On the Behavior of Smart Devices

Peter Borrell* Laura Clayton* James Curry* Daniel Massey*
* *University of Colorado Boulder.*

Objectives

- Explore ways to fortify IoT devices based on their characteristics
- Better understand the characteristics used by IoT devices
- Identify smart devices to fortify
- Define a class of *infrastructure devices e.g.*
  - A device that performs a defined action based on a defined request
- Determine whether the characteristics can form patterns for the router to flag

Status Quo

- Devices exhibited unpredictable network behavior that could yield network vulnerablity
- Devices may be vulnerable to ransomware, leading to leaks or loss of personal information

Frequency/ Predictability

IoT device categories: Highly Active (HA), Moderately Active (MA), Consistently Active (CA), or No packet data (NA).

1. The iSelect outlet constantly did a heartbeat (HA)
2. The TP-Link bulb did a heartbeat at a set interval (MA)
3. Switch and Timer performed routine tasks: either updates or a set timed event (CA)
4. Thermostat had encrypted packets (NA)

Registration vs Normal Operation

- Registration: EAPoL Request and probe request with data packet
- Normal Operation: Sending a probe request to perform an action if device exists

Behavior / Device	No Tracker Cookies recieved	Access defined servers by DNS	Replies to requests with hard coded actions	Exhibits routine traffic if a command is not sent	Only perferms actions if authenticated user requests it
iSelect Smart Outlet	True	True*	False	True	False
TP-Link Smart Bulb	True	True	True	True	True
Nest Thermostat E	True	True	Not exhibited	Not exhibited	True
Nintendo Switch	True±	True±	True	True	True
B-Hyve Smart Faucet Timer	True	True*	True	True	True

± Denotes the behavior of the device in its “vanilla” state. By using a hardware exploit this behavior will be changed due to the device no longer being in its intended sand box state.

* Denotes that the device should exhibit this behavior, but there is no record in network traffic. The firmware does not get updates as mentioned. However, there is a chance no firmware was updated during the test period.

“Not exhibited” means the device may perform the action but it does not display network traffic

Connectivity

- Devices come with encrypted and unencrypted connections
- Encrypted are device to router with header encrypted to router
  - This makes them hide in network traffic
- Unencrypted has the packet header shown on the network
  - Body content may or may not be encrypted

Our Proposal

- Standardize how interactions occur, e.g.:
  - The iSelect keeps pinging the network
  - The Nest Themostat encrypts all traffic once connected
- IoT devices should establish a secure connection with router using EAPoL and once the secure connection is established, all traffic should be encrypted internally
- Only allow authenticated agents to interact with the connected devices

Future Work

- Develop tools to automatically identify Infrastructure devices and add home network protections to prevent unauthorized traffic from these devices.
- Narrow definition of infrastructure devices
- Use with network connected medical devices