Security & Privacy at Home

Blase Ur, Ph.D. Candidate, CMU
Traditional UPS Issues at Home

• Sharing and protecting data in the home
  - Heterogeneous set of (related) users
  - Many devices
  - Lots of sensitive data
• Controlling access to home wi-fi networks
• Device pairing based on location-limited channels
Privacy in the Home

• The home traditionally is considered private (e.g., Warren and Brandeis Harvard Law Review Article)
  – “The right to be let alone”
  – Domestic life is a “sacred precinct”
  – But is the home really private?
Smart Homes and the Internet of Things

• Network everything!
  - Sensors around the house and carried by the user
  - Smart (energy) meters
  - Household appliances
  - Cars
  - Healthcare devices
Smart Homes and the Internet of Things

• Why network everything?
  – Convenience
  – Comfort
  – Customizability
  – Sustainability
Privacy in the Smart Home

• To me, privacy at home is interesting because:
  - Home is traditionally a private space, but increasingly a window to the outside world
  - Heterogeneous occupants with complex power dynamics and perspectives
  - Visitors and guests
  - A large amount of time is spent there
  - Clear intentions for access control (and control considered more broadly)
Privacy Threats in the Smart Home

• Surveillance by the government
• Surveillance by smart-home companies
• Surveillance by third-party security vendors
• Surveillance by Internet behemoths
• Surveillance by other members of the family
  - Parents → teens
  - Teens → parents
  - Spouse → spouse
  - Elder → younger
  - Younger → elder
Privacy Threats in the Smart Home

- Direct data readings
- Inferences
  - What you are doing
  - What you are not doing
  - Incorrect inferences
- Loss of control (e.g., location tracking)
- Loss of autonomy (e.g., eldercare)
- Change of norms about private space
- Threats to security
- Threats to freedom of expression
Photo taken by the authors.
Home security and teen monitoring
Gauge teenagers' and parents' reactions to Internet-connected locks and cameras in home entryways
Methodology

• Two studies:
  – Interviews of parents and teenagers
  – Online configuration study
Interview Study Methodology

• Interviewed 13 teenagers and 11 parents
  – Recruited from Microsoft's participant pool
  – All from different households
  – Limitation: Not a representative sample
  – Limitation: Hypothetical deployment

• Interviews lasted ~1 hour
  – Compensation: $50 gift card or equivalent
Interview Structure

• Parenting-style survey
• Familiarity with, and use of, home technology

• General reactions to Internet-connected locks
• Use of traditional keys and history of burglaries
• Reactions to potential interfaces for audit logs
• Current monitoring practices and attitudes
Analysis

• Transcribed all interviews
  – Two researchers tagged 1,852 quotes as explanatory
• Collaboratively performed affinity diagramming
  – Identified 28 primary themes representing attitudes and influences
Participants

• 13 teenagers (7 male, 6 female)
  – Age 15 – 17
  – Range of family circumstances
• 11 parents (4 male, 7 female)
  – Age 35 – 59
  – Two single parents
  – One parent uses an Internet-connected lock
Participants Liked Connected Locks

• Parents and teens said there were substantial benefits in Internet-connected locks

• Benefits include:
  - Convenience
  - Added control
  - Safety from burglars

• Drawbacks are:
  - High cost
  - Fear of hackers
Auditing Interfaces
## Auditing Interfaces

### Photo log

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rear door</td>
<td>[Image]</td>
<td>19 minutes ago</td>
</tr>
<tr>
<td>Rear door</td>
<td>[Image], Aurora's Phone</td>
<td>20 minutes ago</td>
</tr>
<tr>
<td>Front door</td>
<td>[Image]</td>
<td>39 minutes ago</td>
</tr>
<tr>
<td>Front door</td>
<td>[Image], Billy's PIN Code</td>
<td>40 minutes ago</td>
</tr>
<tr>
<td>Rear door</td>
<td>[Image]</td>
<td>4 hours ago</td>
</tr>
<tr>
<td>Rear door</td>
<td>[Image], Billy's Phone</td>
<td>4 hours ago</td>
</tr>
</tbody>
</table>
## Auditing Interfaces

<table>
<thead>
<tr>
<th>What?</th>
<th>How?</th>
<th>When?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rear door</td>
<td>Aurora's Phone</td>
<td>20 minutes ago</td>
</tr>
<tr>
<td>Front door</td>
<td>Billy's PIN Code</td>
<td>40 minutes ago</td>
</tr>
<tr>
<td>Rear door</td>
<td>Billy's Phone</td>
<td>4 hours ago</td>
</tr>
</tbody>
</table>
Auditing Interfaces

No log
Parents' and Teens' Preferences Differed

• All 11 parents preferred photo log
  - “For safety purposes”
  - “You need to catch a burglar on camera”
• 3 specified monitoring teens as a goal
  - “As my son gets older, I’m going to need to verify if he’s coming home alone”
Parents' and Teens' Preferences Differed

- 6 teens preferred photo log
  - 4 nonetheless expressed privacy concerns
  - “...kind of weird that they could just always look and see exactly who’s over.”
- 3 teens preferred text log
  - Photo “invasion of privacy, ‘big brother’ kind of thing”
- 4 teens preferred no log
  - Photo log “would pretty much ruin a strict parent’s kid’s social life.”
  - “This is like parents going psycho.”
Monitoring Teens

• Some parents wanted to monitor teens
  – “Trust but verify”

• Others chose photo log in spite of monitoring
  – “It’s just a human nature thing that nobody likes when people keep tabs on anybody”
  – “I think [my children] would be paranoid or intimidated by the photos”
Current Monitoring Practices

• Unconstrained monitoring (2 parents)
• No monitoring (3 parents)
  – “I’m just waiting to see if she gives me a reason not to let her just be free.”
• Intentionally limited monitoring (6 parents)
  – “I feel like that’s a violation of their privacy if I were to [log onto their Facebook]. I know that I have their permission, I know that I have the access, but that’s going further than I want to.”
Parental Strictness vs. Auditing Decision

• Compared teens' parenting style survey results with decisions about audit log
• 5 of the 6 teens with comparatively stricter parents chose the photo log
• 1 of the 7 teens with comparatively less strict parents chose the photo log
Potential Unintended Consequences

• Reduced parent-teen trust
  – Spend time at friends' houses instead

• Circumvention reducing security
  – Leaving doors unlocked and windows open
  – Removing window sensors
  – Disabling camera
How might parents configure an auditable security system?
Methodology

• Online configuration study
  - Access & audit settings for entryway security system
• 19 parents recruited from classified ad sites
  - Compensated with $15 gift card
## Configuration Task

### Users

<table>
<thead>
<tr>
<th>First name or nickname</th>
<th>Email address or mobile phone #</th>
<th>Age</th>
<th>Lock PIN</th>
<th>Role</th>
<th>Lock and unlock records can be audited</th>
</tr>
</thead>
<tbody>
<tr>
<td>You, age 30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>only with permission</td>
</tr>
<tr>
<td>Alice</td>
<td><a href="mailto:alice@foo.com">alice@foo.com</a></td>
<td>50</td>
<td>******</td>
<td>administrator</td>
<td></td>
</tr>
<tr>
<td>Husband, age 33</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>anytime with notice</td>
</tr>
<tr>
<td>Bob</td>
<td><a href="mailto:bob@foo.com">bob@foo.com</a></td>
<td>53</td>
<td>******</td>
<td>administrator</td>
<td></td>
</tr>
<tr>
<td>Daughter, age 16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>anytime with notice</td>
</tr>
<tr>
<td>Charlie</td>
<td>202-555-9873</td>
<td>16</td>
<td>******</td>
<td>user</td>
<td></td>
</tr>
<tr>
<td>Uncle Joe</td>
<td><a href="mailto:joe@foo.com">joe@foo.com</a></td>
<td>40</td>
<td></td>
<td>user</td>
<td>anytime w/o notice</td>
</tr>
</tbody>
</table>

### Notifications

Send a notification to [alice@foo.com](mailto:alice@foo.com) whenever Charlie unlocks the door(s)
Configuration Task

You, and other auditors, can view records of when Alice locked or unlocked the door...

**Only with permission from Alice**

Alice will be sent a text or email asking him/her to approve the release of these records.

**Anytime, but a notification will be sent to Alice**

Alice will receive a text or email indicating who accessed his/her records.

**Anytime & without notice**

Alice will not be notified when his/her records are accessed, but will know who can access them.

Alice will be able to see which policy has been assigned to him/her and which users can read his/her lock and unlock records.

Records of lock and unlock events are protected by the policy in place at the time of the event. Changing this policy will only change access to future lock and unlock events.
Results

• Most participants would only allow themselves to be audited with permission or with notice
• Participants assigned less privacy-protective settings for their spouses/partners
• All parents chose to monitor teens' comings and goings without notifying the teens
  – “She doesn’t have anything to hide, so it shouldn’t be a problem”
• Privacy is a negotiation between parents and teens
How can we disentangle decisions about home security and teen monitoring?
Possible Directions

• “Outsource” auditing...
  - ...to a security company
  - ...to each individual
Possible Directions

• Technology-assisted auditing
  - Face detection
  - Context-sensitive auditing
Possible Directions

• Change the interaction with logs
  – Pull instead of push notifications
  – “Approximate” logs
Conclusions

• New technologies can alter dynamics in the home
• Parents & teens had differing perspectives about audit
• Trust and security consequences result from conflating decisions about home security and teen monitoring
  - Potential interfaces and interactions that disentangle these decisions
Future Directions in Smart-Home Research

- Mennicken et al.'s UbiComp '14 survey highlighted:
  - From augmented home to smart home
  - Meaningful technology
  - Working with technology
  - Intelligibility

- Why is intelligibility critical?
  - Debugging when things go wrong
  - Understanding the future
  - Engaging otherwise disenfranchised family members
Future Directions in Smart-Home Research
Future Directions in Smart-Home Research

• Intelligibility can leak private information
  – Imagine the Nest thermostat says, “I adjusted the temperature at 3:00am because people are always at the fridge then”
  – Imagine the smart meter says, “I noticed Johnny wastes energy all the time in his room”
  – Imagine Google shows you an ad for lightbulbs because “we noticed your kitchen is pretty dark”

• How do we support privacy as part of intelligibility?