Digital Investigation 22 (2017) S15–S25

Contents lists available at ScienceDirect

Digital Investigation

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

DFRWS 2017 USA — Proceedings of the Seventeenth Annual DFRWS USA

Digital forensic approaches for Amazon Alexa ecosystem

Hyunji Chung, Jungheum Park, Sangjin Lee*

Center for Information Security Technologies (CIST), Korea University, 145 Anam-ro, Seongbuk-Gu, Seoul, 02841, South Korea

Keywords:
Internet of Things
Cloud-based IoT
Intelligent virtual assistant (IVA)
Amazon Alexa
Amazon Echo
Cloud native forensics
Client centric forensics
CIFT

A B S T R A C T

Internet of Things (IoT) devices such as the Amazon Echo – a smart speaker developed by Amazon – are undoubtedly great sources of potential digital evidence due to their ubiquitous use and their *always-on* mode of operation, constituting a human-life's black box. The Amazon Echo in particular plays a centric role for the cloud-based intelligent virtual assistant (IVA) Alexa developed by Amazon Lab126. The Alexa-enabled wireless smart speaker is the gateway for all voice commands submitted to Alexa. Moreover, the IVA interacts with a plethora of compatible IoT devices and third-party applications that leverage cloud resources. Understanding the complex cloud ecosystem that allows ubiquitous use of Alexa is paramount on supporting digital investigations when need raises. This paper discusses methods for digital forensics pertaining to the IVA Alexa's ecosystem. The primary contribution of this paper consists of a new efficient approach of combining cloud-native forensics with client-side forensics (forensics for companion devices), to support practical digital investigations. Based on a deep understanding of the targeted ecosystem, we propose a proof-of-concept tool, *CIFT*, that supports identification, acquisition and analysis of both native artifacts from the cloud and client-centric artifacts from local devices (mobile applications and web browsers).

Introduction

The Internet of Things (IoT) is evolving rapidly along with the network of physical objects that contain embedded communication technology. Analysts predict that the worldwide IoT market will grow to $1.7 trillion in 2020 with a compound annual growth rate (CAGR) of 16.9% (IDC, 2015). Gartner predicts that 25% of households using an intelligent virtual assistant (IVA) will have two or more devices by 2020 (Gatner). The ubiquitous use of wearables, personal smart devices, smart appliances, etc., will generate a large amount of digital data that can be a great source of digital evidence.

In several recent criminal investigations, law enforcement officials, legal experts and forensics experts attempted to use "always-on" IoT devices as sources of forensic artifacts similar to human-life black boxes. In particular, one recent criminal investigation case involving an Amazon Echo, gained widespread attention in the media. In November 2015, James Bates was charged with first-degree murder of another man, who was found dead in Bates' hot tub. Police in Arkansas seized Bates' Alexa-enabled Echo smart speaker from his home, and asked Amazon to hand over any pertinent information regarding the device's communication with Alexa. However, Amazon denied the request in the absence of a valid and binding legal demand (Techcrunch).

While there are many legal questions regarding the use of this type of evidence, there are also important technical considerations. Most importantly, to efficiently investigate these types of cases, it is first necessary to understand the digital forensic characteristics of Amazon's Alexa and its ecosystem.

When Alexa-enabled, Amazon Echo is not only a smart speaker, but operates as an intelligent, personal virtual assistant. As a cloud service, Alexa interacts with various Alexa-enabled devices such as Echo, and it can communicate with other compatible IoT devices and third-party applications by converting the voice requests to other services' native communication protocol. Also, for customizing these Alexa-related environments, users should access the cloud service using companion clients, such as PC or mobile (Android and iOS) devices. Thus, the ecosystem created by all these interconnected devices, third-party applications and companion clients is complex and heterogeneous (Amazon). In this paper, we will refer to this ecosystem as the *Amazon Alexa ecosystem*.

We propose a new digital forensic approach for the Amazon Alexa ecosystem combining cloud-side and client-side forensics. The acquisition of cloud-native artifacts from the Alexa is very important. Echo operations are based on Alexa, so the cloud includes

* Corresponding author.
E-mail address: sangjin@korea.ac.kr (S. Lee).

http://dx.doi.org/10.1016/j.diin.2017.06.010

many different types of artifacts related to user behaviors. Unfortunately, this approach has two limitations. First, it requires valid user accounts in order to access the cloud. There is, of course, the potential to discover access information through investigation or interrogation, but this information is not always available. Second, it is difficult to recover deleted data on the cloud. Client-side forensics approaches are needed to overcome these limitations. That is, when it is impossible to acquire cloud-native artifacts, companion clients can offer important artifacts for digital investigations.

As a result of our analysis, we introduce a proof-of-concept tool for cloud-based IoT environments, *CIFT: Cloud-based IoT Forensic Toolkit*, which can acquire cloud native artifacts from Alexa using unofficial APIs and analyze client-side artifacts associated with the use of a web-based application. We also tried to normalize all identified artifacts into a database file, and visualize them for evaluating our approach and further supporting the work of the digital forensics community. In a situation where existing tools and procedures cannot meet the demand for this emerging IoT system, our findings and proof-of-concept tool will be helpful for investigators attempting to work in the Amazon Alexa environment.

The rest of the paper is organized as follows. Section Amazon Alexa and digital forensics describes the target system and Section Related works reviews existing works. Section Forensic artifacts on Amazon Alexa ecosystem presents our findings for digital forensics and Section Design and implementation introduces an implementation based on our findings. Section Visualization and evaluation evaluates results with visualization techniques. Finally, Section Conclusion and future works discusses conclusions and next steps.

Amazon Alexa and digital forensics

Research motivation

In the IoT world, the do-it-yourself culture is encouraged, meaning users themselves can develop customized devices and applications for their IoT environments with tiny sensors and programmable brokers (Roeck et al., 2012). However, it is not easy for people who are unfamiliar with state-of-the-art technologies to build customized IoT environments. Thus, most people tend to purchase IoT consumer products, including but not limited to smart assistants, lights, sensors, switches, hubs, thermostats, and fitness devices.

Although a variety of products are available on the market, we focused on one of the most famous products, Amazon Echo. The Amazon Echo family of smart devices, which also includes Dot and Tap, connect to the intelligent cloud-based voice service, Alexa Voice Service (AVS). With Alexa as a voice-activated personal assistant, the Echo is capable of doing various things, such as managing to-do lists, playing music, setting alarms, placing orders, searching information, and controlling other smart devices (Amazon). According to an industry report, the Echo family sold more than 11 million units between the middle of 2015 and 2016 (1redDrop). Additionally, as announced at CES 2017, there is an interesting convergence of the Alexa with various devices, such as connected cars, smart fridges, and robots, which indicates that the Amazon Alexa-related environment will become an important source of potential digital evidence. For these reasons, the Echo and Alexa were selected as the first targets for studying digital forensic approaches inside the IoT world.

Amazon Alexa ecosystem

Before presenting our analysis, we describe the detailed architectures related to the target IoT environment. As mentioned above, the Amazon Echo controls an interface for communicating with the cloud-based service, Alexa. Cloud-based operations, such as Echo and Alexa, represent a general operating method of IoT consumer products because most are inseparable from cloud services in providing interoperability with companion clients and compatible devices for user convenience. Therefore, this subsection describes the target IoT environment focusing on its cloud service, Alexa.

The Amazon Alexa ecosystem is composed of various components, as shown in Fig. 1. First, one or more Alexa-enabled devices are required for talking to the Alexa cloud service. We should note our description specifically relates to the ecosystem associated with Amazon's Echo devices, and other devices exist for communicating with the cloud service. Next, the Alexa in the figure represents all Amazon cloud platforms supporting operation of this ecosystem. So it includes various cloud services for authentication, data management, and logging, as well as the Alexa Voice Service. In addition to these core components, one of the interesting aspects from the viewpoint of digital forensics is that companion clients are essential to managing the overall operating environment through access to the cloud server. The companion client means a personal device for executing Alexa companion applications, such as the Amazon Alexa

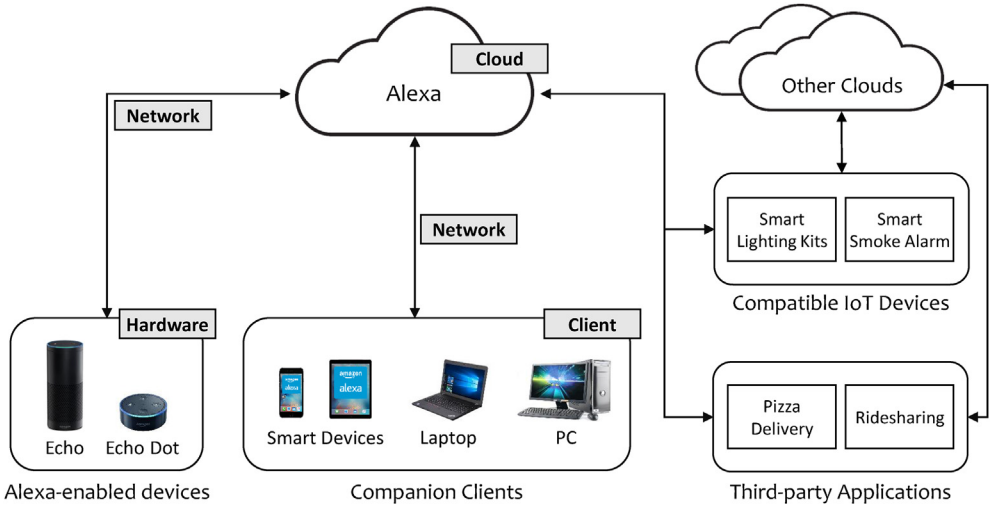

Fig. 1. Amazon Alexa ecosystem.