigning *likelihood* and *consequence* ratings to your identified threats (using the tables from Step 3). Briefly motivate your choice of ratings for each threat.
- Use the risk evaluation matrices from Step 3 to decide which threats that would need to be dealt with.
- Briefly propose/discuss ways to eliminate or mitigate the vulnerabilities that need to be addressed.

Handing in

Send your solution as a PDF to ulf.kargen@liu.se by October 14, 2024 (soft deadline). Figures might be drawn electronically or hand-drawn and photographed/scanned and inserted into the document.