The Current State of Access Control for Smart Devices in Homes

Blase Ur, Jaeyeon Jung, Stuart Schechter
www.blaseur.com
blase@blaseur.com
Smart Devices

• Smart devices: Household devices that are connected to the Internet

• Now marketed to average consumers
Smart Devices

- Smart devices: Household devices that are connected to the Internet

- Now marketed to average consumers
Access Control

• Security is a major barrier to adoption

• Many different models of access control are theoretically possible

Access Control

• Security is a major barrier to adoption

• Many different models of access control are theoretically possible

• What access-control affordances do current devices provide?

Three Case Studies

1. LED Lighting System: Philips Hue

2. Wireless Scale: Withings WS-30

3. Wireless Door Lock: Kwikset 910 TRL ZW and Mi Casa Verde Vera 3 (Z-Wave controller)
Configuration

- **Lighting system**: Plug hub into router (Ethernet), press button on hub to pair with phone
  - Optionally create account

- **Scale**: Pair over Bluetooth with phone, provide Wi-Fi credentials, create mandatory account

- **Lock**: Pair with Z-Wave controller by pressing button on lock
Who Can Control / Access?

- **Lighting system**: Same Wi-Fi network & paired with hub **OR** know account credentials **OR** proximity

- **Scale**: Anyone whose account or email address has been granted access

- **Lock**: Same Wi-Fi network **OR** has account on Z-Wave controller
Scale’s Sharing Affordances

- Share my data with the other users of my scale
- Share my data with other Withings accounts
- Share my data with my doctor
- Share on social networks
- Share on my website
- Save my data and print my graphs
Roles

• **Lighting system**: None

![Lighting system](image1)

• **Scale**: Separate accounts, email sharing

![Scale](image2)

• **Lock**: PIN or {Administrator, guest, notification-only}

![Lock](image3)
Roles

• **Lighting system**: None

• **Scale**: Separate accounts, email sharing

• **Lock**: PIN or {Administrator, guest, notification-only}
Roles

• **Lighting system:** None

• **Scale:** Separate accounts, email sharing

• **Lock:** PIN or {Administrator, guest, notification-only}
Roles

• **Lighting system**: None

• **Scale**: Separate accounts, email sharing

• **Lock**: PIN or {Administrator, guest, notification-only}
Audit Interfaces

• *Lighting system*: None

• *Scale*: None

• *Lock*: Notifications and access log
Audit Interfaces

- **Lighting system**: None
- **Scale**: None
- **Lock**: Notifications and access log
**Audit Interfaces**

- *Lighting system*: None
- *Scale*: None
- *Lock*: Notifications and access log
Audit Interfaces

- **Lighting system**: None
- **Scale**: None
- **Lock**: Notifications and access log

![Audit Interfaces Table]

![Audit Interfaces Diagram]
Conclusions

• Each device confusingly provides different mechanisms and modalities for access control
  • Difficult to share with family, guests

• Audit interfaces sorely lacking

• Each device presents a siloed system

• Opportunities for unified access-control system
The Current State of Access Control for Smart Devices in Homes

Thank You!

Blase Ur, Jaeyeon Jung, Stuart Schechter

www.blaseur.com
blase@blaseur.com