The Security Cards:
A Security Threat Brainstorming Toolkit

securitycards.cs.washington.edu

Tamara Denning,[*] Batya Friedman,[‡] Tadayoshi Kohno[*]

[*]Security and Privacy Research Lab, Computer Science and Engineering, University of Washington
[‡]Value Sensitive Design Research Lab, The Information School , University of Washington

securitycards.cs.washington.edu

Purpose

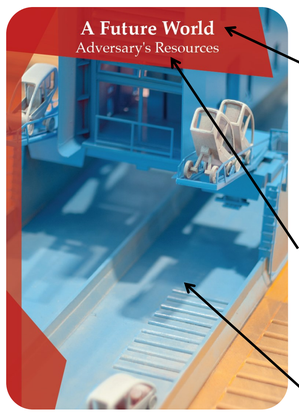
To facilitate the exploration of potential security threats for a particular system; and more broadly, to help develop a security mindset.

If your system is compromised, what **human assets** could be impacted?
Who might attack your system, and **why**?
What **resources** might the adversary have?
How might the adversary attack your system?

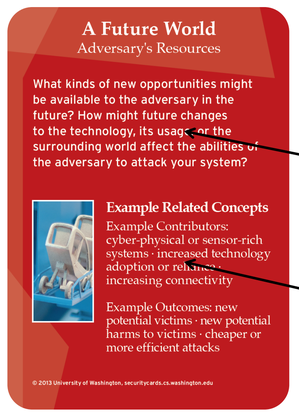
Audience

Educators (for their students), Researchers, and Practicing Professionals

Example Card



- Card topic
- Card dimension
  - Human Impact
  - Adversary's Motivations
  - Adversary's Resources
  - Adversary's Methods
- Evocative photograph



- Questions for clarification and to jumpstart thinking
- Illustrative examples

Card Titles

Human Impact

- The Biosphere
- Emotional Wellbeing
- Financial Wellbeing
- Personal Data
- Physical Wellbeing
- Relationships
- Societal Wellbeing
- Unusual Impacts

Adversary's Motivations

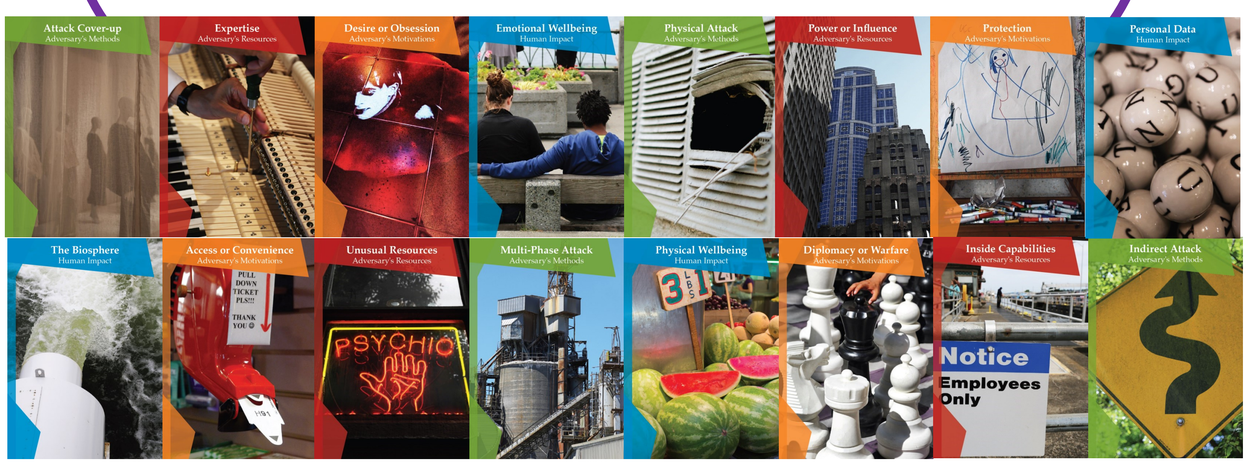
- Access or Convenience
- Curiosity or Boredom
- Desire or Obsession
- Diplomacy or Warfare
- Malice or Revenge
- Money
- Politics
- Protection
- Religion
- Self-Promotion
- World View
- Unusual Motivations

Adversary's Resources

- Expertise
- A Future World
- Impunity
- Inside Capabilities
- Inside Knowledge
- Money
- Power and Influence
- Time
- Tools
- Unusual Resources

Adversary's Methods

- Attack Cover-Up
- Indirect Attack
- Manipulation or Coercion
- Multi-Phase Attack
- Physical Attack
- Processes
- Technological Attack
- Unusual Methods



Example Activity

Full writeup and other activities available at securitycards.cs.washington.edu

1. Work in groups of 3-5.
2. Consider an example technology system or a system that you are designing.
3. Go through the deck and familiarize yourself with the dimensions and the cards. Make sure to read at least one card from each dimension in its entirety.
4. Within each dimension, rank cards in order of how relevant their topics are to your system and how much risk they present overall.
5. Why did you rank the cards in that order?
6. Have you surfaced particular attack scenarios? Do particular attacker profiles begin to emerge?

Card Graphic Design by Daisy Fry. Card Photography by Nell C. Grey, Daisy Yoo, and J. P. Arsenault. Developed in part through the support of NSF grants 0846065, 0905118, 0905384, 0963695, and 1353194. The cards are a collaboration of the Security and Privacy Research Lab (CSE) and the Value Sensitive Design Research Lab (iSchool) at the University of Washington.