CIS 4930: Secure IoT

Prof. Kaushal Kafle

Asynchronous Class

Security Goals

- What are the *security goals* for the smart home?
  - Confidentiality
  - Integrity
  - Availability
  - Privacy

These goals are impacted when there are multiple users.

E.g. Consider that both your spouse and your babysitter have access to your door lock. However, you may allow your spouse to change the door lock key, but not grant the same access to your babysitter.

The adversary

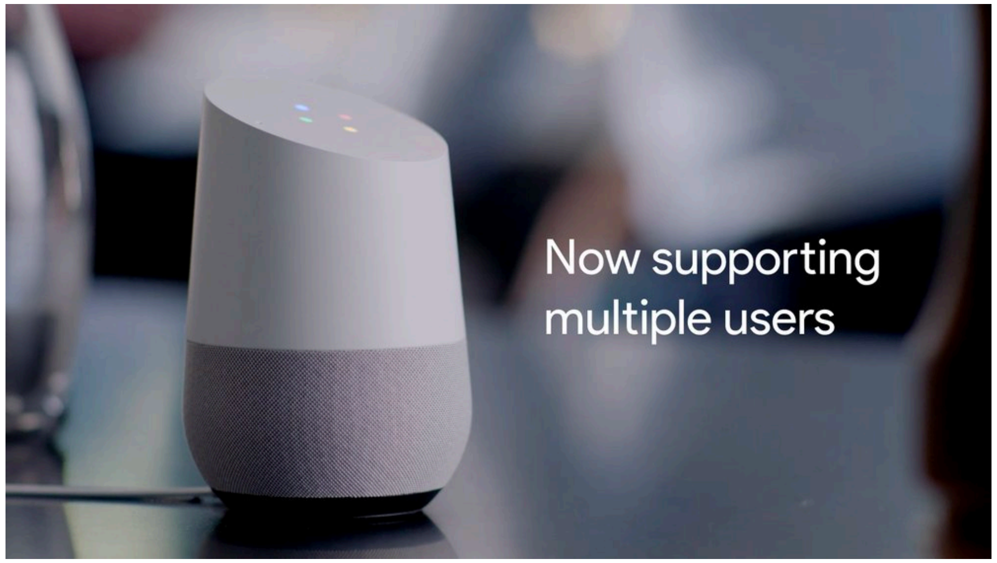
- What common *multi-user* home settings can you think of?
  - Families
  - Roommates/ house mates
  - Landlords and tenants (long-term leases)
  - Short term rentals (e.g., Airbnb)
  - Guests?
  - …?

At my age, do you know how I'm statistically most likely to die?
At the hands of your roommate?
An accident.
That's how I'm gonna make it look.

- Who is the adversary?
  - *Most of the above*

Threats

- To privacy?
- To integrity of one’s environment?
- To availability of resources/services?
- …



Why do these threats exist?

- Because existing smart home platforms do not have *multi-user access control*
  - Simply allowing multiple users *access* to the home does not cut it.

Initial Design Principles

- Access control flexibility
  - Fine-grained management (relationships, location)
- User agency
  - Allow users to *ask* for permission, i.e., prompt the owner
- Respect among users
  - Prevent remote control of devices in the vicinity of others
- Transparency of smart home behaviors
  - Track and notify *why* certain events take place

Types of Access Control Models

- **Role-based**
  - Admins, and others
- **Location-based**
  - Prevent a user from remote-controlling a device in another user’s vicinity
  - Can be set at the per-device, per-subject level

Types of Access Control Models

- **Supervisory**
  - Control only when the an authorized user is nearby (no notification)

- **Reactive**
  - Runtime permission - control provided by asking a permission to the authorized user during runtime.

Major Findings from user study

- People want location-based access control, but not quite as imagined in the paper (i.e., *geofenced device control*)
    - Is geofenced device control the *true guest* user restriction? (e.g., preventing remote access by a guest)
- Social norms obviate access control in some cases
    - Room-specific lamps were only operated by room owners.
    - May not provide protection against accidental (mis)use
- Users want voice authentication as well

Open Questions

- How usable is multi-user access control in the automated home?
    - *Bob wants to turn off the lamp; ‘tap here to allow’ is sent to Alice’s phone.*
- Does access control make things worse?
    - May reduce user agency, relative to an “everyone is admin” model (e.g., user relegates husband to “child” role for a config error)
    - Privacy vs transparency
- Are all device “accesses” the same? E.g., porch light configs, vs turning on a lamp, vs changing the temperature, vs opening a door
- Voice authentication: How to control voice assistants that everyone must have access to, but which do not discriminate?)
- Are there any ***privacy*** implications of in-situ studies?