Initial Design Document and Threat Modeling

Due January 6, 2020, 11:59:59AM (before class)

The overall learning objective of this homework is to get you thinking about the design of your course project prior to development with a specific focus on threats other teams could exploit during the Break It round. The main deliverable for this homework is the initial design document identifying the components of your IoT system (see specification document for detailed requirements). This is the first of three design documents you will submit throughout the course.

In the system design documents, you will answer three main questions: how the system is organized to meet required and optional functions, how an attacker can affect the system (i.e., exploit weaknesses), and mitigations in place against potential attacks.

Note, while the majority of the class project will be completed in teams, this assignment is meant to be completed **individually**.

Design Document - What are you building? (30pts)

Regarding the question of system organization, you must present all components of your system. We know this will likely change later, but this design document should reflect your current plan for the system. This includes describing each independent component and its function and how components interact with each other. This document provides the basis for instructors to understand and evaluate your code, so make sure the document is sufficiently detailed.

You are free to structure your design document according to your preference (e.g., visual and/or textual descriptions). You may want to consider Lucidchart as potential option: all UMD students have access to this online graphing tool through Terpware and it allows collaborative editing--very useful for future iterations when you may be working in teams!

Threat Modeling (70pts)

In addition to laying out the system, you also need to show the system's attack surface and mitigations in place to prevent potential attacks.

What could go wrong? (35pts)

The attack surface includes any points where an attacker can manipulate input to the system and/or the system's actions. Each point where an attacker can manipulate the system should be clearly marked in any visual component of the design and described in the text. Textual descriptions of each attack surface point should include descriptions of attacker interactions and the range of possible malicious actions an attacker could take and their impact on the system.

In the ATM example we discussed in class, one possible attack surface was the network connection between the bank and ATM. In this example, the attacker operates as a Man-in-the-Middle (MitM), proxying traffic between the two endpoints (i.e., bank and ATM). They can read or make changes to all transmitted packets and insert additional packets arbitrarily. The most obvious attack in this case would be for the attacker to simply read all data transmitted between the two parties, violating the communications' privacy. This attack would be represented in the design document with an indicator on the network communication between the ATM and bank signaling the MitM and the above textual description.

Grading

Each unique possible attack described is worth 7pts. To get full credit for this portion of the homework, you need to identify and clearly explain five possible attacks against the system. Also, to ensure you are considering a breadth of attack types, the attacks described must be associated with at least two different points of the attack surface. Note, while this is the minimum requirement, to do well in the BIBIFI competition (the majority of your grade in the course), you should be as thorough as possible here and plan for as many threats as you can think of.

What should you do about those things that could go wrong? (35pts)

For each possible attack described you should also indicate any mitigations put in place to protect the system from those potential attacks. Each mitigation should be presented as a component in the design document, with its function and relation to other components clearly labeled. Also, each mitigation should indicate the security requirement (i.e., privacy, integrity, and availability) the mitigation is intended to protect and the possible attack it mitigates. Note, it is possible that a single mitigation addresses multiple security requirements; however, you need to include a discussion of how the mitigation remediates each possible attack separately.

For the MitM attack against network communication privacy given above, the mitigation would be to encrypt data prior to transmission across the network. This would be indicated in the design document with an additional component on either side of the network communication showing an encryption cipher. In the textual description, the mitigation would be marked as protecting the privacy security requirement and associated with the MitM attack reading all transmitted user data.

Grading

Each possible attack covered by a mitigation is worth 7pts. To get full credit for this portion of the homework, you need to identify and clearly explain enough mitigation to cover five possible attacks. Also, to ensure you are considering a breadth of attack types, the mitigations must be associated with possible attacks against at least two different attack surface points. Again, while we present minimum requirements here, a more thorough document will be advantageous in the BIBIFI competition.

Submission Instructions

Please submit a single pdf file with the following naming convention to the submit server:

<first_name>-<last_name>_designdoc.pdf

This document should include both the visual depiction of your design document and textual details of components, the attack surface, possible attacks, and mitigations.