CSci 4271W Developing Secure Software Systems (section 010)

Homework 1 **Due: Tuesday, February 4, 2025**

Ground Rules. You may choose to complete these exercises in a group of up to three students. Each group should turn in **one** copy with the names of all group members on it. You may use any source you can find to help with this assignment but you **must** explicitly reference any source you use besides the lecture notes or assigned readings. No answers should come from people outside your group, or from AI tools like ChatGPT. If you use an AI tool to revise your writing, save a copy of the first draft you wrote yourself to provide it was originally your work. Electronically typeset copies of your solution should be submitted via Gradescope by 11:59pm on Tuesday, February 4, 2025.

1. **Risk Assessment.** Until 2011, students in CSci courses (and other departments in the College of Science & Engineering) had their homework and exam scores reported through a system called GRIT. GRIT worked as follows:

   a. The configuration system could be used to set up a new course offering and allow graders (instructors and TAs) access to the grade tables.

   b. A CSELabs command line tool run by graders would read input text files in which each line added/modified a student's grade on an assignment, or added/modified an assignment's total score and weight.

   c. A web interface that allowed each student to see their scores for a course offering (each course had a unique identifier number, and these numbers were passed by URL). Students had to sign in to the website with their CSELabs username and password (these were separately managed from UMN internet passwords at the time.)

   Describe a threat model for this system: what should the security goals be? What are reasonable attacks, and who are the potential attackers? What threats should we explicitly exclude from consideration?

   Now propose at least two mitigations that would help counter the threats identified in your analysis. Analyze the net risk reduction of both mitigations. You should justify your estimates for the various incidence rates and costs, but don't spend very long at this part of the assignment.

2. **Diagrams.** Continuing with the GRIT example, create a DFD for the system. Write short descriptions (using your diagram) of how a student's grade on an exam is entered, and how the student retrieves their grade.

3. **STRIDE.** Perform a "STRIDE-per-element" analysis of your DFD from the previous problem. Your solution should include a table listing all of the threats you identified, the DFD elements they target, and potential mitigations, where applicable.

4. **More STRIDE.** Skim through the "Security Assessment Report: GPS Watches for Children" prepared by Mnemonic for the Norwegian Consumer Council at `https://z.umn.edu/585u`. For each of the 5 "Attack scenarios" in section 4 (4.1-4.5), write a paragraph that briefly summarizes the attack and argues for how you think it fits in the STRIDE taxonomy.