The Security Cards – Sorting by Importance

Duration: Single lecture, stand-alone unit

Learning Objectives

1. At the end of this unit: Given the description of a system, students should be able to argue which human assets are the most relevant for designers to protect, which are the least relevant, and why.
2. At the end of this unit: Given the description of a system, students should be able to argue which adversary motivations are the most likely to occur, which are the least likely, and why. These motivations will be the basis for creating profiles of likely adversaries.
3. At the end of this unit: Given the description of a system and a basic profile of likely adversaries, students should be able to characterize the resources available to a particular adversary and argue which resources are the most relevant for enabling or improving attacks against the system.
4. At the end of this unit: Given the description of a system and profiles of likely adversaries, students should be able to articulate a range of potential attacks on the systems, argue which methods are most likely to be exploited by attackers attempting to violate the system, which are the least likely, and why.

Classroom Activity:

Setup

1. **System Description.** Present a system to students for analysis. Just describe the system—no security analysis at this point. If students are working on a particular class project (or if developers are working on a particular product), then this project can be a natural fit. The web site also provides some example systems and links to videos presenting those systems.

Break Into Groups

2. **Break into groups.** Have the students break into groups of three of four.
3. **Look over the cards.** Have the student groups familiarize themselves with the card dimensions and the general format of the cards. Students should read at least one card in each dimension in its entirety. (This step could be done the before class, as an out-of-class task.)

Threat Surfacing Activity

4. **Card sorting task.** Have the students sort the cards within each dimension in order of relevance to the system being analyzed.
    a. We recommend first sorting the Human Impact cards, then the Adversary's Motivations cards, then the Adversary's Resources card, and then the Adversary's Methods cards, and then re-visiting all of the sorted cards.
    b. We recommend announcing 7 to 10 minutes into the working session that students should switch from the Human Impact dimension to the Adversary's Motivations dimension if they haven't already. We recommend similar announcements after the next 7 to 10 minutes (switching from Adversary's Motivations to Adversary's Resources) and again after another 7 to 10 minutes (Adversary's Resources to Adversary's Methods).
        i. Students should understand that there is no "right" nor "wrong" ordering. Students may interpret "relevance" differently—for example, realism of attack attempt vs. likelihood of attack success vs. effect of successful attack. In fact, given two cards—even given the same interpretation of relevance—there may be valid arguments for both possible orderings. The important thing here is to be able to explore and articulate what makes the different cards more or less relevant.

Report Back

5. Pick one or two groups, and have them present their ordering of the Human Impact cards, and why they chose that ordering.
6. Pick one or two groups, and have them present their ordering of the Adversary's Motivations cards, and why they chose that ordering.
7. Pick one or two groups, and have them present their ordering of the Adversary's Resources cards, and why they chose that ordering.
8. Pick one or two groups, and have them present their ordering of the Adversary's Methods cards, and why they chose that ordering.
9. Facilitate a discussion about the security and privacy risks with the chosen technology.
10. Facilitate a discussion about what students learned from this process. Were any of the issues they identified surprising to them?

As an alternative, the report-back for each dimension could happen after the students sort that dimension. For example, after sorting the Human Impacts, the students could present and explain their orderings of that dimension before sorting the Adversary's Motivations dimension.

Closure

11. If applicable, close by watching or reading related work (example systems on the web site) that explores relevant security threats to the system that students explored.

Add-ons

You may consider also incorporating one of the add-on activities listed on the web site.