Contents lists available at ScienceDirect

Digital Investigation

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

A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics

Asanka Sayakkara, Nhien-An Le-Khac, Mark Scanlon*

Forensics and Security Research Group, University College Dublin, Ireland

ARTICLE INFO

Article history:
Received 10 October 2018
Received in revised form
1 March 2019
Accepted 11 March 2019
Available online 15 March 2019

Keywords:
Electromagnetic side-channel attacks
Internet-of-things (IoT)
Digital forensics
Data encryption

ABSTRACT

The increasing prevalence of Internet of Things (IoT) devices has made it inevitable that their pertinence to digital forensic investigations will increase into the foreseeable future. These devices produced by various vendors often posses limited standard interfaces for communication, such as USB ports or WiFi/Bluetooth wireless interfaces. Meanwhile, with an increasing mainstream focus on the security and privacy of user data, built-in encryption is becoming commonplace in consumer-level computing devices, and IoT devices are no exception. Under these circumstances, a significant challenge is presented to digital forensic investigations where data from IoT devices needs to be analysed.

This work explores the electromagnetic (EM) side-channel analysis literature for the purpose of assisting digital forensic investigations on IoT devices. EM side-channel analysis is a technique where unintentional electromagnetic emissions are used for eavesdropping on the operations and data handling of computing devices. The non-intrusive nature of EM side-channel approaches makes it a viable option to assist digital forensic investigations as these attacks require, and must result in, no modification to the target device. The literature on various EM side-channel analysis attack techniques are discussed – selected on the basis of their applicability in IoT device investigation scenarios. The insight gained from the background study is used to identify promising future applications of the technique for digital forensic analysis on IoT devices – potentially progressing a wide variety of currently hindered digital investigations.

Introduction

Digital forensics is the field where legal investigations are assisted by analysing digital sources of evidence. In contrast, cybersecurity is the domain where the concern is to ensure the security of digital data and the privacy of their owners. In today's modern world, technology is becoming increasingly prevalent in everyday life and many people stay almost always connected to the Internet (Nie and Erbring, 2000). While various social networks facilitate their users to share their life events to the rest of the world intentionally, every computer-based device they interact with in everyday life leaves unintentional traces of their activities. Such sources of forensic information include computer hard disks, network activity logs, removable media, internal storage of mobile phones and many others (Soltani and Seno, 2017).

Internet of Things (IoT) is an emerging trend started as a narrow research domain called wireless sensor networks, which evolved into Internet-connected everyday objects. IoT ecosystem includes a wide variety of devices, such as smart-watches, smart TVs, CCTV cameras, medical implants, fitness wearables, etc. The increasing availability of IoT devices across society makes it inevitable to find them in modern crime scenes and digital forensic investigations. Most of these devices comes with limited data processing and storage capabilities and they usually possess limited standard interfaces to the outside world, such as USB ports or WiFi/Bluetooth wireless interfaces, unlike their PC counterparts (Stojkoska and Trivodaliev, 2017).

Due to the increasing concerns regarding security and privacy among communities, modern digital devices, such as computer systems, mobile devices, etc., are designed and shipped with built-in security. Popular smartphones, such as iOS and Android based devices, encrypt their internal storage in order to protect user data from third parties (Ahmad et al., 2013). Each of the mainstream PC operating systems, such as Mac OS, Windows, and Linux, provide built-in hard disk encryption. Meanwhile, network

* Corresponding author.
E-mail addresses: asanka.sayakkara@ucdconnect.ie (A. Sayakkara), an.lekhac@ucd.ie (N.-A. Le-Khac), mark.scanlon@ucd.ie (M. Scanlon).

https://doi.org/10.1016/j.diin.2019.03.002
1742-2876/© 2019 Elsevier Ltd. All rights reserved.

communications, both wired and wireless, commonly employ strong packet encryption mechanisms (van de Wiel et al., 2018). Modern computer hardware has made the automated handling of encrypted data an everyday possibility in consumer, industrial and military applications (Fritzke, 2012). Computer devices seized at a crime scene containing encrypted data poses a significant challenge to the investigation (Lillis et al., 2016; Sayakkara et al., 2018a). The IoT device ecosystem is no exception for this data encryption trend making the challenge of digital forensic investigations on IoT devices even more complex.

Side-channel analysis attacks have been proven to be useful to breach security on computer systems when standard interfaces, e.g., network interfaces and data storage devices, are sufficiently protected (Spreitzer et al., 2018; Dhem et al., 1998; Zhang et al., 2014; O'Malley and Choo, 2014). In order for a side-channel attack to be effective in practical scenarios for a security breach, it has to be executable without having physical access to the device being attacked (Wakabayashi et al., 2017). In the case of digital investigation, the investigator has the freedom to handle the device, and ideally, any investigative activity must not affect or change the digital information in the device (Du et al., 2017). Electromagnetic (EM) Side-channel Attacks is one approach that has shown promising results. It requires minimum physical manipulations to the device being inspected (Hayashi et al., 2013). EM emissions of a device can be passively observed to infer both the internal operations being performed and the data being handled (Sayakkara et al., 2018a). This condition is ideal for a digital investigator who attempts to ensure that the device does not go though any physical changes due to its investigation. It is worth noting that hardware manufacturers are continuously trying to circumvent EM side-channel attack vulnerabilities through EM shielding and operation obfuscating enabled firmware.

This paper discusses the possibility for EM side-channel analysis as a potential case-advancing possibility for digital forensic analysis of IoT devices. A comprehensive analysis of the literature is provided identifying some promising avenues for research and their future potential. EM side-channel attacks for the recovery of cryptographic keys and other forms of important information are evaluated for potentially overcoming the encryption problem in digital forensics on IoT devices. Since the nature of EM emission phenomena is associated with the power consumption of computing devices (Callan et al., 2015a), the literature that focuses on power analysis attacks are also discussed where appropriate.

The contribution of this work can be summarised as follows:

- A comprehensive literature review and a comparative study of the research that has been carried out in EM side-channel analysis is provided and recent advances are summarised.
- The scenarios where different EM side-channel attacks in the literature are relevant and applicable in digital forensic investigations are identified.
- Light is shined on several new avenues of research that are possible to achieve in digital forensic investigations and cybersecurity through the adoption of EM side-channel analysis techniques.
- The shortage of reliable tools and frameworks available to utilise EM side-channel analysis for digital forensic investigations on IoT devices is identified and the recommendations are made to overcome it.

The rest of this paper is organised as follows. Section 2 presents an overview of side-channel attacks. Sections 3, 4, and 5 explores approaches for acquisition, unique identification, and information leakage EM emissions relevant to digital forensics. In Section 6, the advancements in wireless communication technologies and standardisation, and the legal background relevant to EM side-channels are discussed. Section 7 provides insights of possible future ethical directions of this technique. Finally, Section 8 concludes the paper.

Side-channel attacks

The topic of side-channel attacks spans a wide variety of techniques. Each side-channel attack on a computer system focuses on one specific unintentional leakage of information from either hardware or software (Spreitzer et al., 2018). Some of such information leaking side-channels are listed below.

- The memory and cache spaces shared between different software.
- The amount of time a program takes to respond to different inputs.
- The sounds different components of computer hardware make.
- The amount of electricity a computer system draws.
- The EM radiation a computer hardware emits.

Computer programs contain conditional branches and loops in order to handle inputs and produce the intended output. Depending on the input values, the execution path of a program can differ, which may result in a different program execution time. It has been shown that the execution time of encryption algorithms can reveal information regarding the input values provided to it, which includes the encryption key (Dhem et al., 1998). For example, the square and multiplication segment in the RivestShamirAdleman (RSA) algorithm checks whether a key bit is 0 or 1 before moving into multiplication operations. Therefore, the observation of large number of execution times with the same key and different input data can lead to uncovering the key bits effectively (Dhem et al., 1998; Brumley and Boneh, 2005; Kocher, 1996).

In environments where multiple virtual machines (VMs) run on the same hardware, such as cloud infrastructure, cache-based side-channel attacks are possible (Zhang et al., 2014). While each VM has its own virtual resources, many of them are mapped into shared physical resources including shared cache memories. It has been shown that an attacker running a VM on a virtualised environment can spy on a victim VM through the shared cache storage. This can lead to the extraction of sensitive information, including cryptographic keys (Liu et al., 2015).

It has been shown that acoustic emanations from various components and peripherals of computer systems can be used to exfiltrate information (O'Malley and Choo, 2014). Genkin et al. showed that it is possible to distinguish between CPU operations by listening to acoustic emanations resulting in an attack on the cryptographic keys of the RSA algorithm (Genkin et al., 2014).

Computer displays and their video cables have also been identified as an eavesdroppable EM source, which can leak the image being displayed on the display. Such leakages from CRT based displays have been known for several decades (Van Eck, 1985). Video information provided to a computer display has synchronisation information to recognise between different lines of pixels and different frames, which are called horizontal and vertical synchronisations. By recognising this synchronisation information in the EM emissions, an attacker can reconstruct the images being displayed (Hongxin et al., 2009; Elibol et al., 2012).

Kocher et al. were the first to introduce power consumption based side-channel attacks; *simple power analysis* (SPA) and *differential power analysis* (DPA) (Kocher et al., 1999). SPA collects power consumption variation (in mA) over time with a high sample rate, such as twice the clock frequency of target cryptographic device. The waveform of the power consumption, when plotted against