CSci 4271: Introduction to Computer Security

Problem Set 1 **due: Friday February 25th, 2022**

Ground Rules. This is an individual assignment. You may discuss the concepts behind these questions with other students, but you should formulate your answers individually and your answers must be entirely your own writing. You may use any paper or written online source that you find relevant to the questions but you **must** explicitly reference any source you use besides the lectures. An electronic PDF copy of your solution should be submitted on Canvas by 11:59pm on Friday, February 25th.

Before we started using Moodle and then Canvas, classes using the CSE Labs had an internally developed system that allowed students to see information about grades electronically. Here are some basics of the system worked:

- There was a configuration program that could be executed by course instructors and TAs (collectively "graders") to set up the system for a new course, or to directly edit the tables containing grades.
- There was a command-line program executed on CSE Labs machines by graders which interpreted a text input file in which each line was an instruction to add to or modify a student's grade on an assignment, or set or change the total score and weighting of an assignment.
- There was a web interface that allowed each student taking a course to see their scores for assignments in a particular offering of a course. Each course offering had a unique identifying number, which was passed by URL in the web interface. Students could only access the web interface after logging in using a CSE Labs login name and password (which at the time were separate from the UMN ID).

For the next three questions, imagine that the department has decided to implement a new similar system for future use, and you've been asked to help design and implement it securely.

1. Threat model assets and attackers. (25 pts) As a first step in threat modeling, think about what the overall security goals for this system should be. Specifically: what are the assets that need to be protected? Who might be an attacker against the system, and what might their motivations be? Note that the way that an attack is useful to an attacker might be basically the same as the reason it is detrimental to the victim, or these might be different. What are the high-level security policies that should hold? On the other hand, what kinds of threats do not need to be considered?

2. Threat model data flow diagram. (30 pts) Next, think about the software architecture you would build to support this grade viewing functionality, and how users would interact with different parts of the system when carrying out the supported features. Based on this, draw a data-flow diagram showing the users, the software components, the data flows between them, and any trust boundaries. You should aim to include enough details that your data flow diagram shows 5-10 software components. (Users are not software components.)

Point out a place in your data-flow diagram where the data flow edges and threat model boundaries you've drawn represent a design that is easier to secure. Specifically compare your design to another design that would still implement the same visible behavior, but would be harder to build securely.

3. Threat model STRIDE threats. (20 pts)

Finally, apply the STRIDE threat taxonomy to the elements and data flows you diagrammed in the previous question, and create a table enumerating a number of possible threats. For each threat, your table should include a short description, a cross-reference to which elements of the data-flow diagram the attack targets, and a short description of possible mitigations. A good answer should mention at least 10 different threats.

4. STRIDE in another context. (25 pts) A paper written by Florina Almenárez-Mendoza et al, assessing the some of the security properties of fitness tracking devices, is available from its publisher's web site at the this URL: `https://www.mdpi.com/2504-3900/2/19/1235`

Skim sections 1-3 of the paper for context, and then carefully read section 4 which gives a description of vulnerabilities the authors found in some of the devices they studied.

Think about how these vulnerabilities related to the STRIDE taxonomy. For each of the 6 STRIDE threat classes, give one example, if any, of a possible attack found to be possible by the paper which you would classify in that category. You should be able to find examples of at least 4 out of the 6 threat classes.