TDDE49 2023

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 extra power from the battery, the Bluetooth interface is not continuously connected. Instead, the app will connect to the pacemaker only once per day (since connection attempts also draw 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. Specifically, you are expected to do the following:

Step 1 – This can be considered covered by the problem description.

Step 2 – Identify the assets and draw a basic *asset diagram*. Note that this step is crucial for the rest of the process, so you should put some effort into selecting assets that enable a meaningful analysis in the later CORAS steps. Make sure that you have a solid grasp of the CORAS process and have read the instructions for all the following steps in this assignment before you complete the task. To ensure a reasonable workload, it is recommended that you limit the number of final in-scope assets to around 4 or 5. However, be sure to explain why you consider an asset out-of-scope. Your final list of in-scope assets **should contain both *direct* and *indirect* assets**. (Also explain why an asset is direct or indirect.)

Step 3 – *Rank* the assets and create *consequence scales* for each asset. The same consequence categories should be used for all assets, but the definition of categories will be different for each asset. (Also, for some assets, only some of the consequence categories might be used. For example, if the consequence is strictly binary: something bad happens or it doesn't.) Also create a *likelihood scale* (to be used for all threats). Based on these, create a *risk evaluation matrix* for each asset.

Step 4 – Brainstorm about threats, keeping the "C-I-A" properties and the STRIDE keywords in mind. 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).

As part of this step, you should also create at least one **attack tree**. Create the tree for the attacker goal (i.e., deliberate threat) that you feel have the largest number of different possible avenues of attack. (It is not meaningful to create a two-node attack tree…) Annotate the tree with *likelihood estimates* to aid in the risk analysis. Note that an attack three always concerns a deliberate threat. Therefore, it should always have a *concrete attacker goal* as the root node, while child-nodes should represent subgoals to achieve that goal.

Important side note: Keep in mind that the purpose of the analysis is to identify concrete security risks, which could aid the hypothetical provider of the pacemaker system 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 stipulated 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, including viewing pacemaker measurement reports*" 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, short of simply not offering the remote-monitoring functionality at all. Instead, it would have to be assumed that the hospital has a reasonable level of IT security to avoid spyware attacks (e.g., keeping the operating system up-to-date, using antivirus products, etc.).

Step 5 – 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.

Step 6 – Use the risk evaluation matrix to decide which threats that would need to be dealt with.

Step 7 – Briefly propose/discuss ways to eliminate or mitigate the vulnerabilities that need to be addressed.

Discussion – Briefly discuss the outcome of your analysis. Do the results seem intuitively sound? Do you feel like the choice of assets or the scales in Step 3 would need to be revised? What did you find most challenging in carrying out the security analysis?

Handing in

Send your solution as a PDF to ulf.kargen@liu.se by October 5, 2023 (soft deadline). Figures might be drawn electronically or hand-drawn and photographed/scanned and inserted into the document.