A Study of Data Store-based Home Automation

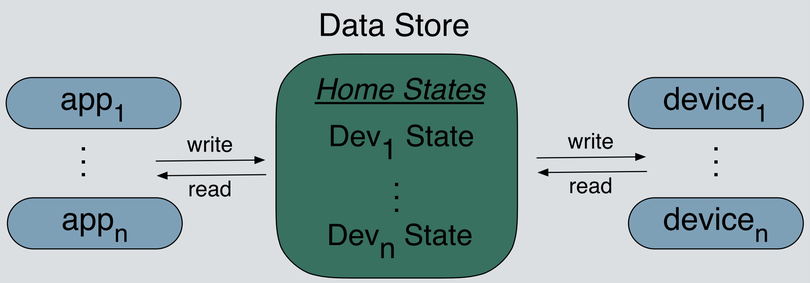
Kaushal Kafle, Kevin Moran, Sunil Manandhar, Adwait Nadkarni, and Denys Poshyvanyk
College of William & Mary, Williamsburg, VA, USA
{**kkafle**, kpmoran, smanandhar, nadkarni, denys}@cs.wm.edu

Motivation

- Smart home platforms enable home automation in the form of small **trigger-action based programs** called **routines**.
- Routines are facilitated by sharing access to a **central data store** to apps and devices in Data Store-Based (DSB) platforms.
- Since all apps/devices communicate through the data store, **potential to launch privilege escalation attacks** from low-security device to a high-security device.

Need to understand the potential of exploitation of routines in DSB platforms as well as platform's defenses.

DSB Platform Architecture



Apps

- Write to change device states
- Read to know device states

Devices

- Read to perform actions
- Write when their state changes

Analysis & Results

$\mathcal{F}$ - Indicates a finding

On 2 Platforms: **Google's Nest** and **Philips Hue**

Permission Enforcement

- Correctly enforced in Nest. $\mathcal{F}_1$
- In hue, **apps can bypass user**'s explicit consent. $\mathcal{F}_2$
- In hue, **apps can add/revoke access** to data store. $\mathcal{F}_3$

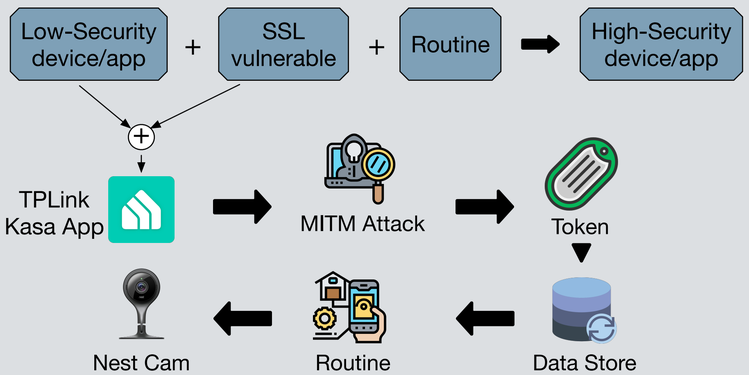
SSL usage

- **20.64**% of general smart home apps
- **19.82**% of Nest-integrated apps had SSL issues. Broken **Trustmanager** and **HostNameVerifier** main causes. $\mathcal{F}_4$

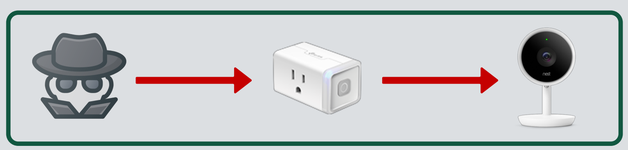
Routines

Apps **without explicit permission** to a sensitive device can legitimately trigger a routine and control the device. $\mathcal{F}_5$

Lateral Privilege Escalation Attack

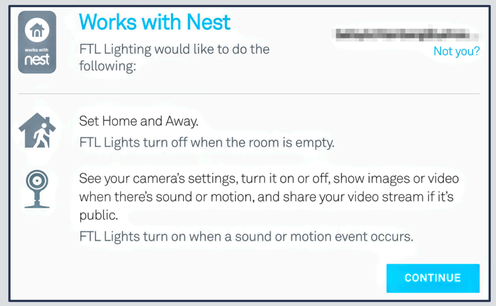


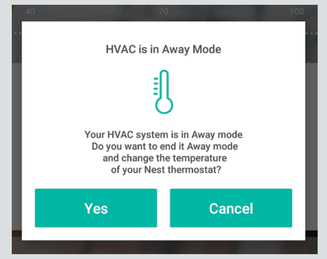
*__Routine__: When user is home (**trigger**), turn the security camera off (**action**).



Permission Prompt Issues

- Nest performs **product reviews** as a defense mechanism.
- Product reviews **insufficient to analyze correctness** of permission prompts $\mathcal{F}_6$





- Violation in **installation-time prompt**.
- Apps asked for **read/write** permission when the app **requires only read** access for functionality $\mathcal{F}_7$
- Apps **associated home/away to just thermostat**, even though it is a central home state $\mathcal{F}_8$

- Violation in **run-time prompt**
- Nest requires **apps to prompt user** when changing sensitive field
- Such prompts misused because Nest has **no constraint on what prompt can say**. $\mathcal{F}_9$

- In total, **16 violations** in **13/39** Nest integrated apps, **4 violation classes** based on the nature of violation $\mathcal{F}_{10}$

Takeaway

- Problems in **one domain can seep into another domain.** SSL issues in smart home apps have more impact as it affects user's physical safety.
- Platforms such as Hue are **not applying even the fundamental aspect of access control** in their data store.
- **Manual product review** in platforms needs to be accompanied with **automatic app analysis** techniques for efficiency, scalability and integrity guarantees.
- 3rd party apps are not trustworthy. They offer a wide attack surface to an attacker. **Smart home security evaluation** needs to include **mobile app evaluation** as well.

References

[1] Kafle, K., Moran, K., Manandhar, S., Nadkarni, A., & Poshyvanyk, D., "A Study of Data Store-based Home Automation", i*n Proceedings of the 9th ACM Conference on Data and Application Security and Privacy (CODASPY)*, Dallas, TX, USA, March 25-27, 2019.

Responsible Disclosure

We have reported these findings to the platform vendors and TPLink. The Phillips Hue team and TPLink have acknowledged the issues and have already fixed them, or are in the process of fixing them.