CPS: Beyond Usability: Applying Value Sensitive Design Based Methods to Investigate Domain Characteristics for Security for Implantable Cardiac Devices

Tamara Denning¹, Batya Friedman², Brian Gill³, Daniel B. Kramer⁴, Matthew R. Reynolds⁵, Tadayoshi Kohno²

¹University of Utah
²University of Washington
³Seattle Pacific University
⁴Beth Israel Deaconess Medical Center
⁵Harvard Clinical Research Institute
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 & Impacts
[Halperin 2008] [Gollakota 2011]

• Private information
  – Obtain serial number, patient name, diagnosis

• Health impacts
  – Turn off therapies (defibrillation)
  – Induce cardiac fibrillation
Wireless ICD Security

• Need more security
  1. No individualized security
  2. Demonstrated security vulnerabilities
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

<table>
<thead>
<tr>
<th>Cost: Inaccessibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>❯ In emergencies</td>
</tr>
<tr>
<td>❯ Travel</td>
</tr>
<tr>
<td>❯ Switching providers</td>
</tr>
</tbody>
</table>
Securing Implantable Cardiac Devices

More security is needed

- Proposal: Password on file

Cost: Inaccessibility
- In emergencies
- Travel
- Switching providers
Security:
The Science and Art of Tradeoffs
Security: The Science and Art of Tradeoffs

Security Solution “Costs”

Value of Human “Assets”
Security: The Science and Art of Tradeoffs

Security Solution “Costs”

Value of Human “Assets”
Implantable Cardiac Devices: Broader Context

- Defense designs require interaction with domain experts
- Exploratory studies surface issues
Quantitative Research

How much?
Qualitative Research

How much of what?
Qualitative Research

How much of what?

Why?
Human-Centric Investigation: Implantable Cardiac Devices

• **Question**: What are relevant costs (to avoid) with respect to security systems for implantable cardiac devices?
Patient Study

- Semi-structured interviews with patients with IMDs
- Investigated patient values and concerns
- Elicited reactions to security system concepts

[Denning 2010]
The Medical Ecosystem: Many Roles, Complex Interactions

- Primary Care Physician
- Medical Technicians
- Nurse
- Cardiologist
- Implanting Surgeon
- Device Manufacturer Representative
- Hospital Billing
- Electrophysiologist
- Insurance Companies
- Nurse Practitioner
- Emergency Room Staff
- Anesthesiologist
- FDA
Informing Security Research via Studying the Application Domain

- Richness of underlying issues
Informing Security Research via Studying the Application Domain

• Richness of underlying issues
  – Stakeholder priorities
Informing Security Research via Studying the Application Domain

- Richness of underlying issues
  - Stakeholder priorities
  - Terminology
Informing Security Research via Studying the Application Domain

• Richness of underlying issues
  – Stakeholder priorities
  – Terminology
  – Concerns
Informing Security Research via Studying the Application Domain

- Richness of underlying issues
  - Stakeholder priorities
  - Terminology
  - Concerns
  - Constraints
Informing Security Research via Studying the Application Domain

• Richness of underlying issues
  – Stakeholder priorities
  – Terminology
  – Concerns
  – Constraints
  – Security system properties
Informing Security Research via Studying the Application Domain

• Richness of underlying issues
  – Stakeholder priorities
  – Terminology
  – Concerns
  – Constraints
  – Security system properties
  – Patient insights
Informing Security Research via Studying the Application Domain

- Richness of underlying issues
  - Stakeholder priorities
  - Terminology
  - Concerns
  - Constraints
  - Security system properties
  - Patient insights

Design better security solutions
Framework: Value Sensitive Design

[Friedman 2006]

Account for people’s **values**
Framework: Value Sensitive Design
[Friedman 2006]

Account for people’s values

Account for direct and indirect stakeholders
Framework: Value Sensitive Design

[Friedman 2006]
Qualitative Study Design

• 3 Workshops:
  – 24 providers
  – Cardiologists, nurses, anesthesiologists, etc.

• Workshop format facilitates:
  – Interactive discourse
  – Surfacing consensus, tensions

• Group Activities & Paper Instruments
Workshop Format

- Stakeholder Perspectives
- Metaphor Generation
- Critiques and Concerns
- Evaluation of Security System Concepts
- Open-ended Discussion

[Kensing 1991]
[Yoo 2013]
Workshop Format

- **Stakeholder Perspectives**
- Metaphor Generation
- Critiques and Concerns
- Evaluation of Security System Concepts
- Open-ended Discussion
Stakeholder Perspective Data Analysis

• Open-ended answers used to develop topic categories

• Independent researcher used categories to code participant responses

• Kappa = 0.745
  – >0.75 is excellent agreement
  – 0.40-0.75 is intermediate to good [Fleiss 2003]
  – 0.61-0.80 is substantial agreement [Landis 1977]
Stakeholder Perspective Results Inform Security Design

- Access & Sharing
- **Compatibility**
- Correct Usage
- **Device Battery Life**
- Device Compactness / Inertness
- Device Ecosystem

- Device Functionality
- Patient / Patient Health
- Programming
- Quality of Data
- Remote Monitoring
- **Security & Privacy**
- **Surgery & Healing**
1. Assets we want to protect from attacks
2. Costs we want to avoid
Workshop Format

- Stakeholder Perspectives
- Metaphor Generation
- Critiques and Concerns
- Evaluation of Security System Concepts
- Open-ended Discussion

[Kensing 1991]
[Yoo 2013]
Security System Concepts

• Surveyed literature for proposed security solutions

• Chose representative concepts with varied properties

• Participants:
  – Provided overall evaluations
  – Commented on properties
Disliked System Concepts: Uncovering Security System Costs

Medical Alert Bracelet with Password
Disliked System Concepts: Uncovering Security System Costs

Medical Alert Bracelet with Password

UV-Visible Tattoo

[Denning 2010]
[Schechter 2010]
Disliked System Concepts: Uncovering Security System Costs

Medical Alert Bracelet with Password

UV-Visible Tattoo

Criticality-Aware IMD

[Denning 2010]
[Denning 2010]

[Schechter 2010]

[Gupta 2006]

Security Costs
Disliked System Concepts:
Uncovering Security System Costs

Positive Properties (of Disliked Systems)

↑ Facilitates emergency access
↑ Reassures patient
↑ Not visible

↑ Cheap
↑ No patient effort
↑ Always present
Disliked System Concepts: Uncovering Security System Costs

Negative Properties

- Access is not guaranteed
- Cultural, social, or personal objections
- Broadcasts patient condition to others
- Potential impact on battery life
Fail-Open Wristband with Safety Features

- **Presence** blocks unauthorized access
- In its **absence**, system fails into an open state—accepts all communications

[Denning 2008]
[Gollakota 2011]
[Xu 2011]
Liked System Concept: Uncovering Security System Costs

Fail-Open Wristband with Safety Features

↑ Fail-open
↑ Safety features
↑ Security
↑ Empowers patient
↑ Visual cue

↓ Security
↓ Maintenance
↓ 911 false positives
↓ Visual indicator
↓ Training
↓ Expense

[Denning 2008]
[Gollakota 2011]
[Xu 2011]
Human-Centric Investigation Indicates Security Costs to Avoid

<table>
<thead>
<tr>
<th>Security Solution Costs</th>
<th>Security Solution Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inaccessibility</td>
<td>Battery life</td>
</tr>
<tr>
<td>Money (→ denied claims)</td>
<td>Patient privacy</td>
</tr>
<tr>
<td>Patient comfort + mental health</td>
<td>Infection</td>
</tr>
<tr>
<td>Implant size</td>
<td>Incompatibility</td>
</tr>
</tbody>
</table>
Human-Centric Investigation: Implantable Cardiac Devices

• Study indicates security costs to avoid when designing security solutions

• Additional features (e.g., safety) may entice buy-in

• Tensions exist (e.g., visual indicators)
Beyond Implantable Cardiac Devices

Connectivity

Sensors

Actuators

Usage Scenario
Human-Centric Investigation: Implantable Cardiac Devices

- Study indicates security costs to avoid when designing security solutions
- Additional features (e.g., safety) may entice buy-in
- Tensions exist (e.g., visual indicators)
- Defense designs require interaction with domain experts
- Exploratory studies surface issues