Malware Detection in Smart Home Devices through Network Traffic Monitoring and Device Attestation

R. T. Prapty, R. Trimananda, S. Jakkamsetti, G. Tsudik, A. Markopoupou
University of California, Irvine

Motivation

- Fast adoption of smart home devices in all aspects of daily lives
- Critical security and privacy risks posed by malware infected smart home devices
- Risk mitigation by frequent device memory attestation highly expensive
- Possible reduction in the attestation cost by utilizing network traffic monitoring

Figure: Robot Vacuum Cleaner

Figure: Smart Plug

Main Idea

- Limited and predictable traffic pattern of smart home devices
- Deviation from normal pattern when infected by malware
- Incorporating network traffic monitoring and device attestation to detect malware infected smart home devices
  1. Network traffic monitoring detects abnormal traffic patterns of a device
  2. This triggers the device attestation
  3. Attestation software verifies the anomaly and gives feedback to the monitoring system
  4. This helps to improve the detection model
- Device assumed to contain a hardware root of trust to execute attestation program

Figure: Smart Lock

Evaluation

- Evaluation done by developing profiles and monitoring 15 smart home devices

Experimental Setup

- A Raspberry Pi 4 machine is configured to work as a wireless access point
- **Device Profile Builder Module** and **Network Monitor Module** are run on this machine
- All the smart home devices are connected to the local area network
- NXP board emulated smart bulb contains the **Device Attestation Module**

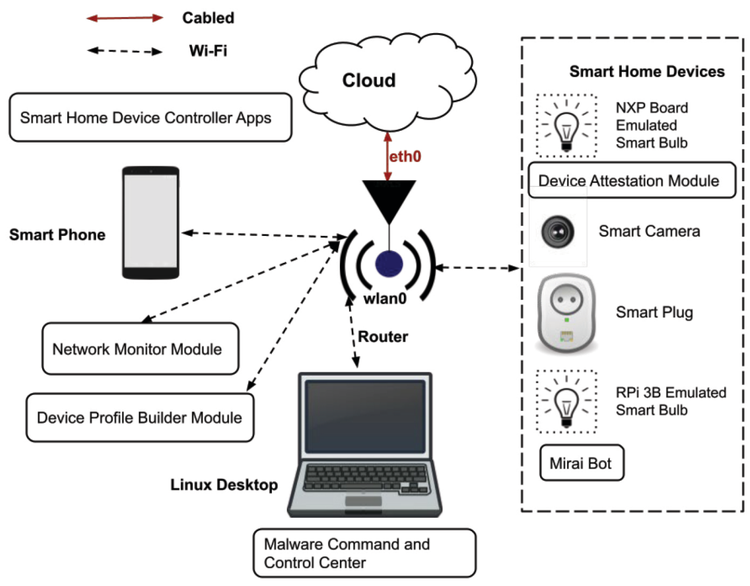

Figure: Network Setup

Result

- The performance of the Network Monitor Module is measured after developing necessary device profiles.
- The system is evaluated for both off the shelf uninfected devices and an infected RPi emulated smart bulb

Monitoring Uninfected Devices

False Positive Rate(FPR) is calculated for each uninfected devices. Two different scenarios:

- Only endpoints from packets are matched with endpoints from profile entries
- Both endpoints and packet length are matched

Monitoring Infected Devices

- An emulated smart bulb on RPi 3 is used for this purpose
- During training period, profile is built for the uninfected bulb
- After that the bulb is infected with Mirai, Bashlite, malware binary files
- The Network Monitor module is able to detect suspicious packets for:
  - The network payload sent from the malware C&C during bot installation
  - Subsequent communication between the bot and the C&C
- The detection **accuracy** of the Network Monitor Module was **100%**

Device Name	FPR (endpoints only)	FPR (endpoints & length)
Amazon Smart Plug	0.0%	0.0591%
HBN Smart Plug Mini	0.0%	0.00274%
Ring Doorbell	0.00046%	0.7513%
Blink Mini Camera	0.0%	0.0835%
Nest Camera	0.0%	0.1076%
Lumiman Smart Bulb	0.0%	0.0142%
Kasa Smart Bulb	0.0%	0.0657%
LIFX Smart Bulb	0.0%	0.0%
NXP Emulated Bulb	0.0%	2.1276%
RPi Emulated Bulb	0.0%	0.0392%
ULTRALOQ U-bolt Pro	0.0%	0.0114%
Sensi Thermostat	0.0%	0.1892%
Nest Protect Smoke Alarm	0.0%	1.3223%
Rachio Sprinkler	0.0217%	1.3018%
iRobot Roomba	0.0%	0.4039%

Table: False Positive Rate of uninfected devices

Methodology

Three main components :

1. Device Profile Builder
2. Network Monitor
3. Device Attestation

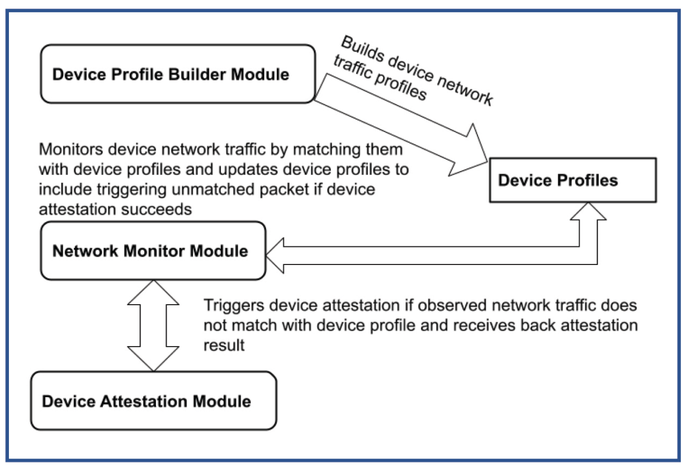

Figure: System Overview

Device Profile Builder Module

- Builds up device profiles during training phase by processing network packets generated by devices
- All possible functionalities of each device triggered
- Network packets filtered per device by using the device mac address
- Five properties extracted from each packet
  1. Source IP Address
  2. Source MAC Address
  3. Destination IP Address
  4. Destination MAC Address
  5. Packet Length
- Each device profile includes multiple entries
- DNS packets specially processed to develop IP address-host name mappings
- MAC addresses used to determine packet direction
- Local source/destination IP address replaced by MAC address in profile entry
- Remote source/destination IP address replaced by host name if available through IP-address host name mapping or Reverse DNS Lookup

Device Name	Packet Direction	External Address	Packet Length
Lumiman Bulb	SERVER_TO_DEVICE	a3.tuyaus.com	145
Lumiman Bulb	DEVICE_TO_SERVER	a3.tuyaus.com	145
Lumiman Bulb	SERVER_TO_DEVICE	ec2-54-188-109-168.us-west-2.compute.amazonaws.com.	123
Lumiman Bulb	DEVICE_TO_SERVER	ec2-54-188-109-168.us-west-2.compute.amazonaws.com.	54
Lumiman Bulb	DEVICE_TO_DEVICE	192.168.4.111	58

Table: Partial Snapshot of Summarized Lumiman Bulb Device Profile

Network Monitor Module

- Matches packets generated by a device to its profile entries
  - A more detailed version of device profile entries used for this purpose
  - We use packet source address and packet destination address for matching instead of packet direction and external address
- Partial matching is used for packet source and destination address
  - At first Top Level Domain Name is matched. Then partial string matching is applied
- A packet fails to match with any profile entry because of two reasons:
  - **Mismatched Endpoints**
  - **Mismatched Length**
- An unmatched packet is considered suspicious, and Device Attestation Module is called
- Network Monitor works as a verifier for the Device Attestation Module and provides three parameters: **Authentication Token, Challenge, PID**
- If the device attestation module gives feedback that it was a false positive, then a new profile entry is created for the device based on the packet

Device Attestation Module

- Attests a predefined memory region of the device when triggered
- It receives ***Challenge***, ***Authentication Token***, ***PID***
  - Authentication token is used to authenticate the verifier,
  - Challenge is used to mitigate replay attack.
  - PID can be used to very the memory of a specific process.
- Calculates the HMAC of the specified memory region and compares it with an expected HMAC value of the region
- The expected value should be calculated initially when the region is known to be fresh/uninfected by malware
- If the currently calculated hmac value does not match the expected value then the device is compromised and the attestation fails. Otherwise attestation succeeds.
- The attestation result is sent back to the verifier

Next Steps

- Evaluating the Network Monitoring Module with large number of different malware
- Building malware profiles from malware generated traffic

SaTC Frontiers: Collaborative: *1956393* [1], *1955227* [2], *2103439* [3], *1956435* [4]
Institutions: UC Irvine [1], Northeastern Univ. [2], UC Davis [3], USC [4]
Lead PIs: A. Markopoulou [1], D. Choffnes [2], Z. Shafiq [3], K. Psounis [4]