CSE 484 / CSE M 584 - Homework 3

Background:
The goal of these exercises is to give you more opportunities to practice threat modeling and to gain experience with two different threat modeling toolkits.

Materials from lecture:

- Threat modeling slides
- In-class worksheet

General Instructions:

1. Form groups of up to 4 people. (If you really want/need to, you may work alone, but we strongly recommend working in groups.)
2. Read the system descriptions of several systems (Aircraft-Service-Scenario-Low4.pdf and Drone-Swarm-Scenario-v05.pdf).
3. Complete the STRIDE and Security Card Exercises outlined below.

STRIDE Exercises

0. Pick one of the two systems (aircraft service or drone swarm) to analyze.

1. Download the documentation and installer for the Microsoft STRIDE tool: https://www.microsoft.com/en-us/download/details.aspx?id=49168.

2. Install the STRIDE tool (either directly on a Windows machine, or into a VM).

3. Watch a video about STRIDE: https://www.microsoft.com/en-us/sdl/adopt/threatmodeling.aspx.

4. Download the simplified STRIDE template (SimpleStride v2.tb7) and load the template into the tool. (*Note: if this causes technical difficulties, it is alright to proceed with the default template. Recall the process used in class to load this template – first start the tool, create a new model, load the template, exist the tool, start the tool again and create a new model.)*

5.. Create a diagram of the system in the STRIDE tool per the information in the system handout.

6. Write a 1-2 paragraph explanation about the interesting/relevant decisions you made when you created the DFD in step #5.

7. Run the tool's threat analysis.

8. Using the output of the tool as guidance/inspiration, create a list of threats to the system. You will be graded on how complete and detailed the list of threats is. Use this form as the template for recording your results.

Each person should spend no more than 3 hours on the STRIDE exercises (either together or separately).

Turn in to the STRIDE Catalyst Dropbox (one submission per group):

- **A README.txt file that includes:**
  - **The names and UWNetIDs of all the group members.**
  - **The name of the system that you chose to analyze.**
  - **If you'd prefer that your files not be used to evaluate the strengths and weaknesses of the different threat modeling methodologies, a statement saying so. (See the Additional Information below.)**
- **Your system diagram and the generated list of threats from the tool (#5, #7).**
- **The explanation of any DFD choices you made (#6).**
- **MAIN OUTPUT: The list of identified threats for the system (#8).**
- **Please indicate:**
  - **Which template you think you used (the default with install or the simplified template linked above).**
  - **Approximately how long you spent on the assignment (not graded).**
- **Optional: the main strengths and weaknesses of using the STRIDE tool, based on your experiences with this exercise.**

Security Card Exercises

0. Pick the other of the two systems (aircraft service or drone swarm) to analyze.

1. Obtain a deck of Security Cards (we will bring them to class during the next few lectures, and we may leave some in a location TBD).

2. As a group, communally rank the cards (within each category) in order of relevance to the system being analyzed. Relevance is an organic judgment as some function of likelihood of the threat and potential damage of the threat. *You will need to supply the ranking, but you will not be graded on it.*

- What is important here is the discussion as to why you are choosing the ranking that you are choosing, not the ranking itself. The purpose is to get you to look at all cards in order to generate potential threats.
- You can look through the categories in any order you choose, but one logical ordering is: (1) Human Impact; (2) Adversary's Motivations; (3) Adversary's Resources; (4) Adversary's Methods.

3. Using the above process as guidance/inspiration, create a list of threats to the system. You will be graded on how complete and detailed the list of threats is. Use this form as the template for recording your results.

Each person should spend no more than 2 hours on the Security Card exercises (either together or separately).

Turn in to the Security Cards Catalyst Dropbox (one submission per group):

- **README.txt file that includes**
  - **The names and UWNetIDs of all the group members.**
  - **The name of the system that you chose to analyze.**
  - **If you'd prefer that your files not be used to evaluate the strengths and weaknesses of the different threat modeling methodologies, a statement saying so. (See the Additional Information below.)**
- **The rankings of the cards in each dimension (not graded).**
- **The list of identified threats for the system (#3).**
  - **Indicate which three threats you think are most likely.**
  - **Indicate which three threats you think are most damaging.**
- **Please indicate approximately how long you spent on the assignment (not graded).**
- **Optional: the main strengths and weaknesses of using the Security Cards, based on your experiences with this exercise.**

Additional Information

- One submission per group.
- Submit the STRIDE portion to the STRIDE dropbox, and submit the Security Cards portion to the Security Cards dropbox.
- Researchers at UW, CMU, and the University of Utah (though no one involved in the teaching of this course) are interested in studying the efficacy of different threat modeling techniques, with the goal of creating better threat modeling tools. (No existing tools today are "perfect," and there is a lot of room/need for better tools.) To help them with their research, they would like to analyze the *anonymized* results of your analyses of these two systems, using these two different (standard) toolkits. They will only get anonymized results. They are not involved in the teaching of this course, and hence your participation in their research will not have any effect on your course grade. *If you would prefer not to have your anonymized solutions shared with the research group, please indicate your decision in your README.txt file.*