The Security Cards – Multi-Dimensions of Threat Discovery

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 identify likely direct and indirect stakeholders in the system.
2. At the end of this unit: Given the description of a system, students should be able to argue how a compromised system might negatively impact direct or indirect stakeholder assets.
3. At the end of this unit: Given the description of a system, students should be able to identify at least 3 security threats that are relevant to the system.

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 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. **Identify Direct and Indirect Stakeholders (5 min).** Groups should identify direct stakeholders in the system—that is, a user or someone who otherwise has direct interaction with the system. Groups should also identify indirect stakeholders—that is, people who do not directly interact with the system, but who may nonetheless be affected by its usage or design.
5. **Identify Human Assets at Stake (7 min).** Using cards in the Human Impact dimension, groups should identify ways that the system could potentially be used or abused to negatively impact direct and indirect

stakeholders.

6. **Threat Surfacing Task: Multi-Dimension Combinations (10-15 min).**
    - **a.** Groups should spend time exploring potential threats to the system, where a threat is defined as a potential action from an adversary. Groups should consider a series of threats by (randomly or purposefully) selecting sets of cards; these sets should contain cards from at least two different dimensions (e.g., Adversary's Motivations and Adversary's Resources, or Adversary's Resources and Adversary's Methods).
    - b. Groups should discuss which 3 threats to the system are the most relevant to the system.
        - 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. The important thing here is to be able to explore and articulate what makes the different threats more or less relevant.

Report Back

7. Pick one or two groups, and have them present their identified stakeholders.
8. Pick one or two groups, and have them present the human assets that they identified might be impacted by system compromise.
9. Pick two or three groups, and have them present threats that they identified to the system.
10. Facilitate a discussion about the security and privacy risks with the chosen technology.
11. 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 could happen in stages. For example, after identifying the stakeholders, the students could present the stakeholders before identifying human assets.

Closure

12. 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.