Security and Privacy in the Smart Home Ecosystem

Kaushal Kafle, PhD Student, William & Mary, kkafle@wm.edu, *Advisor*: Prof. Adwait Nadkarni

William & Mary, CHARTERED 1693

Secure Platforms Lab

Motivation

- Smart Home Devices may collect and transmit sensitive user data.
- Attack surface is large due to multiple, heterogeneous system components (devices, apps, cloud), and third-party vendors.
- Security and privacy issues can compromise user's physical safety.
- Hence, it is critical to understand what security problems may exist, and how effectively vendors inform the users about their privacy practices.

RQ1: Are users informed of data collection and sharing?

- *Large-scale Privacy Policy Analysis*
- *Includes 596 vendors with 2442 devices*

Analysis of 3 properties

***Availability**: Are policies obtainable?*
***Content**: Does policy describe collection/sharing?*
***Coverage**: Does policy cover all devices?*

Availability

63/596 (10.57%) No privacy policy

225/517 (43.52%) No smart home privacy policy

104/292 (35.62%) Not available from website

Lesson:
Privacy policy for smart home devices can be difficult to obtain for users prior to purchase.

Content

***26.05%** - Discuss collection using broad terms (e.g. usage info)*

***70.42%** - Discuss collection at the granularity of device (e.g. temperature)*

***65.49%** - Discuss sharing of user's PII but not device data*

***34.28%** - Do not specify with whom data is shared*

Lesson:
Even when policy is available, users may not know what happens to their device data.

Coverage

***50/200 (25%)** – Policies that are granular discuss only a subset of vendor devices*

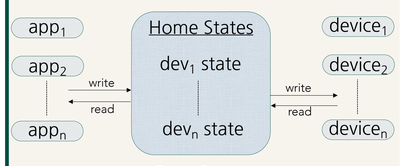
***23/26 vendors** – Do not differentiate policy for devices that produce similar data but have different privacy implications (e.g. baby monitor vs video doorbell)*

***29 vendors** – Describe collection at a granular level, but also discuss irrelevant data that their devices may not produce*

Lesson:
Even when vendors make smart home policy available, it may not cover all devices they sell.

RQ2: Are smart home platforms secure?

Platform Architecture



We analyzed 2 platforms

PHILIPS hue
- *Only lights and motion sensors*
- *Simple automation*
- *3rd-party apps*

nest
- *Supports diverse devices (doorlock, camera, sensors)*
- *Complex automation*
- *3rd-party apps*

Permission Enforced?

nest
- Permissions enforced correctly
- 3rd-party apps can only access limited portion of datastore

PHILIPS hue
*- 3rd party apps can bypass user consent**
*- Can remove/add other apps**
- Access all of datastore

Secure Communication?

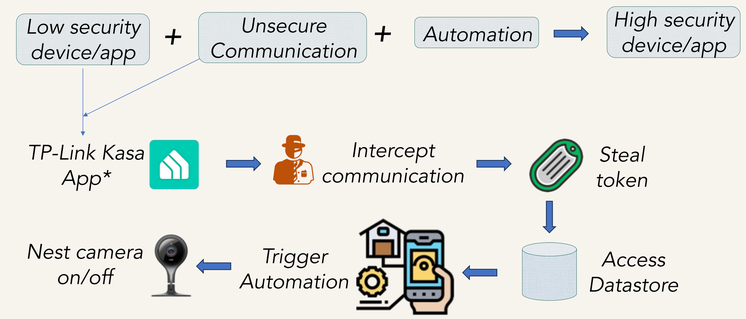
- Automated SSL analysis
- Analyzed 111 'works with Nest' apps
*- **19.82%** with at least 1 SSL issue*

Most Common Issues in:

***TrustManager** – Accept all Certificates – 20/111*

***HostNameVerifier** – Signed certificate, any hostname - 11/111*

Lateral Privilege Escalation Attack



***Lesson:** Vulnerability in one domain (apps) can permeate to a different domain (smart home), leading to vastly different consequences.*

** - Problems have been fixed since.*

RQ3: Are mobile-IoT apps secure?

Developed IoTSpotter Framework to identify IoT apps from their app descriptions.

Using IoTSpotter, we identified 37k mobile-IoT apps (accuracy ~88% upon manual validation).

Performed security analysis of 917 apps (>1M+ installs) for cryptographic vulnerabilities

Crypto-API Misuses

Automated analysis using CryptoGuard

***94.11% apps** – Contain at least 1 crypto-API misuse*

82.5% – High severity violations detected by Cryptoguard is True Positive upon manual validation

Other Vulnerabilities

***7887/37k (20.87%)** – Susceptible to Janus vulnerability, which allows attackers to modify installed apps without detection.*

***40 popular** apps (>50k installs) used vulnerable IoT libraries with known CVEs, with 6 over 1M installs.*

Lesson:
- *These vulnerabilities (crypto, janus, vulnerable library) impacts critical IoT components such as firmware integrity, app/device functionality, user authentication.*
- *App/device functionality includes security/privacy critical devices such as security cameras.*
- *Security tools need to be contextualized/targeted for IoT to prevent these mobile-IoT vulnerabilities.*

Conclusion

- Our studies highlight multiple security and privacy concerns in the smart home and IoT ecosystem.
- Security and privacy need to be enforced at every system components (platforms, apps, vendors) to prevent attacks on the user. As components are interconnected, only securing the whole ecosystem can secure the smart home effectively.
- Due to the multiple layers (3rd party vendors, apps, cloud), it is very difficult for the user to keep track of data collection and exfiltration. Hence, vendors need to be precise, and comprehensive about informing the users of data collected through their devices.

References:

RQ1: Manandhar, S., **Kafle, K.**, Andow, B., Singh, K., & Nadkarni, A. (2022). Smart Home Privacy Policies Demystified: A Study of Availability, Content, and Coverage. In *31st USENIX Security Symposium (USENIX Security 22)* (pp. 3521-3538).
RQ2: **Kafle, K.**, Moran, K., Manandhar, S., Nadkarni, A., & Poshyvanyk, D. (2020). Security in centralized data store-based home automation platforms: A systematic analysis of nest and hue. *ACM Transactions on Cyber-Physical Systems*, *5*(1), 1-27.
RQ3: Jin, X., Manandhar, S., **Kafle, K.**, Lin, Z., & Nadkarni, A. (2022, November). Understanding iot security from a market-scale perspective. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1615-1629).