CIS 4930: Secure IoT

Prof. Kaushal Kafle

Lecture 14

Class Notes

- **Project report reminder**
  - Demo your project by meeting in-person
  - All team members should be on the same page regarding
    - *How the system works*
    - *What methodology is implemented*
    - *What each team member contributed..*
- Report submission extended to accommodate demos
  - **Submit by 11/05, but meet by this week!**

Multiuser Smart Homes

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.

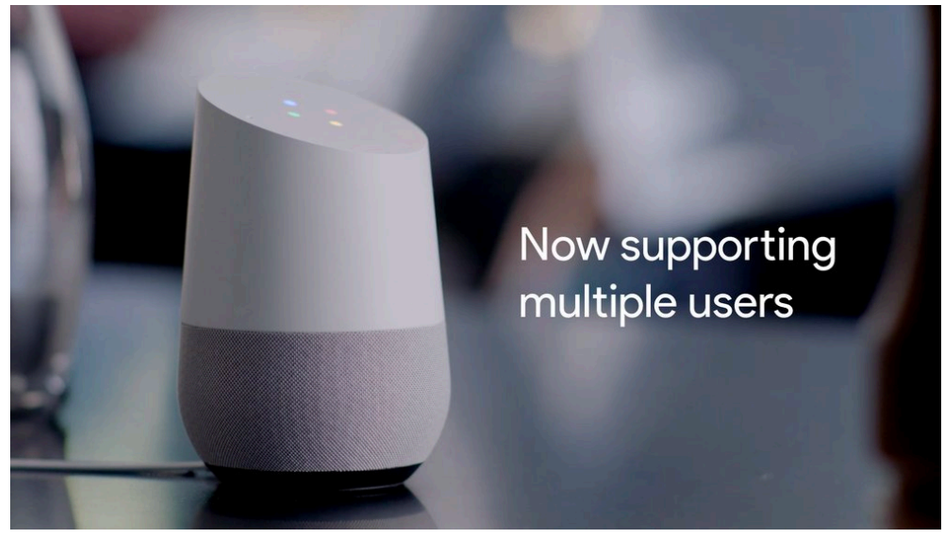
The adversary

- 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?
  - …?

- 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

Questions

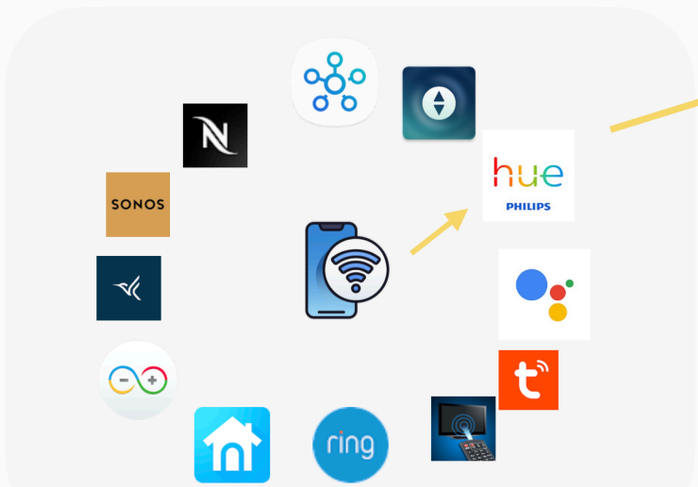
- Specify at least two factors that are currently lacking in access control models that are typically built for single-user environments.
- Specify two design changes that smart home platforms can make to enable multi-user access control.
- Provide two examples of how user relationships impact access control in a multi-user smart home environment.
- Identify three contextual factors that impact how user's perceive access control in a multi-user setup.

Open Questions

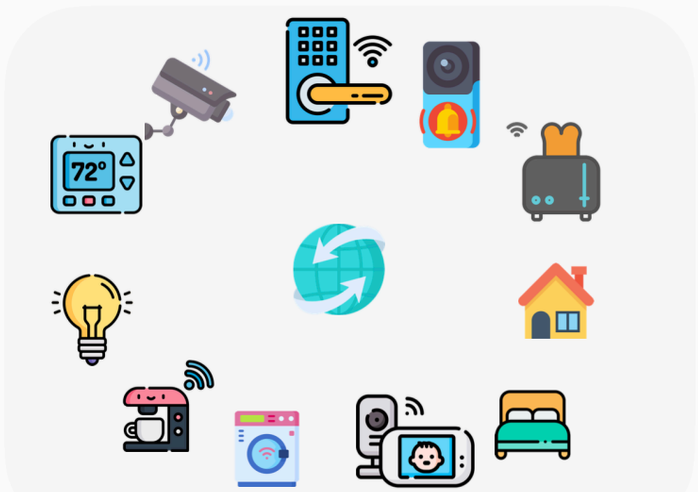
- **Are there any *<u>privacy implications</u>* of in-situ studies?**
- How usable is multi-user access control in the automated home?
    - *Bob wants to turn off the lamp; ‘tap here to allow’ is sent to Alice’s phone.*
- Does multi-user access control make things worse?
    - May reduce user agency, 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?)

IoT App Analysis

IoT Security



Mobile-IoT Apps



IoT Devices

Automations

Firmwares

Cloud Backends

IoT Libraries

Attack Surface

IoT Security

Hacker spoke to baby, hurled obscenities at couple using Nest camera, dad says

Dozens sue Amazon's Ring after camera hack leads to threats and racial slurs

Home › News › Hackers take over Smart Home

NEWS THREATS

Hackers take over Smart Home

By CISOMAG - September 26, 2019

Consumer Tech • Perspective

Alexa has been eavesdropping on you this whole time

When Alexa runs your home, Amazon tracks you in more ways than you might want.

TECHNOLOGY

Is your Christmas present spying on you? How to assess gifts' privacy risks

Siemens SIMATIC PLCs (Security Bug Reveals Hardcoded Universal Key)

Cyber Security Today, Oct. 26 2022 – American schools increasingly hit by ransomware, an event ticket agency is hacked and more

Yes, Your Video Baby Monitor Can Be Hacked. No, You Don't Have to Stop Using It

By Jack Busch

Last Updated on June 24, 2021

Bluejacking: How Bluetooth Can Be Used to Hack Your Devices

New PoC Shows IoT Devices Can Be Hacked to Install Ransomware on OT Networks

Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals

European Police Arrest a Gang That Hacked Wireless Key Fobs to Steal Cars

Critical Amazon Ring Vulnerability Could Expose Camera Recordings

Public electric car chargers are an 'open door' to drivers being hacked – urgent warning

Buggy software in off-brand smart home devices is a hacker's playground

Samsung SmartThings Hub Vulnerable to Hacks: Check Yours Now

Crooks are jamming security cameras — Protect yours now!

SMART HOME TECH CYBERSECURITY

Your Philips Hue light bulbs can still be hacked — and until recently, compromise your network

Might want to check if you've got firmware 1935144040

Police dismantles criminal ring that hacked keyless cars

Wisconsin couple describe the chilling moment that a hacker cranked up their heat and started talking to them through a Google Nest camera in their kitchen

IoT Security Challenges

Secure IoT Products at scale → **Triaging?**

We do not know what products constitute IoT Ecosystem!

Mobile-IoT Apps

Unique features for **Identification**

Metadata to build **understanding of IoT Market**

Critical **Attack Surface**

Security ramifications of vulnerabilities **beyond Mobile Space**

IoT Security Challenges

We do not know what products constitute IoT Ecosystem!

Research Questions

RQ1: How can we automatically ***develop a market-scale snapshot*** of mobile-IoT apps from markets containing heterogeneous apps?

RQ2: How can we ***make the snapshot useful for security***?

Intuition:

Security Analysis: Crypto APIs

Findings

Ran CryptoGuard on Apps with 1M+ Installs!

Flaws detected by CryptoGuard

Finding 5: 94.11% apps contain at least 1 Crypto-API misuse according to CryptoGuard out of *917 apps with 1M+ installs (96.29% non-IoT).*

Finding 6: 82.5% (486/589) high severity violations detected by CryptoGuard is **true positive**.

CryptoGuard's Rules (IDs as per [55])		# Vulnerable Apps	
ID	Rule Name	Mobile-IoT	Non-IoT
9	Insecure PRNGs (e.g., java.util.Random) [M]	842	870
16	Insecure cryptographic hash (e.g., SHA1, MD5) [H]	825	865
1	Predictable/constant cryptographic keys [H]	577	669
7	Occasional use of HTTP [H]	438	441
14,11	*64-bit block ciphers (e.g., DES, RC4), ECB mode [M]	406	376
5	Custom TrustManager to trust all certificates [H]	380	302
4	Custom Hostname verifiers to accept all hosts [H]	293	269
12	Static IVs in CBC mode symmetric ciphers [M]	239	208
6	SSLSocketFactory w/o hostname verification [H]	186	86
3	Predictable/constant passwords for KeyStore [H]	142	60
13	Fewer than 1,000 iterations for PBE	70	26
15	Insecure asymmetric cipher use	66	19
2,10	*Predictable passwords, static salts in for PBE [H/M]	63	47
8	Predictable/constant PRNG seeds [M]	50	23
-	**Number of apps that violated at least one rule**	863	883

* = CryptoGuard reports combined results for rules indicated by combined rule IDs.

Discussion

Discussion point 1: Are consumers buying the IoT products benefiting from these security studies? If so, how?

Discussion point 2: How much do the computational restrictions of static analysis affect security research?

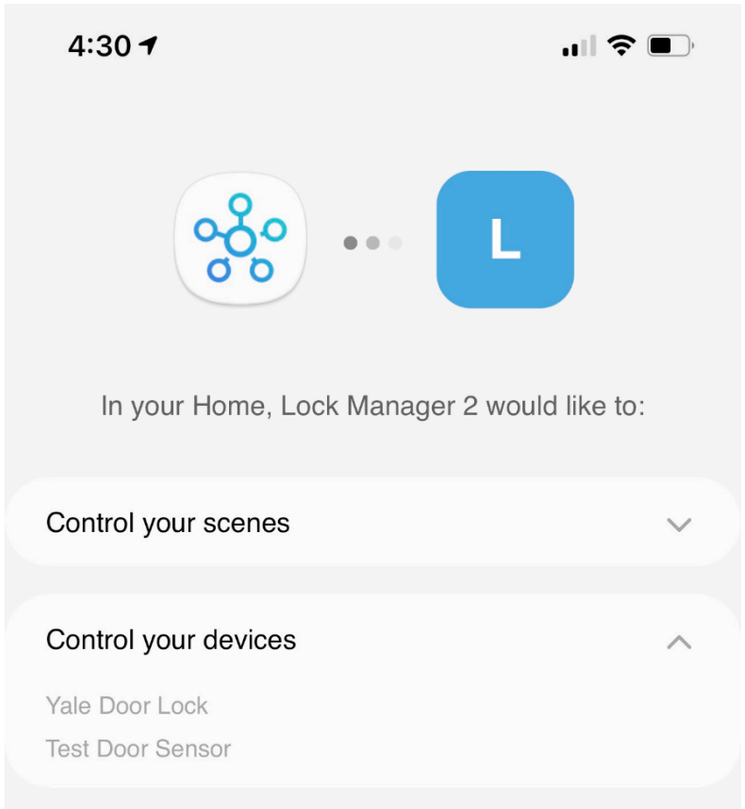
Discussion Point 3: Should the Government Regulate IoT App Safety? If So, How?

Discussion Point 4: Does the app have an obligation (moral or legal) to inform the user when multiple threats are accessed and open within the application itself?

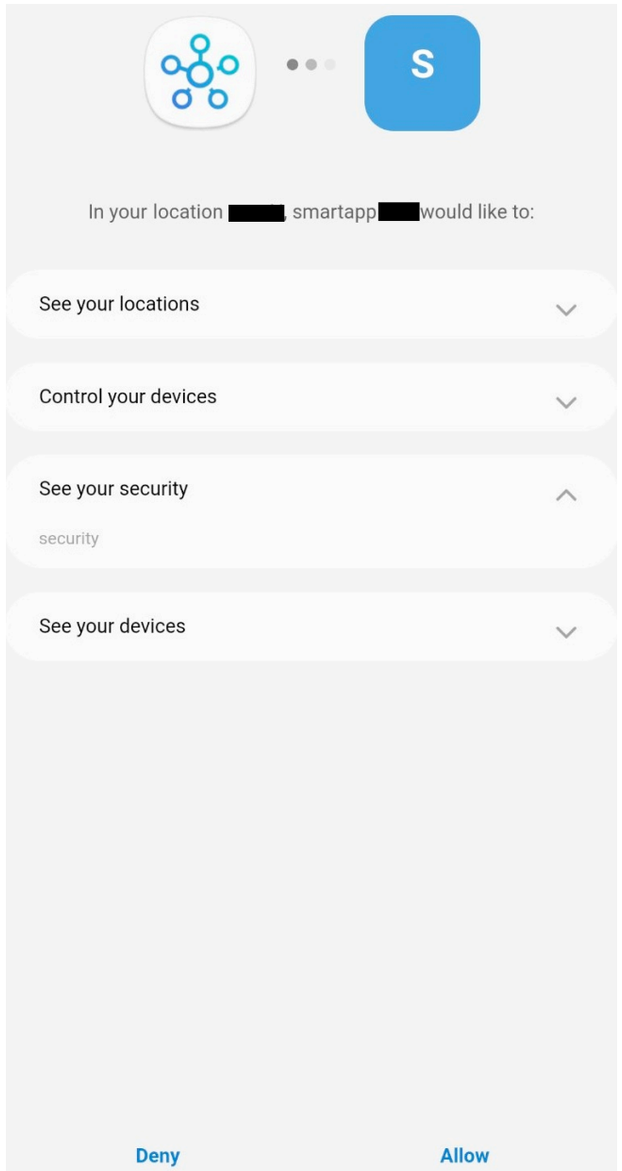
Smart Home Permission Model

Smart Home Permission Model

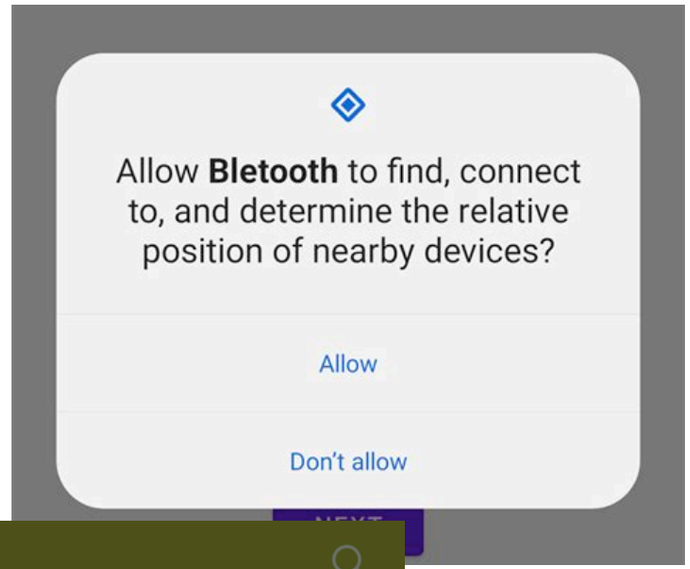
- ***A form of User-driven access control***

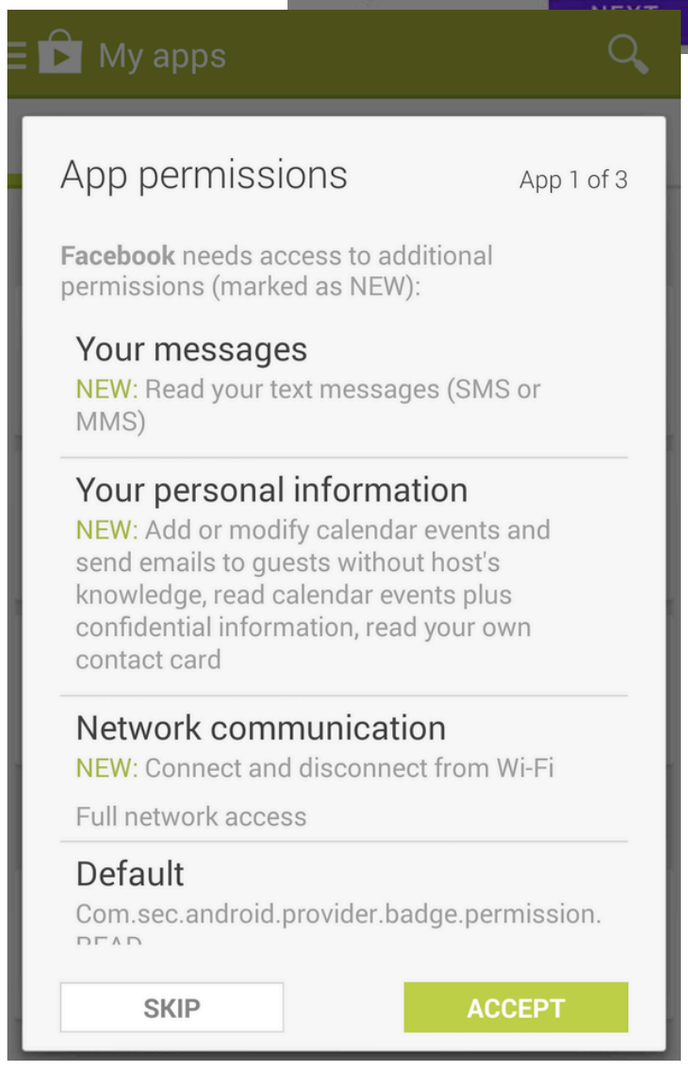


SmartThings



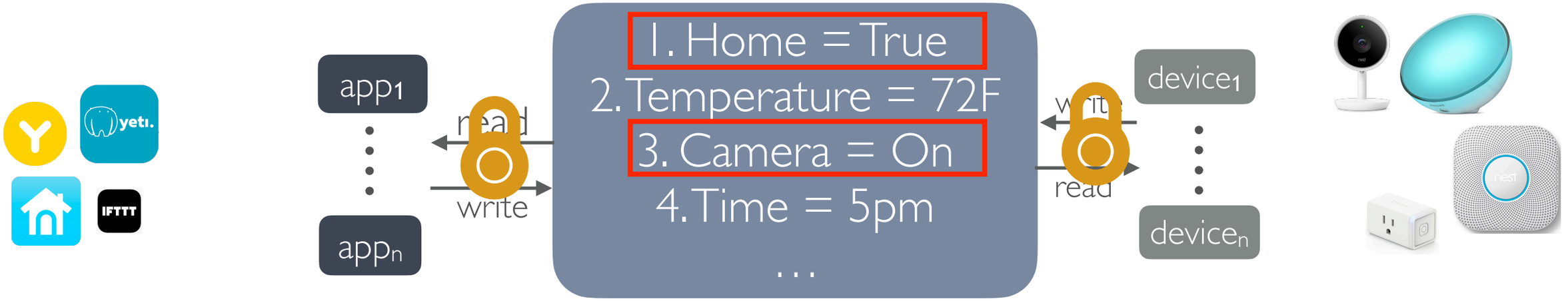
Android





Blast from the past..

Data Store-Based (DSB) platforms



Permissions protect reads/writes to high-security variables (e.g., Camera ON/OFF, user home/away)

Nest Developer Documentation

Caution: You must ask the user if it's ok to change streaming status (turn the camera on/off). The user must agree to this change before your product can change this field.

Platform Defenses

Nest Product Review

Platform Defenses

Nest Product Review

Analyze apps/services that request connection to nest

Set of guidelines for developers to follow

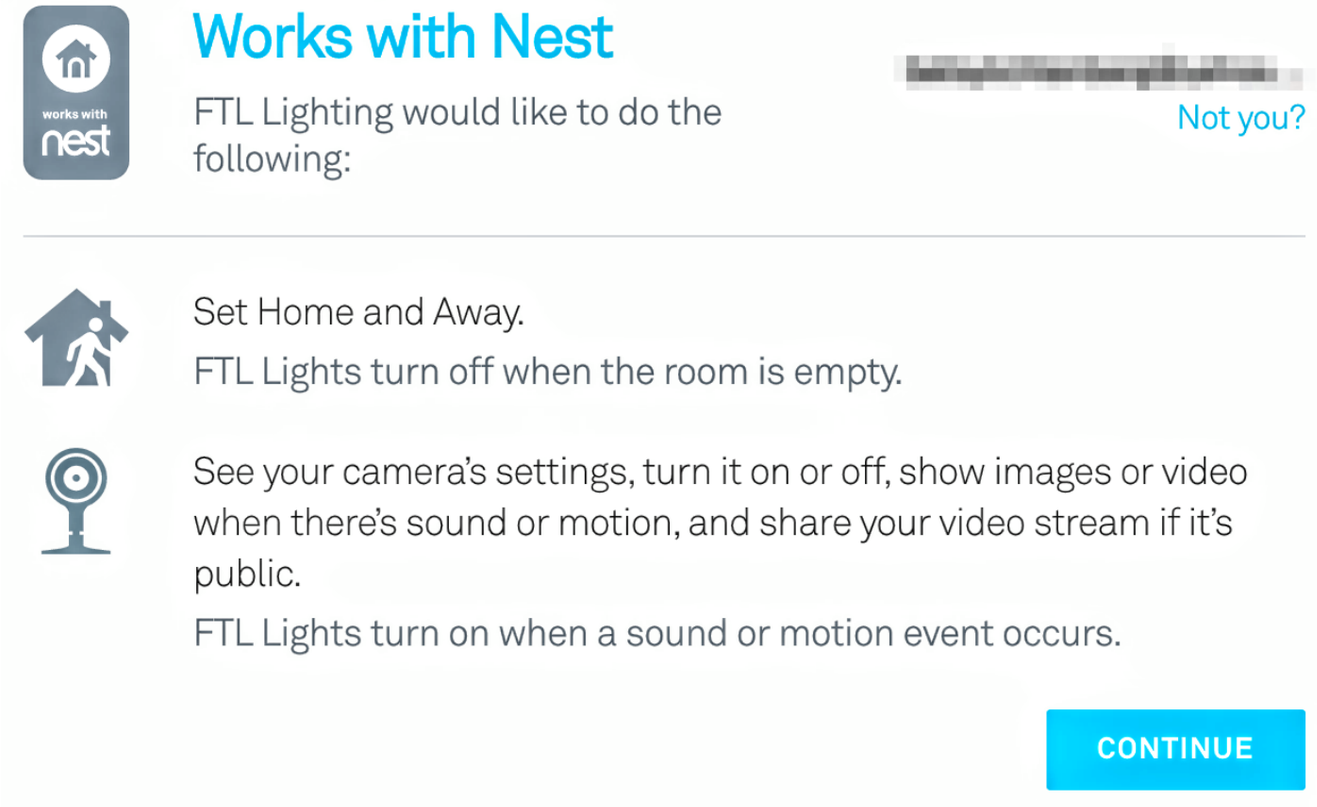
3.3 Products with names, descriptions, or permissions not relevant to the functionality of the product will be rejected.

5.8 Products that modify Home/Away state automatically without user confirmation or direct user action will be rejected.

Platform Defenses

Nest Product Review

3.3 Products with names,



confirmation or direct user action will be rejected.

Platform Defenses

Incorrect permission description in many apps

16 violations in 13/39 apps

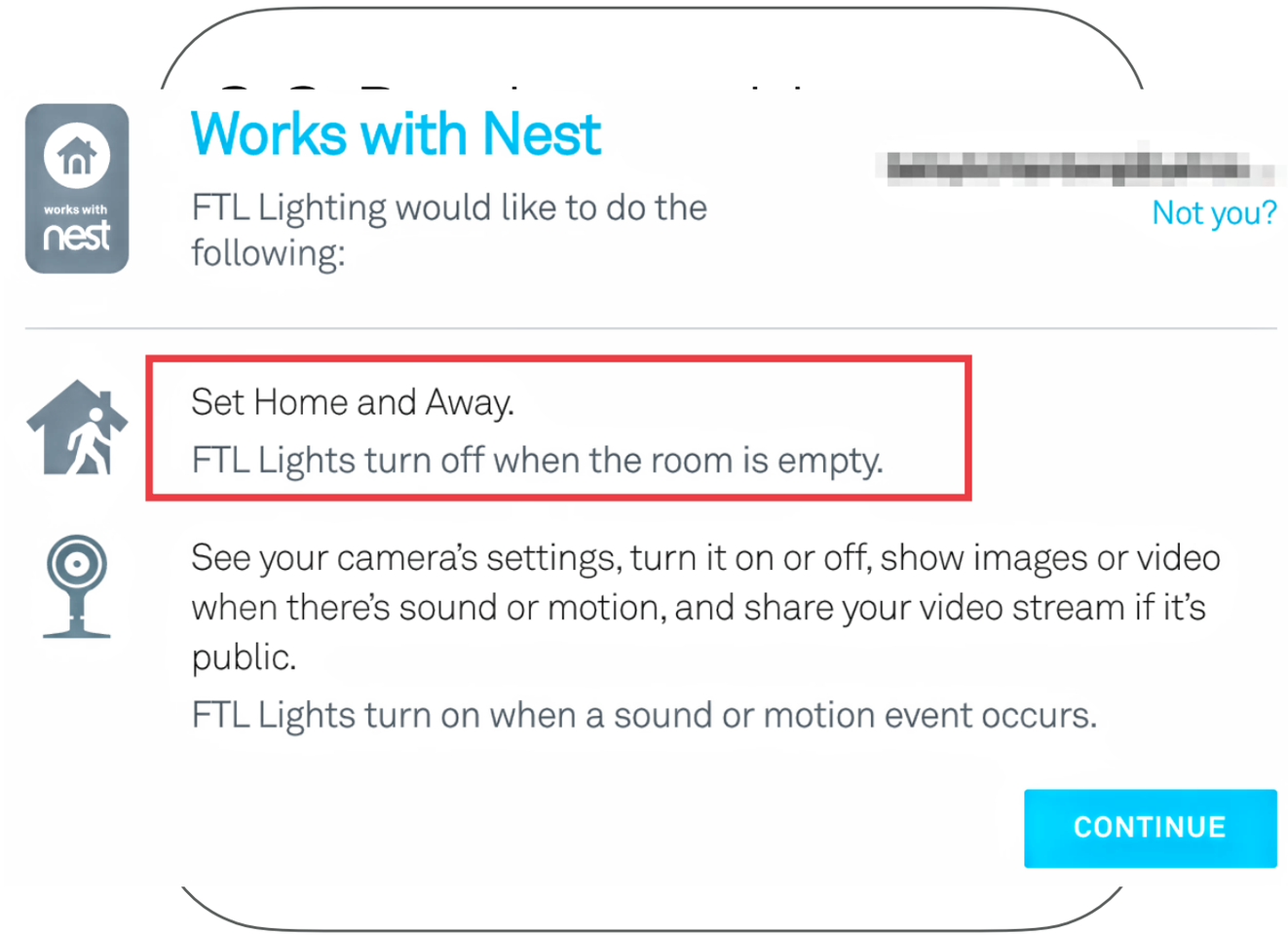
3.3 Products with names, descriptions, or permissions not relevant to the functionality of the product will be rejected.

5.8 Products that modify Home/Away state automatically without user confirmation or direct user action will be rejected.

Platform Defenses

Incorrect permission description in many apps

16 violations in 13/39 apps

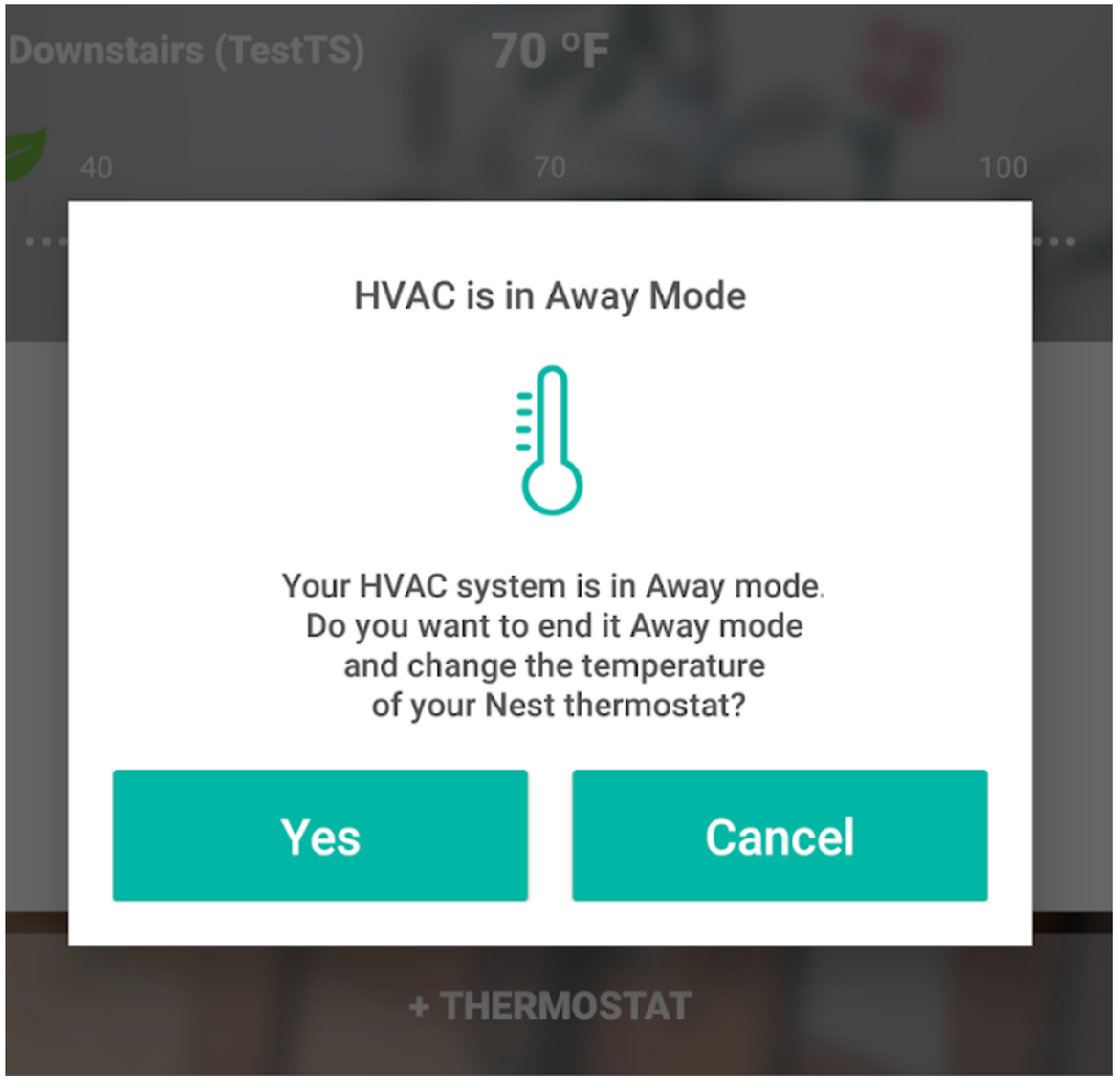


Source: NEST Documentation!

Platform Defenses

- A significant number of apps (~33%) provided incorrect permission descriptions
- In most cases of violations, apps request read/write permissions instead of read
  - ***Leads to overprivileged apps***

Runtime Prompt Violations



3.3 Products with names, descriptions, or permissions not relevant to the functionality of the product will be rejected.

5.8 Products that modify Home/Away state automatically without user confirmation or direct user action will be rejected.

RUNTIME PROMPT VIOLATIONS

- Nest product review has no constraints on *what* apps can display in run-time prompts
  - *Trusting the third-party?*

- Apps often incorrectly describe the *Away* field as a local field of the thermostat
  - *Coarse-grained view of permissions from the developers?*

- Product review is insufficient at reviewing correctness of permission descriptions and requests by apps
  - ***Manual?***

Lesson:

*Manual product reviews need to be accompanied by **static and dynamic analysis techniques** for efficiency and integrity guarantees*

Smart Home Privacy

Smart Homes

Transmit *device and environment data* to remote servers!

↓

Vendors may **process privacy-sensitive information** about home usage!

Behavior Profiling

Affecting Insurance Claims

Inferring Sensitive Information

Smart Homes

Transmit *device and environment data* to remote servers!

↓

Vendors may **process privacy-sensitive information** about home usage!

↓

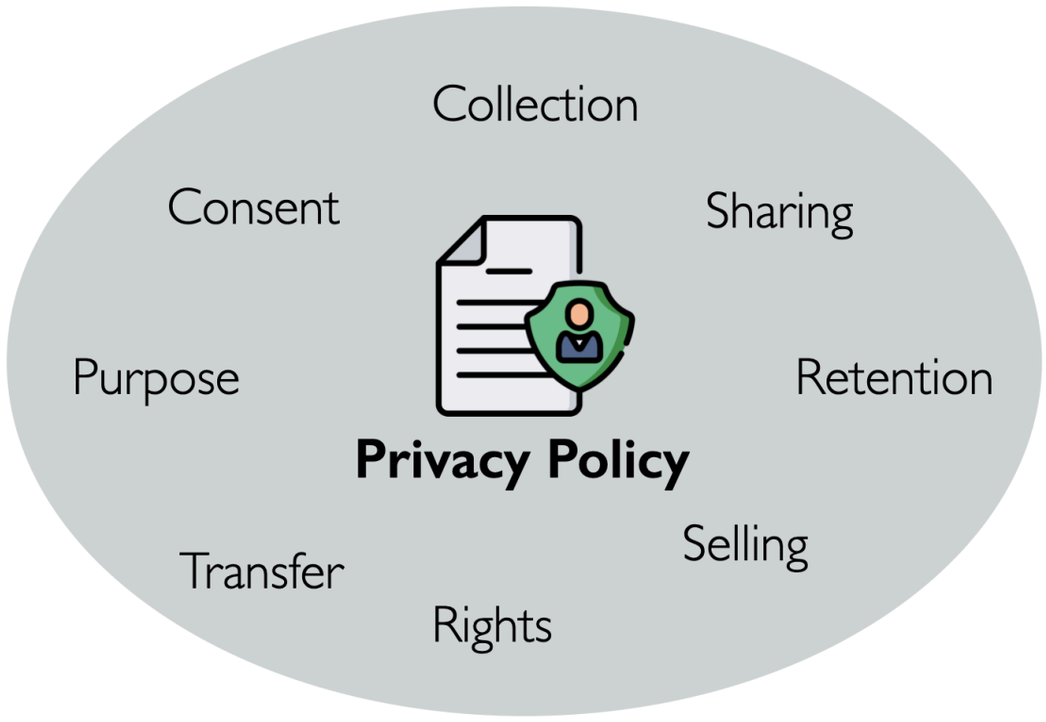
Consumers should be informed about the privacy practices with regard to device data.

Behavior Profiling

Affecting Insurance Claims

Inferring Sensitive Information

Privacy Policies



- **Legally Binding**
- **Conveys Data Handling Practice**
- **Informed Decision Making**

Privacy Policies

Inferring Sensitive Information

"XYZ may be required to process data that are deemed by applicable legislation to be sensitive, since they may incidentally reveal Users' religious beliefs or sexual orientation.

This may be the case if electricity and the Application are not recorded as being used between Friday night and Saturday night (***which could suggest that users belong to the Jewish faith***) or if only one room (such as a bedroom) is registered on the Application for a home shared by two people of the same sex (***which could suggest the occupants' homosexual or bisexual orientation***)."

Understanding Smart Home Privacy

How difficult is it for consumers to *obtain* privacy policies that apply to their smart home devices?

Availability

How *precisely* is the collection and sharing of device data described in smart home product privacy policies?

Content

How *comprehensive* are smart home product privacy policies in describing the collection/ sharing of device-data?

Coverage