Usable Privacy and Security in the home

Ashutosh Pandey
Outline

• Threats to privacy & security at home
• Challenges
• Key Design Guidelines
• Exercise on smart home models
• Readings for the week
• Stakes are high!!
Threats to Privacy & Security at Home

• Internal threats
  – Roommates/visitors accessing personal devices
  – Toddlers deleting important files from the computer or turning on the thermostat

• External threats
  – Remotely unlocking the doors
  – Spying through cameras
  – Targeting entire communities by coordinating their devices to overload power grid

Then why to use smart devices at home?
Challenges (1\2)

• Mixed ownership - family members, visitors, roommates, neighbors
  – Different preferences
  – Different visitors: Friends, close friends, neighbors, relatives

• Diverse devices implies different use model
  – Computers: Desktops, laptops, tablets, smartphones
  – Home Appliances: Washing machine, TV, thermostat
  – Safety devices: Alarms, smoke detectors, security cameras
Challenges (2\2)

• Dealing with tradeoff between sensing vs. inference
• Naïve users
• Immersed devices
• Multidimensional policies
  – Identity and location of accessor
  – Device used for access
  – Duration of access
Key Design Guidelines

- Fine grained control
- Avoid upfront complexity
- Obscure/scrubbed data storage
- Provide feedback to users
- Replace denials with redirects
  - Helps in acknowledging social conventions
- Devices sensing the users
Model for Smart Home Environments (1/2)

Centralized Control Model
Model for Smart Home Environments (2/2)

Distributed Model
Exercise

• With respect to centralized and distributed architectures described in previous slides, analyze
  – Privacy & security vulnerabilities
  – Usability challenges
Readings for the week

Interesting things about the studies discussed in the reading

– “Cultural probes” in Choe et. al. Why?
– Interview study “without hypothesis” in Mazurek et. al. Why?
Stakes are high!!

- Benefits should compensate for privacy risks
- Privacy expectations of users may change
  - Educate them
- Don’t design in isolation