Security (Threats):
Teaching, Exploring, Communicating

Tamara Denning

School of Computing
University of Utah

Internet of Things: The Landscape

Connectivity

Sensors

Actuators

Usage Scenario

A New Landscape of Attack Impacts

A New Landscape of Attack Impacts

A New Landscape of Attack Impacts

A New Landscape of Attack Impacts

Forbes

New Posts | Most Popular: The WhatsApp Billionaires | Lists: The Business Of Nascar | Vi Oly

12 Stocks to BUY for 2014

0 Share 0 0 Share 8 reddit 0 Submit

Kashmir Hill, Forbes Staff

Welcome to The Not-So Private Parts where technology & privacy collide

+ Follow (1,716)

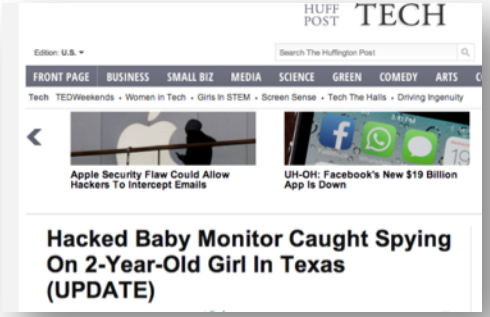
TECH | 7/05/2011 @ 7:58AM | 35,022 views

Fitbit Moves Quickly After Users' Sex Stats Exposed

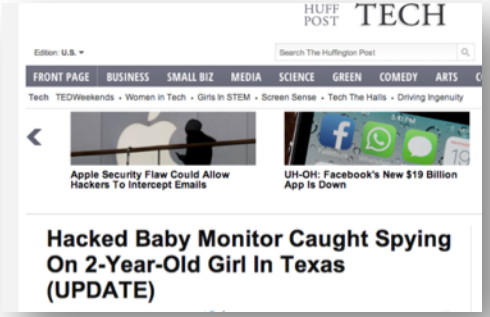
+ Comment Now + Follow Comments

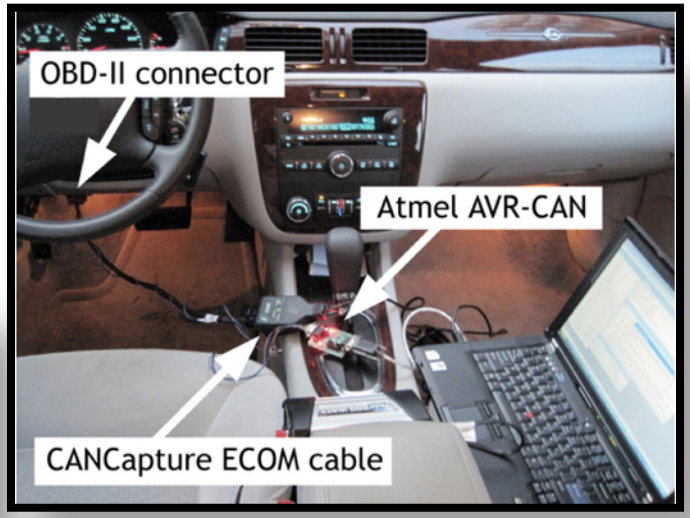
Over the holiday weekend, there were fireworks over at Fitbit.com after techie Andy Baio noticed that the self-trackers the company caters to were revealing their sexual activity stats online.

A New Landscape of Attack Impacts

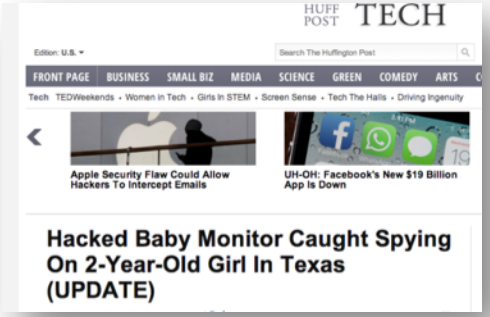


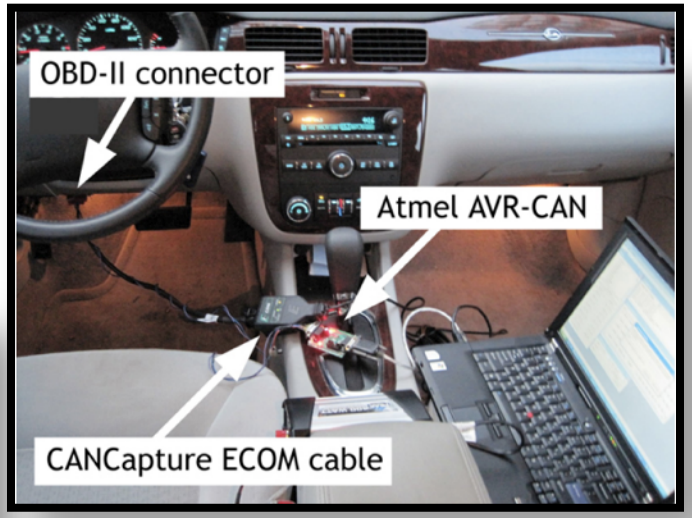
A New Landscape of Attack Impacts





A New Landscape of Attack Impacts

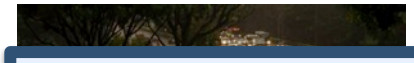




Internet of Things: The Landscape

Connectivity

Sensors



These technologies need to be secured.

Actuators

Usage Scenario

A (Related) Detour

Human-Centered

How can people be hurt?

Human-Centered

How can people be hurt?

What do people want?

Human-Centered

How can people be hurt?

What do people want…
Security + Privacy?

Human-Centered

How can people be hurt?

What do people want…
Surrounding Context?

Human-Centered

How can people be hurt?

What do people want?

How can we design systems?

Human-Centered

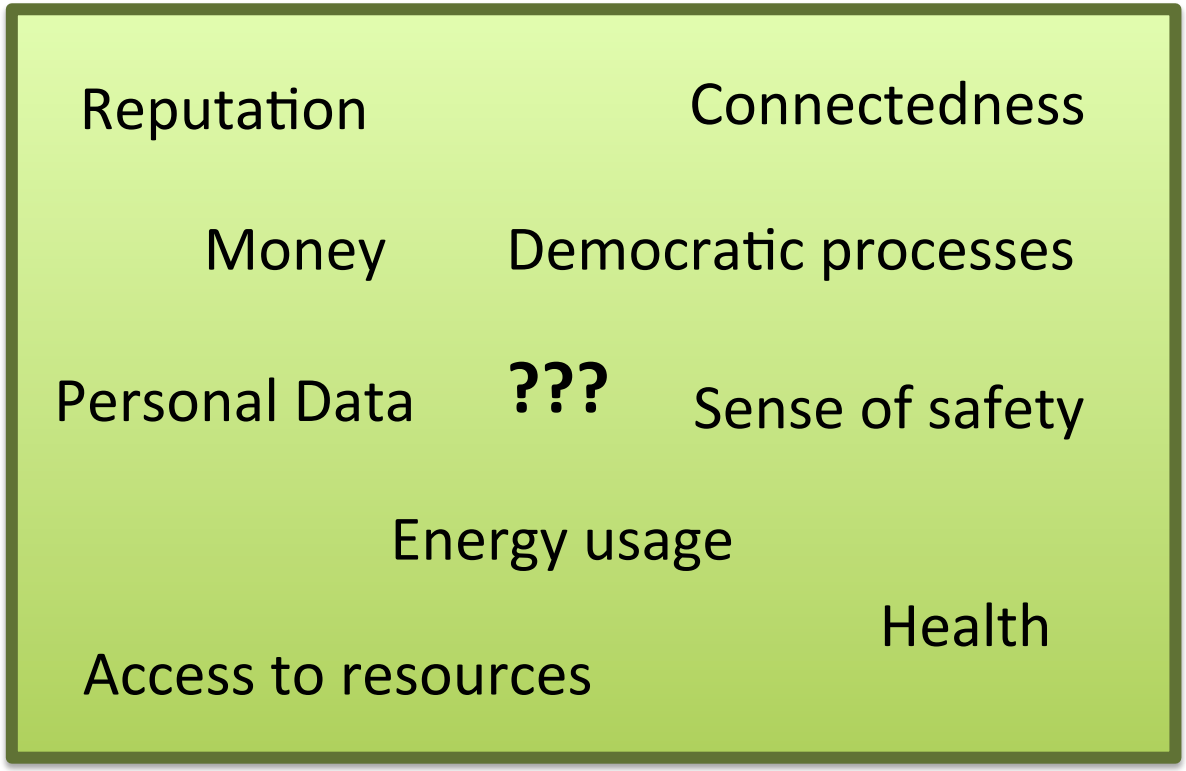
How can people be hurt?

What do people want?

How can we design systems?

How can we inform/explore?

Human Assets: Broadly Defined



Security Costs: Broadly Defined

Development time

Stress

Money

Decreased functionality

Training time

???

Usage time

Failed tasks

Maintenance time

Attention

Incompatibility

Implantable Medical Devices

Connectivity

implantable defibrillator (ICD)

Sensors

continuous glucose monitoring

Actuators

drug pump

Usage Scenario

Memory therapy (hippocampus)

Depression

Prosthetic limbs + exoskeletons

Parkinson's

Implantable Cardiac Devices

- Pacemakers
  - Correct for slow heart rhythms
  - Correct for *no* heart rhythm

- Implantable Cardioverter-Defibrillators
  - “Reset” potentially fatal heart rhythms

Wireless ICD Security

- **Need more security**
  1. **No individualized security**
  2. **Demonstrated security vulnerabilities**

Human-Centered

How can people be hurt?

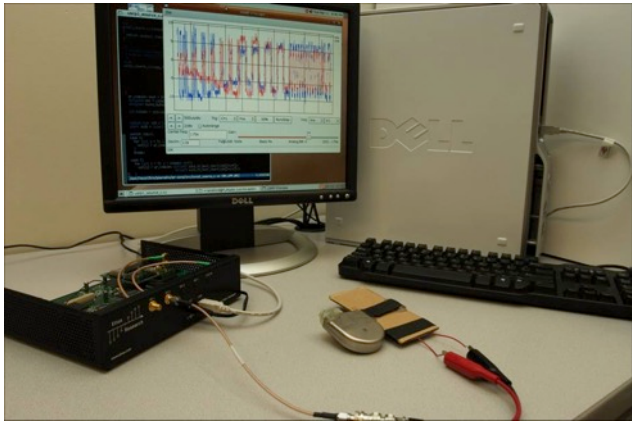
What do people want?

How can we design systems?

How can we inform/explore?

Wireless ICD Security & Impacts

- Private information
  - Obtain serial number, patient name, diagnosis
- Health impacts
  - Turn off therapies (defibrillation)
  - Induce cardiac fibrillation



Securing Implantable Cardiac Devices

More security is needed

Securing Implantable Cardiac Devices

More security is needed

- **Proposal:** Password on file

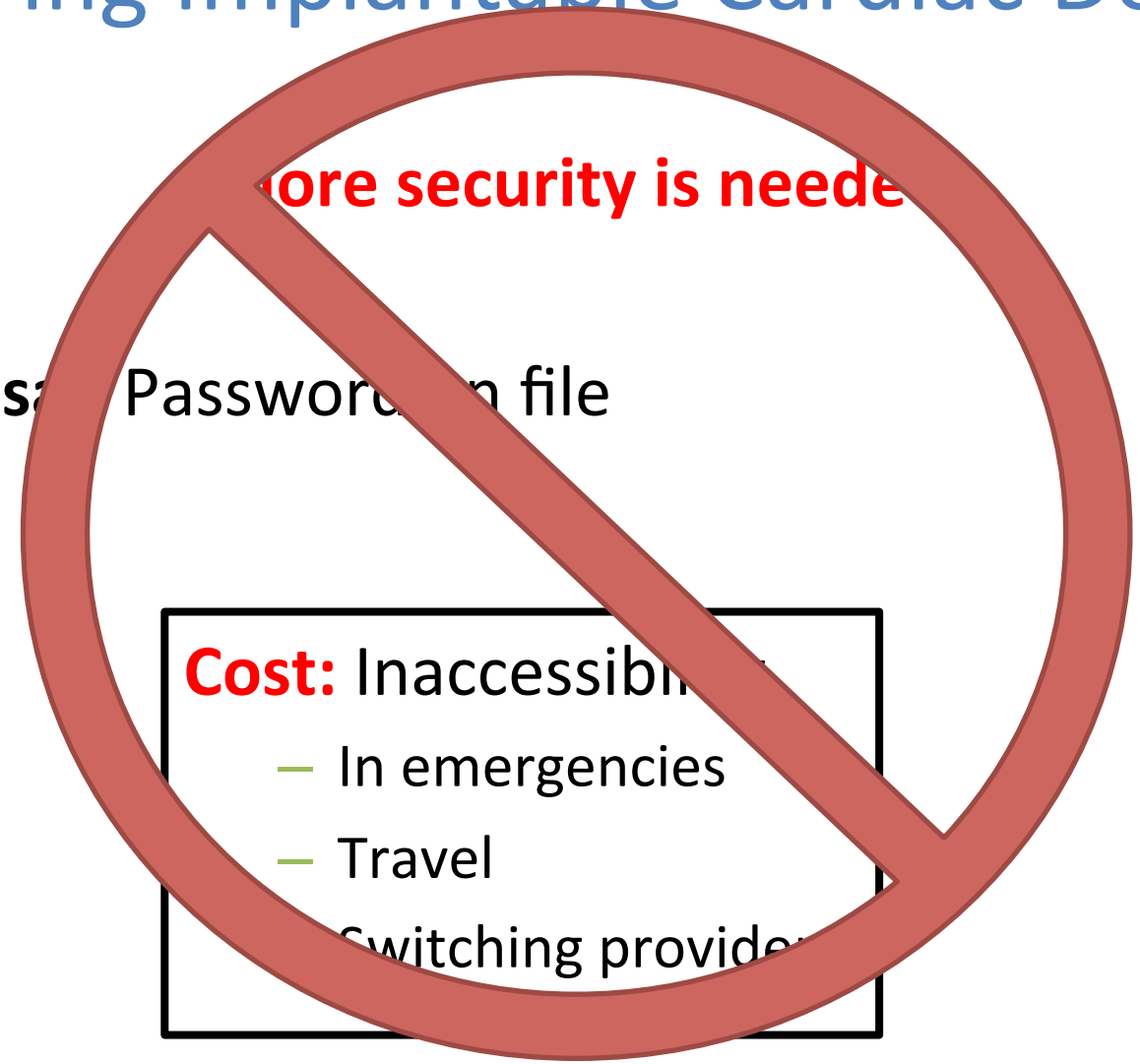
Securing Implantable Cardiac Devices

More security is needed

- **Proposal:** Password on file

Cost: Inaccessibility
- In emergencies
- Travel
- Switching providers

Securing Implantable Cardiac Devices



- **Proposa** Password n file

Human-Centered

How can people be hurt?

What do people want…
Surrounding Context?

How can we design systems?

How can we inform/explore?

The Medical Ecosystem: Many Roles, Complex Interactions

Primary Care Physician

Hospital Billing

FDA

Medical Technicians

Electrophysiologist

Insurance Companies

Nurse Practitioner

Nurse

Cardiologist

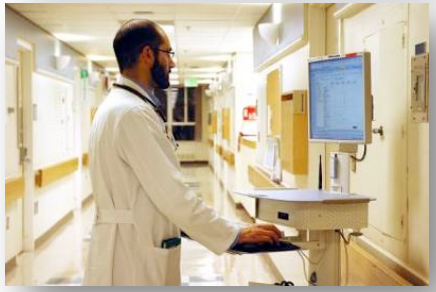
Emergency Room Staff

Implanting Surgeon

Anesthesiologist

Device Manufacturer Representative

Security System Concepts



Human-Centered

How can people be hurt?

What do people want?

How can we design systems?

How can we inform/explore?

Human-Centered

How can people be hurt?

What do people want…
Security + Privacy?

How can we design systems?

How can we inform/explore?

Augmented Reality

- Coming to market
  - Glass
  - SpaceGlasses
  - castAR
- Incorporates wearable camera
- Defenses being considered
  - [Templeman 2014], [Barhm 2011], [Brassil 2009], [Patel 2009], [Schiff 2009], [Halderman 2004]

In-Situ Interviews with Bystanders

- Observation & semi-structured interviews in cafes
- Researcher pair:
  A. Wear AR device (confederate)
  B. Approach and interview bystanders

Human-Centered

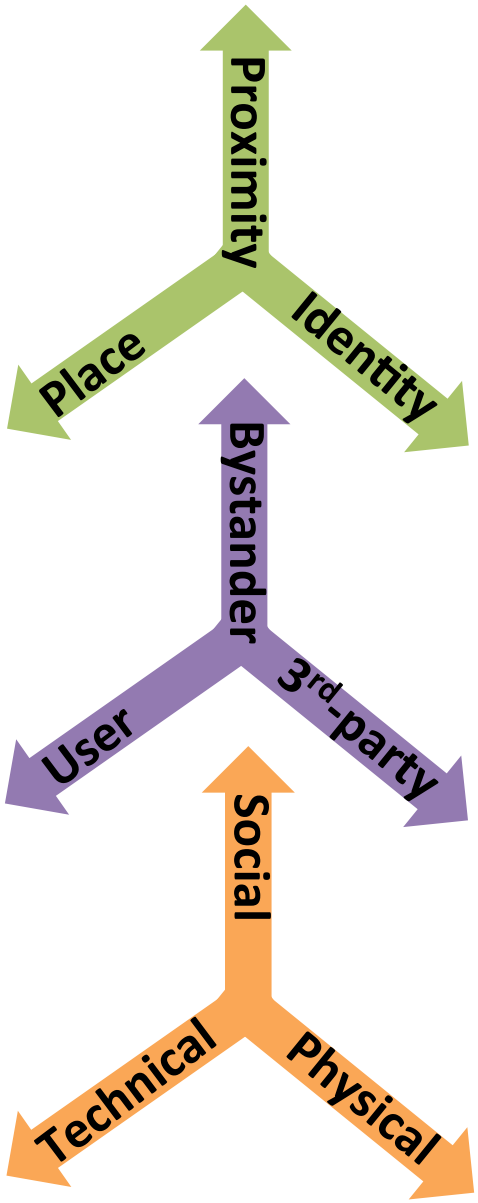
How can people be hurt?

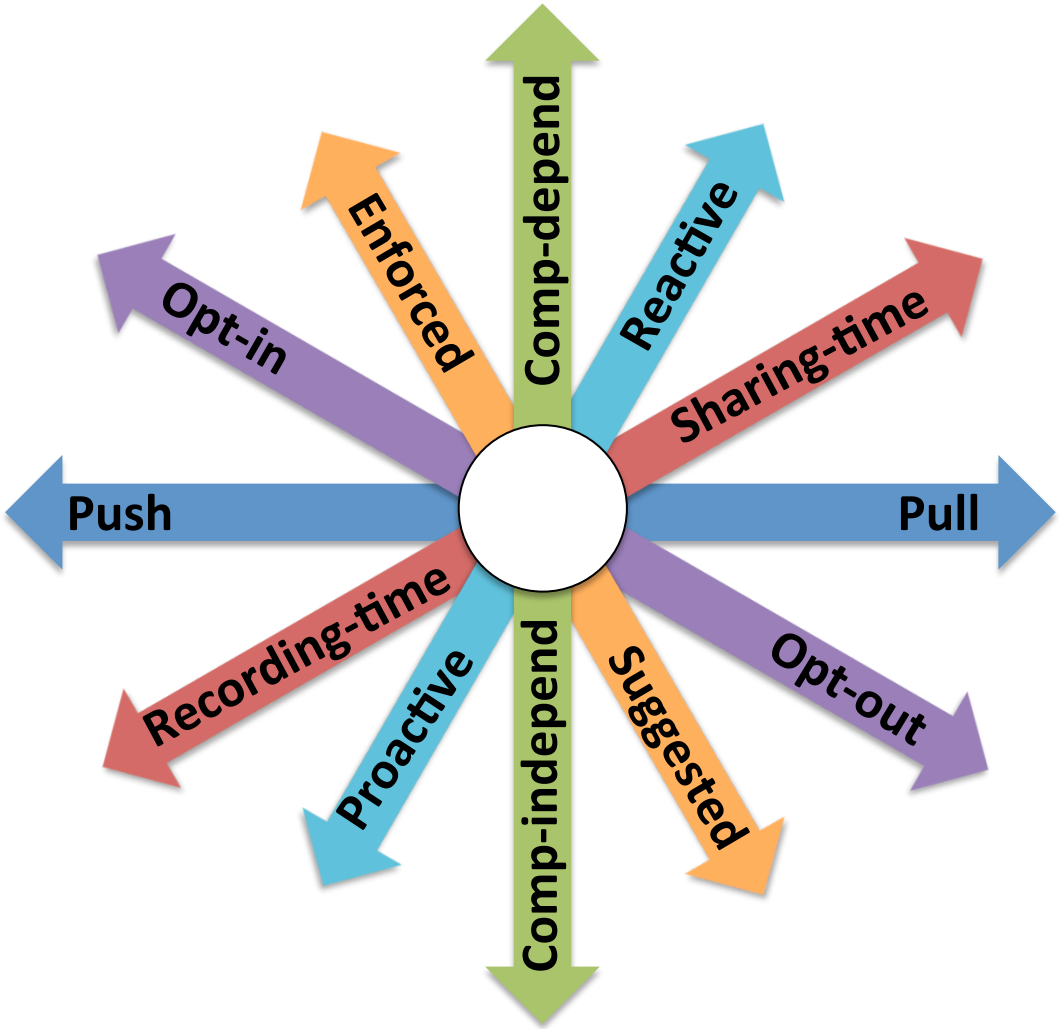
What do people want?

How can we design systems?

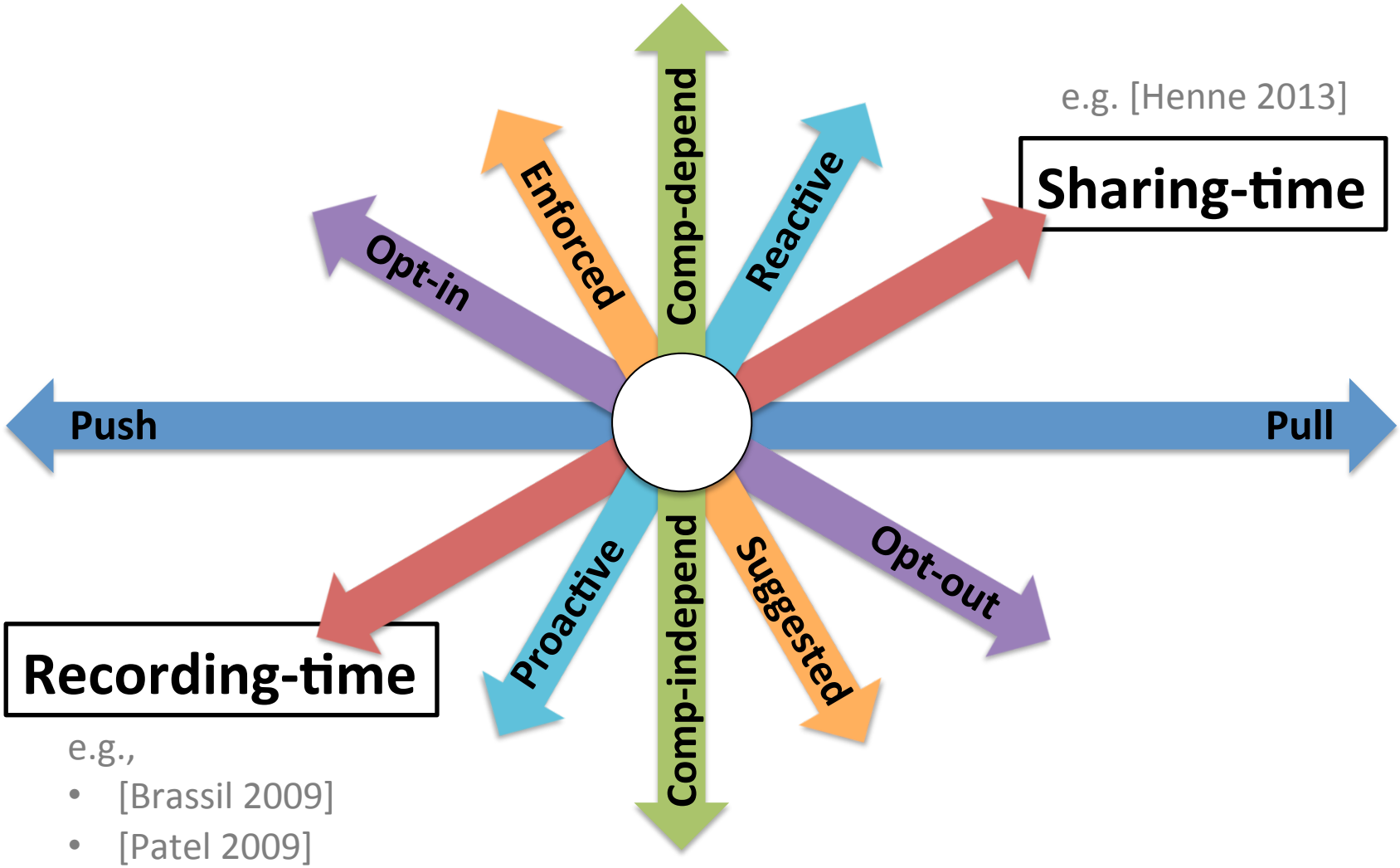
How can we inform/explore?

Design Axes for Privacy-Mediating Technologies





Design Axes for Privacy-Mediating Technologies



e.g. [Henne 2013]

Sharing-time

Recording-time

e.g.,

- [Brassil 2009]
- [Patel 2009]
- [Schiff 2009]
- [Templeman 2014]

Other Projects

Tabletop games to promote security awareness
[Denning 2013], [Denning 2013]

Threats and risks with household technologies
[Denning 2009], [Denning 2013]

Authentication via implicit memory
[Denning 2011]

What are some themes / issues?

What are some themes / issues?

- Same old problems

What are some themes / issues?

- Same old problems
  - How can we address awareness?

What are some themes / issues?

- Same old problems
  - How can we address awareness?
  - How can we automate/supply a framework for solutions?

What are some themes / issues?

- Same old problems
  - How can we address awareness?
  - How can we automate/supply a framework for solutions?
- New (returning) resource constraints

What are some themes / issues?

- Same old problems
  - How can we address awareness?
  - How can we automate/supply a framework for solutions?
- New (returning) resource constraints
  - What old solutions might work?

What are some themes / issues?

- Same old problems
  - How can we address awareness?
  - How can we automate/supply a framework for solutions?
- New (returning) resource constraints
  - What old solutions might work?
  - Where do we need new solutions?

What are some themes / issues?

- Same old problems
  - How can we address awareness?
  - How can we automate/supply a framework for solutions?
- New (returning) resource constraints
  - What old solutions might work?
  - Where do we need new solutions?
- New usage scenarios → New consequences

What are some themes / issues?

- Same old problems
  - How can we address awareness?
  - How can we automate/supply a framework for solutions?
- New (returning) resource constraints
  - What old solutions might work?
  - Where do we need new solutions?
- New usage scenarios → New consequences
  - What are the threats? What are the risks?

What are some themes / issues?

- Same old problems
  - How can we address awareness?
  - How can we automate/supply a framework for solutions?
- New (returning) resource constraints
  - What old solutions might work?
  - Where do we need new solutions?
- New usage scenarios → New consequences
  - What are the threats? What are the risks?
  - What are goals and constraints in the domain?

What are some themes / issues?

- Same old problems
  - How can we address awareness?
  - How can we automate/supply a framework for solutions?
- New (returning) resource constraints
  - What old solutions might work?
  - Where do we need new solutions?
- New usage scenarios → New consequences
  - What are the threats? What are the risks?
  - What are goals and constraints in the domain?
- New industries

What are some themes / issues?

- Same old problems
  - How can we address awareness?
  - How can we automate/supply a framework for solutions?
- New (returning) resource constraints
  - What old solutions might work?
  - Where do we need new solutions?
- New usage scenarios → New consequences
  - What are the threats? What are the risks?
  - What are goals and constraints in the domain?
- New industries
  - How can we raise prioritization with management?

What are some themes / issues?

- Same old problems
  - How can we address awareness?
  - How can we automate/supply a framework for solutions?
- New (returning) resource constraints
  - What old solutions might work?
  - Where do we need new solutions?
- New usage scenarios → New consequences
  - What are the threats? What are the risks?
  - What are goals and constraints in the domain?
- New industries
  - How can we raise prioritization with management?
  - How can we change the incentives w.r.t. security?

Human-Centered

How can people be hurt?

What do people want?

How can we design systems?

How can we inform/explore?

Beyond the Study: Bootstrapping the Process

- Developers, managers, policymakers, users, students need computer security tools

- We need to provide tools to:
  - Explore:
    - Threats
    - Values
    - Consequences
    - Design of mitigations
  - Measure/Determine:
    - Risks
    - Usage
    - Performance
  - Facilitate Communication

Beyond the Study: Bootstrapping the Process

- Developers, managers, policymakers, users, students need computer security tools

- We need to provide tools to:
  - Explore:
    - Threats
    - Values
    - Consequences
    - Design of mitigations
  - Measure/Determine:
    - Risks
    - Usage
    - Performance
  - Facilitate Communication

Specificity?

Flexibility?

Automation?

Expertise?

Creativity?

Cost?

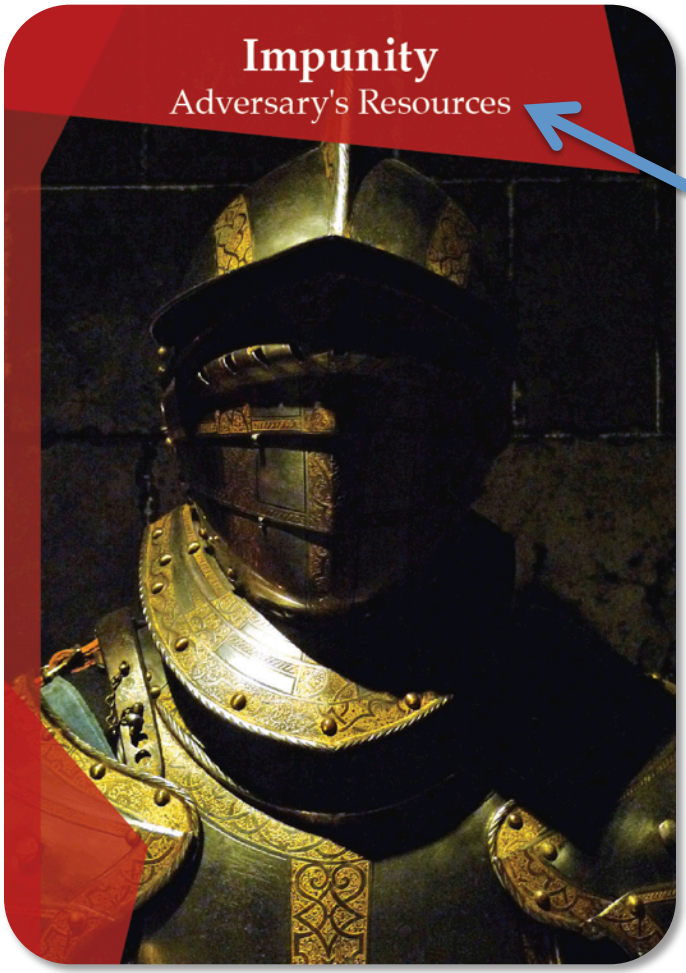
Security Cards:
A Threat Brainstorming Toolkit

Purpose: To facilitate the broad exploration of potential security and privacy threats to a system: the "security mindset"

Example Card (Front)

Card topic

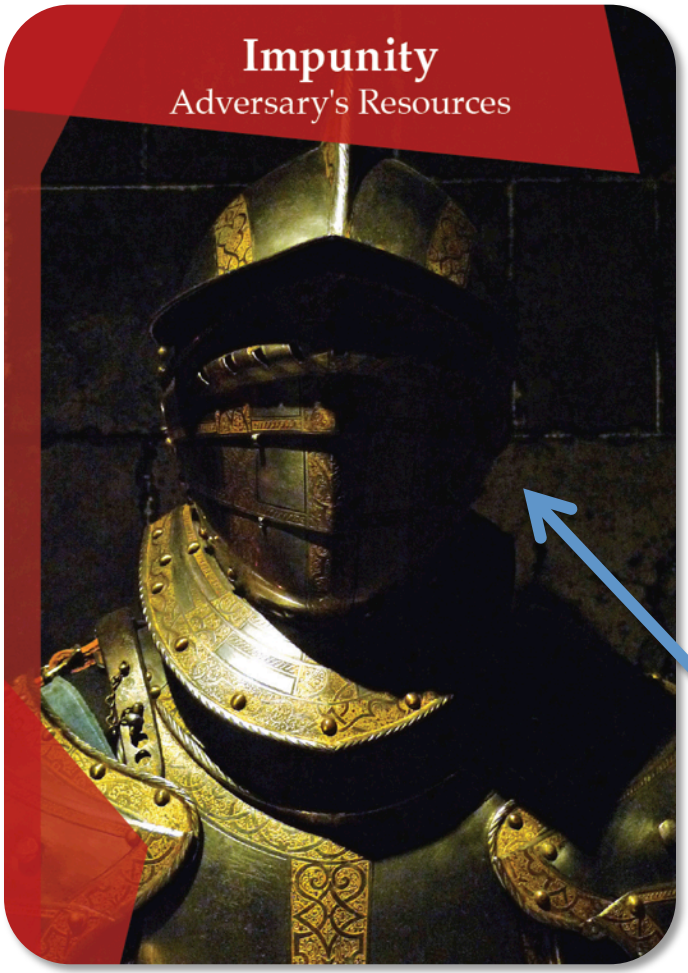
Example Card (Front)



Card topic

Card dimension

Example Card (Front)



Card topic

Card dimension

Evocative photograph

Example Card (Back)

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

Questions for clarification and to jumpstart thinking

Example Card (Back)

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

Questions for clarification and to jumpstart thinking

Illustrative examples

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

Threat Brainstorming Activity

1. Form groups of 4
2. (Say hello)
3. Take time to read all the cards
4. Decide a system to look at, e.g.:
    1. A recipe and grocery shopping organization app
    2. Internet-enabled light bulbs
    3. An exercise and sleep tracking device
    4. An internet-enabled washing machine
    5. A university records system (grades, medical ,and/or financial)
    6. A web browser plugin to change the display of Wikipedia pages

Threat Brainstorming Activity

- **Communally sort the cards within each dimension in order of relevance to the system being analyzed.**
- Have discussions as to **why** a sorting is valid. Give **specific** (potential) examples.
- *Recommended order:*
  1. Sort the Human Impact cards
  2. Sort the Adversary's Motivations cards
  3. Sort the Adversary's Resources card
  4. Sort the Adversary's Methods cards
  5. Re-visit all of the sorted cards.