Digital Investigation 26 (2018) S38–S46

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

DFRWS 2018 USA — Proceedings of the Eighteenth Annual DFRWS USA

Welcome pwn: Almond smart home hub forensics

Akshay Awasthi [a], Huw O.L. Read [a, b, *], Konstantinos Xynos [c, b], Iain Sutherland [b, d]

[a] Norwich University, Northfield, VT, USA
[b] Noroff University College, Elvagata 2a, Kristiansand, Norway
[c] DarkMatter LLC, Dubai, United Arab Emirates
[d] Security Research Institute, Edith Cowan University, Perth, Australia

Keywords:
Internet of things
Extraction
Smart sensor
Smart home hub
iOS
Android
Cloud

A B S T R A C T

Many home interactive sensors and networked devices are being branded as “Internet of Things” or IoT devices. Such disparate gadgets often have little in common other than that they all communicate using similar protocols. The emergence of devices known as “smart home hubs” allow for such hardware to be controlled by non-technical users providing inexpensive home security and other home automation functions. To the cyber analyst, these smart environments can be a boon to digital forensics; information such as interactions with the devices, sensors registering motion, temperature or moisture levels in different rooms, all tend to be collected in one central location rather than separate ones. This paper presents the research work conducted on one such smart home hub environment, the Securifi Almond+, and provides guidance for forensic data acquisition and analysis of artefacts pertaining to user interaction across the hub, the iPhone/Android companion applications and the local & cloud-based web interfaces.

1. Introduction

The rapid expansion of internet enabled devices has lead to the realization of the “Internet of Things” (IoT) as first mentioned by Ashton (2009). These devices have expanded the interaction between humans and technology, but also increased the risk and impact of possible vulnerabilities in devices or their implementation. IoT devices are advancing at a considerable rate. Currently, there is estimated to be more than 6.4 billion IoT devices connected, and the number is expected to reach a total of 8.4 billion connected IoT devices in 2017 (Gartner, 2017), other estimates suggest this rising to 30.7 billion devices in 2020 and estimated to increase to 75.4 billion in 2025 (Columbus, 2016). The volume and variety of IoT devices presents a challenge to the digital forensics examiner. One particular market for IoT devices is developing the “Smart Home” as evidenced in the USA where the real estate market is adapting a “Smart Home” policy and is trying to sell more houses that have IoT devices installed (Paxton, 2017). Smart homes use a variety of devices, integrated to provide intelligent features such as providing security, automation and energy conservation.

The degree of human interaction with these systems suggests that they have the potential to provide a significant amount of information to a digital forensics investigation. Currently there is limited information available offering forensic investigators an insight into what information of interest is stored on the vast range of devices, or how to acquire data in a forensically sound fashion. This paper seeks to provide a greater insight into the types of information available in Home Automation Smart Hubs that may be of value to law enforcement agencies in those territories where these devices are available.

The rest of this paper is organised as follows: Section 2 describes similar forensic examinations on other smart hub devices, section 3 presents our experiment configuration and introduces features of the device, section 4 identifies issues faced during the course of investigation, section 5 describes the process taken to identify artefacts, section 6 details how an investigator may extract artefacts from devices in the Almond environment, section 7 identify locations where evidence of note may be found, section 8 provides a summary of data extraction and analysis, and finally, section 9 provides a summary of the research presented in this paper and thoughts for continuing the examination.

2. Related work

There are a number of challenges presented by IoT devices in terms of extracting, accessing, interpreting and verifying the data. This is because devices have widely varying functionality, often a customised operating system and may use one or more of a number

* Corresponding author. Norwich University, Northfield, VT, USA.
E-mail address: hread@norwich.edu (H.O.L. Read).

https://doi.org/10.1016/j.diin.2018.04.014

wireless network transmission protocols. This is now a significant area of concern with research efforts focused on the analysis and data extraction from popular IoT devices, e.g. Meffert et al. (2017) and Oriwoh et al. (2013). The complexity, variety and distribution of IoT devices, which are by their nature part of an infrastructure, may cause significant problems. Simply gaining physical access to the systems can be a separate challenge altogether for the analyst. However, in many cases, there is little of forensic value on the devices themselves. What may prove to be of greater importance is accessing any system used to integrate IoT devices providing centralised control (Sutherland et al., 2015). Typically, domestic systems are connected via some form of hub or central service to facilitate a "Smart Home". The integration of these devices has already raised security concerns (Plachkinova et al., 2016). Generally, the forensic analysis of Smart Hubs thus far has been limited. The following section describes related work carried out to date on three such systems; Amazon Alexa, Apple HomeKit and Google OnHub or Google Home.

2.1. Amazon Alexa

The Amazon Alexa system is a combination of specific hardware (Echo and Echo Dot) and the cloud based Alexa personal assistant. The considerable popularity of the Amazon Alexa System has led to some community efforts exploring the analysis of the device including the hardware (dj_skully, 2016). An analysis by the LCDI (2016) provided some insight regarding performing a forensic analysis on the Amazon Alexa, via third party devices. The report explains techniques for data collection and data extraction. The greatest challenge they encountered was third-party device integration with the Echo. The data collection using such devices and their companion applications was found to be generating possible discrepancies in the data. Chung et al. (2017) considered the Alexa ecosystem and proposed a possible toolkit to support forensic analysis; it *tries to acquire (download) cloud-native artifacts from the server using the unofficial APIs*…. A challenge experienced by the authors in the past is unofficial APIs are subject to change without warning which could then require revising of code, that is if the functionality is still available. Hyde and Moran (2017) describe both destructive and non-destructive methods of accessing the Amazon hardware to extract evidence.

2.2. Apple HomeKit

The Apple system uses the iCloud keychain to retain information on devices and other information and requires an Apple iOS device or Apple TV to remain in the home to act as a hub for external access (Apple, 2017a). Apple released the HomePod in early 2018, which appears to be limited in capacity acting as a speaker and an interface to Siri and HomeKit devices (Apple, 2017b). Given Apple's public stance on encryption and working with law enforcement (Cook, 2016), the challenge of extracting forensic data from the Home environment will likely be of particular interest to digital forensic researchers.

2.3. Google OnHub and Google Home

Google Home provides a similar service to that of Alexa with access to various Google services and Google assistant. It is capable of running on either the Android or Apple iOS Operating Systems. Launched in 2017, it can interface with a number of IoT devices, there is however very limited information on forensic best practice with this system. Another possible device the investigator might encounter is the Google OnHub (Google, 2017) which takes a different approach than that adopted by Amazon. Rather than becoming an additional device on the network, the OnHub is intended to replace the home router with one system that can interface with Smart/IoT devices.

3. Almond ecosystem

The Almond+ is a smart home hub that integrates the functionality of a router with the ability to control and respond to IoT sensors and devices. It has the ability to work with or without Internet connectivity (Securifi, 2017). It is more akin to devices such as Googles OnHub, than Amazon's Echo, in that it is designed to replace an existing router. The device also provides the facility to be setup as a repeater or an access point. The Almond + supports two IoT protocols, namely Zigbee and Z-Wave. Fig. 1 demonstrates how the following sensors were connected to the Almond + environment for the experiment:

- Three Philips Hue Lamps via a Philips Hue Bridge - changes colour, dimming, on/off
- Jasco Dimmer Plug, 3-pronged dimmer device
- Securifi Peanut Plug, on/off power device
- Fibaro Door/Temperature Sensor, two-components
- NYCE Motion/Temperature/Humidity Sensor, positioned on ceiling
- Two NYCE Door Sensors, alternative to Fibaro

There are four ways for a user to interact with the Almond ecosystem, via the hardware itself, a companion app on iOS or Android, and through Cloud or local web interfaces.

3.1. Via the touchscreen

The Almond + provides an interactive touch screen to the user as depicted in Fig. 2. The interface on the Almond + provides a myriad of information to the user: settings, adding and controlling sensors, weather, list of users, firewall, security and sharing features.

3.2. Via the companion app

The smart app for the Almond+ is available for iOS and Android (Fig. 2) and both have a consistent look and feel. The app provides more information than the web interface and is able to connect locally (LAN) or via cloud to the Almond + router. In local mode, the environment does not need Internet connectivity to work. The Cloud connectivity feature provides the user facility to monitor and control the smart sensors connected to the Almond + remotely. The cloud connectivity also provides the history for the sensor activity.

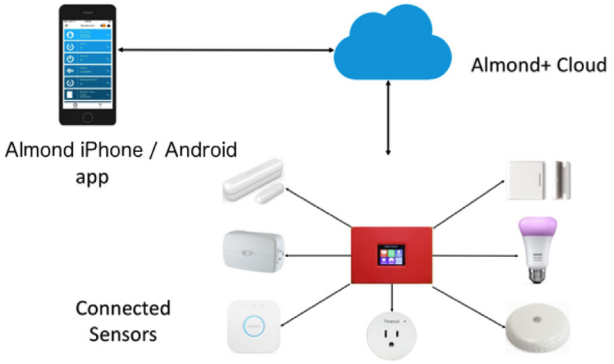

Fig. 1. Almond+ Environment Setup.