IoT Device Vulnerability Exploitation

JONATHAN DERENGE, ALEXANDRA LEE
MENTOR: ROBERT RICHARDSON

Introduction

Consumer demand for convenience, accessibility, integration, and remote management of electronic devices has led to the rapid growth of the Internet of Things (IoT). The rapid adoption of edge computing and 5G in addition have increased in the manufacturing, retail, and health care sectors. Cost is a significant factor in consumer choice of IoT devices. Vendors have responded by producing a wide variety of capable devices in a wide range of categories., including the domain of home automation (see Fig. 1).

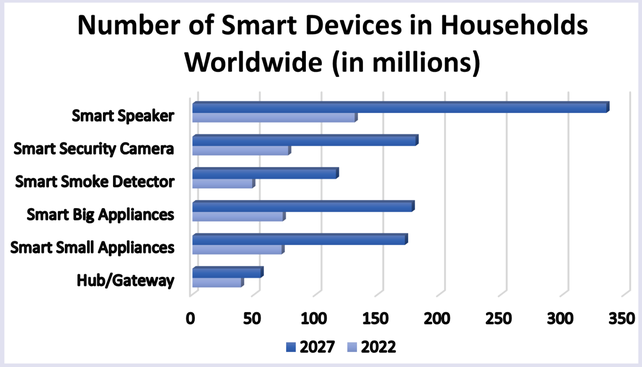

Figure 1. Adapted from Reference 1

Background

Our research is focused on house-hold smart consumer grade IoT Appliances. To represent the multitude of devices currently on the market, we examined a smart electric space heater, a smoke detector, and a wireless security camera. A testing environment (see Fig. 3) was created consisting of all the devices connected to one access point—a Hak5 Mark VII Wi-Fi Pineapple (see Fig. 3). Most of the tools that were used come pre-installed on the Kali distribution of Linux (see Table 1). Our mobile application testing was conducted on Android x86 running on VirtualBox, and a rooted Motorola G 7 Power running Magisk.

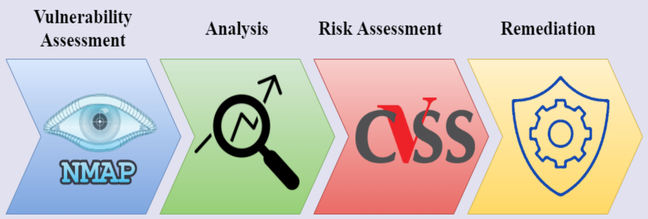

Figure 2. Vulnerability Assessment (image adapted from Reference 2)

Tools Utilized	Type	Function	Outcome
Nmap	Port Scanner	. Network recon tool	. Scanned all ports . Service Detection
TCPdump/Wireshark	Packet Analyzer	. Record & analyze Wi-Fi traffic from the Pineapple	. Examined port traffic to & from router
Magisk TrustUserCerts	Android system mask	. Used to install packages & certificates on Android	. Imports user certs into system directory
Burpsuite/Mitmproxy	Proxy interceptor	. Man-in-the Middle	. Viewed unencrypted application network traffic
Aircrack-ng suite	Wireless network sniffer/injector	. Wireless pen-testing and reconnaissance tool	. Performed deauthentication attack

Table 1. Security Tools

Methodology

Vulnerability assessment is the evaluation of a system's overall security by analyzing various components of a system's architecture. The first step was examining aspects of each device's functionality by identifying its features advertised in the user manual and exploring its mobile application. Additionally, examined how the devices interacted with each other over the wireless network (see Fig. 3). After hypothesizing and investigating potential vulnerabilities, several security tools were used to conduct testing (see Table 1). By forwarding all mobile traffic to a local computer on the network, encrypted network traffic could be viewed. After importing a certificate generated by Mitmproxy into the system/security/cacerts directory of the Android device, this data could be viewed in clear text from the remote host (see Fig. 4).

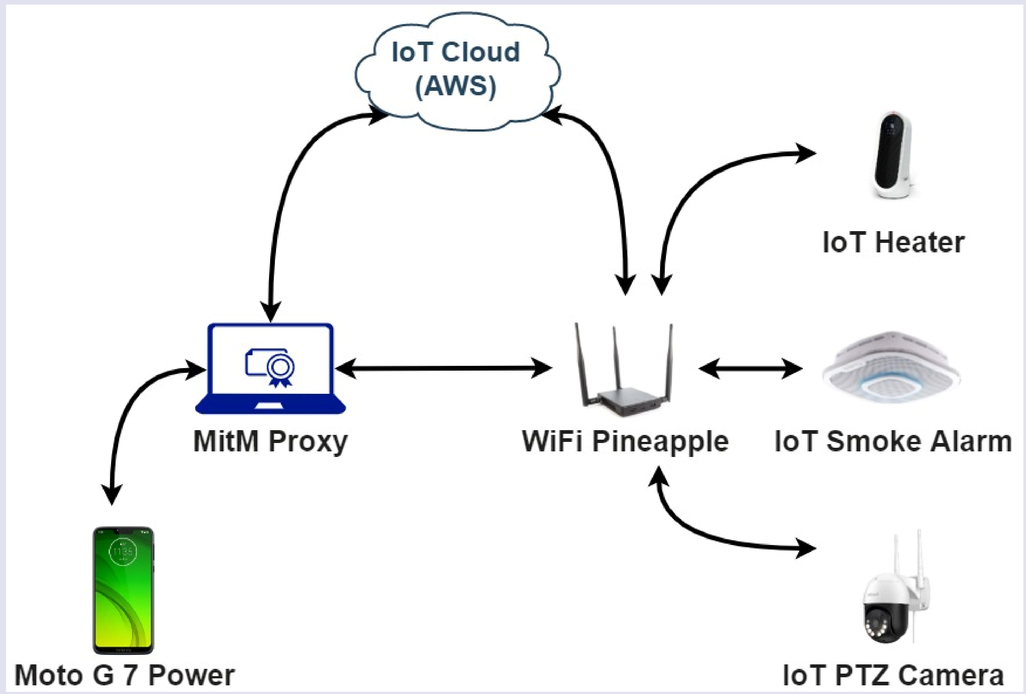

Figure 3. Network Diagram with Mitmproxy

Significant Findings

- Some functions can't be performed outside the device network
  - Change alarm language; Bluetooth speaker
- No certificate pinning on smoke detector application
- All applications support TLS 1.3
- Root detection on smart heater application

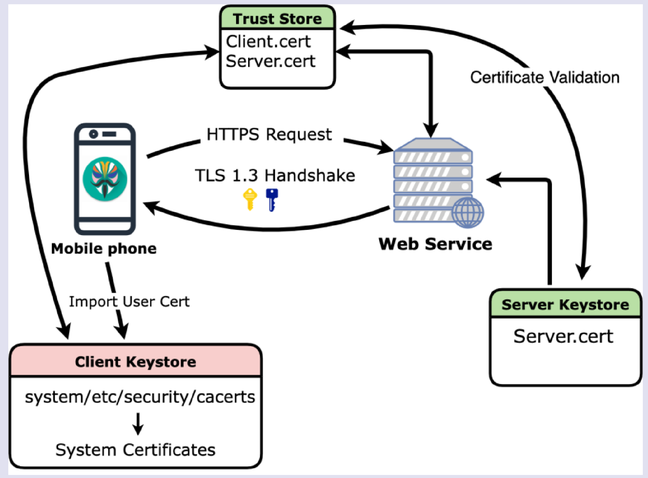

Figure 4. Cert.-Based Mutual Authentication (adapted from Ref. 3)

Remediation & Continued Work

This research highlights the important security consideration of household smart appliances. The man-in-the-middle attack performed using Mitmproxy revealed the various functions which handled device information including user emails, security tokens, and device configurations. One method that can mitigate this risk is a technique known as certificate pinning. Wherein, a server only allows select certificates, generally from reputable Certificate Authority (CAs) when establishing a secure connection. Because changes in CAs can cause users to lose the ability to connect with the server, it's not a recommended practice (Android Developers, 2022). Future plans involve continued enumeration of the devices to uncover additional information. Upon conclusion, the vendors will receive a report highlighting the security issues affecting their product.

References

[1] M. Armstrong and F. Richter, "Infographic: Homes are only getting smarter," *Statista Infographics,* 26-Apr-2022. [Online]. Available: www.statista.com/chart/27324/households-with-smart-devces-global-iot-mmo/. [Accessed: 20-Jul-2022].
[2] "Silent breach," *Vulnerability Assessment.* [Online]. Available: silentbreach.com/vulnerability-assessment.php. [Accessed: 20-Jul-2022].
[3] HTTPS Client Authentication," *HTTPS client authentication (the java EE 6 tutorial, volume I).* [Online]. Available: docs.oracle.com/cd/E19226-01/820-7627/bncbs/index.html. [Accessed: 20-Jul-2022].
[4] "Security with HTTPS and SSL: android developers," *Android Developers.* [Online]. Available: developer.android.com/training/articles/security-ssl. [Accessed: 20-Jul-2022].

Acknowledgements

This research was supported by the National Science Foundation (NSF) under Award CNS-1852145. We would like to thank the NSF for funding this research.
Additional assistance provided by Angel Gamboa, Aiden Schramm, and Riley Basaran.