Security Assertions for Samsung SmartThings Apps

Max von Hippel

October 13, 2018

Definitions

Control: I say that a device x "controls" a device y if x can send meaningful instructions over a single channel to y under a gaurantee that y will deterministically follow those instructions. A non-meaningful instruction would be "do nothing"; conversely, I consider an instruction meaningful if it entails a change in state other than whatever state would have been attained in the absense of the instruction.

Structure of this Document

The remainder of the document consists of lists of loose security assertions. Devices inherit all of the assertions of their capabilities. Devices inherit all of the assertions made under Universal Security Assertions. Smart homes inherit all of the individual and interactive assertions of their devices.

Security Assertions Governing Device Interaction

1. Loosely speaking, devices should not disagree on the security status of a building. For instance, if the front door is set to "away mode" (locked, and alarm goes off if someone enters the house without entering the correct pin code), then the kitchen window should not be allowed to open.
2. Loosely speaking, smart hub devices should negotiate contradicting sensor readings from different devices.
3. Loosely speaking, users should be prompty alerted of off-nominal device behaviour.

Universal Security Assertions

1. The device cannot perform arbitrary network actions [RSWO17].
2. Over cyber-channels, the device can only deliberately communicate with a finite, authenticated, non-repudiated, and documented list of other devices.
3. All data and metadata generated or recieved by the device (locally stored or in transit) is encrypted under a NIST-approved cryptosystem and with a user-supplied, nontrivial key.
4. The device will detect anomolous readings from any of its sensors, and respond by notifying the user and other connected devices. In this case the device will enter a safe mode, where it does not perform potentially sensitive actions in response to sensor stimulus.
5. If the device is battery-powered, it will preiodically report its battery status to the user, along with a conservative estimate of remaining charge. In particular the device will alert the user in advance of complete discharge.
6. Sensors accurately observe environmental variables within their known hardware limitations. Variables outside of those limitations are recognized as immeasurable by the sensors, and evaluated accordingly.

7. Every value should be type-checked. For instance, the relative-humidity is by definition a value on the scale $[0, 100]$, so a relative-humidity of 101 should never be reported. Type violations should be reported to the end-user and any connected devices.
8. If an actuator fails, this failure is detected and reported to the user.

Capability-Specific

Acceleration Sensor, Button, Contact-Sensor, Illuminance Measurement, Motion Sensor, Presense Sensor, Relative Humidity Measurement, Temperature Measurement, Three-Axis Sensor (IMU), Water Sensor

No additional security assertions.

Alarm

Example: Fortrezz Siren Strobe Alarm [For18].

Security Assertions:

1. The alarm will go off when triggered, at the intended volume etc.

Lock

Example: Yale Assure Lock with BlueTooth (ZigBee) [Yal18].

Security Assertions:

1. The lock cannot be non-destructively dissembled without access to the side of the door facing the interior of the locked volume [Jer18].
2. The lock cannot unlock for more than 10 unique codes.
3. If an unlock code is not used to unlock the lock over any consecutive 60-day span, the user will be notified, and explicitly given the option to remove that code from the list of codes which unlock the lock.
4. The lock unlocks if and only if an unlock key code is physically entered into the keypad.

Momentary

1. The "moment" in a momentary command cannot exceed 15 minutes in delay.
2. A momentary command cannot invoke another momentary command.

Switch

Example: Lutron Caseta Wireless Plug-In Lam Dimmer [Lut18].

Security Assertions:

1. The switch cannot directly control supply of more than $250W$ of power [SMP18].
2. The outlet cannot switch between "On" and "Off" states more than twice per second [SMP18, Pho18].

Switch Level

Example: Devices of the type "Universal Dimmer".

Security Assertions:

1. The switch level cannot control more than 10 devices at once. If it sends an instruction to any one of those devices, it must also send the same instruction to the other devices under its control.
2. The controlled-devices list of the switch level cannot change more than twice per minute.
3. The switch level cannot control any device exceeding $500W$ in power demand [SMP18].

4. Let $x(t) \in [0,1] \subset \mathbb{Q}$ represent the graduated state of the switch level at a time t, where 0 denotes "completely off" and 1 denotes "completely on". Then for any time t_0 and constant $0 < \delta < 1$, there can exist at most two distinct times t_1, t_2 in $(t_0, t_0 + \delta)$ at which $\frac{dx(t)}{dt}\Big|^{t_1} < 0 < \frac{dx(t)}{dt}\Big|^{t_2}$ [Pho18].

Thermostat

Example: ecobee ecobee4 Thermostat [Eco18].

Security Assertions:

1. The thermostat is controlled over encrypted communication by a Smart Hub device in the same building [Eco18]. The only way to control the thermostat is through the intermediary Smart Hub device.

Device-Specific

Light Bulb

Example: Philips Hue White LED Bulb (A19) [Phi18].

Security Assertions:

1. The light-bulb cannot switch between off and on states more than once in a single second [Pho18].
2. The only way to control the light-bulb is through a specific intermediary Smart Hub device in the same building [Phi18].

Universal Dimmer

Subset of Switch Level Capability.

Example: Leviton Universal Dimmer [Lev18].

Security Assertions:

1. The dimmer cannot directly control any device which is not a light [Lev18].

HD Camera

Example: Netgear Arlo Wire-Free Pro HD Camera [Net18].

Security Assertions:

1. The camera cannot physically interact with any external memory hardware without explicit authorization by an authenticated and non-repudiated user [Net18].
2. No more than 100 cameras can connect over a single network and user account at once [Oli18] [SMP18].

Voice Assistant

Example: Google Home [Goo18].

Security Assertions:

1. The device differentiates between sensitive and non-sensitive instructions. Sensitive instructions require authentication commenserate with the authentication required to perform the action without a voice assistant. For example, if a smart lock requires a 10-key code to unlock, then the voice command to unlock the smart lock via the voice assistant should require a 10-key spoken code.
2. Voices are ID'd through some robust learning system. If a new voice interacts with the device, a unique ID is generated for this voice against which it can be matched in the future, and the ID is stored on the device.
3. The cumulative power requirements of devices controlled by the voice assistant cannot exceed 1 kW [SMP18].
4. The device robustly differentiates between anologue voices (a person actually talking) and digital voices (a voice recording being played through a digital speaker system), and does not respond to the latter.

Power Outlet

Subset of Switch Capability.

Door Lock

Subset of Lock Capability.

References

[Eco18] ecobee ecobee4 thermostat. https://www.smartthings.com/products/ecobee-ecobee4-thermostat, 2018.

[For18] Fortrezz siren strobe alarm. https://www.smartthings.com/products/fortrezz-siren-strobe-alarm, 2018.

[Goo18] Google home. https://www.smartthings.com/products/google-home, 2018.

[Jer18] JerryRigEverything. Do not buy this $100 smart lock... https://www.youtube.com/watch?v=RxM55DNS9CE, June 2018.

[Lev18] Leviton universal dimmer. https://www.smartthings.com/products/leviton-universal-dimmer, 2018.

[Lut18] Lutron caseta wireless plug-in lamb dimmer. https://www.smartthings.com/products/lutron-caseta-wireless-plug-in-lamp-dimmer, 2018.

[Net18] Netgear arlo wire-free pro hd camera. https://www.smartthings.com/products/netgear-arlo-wire-free-pro-hd-camera, 2018.

[Oli18] Olivia. https://reolink.com/cctv-ip-security-camera-power-consumption/, October 2018.

[Phi18] Philips hue white led bulb (a19). https://www.smartthings.com/products/philips-hue-white-led-bulb-a19, 2018.

[Pho18] https://www.epilepsy.org.au/about-epilepsy/understanding-epilepsy/photosensitive-epilepsy/, 2018.

[RSWO17] E. Ronen, A. Shamir, A. Weingarten, and C. O'Flynn. Iot goes nuclear: Creating a zigbee chain reaction. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 195–212, May 2017.

[SMP18] Saleh Soltan, Prateek Mittal, and H. Vincent Poor. Blackiot: Iot botnet of high wattage devices can disrupt the power grid. In *USENIX Security Symposium*, 2018.

[Yal18] Yale assure lock with bluetooth (zigbee). https://www.smartthings.com/products/yale-assure-lock-with-bluetooth-zigbee, 2018.