Activity: Abuse Cases

Overview

The purpose of this activity is to get you acquainted with writing abuse cases.

Setup

This activity is for groups of 4-6 people. You will need a shared document that multiple people can edit. Have someone create a Google Doc and share it with your team and the instructor.

We are going to practice with the Abuse Case development process described in **Slides 04 - Lifecycle and Abuse Cases.pdf (https://uncw.instructure.com/courses/16302/files/434480/download?wrap=1) (https://uncw.instructure.com/courses/16302/files/434480/download?wrap=1)** .

Activity

1. (10 minutes) Begin by reading through the document **4 - Use Case Specifications.pdf (https://uncw.instructure.com/courses/16302/files/434350/download?wrap=1) (https://uncw.instructure.com/courses/16302/files/434350/download?wrap=1)** , which describes several use cases for a theoretical system called HPCA.
    - The HPCA is an assistive technology device that helps elderly sick persons that helps the user: a) make emergency phone calls or send SMS texts, b) speaks preset sentences to a care provider, and c) provides reminders to take prescription drugs.
    - Focus primarily on Use Case IDs 1-2 and 11-13.
2. (5 minutes) Create a shared Google document for your team and also share it with the instructor. Assign one person to the be the scribe for this step.
    - Copy Use Case IDs 1-2 and 11-13 into your Google Doc. You do not need to copy the figures if you don't want.
    - Brainstorm threats to your system, using the definition that a *threat* is a malicious actor. Document potential threats (regardless of their likelihood) in the Google doc under the heading Threats.
3. (15 minutes) Divide your group in two. Each subgroup will need a scribe to edit the Google doc.
    1. One subgroup will create *anti-requirements.* What are the things you *don't want* your software to do that would violate the CIA model? Don't worry about *how* these things could happen, just think about what should not happen! Write down your anti-requirements, 1-2 sentences each, in the Google doc under the heading Anti-Requirements.
    2. One subgroup will create an *attack model*. Which attacks do you think this system would likely be susceptible to? Read through **the attack patterns on pp. 218-221 of McGraw (https://uncw.instructure.com/courses/16302/files/434542/download?wrap=1)**

(https://uncw.instructure.com/courses/16302/files/434542/download?wrap=1) . You do not know anything about the implementation of the system, but you can assume that there will be the device, a webapp for handling requests and sending responses to the device, and a database on the web side. You will have to do some extrapolating, but think of how someone might attack the system. Write down your attack pattern ideas, 1-2 sentence each, in the Google Doc under the heading Attack Patterns.

4. (15 minutes) Generate Abuse Cases by, as a group, looking together at your Anti-Requirements and Attack Patterns. Focus primarily on Use Case IDs 1-2 and 11-13 and add steps to those use cases (feel free to copy and paste from the PDF) that would abuse the system, a.k.a., attack the system and cause undesirable behavior. Document your in the Google Doc under the heading Abuse Cases. Highlight the "abuse steps" in red or boldface. You may have multiple Abuse Cases for each original use case. Edit the Main Flows and Alternative Flows
5. (10 minutes) Create security requirements. Security requirements can be broad, e.g., "All passwords will be encrypted on the client prior to transmission". Give each security requirement a label (e.g., SEC-1), and add security requirement references to the step in the main flows (and alternative flows if you added any) of the use cases.
6. Given your abuse cases, go back to the original use cases and add in steps that might help promote security. Edit the Main Flows and Alternative Flows.
7. Be ready to discuss your materials with the rest of the class.