Security and Privacy Threat Discovery Cards

The **Security and Privacy Threat Discovery Cards** encourage you to think broadly and creatively about computer security threats. Explore with 42 cards in 4 categories: Adversary's Motivations, Adversary's Resources, Adversary's Methods, and Human Impact, or use the included templates to make custom cards.

Find further information and possible card activities at: **securitycards.cs.washington.edu**

Developed by Tamara Denning, Batya Friedman, and Tadayoshi Kohno

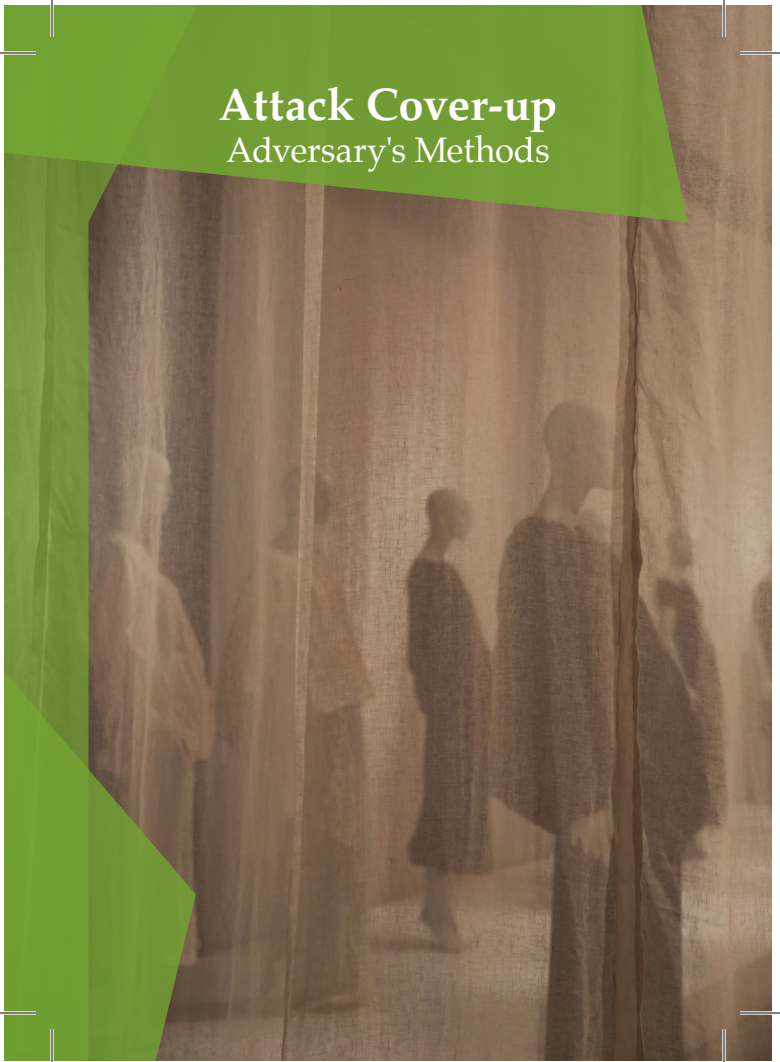
Photography by Nell C. Grey, Daisy Yoo, and J. P. Arsenault

Graphic Design by Daisy Fry

© 2013 University of Washington. This work is made available under the terms of the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license, http://creativecommons.org/licenses/by-nc-nd/3.0/.

The cards are a collaboration of the Security and Privacy Research Lab and the Value Sensitive Design Research Lab at the University of Washington. Developed in part through the support of NSF Grants 0846065, 0905118, 0905384, and 0963695.

Attack Cover-up
Adversary's Methods



Attack Cover-up
Adversary's Methods

How might the adversary alter the awareness, understanding, or evidence surrounding an attack? How would this enable or amplify an attack on confidentiality, integrity, or availability of the system or the system's data?

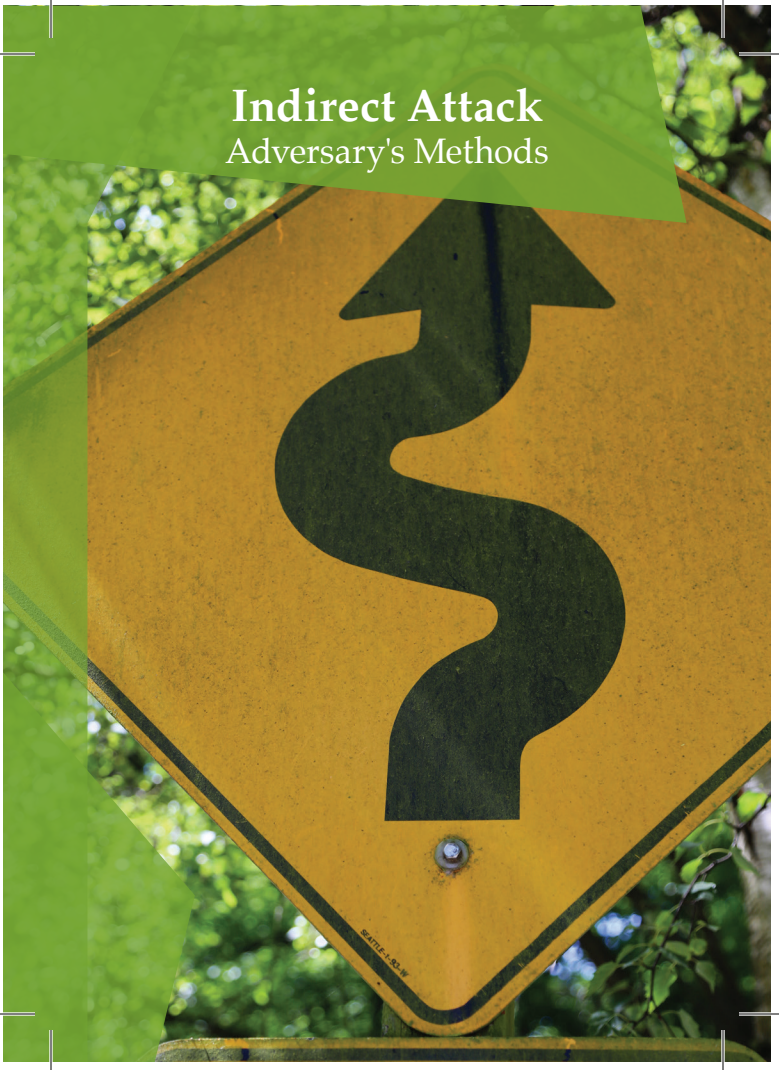
Example Related Concepts

Example Attacks: destroy hard drives · use an anonymizing proxy · use another attack as a distractor · subtle attack effect (e.g., fractional cent attack)

Example Outcomes: conceal the attack's existence · conceal attack effects · incriminate another party

© 2013 University of Washington, securitycards.cs.washington.edu

Indirect Attack
Adversary's Methods



Indirect Attack
Adversary's Methods

How might the adversary use an unexpected or overlooked system property in order to bypass your system's direct defenses? How would this enable or amplify an attack on confidentiality, integrity, or availability of the system or the system's data?

Example Related Concepts

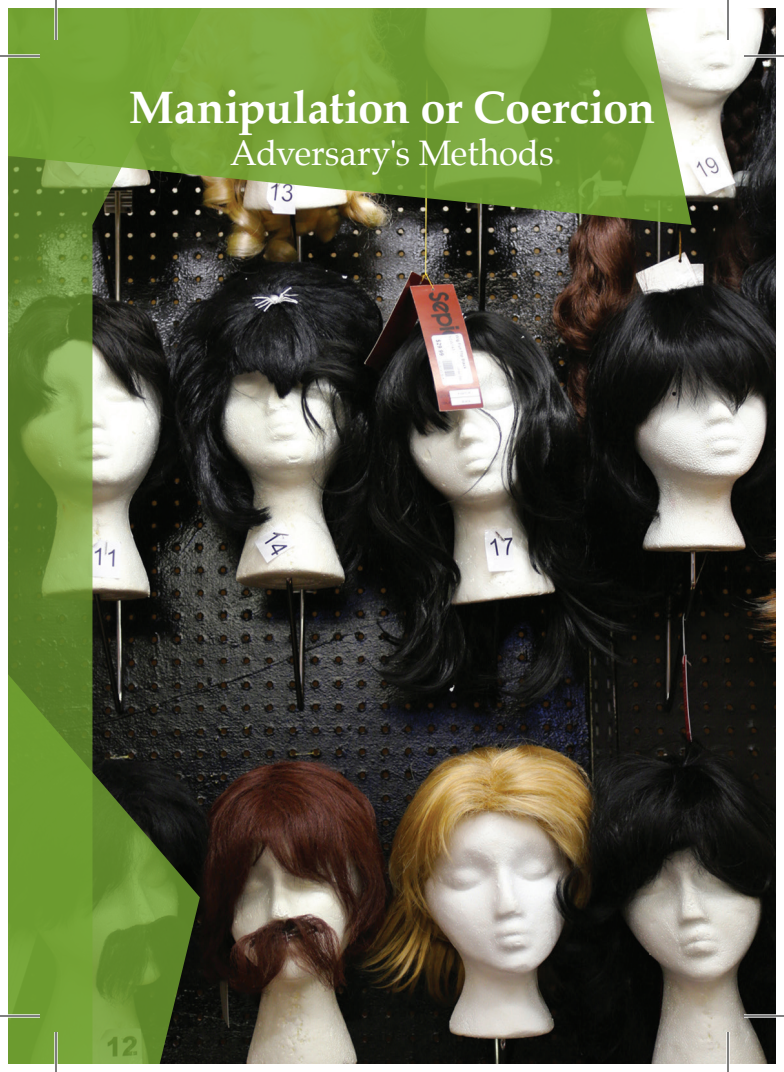
Example Attacks: timing attacks · monitoring electromagnetic emanations · power usage analysis

Example Outcomes: reconstruct passwords · reconstruct computer screen content

© 2013 University of Washington, securitycards.cs.washington.edu

Manipulation or Coercion

Adversary's Methods



Manipulation or Coercion

Adversary's Methods

How might the adversary manipulate or coerce people into divulging information or performing actions that affect your system's security? How would this enable or amplify an attack on confidentiality, integrity, or availability of the system or the system's data?

Example Related Concepts

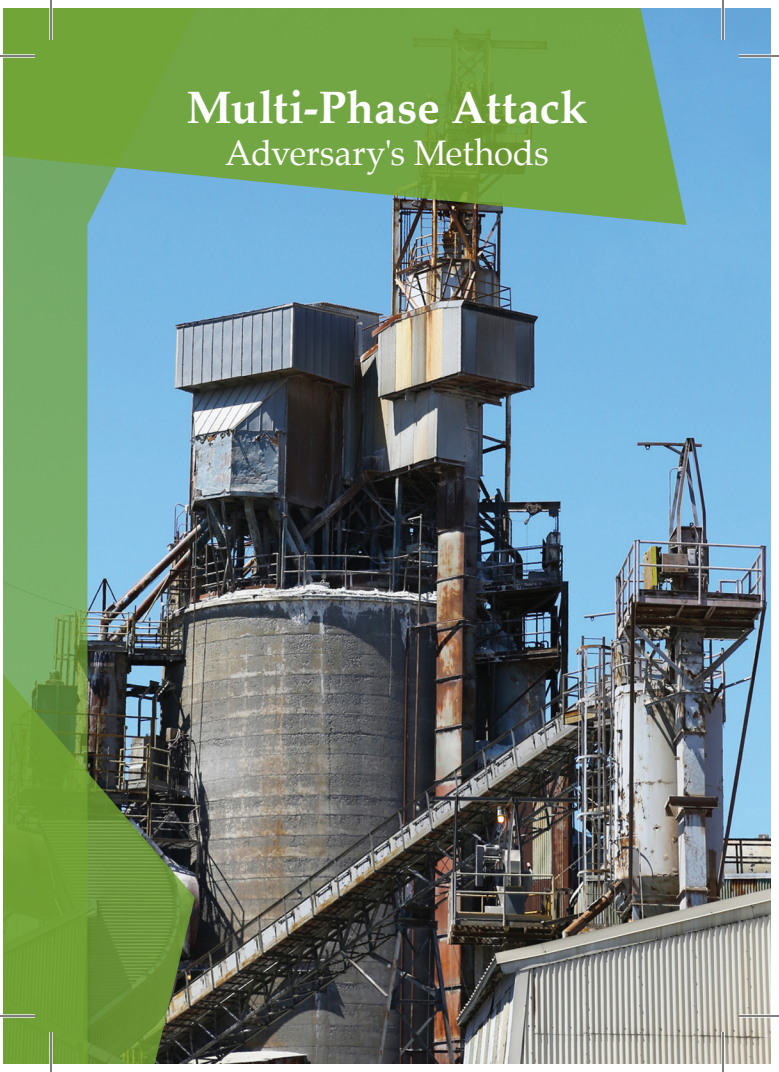
Example Attacks: impersonation · phishing · blackmail · bribery

Example Outcomes: change administrator passwords · obtain physical access · destroy audit logs

© 2013 University of Washington, securitycards.cs.washington.edu

Multi-Phase Attack

Adversary's Methods



Multi-Phase Attack

Adversary's Methods

How might the adversary leverage multiple attack phases on a single or multiple targets in order to execute more complicated or covert attacks? How would this enable or amplify an attack on confidentiality, integrity, or availability of the system or the system's data?

Example Related Concepts

Example Attacks: obtaining signing keys or certificates · altering whitelists or blacklists · staging attacks from compromised computers

Example Outcomes: exfiltrating data over time · bypassing a layer of security measures

© 2013 University of Washington, securitycards.cs.washington.edu

Physical Attack
Adversary's Methods

Physical Attack
Adversary's Methods

How might the adversary gain or take advantage of physical access to a system component? How would this enable or amplify an attack on confidentiality, integrity, or availability of the system or the system's data?

Example Related Concepts

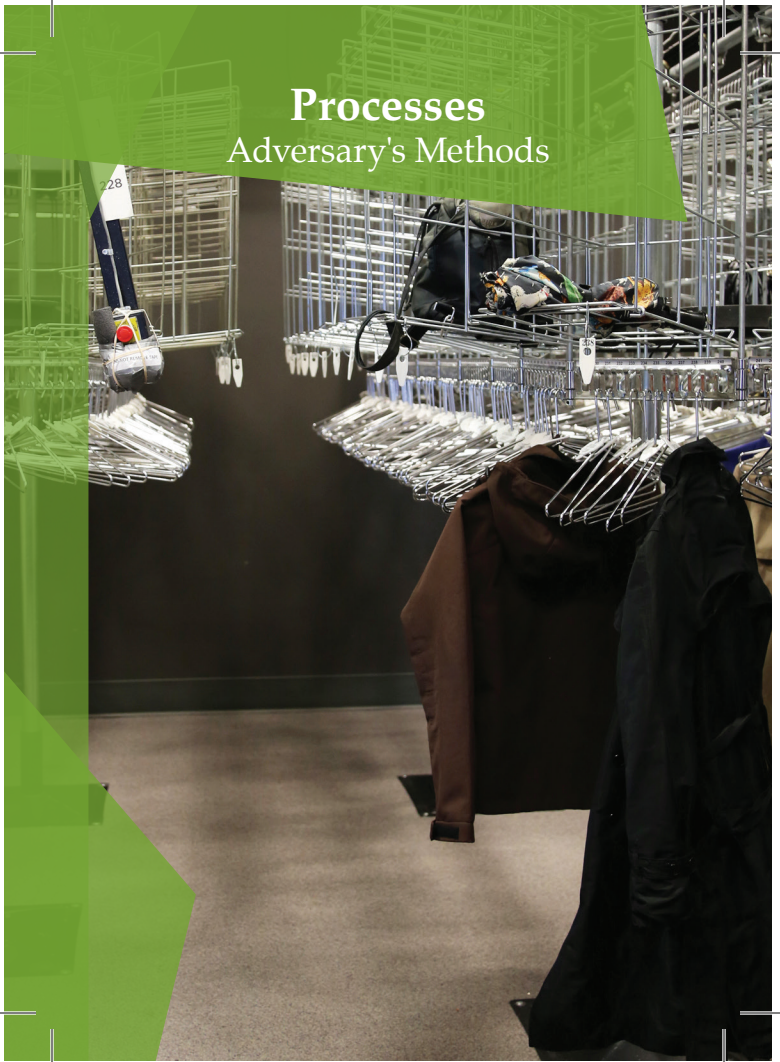
Example Attacks: wiretapping · tampering with hardware · installing software

Example Outcomes: install keyloggers · destroy equipment · access confidential files

© 2013 University of Washington, securitycards.cs.washington.edu

Processes

Adversary's Methods



Processes
Adversary's Methods

How might the adversary take advantage of technical or bureaucratic processes to perform an attack? How would this enable or amplify an attack on confidentiality, integrity, or availability of the system or the system's data?

Example Related Concepts

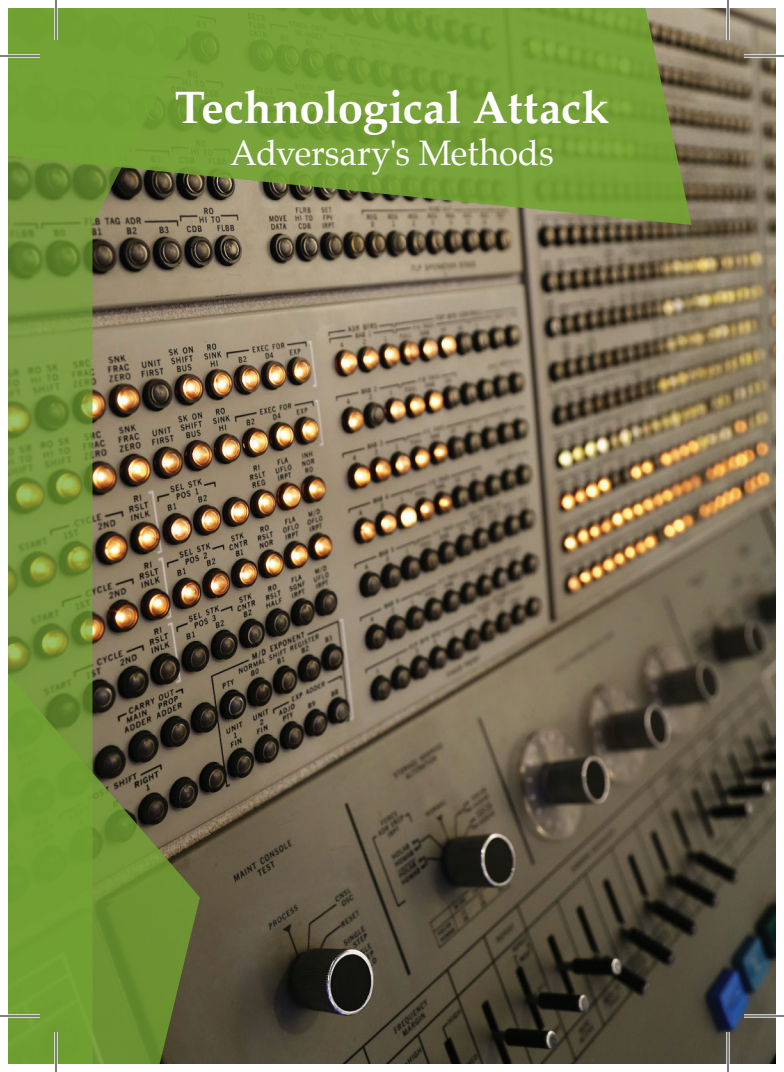
Example Processes: backups · password recovery · error recovery

Example Attacks: activate debug mode · try default passwords · con technical support

© 2013 University of Washington, securitycards.cs.washington.edu

Technological Attack

Adversary's Methods



Technological Attack
Adversary's Methods

What kinds of technical attacks might the adversary perform over an analog or digital link? How would this enable or amplify an attack on confidentiality, integrity, or availability?

Example Related Concepts

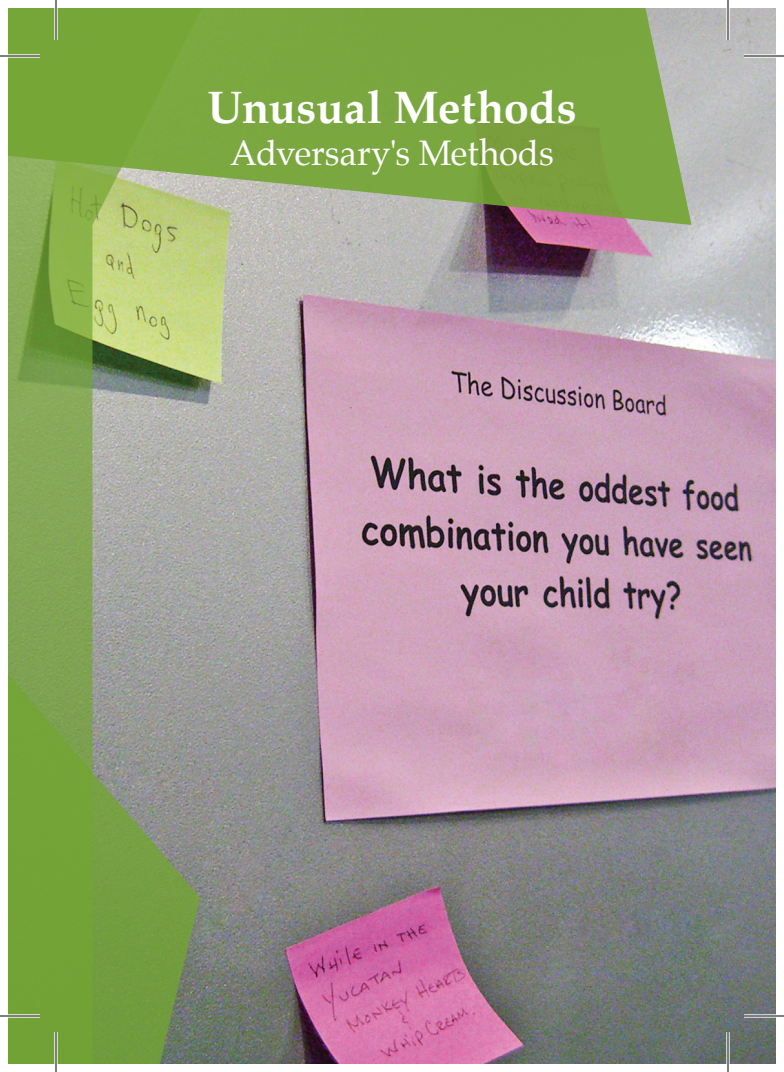
Example Attacks: denial-of-service · spoofing · repudiation · elevation of privilege · replay attacks · relay attacks · jamming

Example Outcomes: acquire password files · eavesdrop on confidential exchanges · install bot software

© 2013 University of Washington, securitycards.cs.washington.edu

Unusual Methods

Adversary's Methods



Unusual Methods

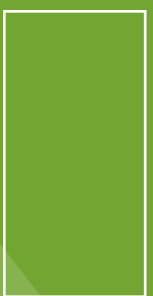
Adversary's Methods

What kinds of unusual methods might the adversary use to attack the system? How would this enable or amplify an attack on confidentiality, integrity, or availability of the system or the system's data?

© 2013 University of Washington, securitycards.cs.washington.edu

Adversary's Methods

Adversary's Methods



Example Related Concepts

© 2013 University of Washington, securitycards.cs.washington.edu

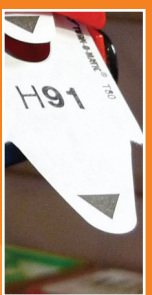
Access or Convenience

Adversary's Motivations

Access or Convenience

Adversary's Motivations

How might the adversary use or abuse your system for the purpose of convenience or to gain access to a resource? What kind of individual or group might target your system because it is more convenient than some alternative, or because it is the only way to achieve their goal?



Example Related Concepts

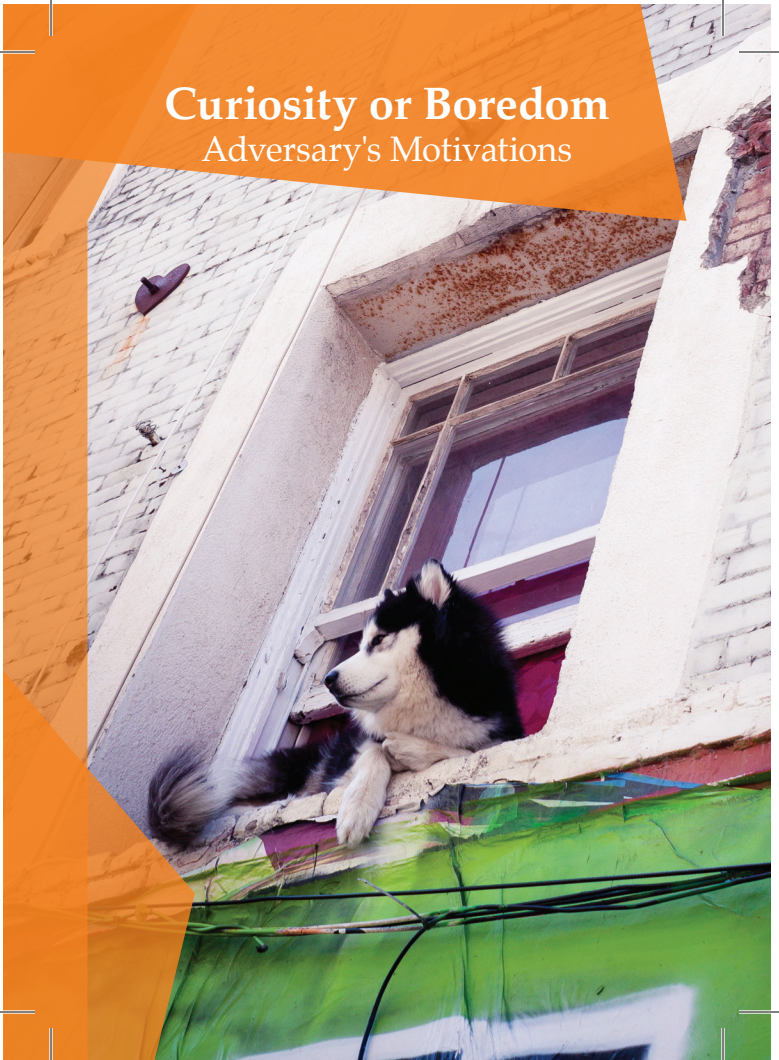
Example Targets: appointment-based online enrollment systems · sales of limited tickets · personal electronics with restricted permissions

Example Actions: modify personal electronics · bypass company filtering to access personal email · access a protected wireless network

© 2013 University of Washington, securitycards.cs.washington.edu

Curiosity or Boredom

Adversary's Motivations



Curiosity or Boredom

Adversary's Motivations

How might the adversary use or abuse your system to satisfy curiosity or to alleviate boredom? What kind of individual or group might target your system out of curiosity or boredom?

Example Related Concepts

Example Targets: acquaintances · strangers · institutions · celebrities

Example Actions: look up celebrity's medical record · browse personal photos · attack a random system

© 2013 University of Washington, securitycards.cs.washington.edu

Desire or Obsession

Adversary's Motivations

Desire or Obsession

Adversary's Motivations

How might the adversary use or abuse your system to feed a desire or obsession? What kind of individual or group might target your system due to a desire or obsession?

Example Related Concepts

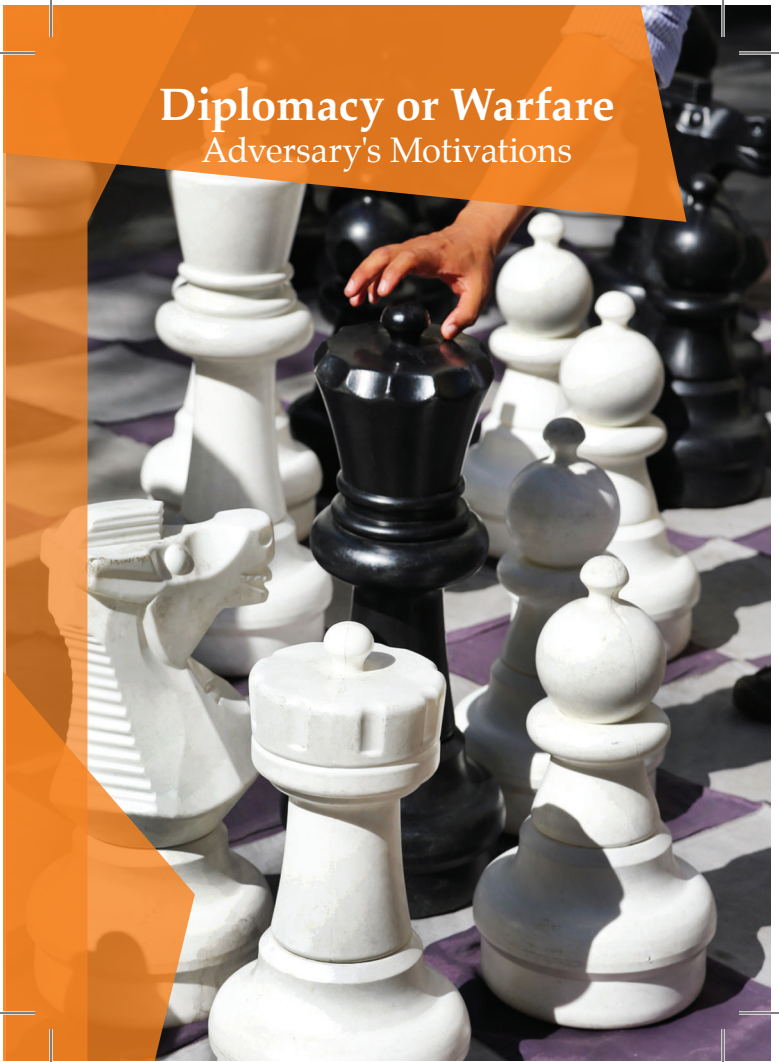
Example Targets: ex-boyfriend or -girlfriend · celebrities · children

Example Actions: harassing messages · sexual blackmail · covert webcam activation · monitoring communications · location tracking

© 2013 University of Washington, securitycards.cs.washington.edu

Diplomacy or Warfare

Adversary's Motivations



Diplomacy or Warfare

Adversary's Motivations

How might the adversary use or abuse your system to give them an edge in diplomacy or warfare? What kind of individual or group might target your system for these purposes?

Example Related Concepts

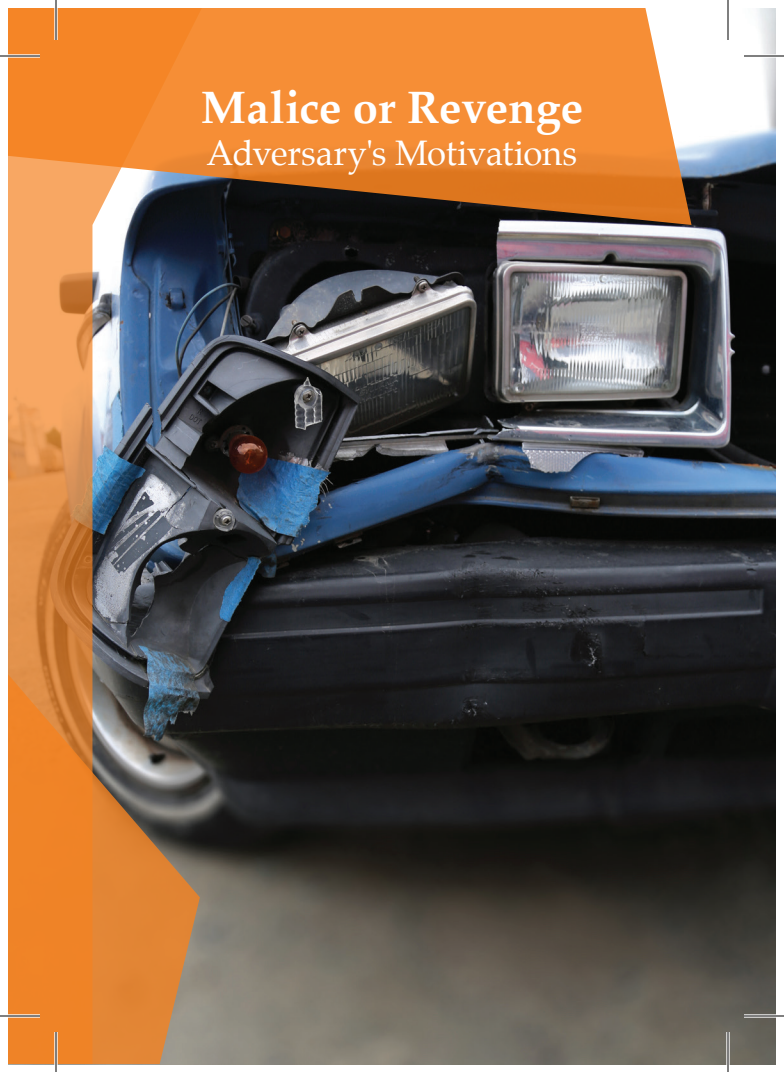
Example Targets: public infrastructure, cyber-physical, communication, and emergency systems

Example Goals: gather data · spread misinformation · track individuals · disable equipment · cause distractions · cause bodily harm · disable communications

© 2013 University of Washington, securitycards.cs.washington.edu

Malice or Revenge

Adversary's Motivations



Malice or Revenge

Adversary's Motivations

How might the adversary use or abuse your system for malice or to exact revenge? What kind of individual or group might target your system out of malice or revenge?

Example Related Concepts

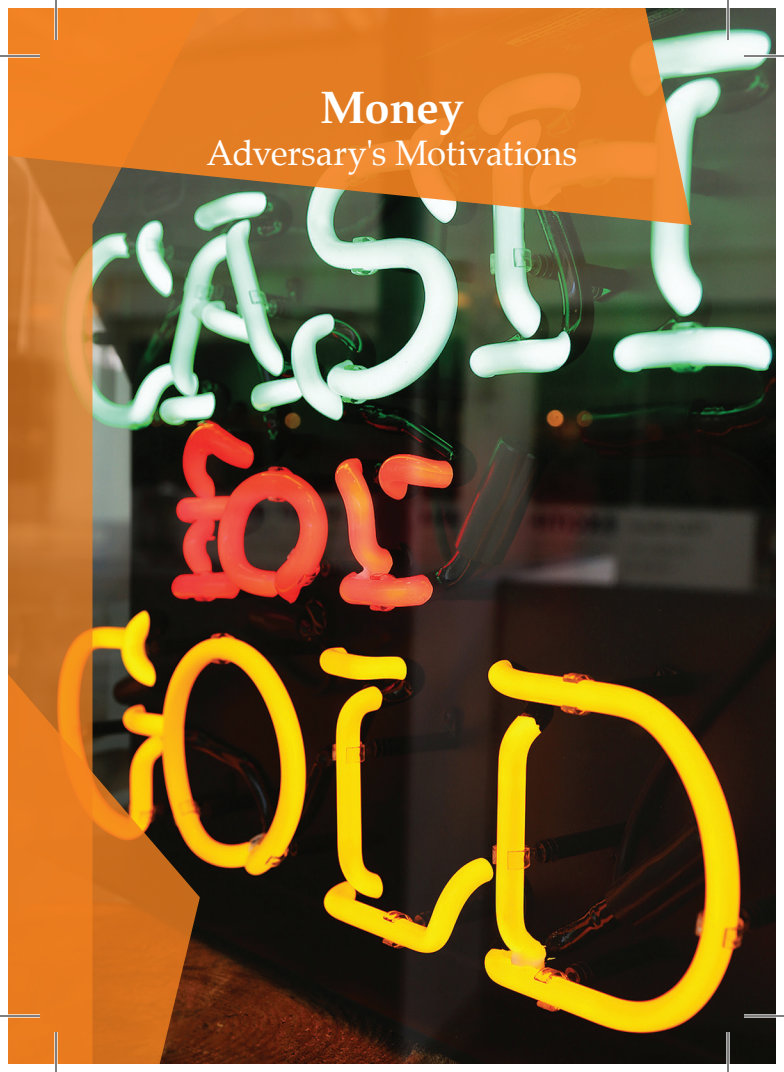
Example Targets: ex-employer · neighbor · rival

Example Actions: misinformation · cause physical harm · cause monetary damage · cause emotional damage

© 2013 University of Washington, securitycards.cs.washington.edu

Money

Adversary's Motivations



Money

Adversary's Motivations

How might the adversary use or abuse your system for financial gain? What kind of individual or group might target your system for financial gain?

Example Related Concepts

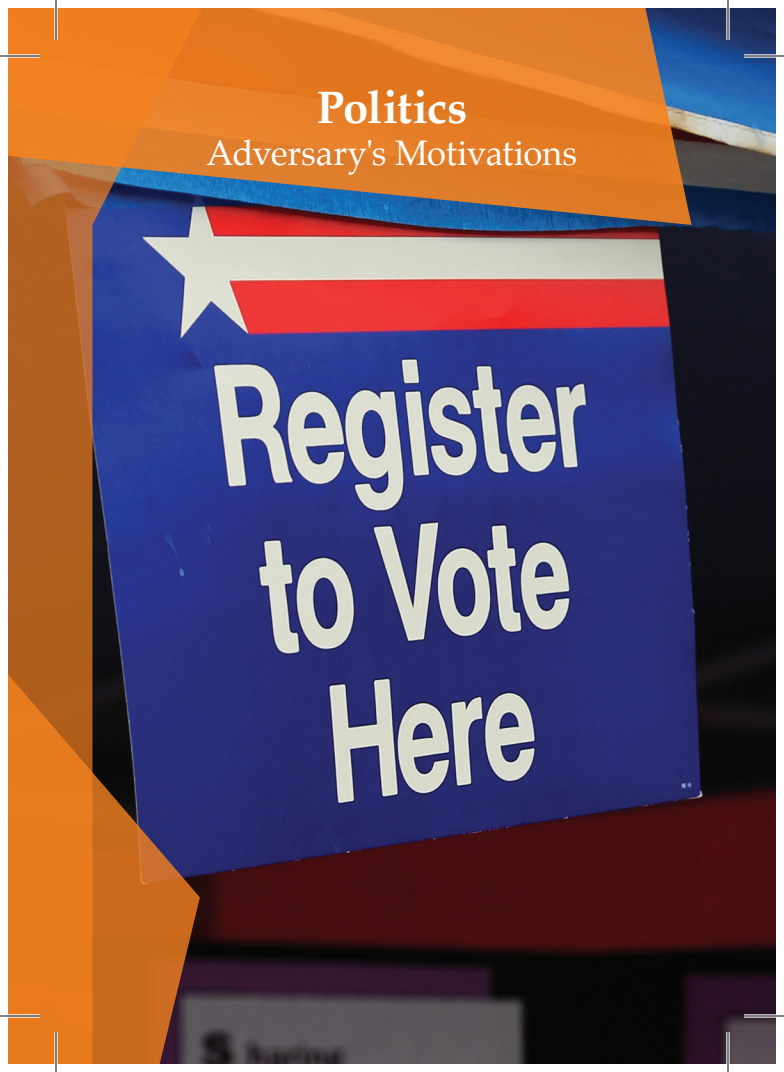
Example Goals: drain assets · sell DoS services · extort organization · sell user data · sabotage competitor's system · manipulate market

Example Actions: steal data · disclose data · misinformation · sabotage competitor's system

© 2013 University of Washington, securitycards.cs.washington.edu

Politics

Adversary's Motivations



Politics

Adversary's Motivations

How might the adversary use or abuse your system to affect politics? What kind of individual or group might target your system for political gain?

Example Related Concepts

Example Goals: alter, prevent, or invalidate votes · discredit political figures · alter the public's understanding or impression

Example Actions: DoS attack · steal data · disclose data · misinformation

© 2013 University of Washington, securitycards.cs.washington.edu

Protection

Adversary's Motivations

Protection
Adversary's Motivations

How might the adversary use or abuse your system for self-protection or to protect others? What kind of individual or group might target your system to protect something or someone?

Example Related Concepts

Example Targets: employers · government · family

Example Actions: monitor behavior · evade censorship · pre-emptive attack

© 2013 University of Washington, securitycards.cs.washington.edu

Religion
Adversary's Motivations

Religion

Adversary's Motivations

How might the adversary use or abuse your system to further a religious agenda? What kind of individual or group might target your system for religious reasons?

Example Related Concepts

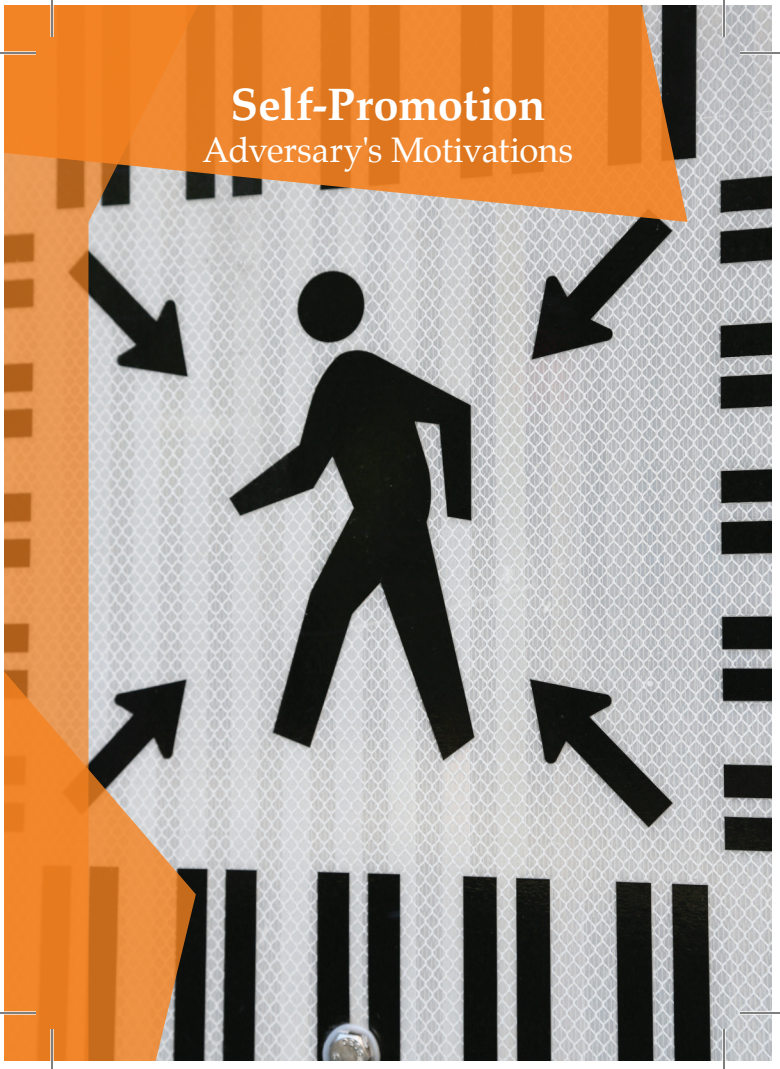
Example Goals: spread information about beliefs · discredit another group

Example Actions: disclose data · misinformation · cause physical harm · cause monetary damage

© 2013 University of Washington, securitycards.cs.washington.edu

Self-Promotion

Adversary's Motivations



Self-Promotion

Adversary's Motivations

How might the adversary use or abuse your system for self-promotion or to gain notoriety? What kind of individual or group might target your system out of a desire for self-promotion or notoriety?

Example Related Concepts

Example Targets: systems with personal information · prominent systems · challenging systems

Example Actions: change grades · redact information · deface a corporate website · crack an encryption scheme

© 2013 University of Washington, securitycards.cs.washington.edu

Unusual Motivations

Adversary's Methods

Unusual Motivations
Adversary's Methods

What other, unusual motivations might drive an individual or a group? How would the adversary use or abuse your system to further this cause? What kind of adversary might target your system with this motivation?

© 2013 University of Washington, securitycards.cs.washington.edu

World View

Adversary's Motivations

World View

Adversary's Motivations

How might the adversary use or abuse your system to further a particular ideological outlook? What kind of individual or group might target your system for ideological reasons?

Example Related Concepts

Example Issues: corporations · environmentalism · reproductive rights · drugs · violence · sexuality

Example Actions: DoS attack · disclose data · misinformation · cause physical harm · cause monetary damage

© 2013 University of Washington, securitycards.cs.washington.edu

Adversary's Motivations

Adversary's Motivations

Example Related Concepts

© 2013 University of Washington, securitycards.cs.washington.edu

Expertise

Adversary's Resources

Expertise

Adversary's Resources

What levels of expertise does the adversary have (or have access to)? How do different kinds of expertise allow the adversary to execute a broader range of attacks on your system?

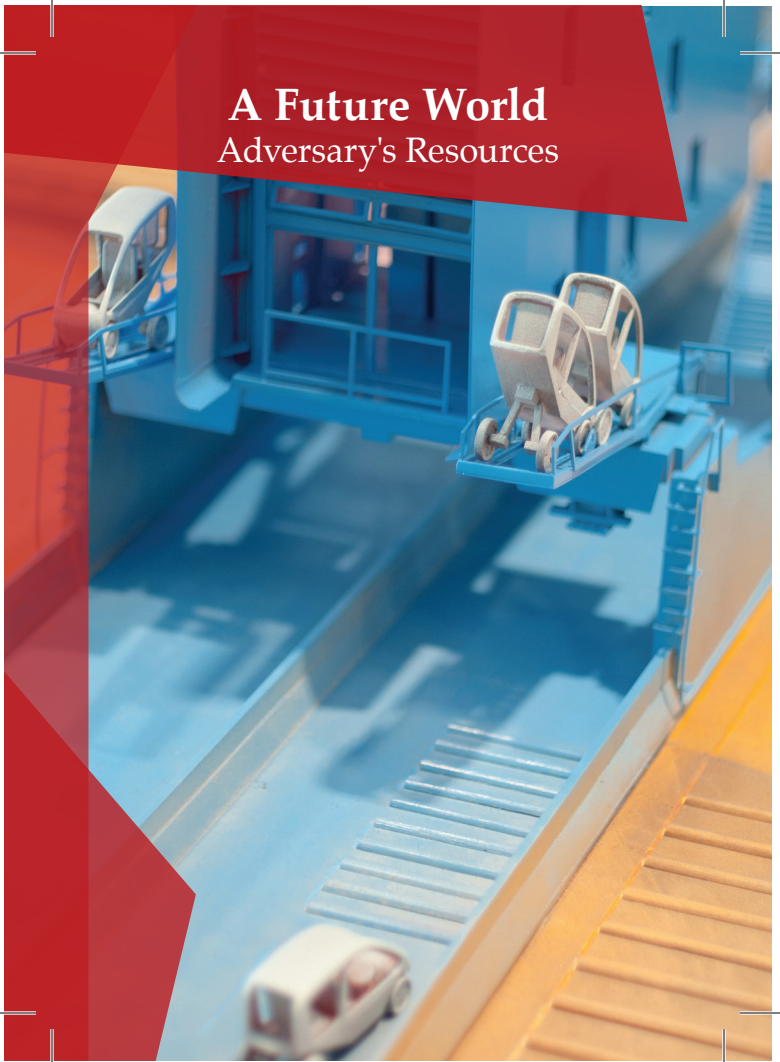
Example Related Concepts

Example Expertise: novice at network penetration · expert at picking locks · proficient con artist

Example Contributors: hobbyist adversary · government adversary

© 2013 University of Washington, securitycards.cs.washington.edu

A Future World
Adversary's Resources



A Future World

Adversary's Resources

What kinds of new opportunities might be available to the adversary in the future? How might future changes to the technology, its usage, or the surrounding world affect the abilities of the adversary to attack your system?

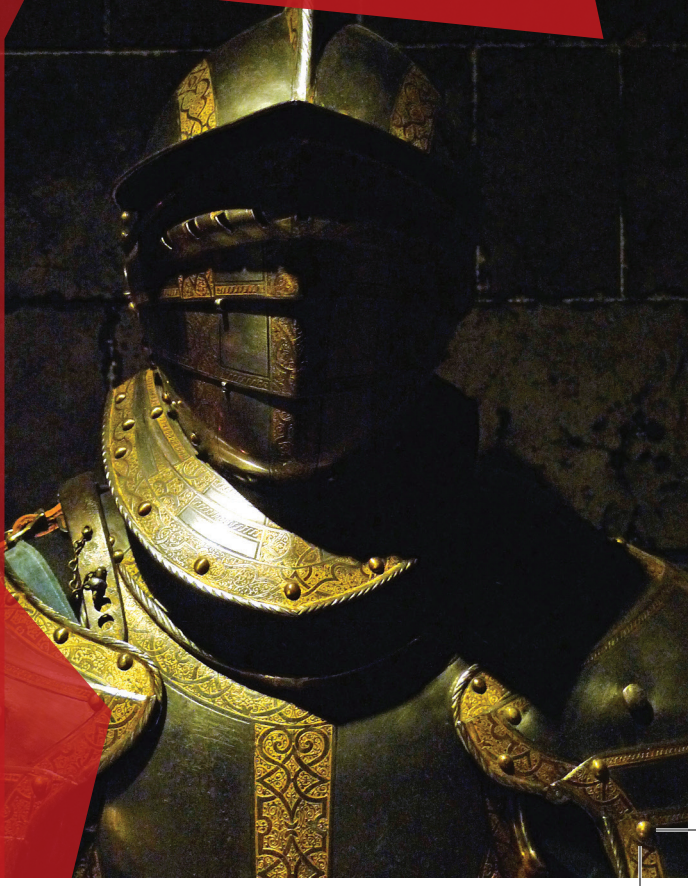
Example Related Concepts

Example Contributors: cyber-physical or sensor-rich systems · increased technology adoption or reliance · increasing connectivity

Example Outcomes: new potential victims · new potential harms to victims · cheaper or more efficient attacks

© 2013 University of Washington, securitycards.cs.washington.edu

Impunity
Adversary's Resources



Impunity
Adversary's Resources

What kinds of impunity might the adversary have? How might impunity for their actions make adversaries free to execute more frequent, longer-lasting, or more obvious attacks on your system?

Example Related Concepts

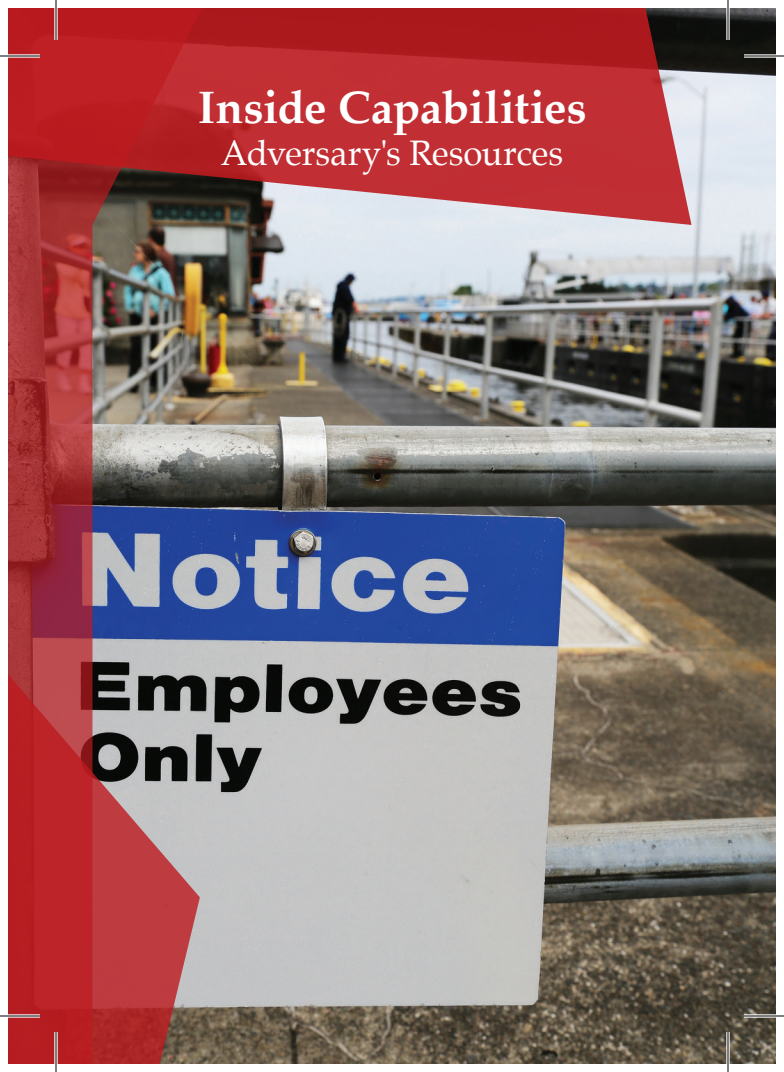
Example Causes: unafraid of incarceration · government sponsorship · utilizing network proxies and redirection

Example Contributors: geo-political diversity · anonymity

© 2013 University of Washington, securitycards.cs.washington.edu

Inside Capabilities

Adversary's Resources



Inside Capabilities

Adversary's Resources

What kinds of inside capabilities might the adversary have (or gain) access to? How might inside access or influence allow the adversary to execute new or more effective attacks on your system?

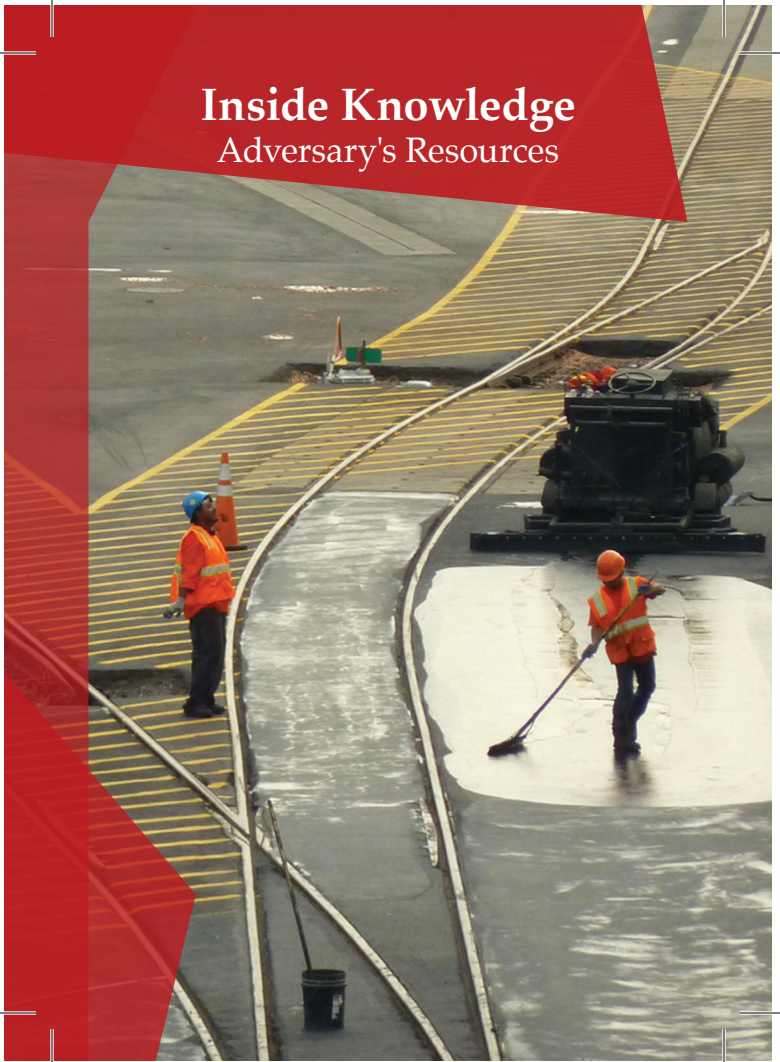
Example Related Concepts

Example Capabilities: physical access · user or admin account · system backdoors · affect system design

Example Sources: a collaborating insider · blackmail · bribery · counterfeit hardware

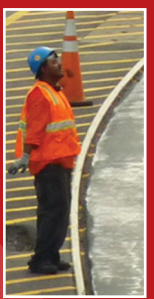
© 2013 University of Washington, securitycards.cs.washington.edu

Inside Knowledge
Adversary's Resources



Inside Knowledge
Adversary's Resources

What kinds of inside knowledge might the adversary have (or gain) access to? How might inside knowledge allow the adversary to execute new or more effective attacks on your system?



Example Related Concepts

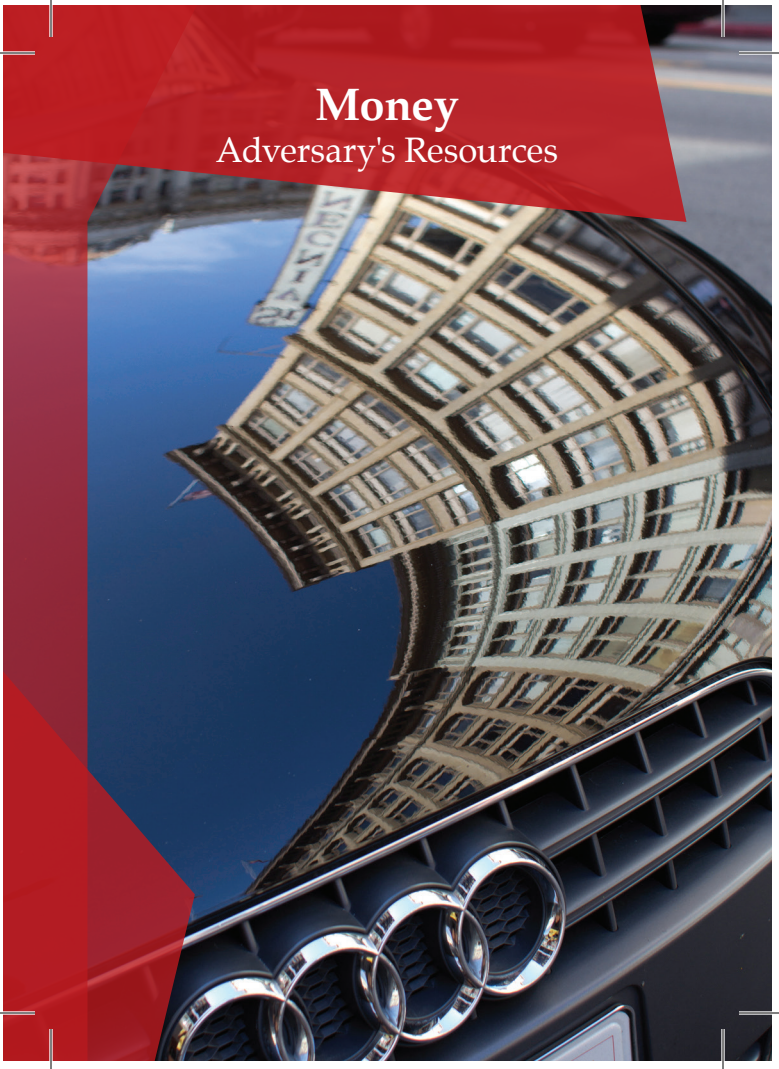
Example Knowledge: design documents · system usage or maintenance patterns · implementation details · bureaucratic processes

Example Sources: employment · a collaborating insider · discarded documents

© 2013 University of Washington, securitycards.cs.washington.edu

Money

Adversary's Resources



Money

Adversary's Resources

What kinds of liquid assets might the adversary have access to? How might different levels of liquid assets amplify or enable attacks on your system?

Example Related Concepts

Example Contributors: organized crime adversary · corporate adversary

Example Uses: pay bribes · purchase equipment · hire help

© 2013 University of Washington, securitycards.cs.washington.edu

Power or Influence

Adversary's Resources

Power or Influence

Adversary's Resources

What kinds of power or influence does the adversary have? How can the adversary leverage them to amplify or enable attacks on your system?

Example Related Concepts

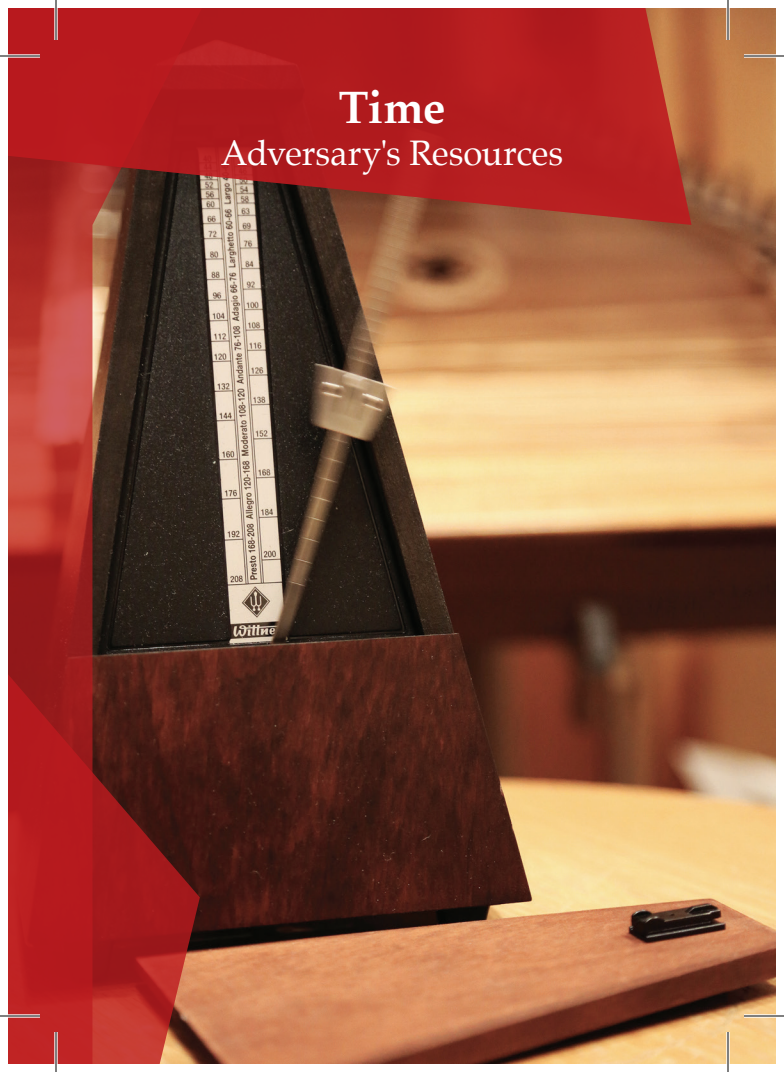
Example Uses: mobilize large volunteer force · affect laws or regulations · coerce employees

Example Contributors: government adversary · religious or movement leader

© 2013 University of Washington, securitycards.cs.washington.edu

Time

Adversary's Resources



Time

Adversary's Resources

What kinds of time limits does the adversary have (or not have) on attacks? How do different timeframes allow the adversary to execute different kinds of attacks or cause more damage to your system?

Example Related Concepts

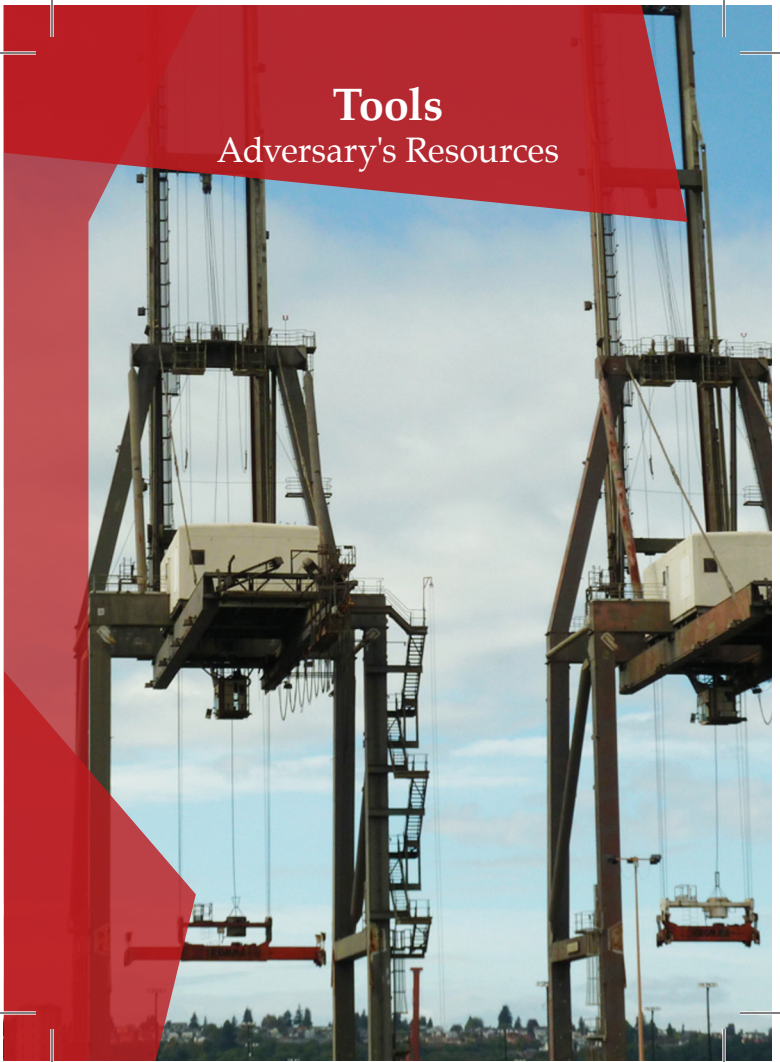
Example Timeframes: seconds · hours · decades

Example Contributors: a current or upcoming event (e.g. election) · ability to execute a time-independent attack · scheduled system maintenance

© 2013 University of Washington, securitycards.cs.washington.edu

Tools

Adversary's Resources



Tools

Adversary's Resources

What kinds of specialized or generic hardware, software, or other equipment might the adversary have access to? How might different kinds of tools allow the adversary to execute new or more effective attacks on your system?

Example Related Concepts

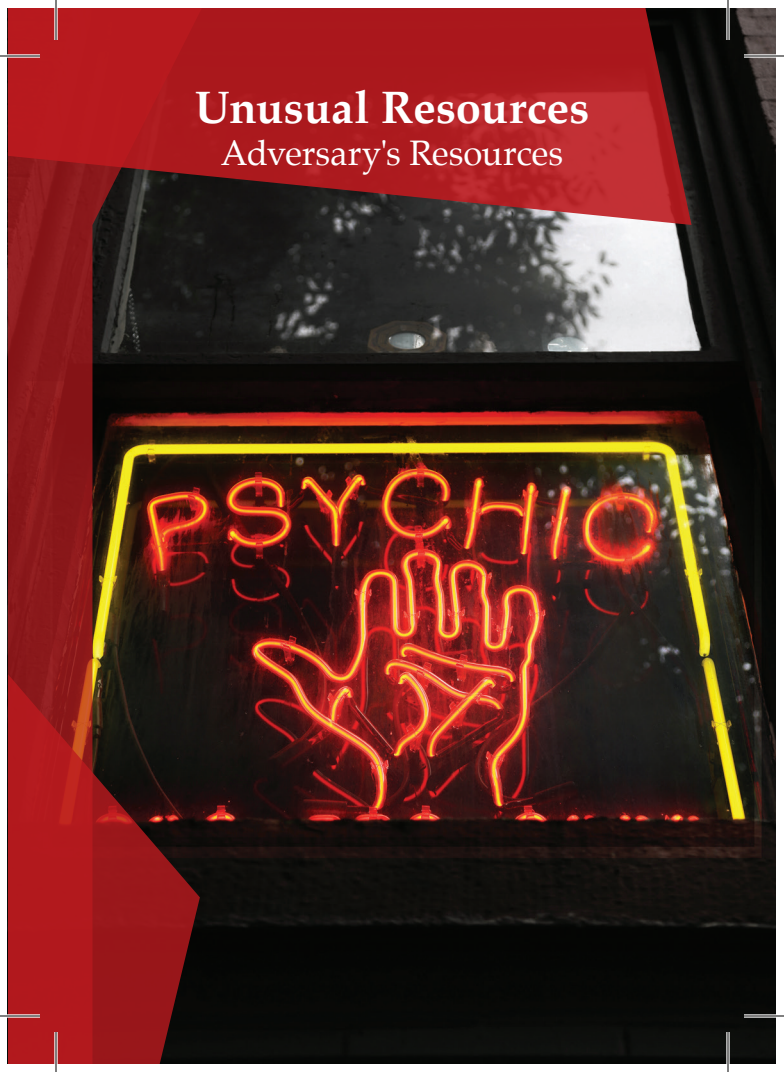
Example Tools: cryptographic key crackers · reverse engineering tools · helicopters

Example Contributors: hobbyist adversary · government adversary · corporate adversary

© 2013 University of Washington, securitycards.cs.washington.edu

Unusual Resources

Adversary's Resources



Unusual Resources

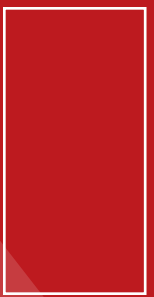
Adversary's Resources

What kinds of unexpected or uncommon resources might the adversary have access to? How might unusual resources enable or amplify attacks on your system?

© 2013 University of Washington, securitycards.cs.washington.edu

Adversary's Resources

Adversary's Resources



Example Related Concepts

© 2013 University of Washington, securitycards.cs.washington.edu

Emotional Wellbeing

Human Impact

Emotional Wellbeing

Human Impact

How might your system have direct or indirect impact on people's emotional or mental wellbeing? How might data or system unavailability, unauthorized alterations, or confidentiality breaches cause harm?

Example Related Concepts

Example Assets: attachment to keepsakes · peace of mind · convenience

Example Outcomes: cause fear, anger, loneliness, or confusion

© 2013 University of Washington, securitycards.cs.washington.edu

Financial Wellbeing

Human Impact

Financial Wellbeing

Human Impact

How might your system have direct or indirect impact on people's financial assets or worldly possessions? How might data or system unavailability, unauthorized alterations, or confidentiality breaches cause harm?

Example Related Concepts

Example Targets: electronic home-entry systems · online bank credentials

Example Attacks: theft · extortion or blackmail

© 2013 University of Washington, securitycards.cs.washington.edu

Personal Data
Human Impact

Personal Data
Human Impact

What kinds of personal data does (or could) your system collect, store, or share? How might current or future compromise, corruption, or unavailability of this data cause harm?

Example Related Concepts

Example Data: medical records · embarrassing pictures · browsing history

Example Uses: perform identity theft · perform blackmail · delete financial records

© 2013 University of Washington, securitycards.cs.washington.edu

Physical Wellbeing

Human Impact

Physical Wellbeing

Human Impact

How might your system have direct or indirect impact on people's physical wellbeing? How might data or system unavailability, unauthorized alterations, or confidentiality breaches cause harm?

Example Related Concepts

Example Assets: access to food and water · access to electricity · an individual's location

Example Targets: medical devices · cars · medication or allergy records

© 2013 University of Washington, securitycards.cs.washington.edu

Relationships
Human Impact

Relationships
Human Impact

How might your system have direct or indirect impact on relationships? How might data or system unavailability, unauthorized alterations, or confidentiality breaches cause harm?

Example Related Concepts

Example Relationships: interpersonal · inter-organizational · international

Example Outcomes: damage a company's reputation · cause family arguments

© 2013 University of Washington, securitycards.cs.washington.edu

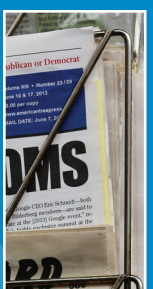
Societal Wellbeing

Human Impact

Societal Wellbeing

Human Impact

How might your system have direct or indirect impact on the financial, physical, or emotional wellbeing of a society? How might data or system unavailability, unauthorized alterations, or confidentiality breaches cause harm?



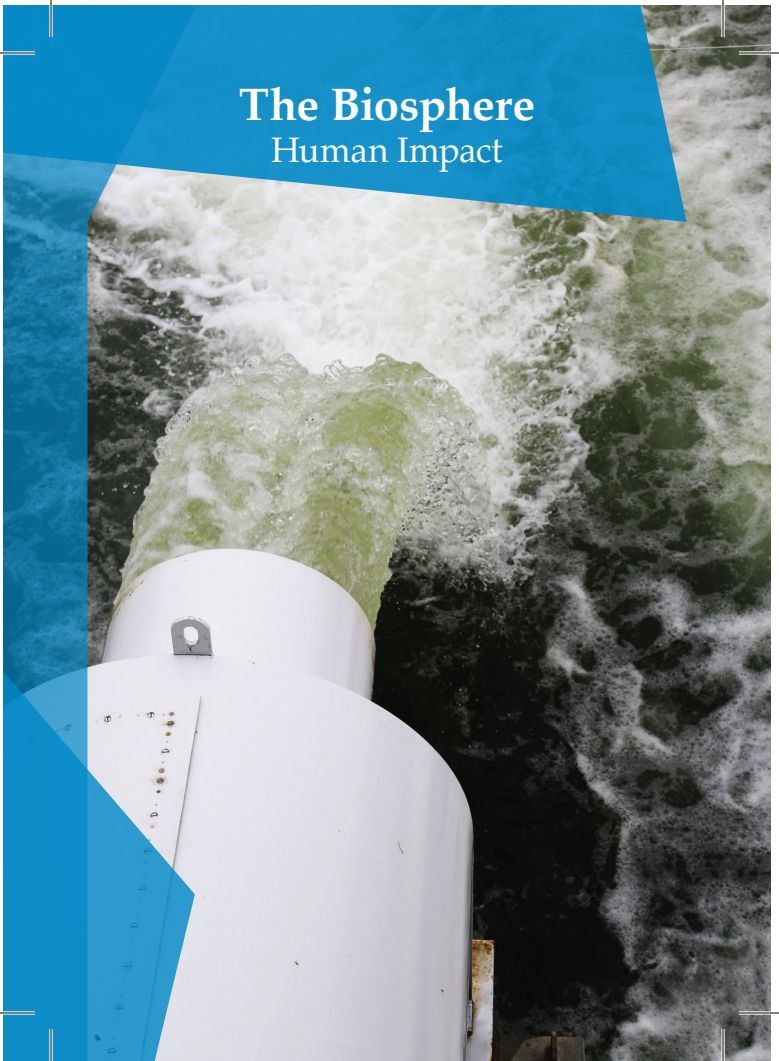
Example Related Concepts

Example Outcomes: create mass hysteria · alter public discourse · cause physical harm · affect access to resources

Example Targets: online voting systems · public infrastructure and cyber-physical systems · government record databases

© 2013 University of Washington, securitycards.cs.washington.edu

The Biosphere
Human Impact



The Biosphere
Human Impact

How might your system have direct or indirect environmental impacts? How might data or system unavailability, unauthorized alterations, or confidentiality breaches cause harm?

Example Related Concepts

Example Outcomes: use excessive resources · pollute water sources · cause fires

Example Targets: public infrastructure and cyber-physical systems · data centers

© 2013 University of Washington, securitycards.cs.washington.edu

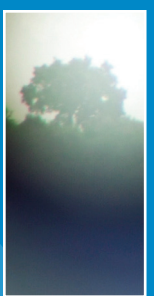
Unusual Impacts

Human Impact

Unusual Impacts

Human Impact

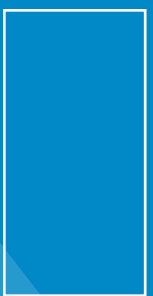
What kinds of special or unique values might be impacted by your system? How might data or system unavailability, unauthorized alterations, or confidentiality breaches cause harm?



© 2013 University of Washington, securitycards.cs.washington.edu

Human Impact

Human Impact



Example Related Concepts

© 2013 University of Washington, securitycards.cs.washington.edu