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

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.

© 2019 Elsevier Ltd. All rights reserved.

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).

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

time, contained patterns that corresponded to the instructions of the data encryption standard cryptographic algorithm (DES). If SPA can reveal the sequence of operations, it follows that this sequence depends on the data being handled by the algorithm (due to conditional branching). Designing code to minimise data dependent branching, which does not show characteristic power consumption patterns for specific operations, can prevent attackers from recognising what is executing on the device (Zankl et al., 2018).

DPA is a technique that can be custom tailored for specific encryption algorithms. Kocher et al. used the DPA technique against DES (Kocher et al., 1999). The technique was able to guess the encryption key accurately, given sufficient cipher texts and power traces for those encryption operations. The authors claim that they have used DPA to reverse engineer various unknown algorithms and protocols on devices. The authors state that it may be possible to automate this reverse engineering process. Kocher et al. hints that these techniques (SPA, DPA) might be useable with EM emissions too in addition to power consumption.

While various side-channel attacks are possible on computer systems, it is possible to increase the advantages achievable by combining multiple side-channels that leak different kinds of information together (Agrawal et al., 2003). For example, power analysis and EM analysis can be performed together in order to reduce the errors and improve the accuracy of inferring the leaked information from a computer system.

Unintentional electromagnetic emissions

EM radiation is the underlying technology for numerous of wireless communication. Meanwhile, it is a well documented fact that electronic devices generate EM radiation on unintended frequencies as a side effect of their internal operations (Getz and Moeckel). Such unintended EM radiation are regulated by government agencies, such as *Federal Communications Commission* (FCC) in the USA, due to the possible interference they can make on legitimate wireless communication and the potential health issues they can cause to the users of these devices. However, it is not possible to entirely avoid such emissions. Equipment manufacturers attempt to minimise it as much as possible (Ott, 2011). This section discusses how EM signals are generated from different components of a computer system, what kind of information they may carry, and what types of methods and tools can be used to capture these signals.

Hardware that causes electromagnetic emissions

As derived from Maxwell's equations, EM waves can be generated by electric currents varying over time. Characteristics of the EM waves being generated, such as frequency, amplitude, and phase, depends on the nature of the time varying electric current (Maxwell, 1865). Based on this principle, modern communication systems generate oscillating currents on antennas that generate EM waves that propagate over free space. They can be captured by another antenna with appropriate properties. Modern digital computer systems have a large number of components that depend on electric pulses or alternating currents for their operations. That leaves the space for EM waves to be generated at unexpected frequencies without the intention of the system manufacturer.

There are multiple computer components that operate in a co-ordinated, sequential fashion according to clock signals. Among them, both the CPU and RAM are of particular interest. The CPU performs a cycle of fetching instructions, decodes and executes them, while RAM maintains the data and corresponding instructions when a computing device is powered on. EM emission signals from these components contain a significant amount of side-channel information regarding the events related to software execution and data handling. On most IoT devices, the CPU and RAM are included in microcontroller (MCU) chips making it the most important EM source on-board.

Sampling electromagnetic emissions

The EM emission frequencies of a target device is unpredictable due to its dependability on various hardware characteristics. Therefore, it is difficult to have a universal purpose device that can be used to observe EM emissions from a target device and interpret side-channel information. It has been shown that small magnetic loop antennas can be used for the purpose of detecting EM emissions from computing devices (Peeters et al., 2007). When EM signals are captured by a loop antenna, it requires digital sampling before the data can be used for analysis. Theoretically, the sample rate of the equipment should be twice that of the maximum EM frequency required to be captured — referred to as Nyquist frequency (Smith, 1997). For this reason, EM signal sampling equipment must have a very high sample rate. The most commonly used equipment to capture EM signals are oscilloscopes and spectrum analysers with high sample rates. The digitised data these devices capture can be subsequently analysed in signal analysis software. However, access to such devices for information security professionals is not very common (Wolfe, 2003).

Software defined radios (SDRs) are getting increasingly popular among wireless hackers, hobbyists, and security enthusiasts who are interested in access to the radio frequency (RF) spectrum. An SDR consists of a minimal hardware component, which can be tuned to a range of RF frequencies and then digitise it with a fast analogue-to-digital converter (ADC). The processing of digitised RF data is handled entirely on software (Tuttlebee, 2003). A wide variety of SDR hardware and software platforms are available (Cass, 2013; Ossmann; Ettus and Braun, 2015; Blossom, 2004). Due to the enhanced flexibility provided by software, SDR platforms have become a perfect candidate for EM side-channel attack analysis research. A SDR can be used to scan through a wide range of frequencies to locate potential EM emissions from a computer system.

A simple set-up with an SDR platform can be used to demonstrate the unintentional EM signals. An *Arduino Leonardo* prototyping board is loaded with a simple program to blink an LED connected to it via the general purpose I/O pins. An antenna connected to an RTL-SDR dongle is placed close to the Arduino board in order to receive unintentional EM signals emitted from the board. The Arduino board consists of a microcontroller chip that operates at 16 MHz. However, the RTL-SDR dongle cannot be tuned to frequencies below 22 MHz. Therefore, a GNURadio script was programmed to tune the RTL-SDR dongle to the first harmonic of the Arduino clock, i.e., 32 MHz. Fig. 1 illustrates the spectrograms of three different EM signal samples gathered.

When two different LED blinking patterns are performed by two different programs separately, the Arduino emitted two completely different EM signal patterns. The spectrogram shown in Fig. 1 (a) illustrates the EM signal observed from a simple LED blinking program, while the spectrogram in Fig. 1 (c) illustrates the EM signal of a more complex LED blinking program. The spectrogram depicted in Fig. 1 (b) shows the EM signal observed during the re-programming stage of the Arduino device from the first program to the second.

Connection between CPU instructions and electromagnetic emissions

As a result of executing instructions in different combinations by the CPU, EM signal patterns are emitted at various frequencies and
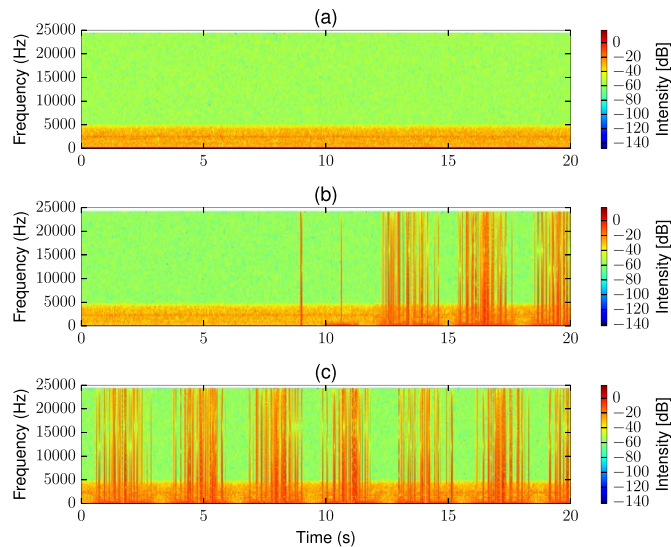
Fig. 1. Spectrograms of AM demodulated EM emissions acquired from an Arduino device where (a) running a simple LED blink program, (b) reprogramming the device, and (c) running a complex LED blink program are depicted.

amplitudes. Depending on the sequence of instructions, i.e., the exact program being executed, the output of EM noise from the CPU varies significantly. Due to this, systematically modelling and predicting possible EM signal characteristics of a computer processor is a difficult task. In order to identify unintentional EM emissions of a computer processor, the most practical method is scanning a large frequency spectrum for suspected EM signals and subsequently trying to interpret these identified signals for potential side-channel information. This arduous approach is a time consuming task that requires manual inspection by a human user.

In 2014, Callan et al. introduced a metric called SAVAT (Signal AVailability for an ATtacker) that measures the EM signal power emitted when a CPU is executing a specific pair of instructions (A and B). The authors show that different selections of A/B instruction pairs emit different SAVAT values, i.e., signal power (Callan et al., 2014; Zajic and Prvulovic, 2014). An improvement to the SAVAT technique is a method called *Finding Amplitude-modulated Side-channel Emanations* (FASE). The key idea behind the FASE technique relies on the phenomena that when a program activity is alternating at a frequency (f_{alt}) that affects any periodic EM signal originating from any source at a frequency f_c, it is possible to observe two side-band signals at $f_c - f_{alt}$ and $f_c + f_{alt}$ between the f_c signal. Further improvements to SAVAT technique enabled the possibility of identifying both amplitude and frequency modulated EM emissions from CPUs (Callan et al., 2015b; Prvulovic et al., 2017; Yilmaz et al., 2018). While it is evident from existing studies that EM side-channel leakage is available across various type of CPUs, further studies are necessary to identify the effect of different CPU architectures to the produced EM emissions.

Electromagnetic emissions as a signature

When a computing device running a program generates EM emissions, the patterns observable depend on the precise settings of the device. In the EM emission spectrum of the Arduino device in Fig. 1, it is clearly evident that both the hardware and software settings have influenced the EM emission patterns. The signal captured at the first harmonic frequency of the Arduino device's system clock, i.e., 32 MHz, is showing a varying patterns in the spectrogram view according to the changes made to the device.

Therefore, it is clear that the target device's system clock is the main source of EM radiation. The design of the printed circuit board (PCB), and characteristics of the electronic components provide variations to this strong signal. Meanwhile, subfigures (a), (b), and (c) of Fig. 1 clearly show that the instruction sequence, i.e., the program being executed on the CPU, has a significant influence to the EM emission pattern.

Electromagnetic emissions as a hardware signature

Despite the software components available on a computing device, it is important to investigate whether the hardware alone can provide a recognisable EM emission pattern. Such a capability can lead to profiling of hardware devices and components uniquely. It has been shown that a simple EM signal acquisition device called RTL-SDR, which demonstrated the capability to capture EM emissions from an Arduino device, can be used to profile computing devices uniquely. Laput et al. used a similar device to acquire EM signals that were successfully applied to a support vector machine (SVM) classifier to uniquely distinguish the EM source device (Laput et al., 2015). This possibility has led to the idea that EM emissions from an electronic device owned by a person can be used as an authentication token of the person instead of relying on conventional methods, such as Radio Frequency Identification (RFID) tags (Bianchi and Oakley, 2016; Yang and Sample, 2016).

This uniquely distinguishable EM emission patterns of a known electronic device can help to identify any potential alteration that may have applied to it. For example, a known electronic device can be altered at the hardware fabrication level for malicious purposes, such as accessing stored data or eavesdropping on users' activities. Such hardware modifications result in a changed EM emission pattern that can be used to identify it (Yang et al., 2017). Similarly, a genuine electronic device can be replaced by a counterfeit electronic device for a malicious objective. It has been shown that even when counterfeit hardware attempts to follow the design of the genuine device, it still creates distinguishably different EM emission patterns compared to their original product (Ahmed et al).

Electromagnetic emissions as a software signature

When software runs on different computing devices, it is clear that the hardware EM emissions are influenced by the software instructions being executed. It is important to consider this influence from two different aspects. The first aspect is how uniquely the EM emissions of different software running on the same hardware platform can be recognised. This can be used to pin point to the exact software running on a device. The second aspect is how unique the same software program is when it is running across various hardware platforms. It facilitates the unique detection of a specific piece of software.

When software systems are being developed, requirements arise to debug their behaviour or find ways to increase their performance. Instrumenting software by applying logging events and break points are the most common ways to identify where complex software is not performing as expected. These developmental options affect the performance of the software being inspected in addition to the overhead of their placement each time a copy of the software needs to be inspected. It has been shown that unintended EM emissions of the CPU can be used to inspect software execution sequences without having to instrument the software (Callan et al., 2016; Callan, 2016; Han et al., 2017; Espitau et al., 2017). Even when the same program is running on different devices, the ability to identify the instruction execution sequence can help to uniquely identify the software itself.

The capability to detect software code execution sequence has

opened up the opportunity to identify when a computing device is running software code not intended by the manufacturer or the owner. One possible scenario can be software bugs or hardware faults that cause an IoT device to execute unexpected instruction sequences. Another possible scenario can occur when an IoT device is under an attack causing it to run malware or an unintended part of the device's genuine software. Stone et al. (Stone and Stone, 2015; Stone et al., 2015) and Nazari et al. (2017) showed that such abnormal deviations of software code executions on computing devices can be detected using the corresponding EM emission patterns from its execution.

Even though it has been identified that EM emission patterns are associated with both the hardware and software characteristics of the source device, the format of a captured EM signal used for this identification can vary. Instead of directly using time-domain EM signal traces, one such alternative format is RF-DNA finger-printing. This is a technique to fingerprint the physical layer of RF transmitting devices, which includes WiFi, Bluetooth, Zigbee, GSM devices, and even RADAR antennas. This technique has been used to identify rogue devices in a deployment using their RF signals without physically inspecting them (Reising, 2012; Dubendorfer, 2013; Danev et al., 2012; Lukacs et al., 2015). Deppensmith et al. showed that RF-DNA technique can be applied to unintentional EM emission fingerprinting on computing devices reliably (Deppensmith and Stone, 2014). However, the evaluations performed by Stone et al. on microcontroller based IoT devices indicates that further studies are necessary to conclude the most reliable format to represent unintentional EM signals (Stone and Stone, 2016).

Fig. 2 illustrates the structure of an RF-DNA fingerprint. When calculating it, the EM signals emitted from a device on a selected frequency is captured, filtered, and amplified appropriately to achieve a clean trace. From this acquired time-domain EM trace, the three signal characteristics; *Amplitude*, *Phase* and *Frequency*, are separately considered for further processing. Each signal characteristic is broken into N equally sized regions and then for each region, four statistical metrics; *standard deviation*, *variance*, *skewness*, and *kurtosis* is calculated. The standard deviation and variance metrics measure the spread of data samples, while the skewness and kurtosis metrics measure the symmetry and the sharpness of a data sample. Furthermore, the signal itself is again considered as a one entire region, i.e., the $(N+1)^{th}$ region, to calculate the same statistical metrics. As Fig. 2 illustrates, each of these calculated statistical metrics are arranged in a single vector, which becomes the RF-DNA fingerprint of the originally acquired EM trace from the device.

Information leaking electromagnetic emissions

This section dives into the question of what information is contained in an EM emission trace of a particular computing system. From a digital forensic perspective, both the kind of software running on IoT devices and the data being handled by each software application are potentially of significant interest. Even if EM side-channel analysis cannot reveal all of data being handled by an IoT device platform, extracting critical information, e.g., cryptographic keys, can help progress forensic analysis.

Observable electromagnetic spectrum patterns

While there exists a wide variety of microcontroller chips used on IoT devices, Sohaib et al. has shown that it is still viable to perform EM side-channel attacks on them (Sohaib ul Hassan). When considering information leakage from an EM emission trace, visually inspecting the time-domain signal is the first observational technique. This approach is called simple electromagnetic analysis (SEMA), which evolved from the simple power analysis (SPA) introduced by Kocher et al. (1999). Another way of performing visual observations is by transforming the EM trace into the frequency domain and plotting it as a spectrogram. This enables observation of different signal patterns distributed over multiple frequencies.

Multiple published works have demonstrated the effectiveness of the SEMA approach in extracting critical data from computers, including cryptographic keys. The El Gamal and RSA algorithms implemented using GnuPG library were attacked by observing critical CPU operations (Genkin et al., 2015a). Furthermore, elliptic curve based cryptographic algorithms (ECC), such as Elliptic Curve based Diffie Hellman (ECDH) and Elliptic Curve based Digital Signature Algorithm (ECDSA), are identified to be vulnerable to EM side-channel attacks with the SEMA approach (Goubin, 2003; Genkin et al., 2016a, 2016b). Due to the low computational overhead in ECC algorithms, many mobile devices and IoT platforms tend to employ ECC algorithms to secure data. This indicates that such devices can be inspected through EM side-channels to access cryptographically protected data.

Differential electromagnetic analysis (DEMA)

If a large number of EM traces from a computing system can be observed executing specific software, it is possible to identify the data bits involved in the operations that appear across the large number of EM traces. While being impractical to perform under real-world attack scenarios due to the challenge of collecting such a large number of EM traces from a target computer, this may be the only resort for EM side-channel analysis when it is not possible to extract information from visual observation of a single EM trace.

DEMA, a variant of Differential Power Analysis (DPA), uses the variation of EM emissions of a CPU to discover variables used in an executing program, such as encryption algorithms (Kocher et al., 1999, 2011). When a bit in a CPU register is flipped from 0 to 1 or vice versa, it consumes an amount of energy, which is reflected in the corresponding EM emission. Some CPUs may emit a higher EM signal when switching a register bit from 0 to 1 than vice versa since that operation can lead to a higher energy consumption (Peeters et al., 2007). Due to this, when the contents of a complete CPU register are modified, it is possible to identify the *hamming distance* between the previous and new state using the resulting
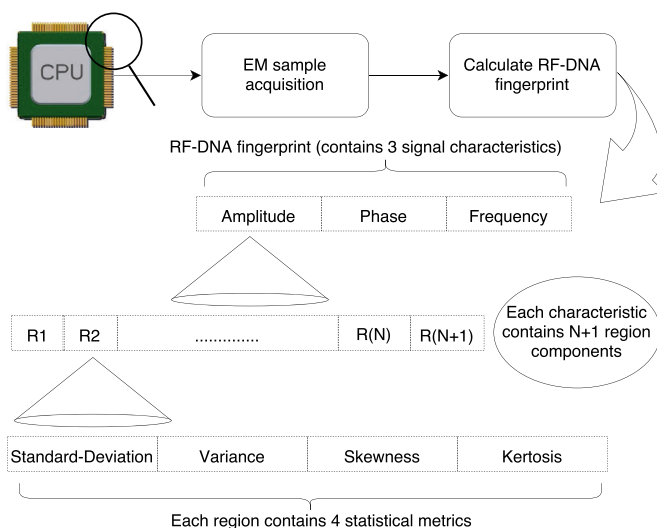

Fig. 2. The RF-DNA fingerprinting process.

EM emission. Since every instruction running on a CPU affects the values on different registers, this means that attackers can identify instructions being executed and intermediate variables used based on the EM observation.

Fig. 3 illustrates how differential EM analysis is used to identify the key of a simple XOR-cipher. Initially, a large set of input data bytes and all possible key bytes are used to perform XOR-operations and the hamming distances of the resulting values are stored in a matrix called *Hypothetical Matrix*, as shown in Fig. 3. The objective is to find the hypothetical key of the matrix that generates matching hamming distances for the same input values. For this, the input values are fed to software running on the CPU, where the XOR operation is performed with the unknown key. EM emissions are sampled for each input value to generate the *Real Matrix*, where each column contains an EM signal sample for its corresponding input. Calculating cross-correlations between rows of the two matrices can find the corresponding row in the *Hypothetical Matrix* that provides the best correlation of hamming distances. The hypothetical key corresponding to this row is likely the encryption key used for the XOR operation inside the CPU.

Standard encryption algorithms, such as the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES), employ XOR operations at various stages in their functionality using chunks of the encryption key and input data. Therefore, DEMA attacks are possible by attacking each chunk of the key being used with the XOR operations. Such an attack reveals parts of the encryption key, which have to be combined at the end. However, in a real-world setting, the attacker may not have enough EM emission samples of the encryption operations to calculate the correct part of the key used. This results in lists of possible key chunks for each segment of the encryption key used in the algorithm. The problem of identifying the correct parts of the key to build the complete encryption key is called the *Key Enumeration Problem*, which can be solved within a reasonable computational overhead (Bogdanov et al., 2015).

Quisquater et al. practically demonstrated that EM analysis is a viable option to the aforementioned power analysis attack on computer CPUs (Quisquater and Samyde, 2001). By precisely moving the EM probe over a microcontroller, the authors were able to build an a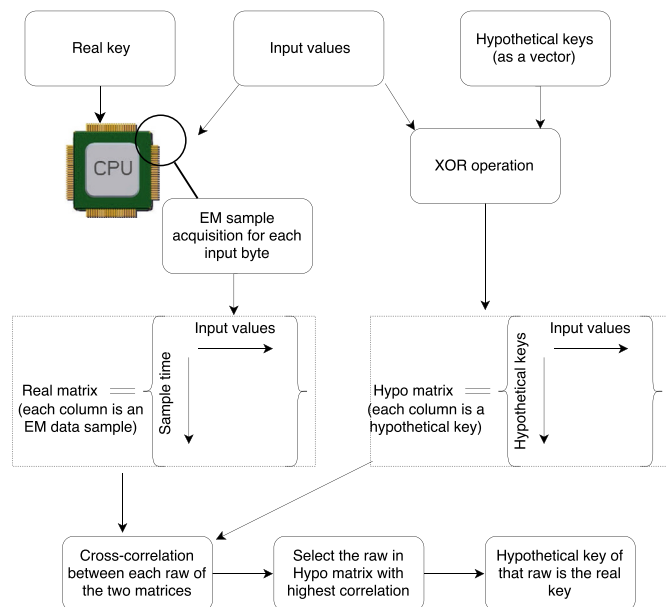ccurate 3-dimensional EM signature of the chip running an idle loop. It was shown that the radiation spectrum of each processor was sufficiently unique to use as a distinguishable feature for processor identification. These experiments were performed in a Faraday cage to minimise the external noise effects and the EM emissions were captured using a small magnetic loop antenna (diameter $\approx$ 3 mm). An oscilloscope digitised the signal for analysis. Gandolfi et al. (2001) applied DEMA to extract encryption keys from three different chips used on smartcards namely; COMP128, DES, and RSA. According to this study, the SNR of EM emissions from these chips is higher than the SNR of power consumption analysis. This results in the extraction of more information from the DEMA technique as compared to simple power analysis attacks (Messerges et al., 1999). Asymmetric key encryption, such as RSA, can also be attacked by identifying the individual modular exponentiation operations performed within the algorithm through EM emissions (Witteman et al., 2011).

Due to the modern electronic multimedia distribution model, e.g., music, movies, and ebooks, end-users can often become the attackers. These users might have the malicious intention of breaking encryption or sharing Digital Rights Management (DRM) protected data. Since the victim device is owned by the attacker, unlimited physical access to the hardware and software becomes available for the attacker through various side-channel attacks. White Box Cryptography (WBC) was introduced as a solution to this; whereby cryptographic algorithms and keys are combined with random codes and random data to create an obfuscation that makes side-channel attacks more difficult. However, it has been shown that EM side-channel attacks, such as DEMA, are still capable of extracting encryption keys despite of the application of WBC techniques (Sanfelix et al., 2015).

Recently, Camurati et al. made an important discovery that extended the previously known capabilities of EM side-channel analysis of cryptographic operations on IoT devices (Camurati et al., 2018). It was shown that mixed-signal processors, such as system-on-chips (SoCs), that contains a radio transceiver and a CPU on the same silicon die, can cause long distance EM leakages. This occurs when the CPU noise gets modulated into the radio transceiver's emission — extending the range of the CPU EM side-channel. As the usage of SoCs is getting increasingly popular on IoT devices, this latest type of EM side-channel leakage, called *screaming channels*, has significantly increased the potential attack surface.

Analysis on wireless-powered devices

Unlike traditional computing devices that have their own power source to run CPU operations, wireless-powered devices, e.g., passive RFIDs, depend on an external RF field provided by the device's reader for power (Calari and Lampkin, 1997). IoT devices are ideal candidates to be powered by wireless means. EM side-channel analysis on such devices is challenging due to the presence of a strong RF field from the reader, which obfuscates the weak EM emissions of the devices themselves. However, RFID based devices are being used in critical systems, such as secure access control to buildings and electronic payments, where cryptographic operations are performed on-board. Therefore, investigating the EM side-channel capability on such devices is important from both security and forensic standpoints.

Hutter et al. demonstrated the capability to perform EM side-channel analysis on RFID based devices using a custom-made RFID tag as a proof of concept (Hutter et al., 2007). Using this custom set up, the authors were able to recover the AES key used in a challenge response protocol between the RFID tag and the reader. In order to avoid the disturbance from the RF field of the reader device, the RFID circuitry was placed outside the reader's RF field,

Fig. 3. EM analysis of XOR-Cipher algorithm to extract the encryption key.

while the power harvesting antenna is kept inside the reader's RF field. The two components were connected through a sufficiently long wire. This enabled the measurement of the EM emissions from the RFID circuitry without interference. However, it is not possible to follow a similar approach in a regular RFID tag as the antenna and RFID circuitry are inseparable by any reasonable means.

Kasper et al. performed EM side-channel attacks on RFID based smart-cards in a more realistic setting. This research employed commercially available smart-cards and performed the attacks within the RF field of the RFID reader (Kasper et al., 2009). When the RFID smart-card is consuming more energy, the amplitude of the RFID readers RF field becomes lower. Similarly, when the RFID smart-card is consuming less energy, the amplitude of the RFID readers field is higher. This means, the power consumption of the RFID tag is reflected in the amplitude of the RFID readers carrier frequency. Kasper et al. used this signal as the EM side-channel to attack internal operations of the RFID reader. A computer-controlled USB-oscilloscope and a computer-connected custom-made RFID reader was used to attack the RFID tag while capturing EM fluctuations using a small RF loop probe. This set up was used to perform a *correlation power analysis* (CPA) attack to extract the symmetric keys used in DES and 3-DES implementations on the smart-card successfully.

Recent research by Xu et al. demonstrated that RFID based smart-cards that employ side-channel attack mitigation techniques, such as *head and tail protection*, are not effective enough against EM side-channel analysis attacks (Xu et al., 2018). In their work, encryption keys used for the 3DES algorithm were demonstrated to be recoverable. In light of this attack vector, it is important to note that wireless-powered IoT devices are also susceptible to threats from EM analysis based attacks.

Many smart-card-based fraud, such as stealing credit card details, involve malicious devices, such as *card skimmers*, that can read and store data from the cards. Investigators face the challenge of identifying victims of such skimming devices due to the fact that card details are encrypted when stored on these devices. Souvignet and Frinken demonstrated that correlation power analysis, which is a variant of DPA attack, can be used to extract the details of victim smart-cards from such skimmer devices by physically tapping into a seized device (Souvignet and Frinken, 2013). The success of their work indicates that EM side-channel analysis can be even more promising in extracting such evidence without requiring any physical alterations to the device itself.

Countermeasures to electromagnetic side-channels

As EM side-channel analysis has been shown to be successful on recovering data from computing devices, various countermeasures have been explored to counteract it on both software and hardware levels (Zankl et al., 2018). Masking variables by using random values alongside the operations is a basic software-based countermeasure that has been proven to not be effective enough against EM side-channel attacks (Kim et al., 2008; Chari et al., 2002). Various other approaches including the randomisation of the operation sequences or lookup tables of algorithms (Saputra et al., 2003; Kim et al., 2016), avoiding instructions pairs executing adjacently that are known to emit distinguishable EM patterns (Callan et al., 2014; Zajic and Prvulovic, 2014), and accessing critical data using pointers instead of values (Witteman and Oostdijk, 2008) require further studies to see how effective they are against EM side-channel attacks.

Quisquater et al. suggests several hardware design countermeasures to these attacks (Quisquater and Samyde, 2001). Actions that can be taken by hardware designers includes minimising metal parts in a chip to reduce EM emissions, the use of Faraday cage like

packaging, making the chip less power consuming (which leads to less unintentional emissions), asynchronism (i.e., design the chip not to use a central system clock and instead operate asynchronously), and the use of dual line logic (i.e., using two lines that in combination of two bits represents a state instead of a single line that simply represent 0 or 1 states). Furthermore, it has been shown that it is possible to mathematically model an electronic chip during the design phase to identify and avoid potential information leakages through EM side-channels (Ishai et al., 2003; Standaert et al., 2009).

Standards and tools

EM side-channel attacks are not currently commonly being used for digital forensics purposes. Therefore, it can be too early to find any existing standards or tools on EM side-channel analysis for digital forensics. However, in order for future establishment of standards and tools, it is important to review the relevant standards and tools in both hardware and software security domains.

The concerns of electromagnetic wave emissions from IoT devices from the software perspective are mostly concentrated towards the wireless communication technologies, such as WiFi, Bluetooth, and proprietary IoT protocols, e.g., Zigbee (Golmie et al., 2003; Iyer et al., 2015). Meanwhile, unintentional EM emission minimisation is generally left to those involved in the hardware design and manufacturing process. The term *electromagnetic compatibility* (EMC) refers to a device's unintentional EM emissions that can affect the functionality of other devices and the health of humans who are exposed to it (Getz and Moeckel). The Federal Communications Commission (FCC), the Food and Drug Administration (FDA), the International Electrotechnical Commission (IEC), and the European Union (EU) are examples of authorities concerned with EMC (Barron, 2007; Hayashi, 2016). However, regarding the question of EM side-channel information leakage from general purpose electronic devices, there are no such rules to govern the manufacturers. Instead, only guidelines exist, which may or may not be followed (ISO/IEC 17825:2016; ISO/IEC TS 30104:2015).

Once a hardware device's design is completed and manufacturing commences, it is a challenging task to apply mitigation steps should the EMC tests reveal that it does not meet requirements. In the worst case scenario, the minimisation of EM emissions may require a complete reworking of the PCB used in the device or a replacement of a critical electronic component. Due to the potential for costly manufacturing disruption, the minimisation of EM emissions is necessary from the initial hardware design phase. Due to the fact that EM side-channel information leakage is not a problem limited to hardware manufacturers, a joint effort by both hardware and software developers to establish standards is necessary.

In order to facilitate the assessment on EM side-channel security threats, standardised tools and frameworks are highly necessary. *Test vector leakage assessment* (TVLA) is a technique that can be used to assess the resistance of cryptographic implementations against hardware side-channel attacks (Becker et al., 2013). TempestSDR is a software tool that can be used with a large variety of hardware platforms, e.g., the universal software radio peripheral[1] (USRP) or HackRF,[2] to eavesdrop on computer monitors by capturing the EM signals emitted by the video cables (Marinov, 2018; Sayakkara et al., 2018b). Multiple commercial and open source products exist that can be used to break encryption on microcontroller based IoT devices, such as ChipWhisperer (ChipWhisperer embedded ha, 2018;

---

[1] https://www.ettus.com/.
[2] https://greatscottgadgets.com/hackrf/.

O'Flynn and Chen, 2014) and Riscure Inspector (Riscure, 2018; Ramsay and Lohuis). Blanco et al. presented a side-channel trace acquisition framework called SCAP, which is targeted at general purpose computing devices (including mobile devices). While the framework does not currently perform side-channel attacks, the objective is to provide a platform to build future analysis tools (Blanco et al., 2017). Such tools enable IoT system developers to test the robustness of their hardware against physical side-channel attacks and identify information leakage.

Discussion

Having discussed the scientific literature related to EM side-channel analysis attacks, it is important to identify the future impact it may cause in the domain of digital forensics on IoT devices. This section highlights some of the potential ways this impact may occur in the future under different themes. Fig. 4 illustrates the avenues for future research in this direction. Many of these future potentials are already starting to be realised and others are ambitious predictions that can prove significantly beneficial to digital forensics.

Recent versions of mobile operating systems, e.g., Android and iOS, secure their internal storage using encryption. Critical information necessary for digital forensic investigation can be inaccessible due to being stored in an encrypted form (Casey and Stellatos, 2008; Zdziarski, 2008; Hoog, 2011). This includes encrypted emails, encrypted instant messenger applications, encrypted files, and encrypted storage partitions. While the increasing application of cryptographic protection on computing devices poses a challenge to traditional digital forensics, it can open up new opportunities to EM side-channel attacks (Lillis et al., 2016). EM side-channel attacks require a large number of traces acquired from a victim device while the device is performing cryptographic operations using a single key. The most common encryption operations occurring on older systems are the secure socket layer (SSL) based web traffic (Fahl et al., 2013). With encrypted data storage becoming commonplace, EM side-channel attacks can potentially be performed by observing cryptographic operations during live data forensic analysis procedures (Hay et al).

Instead of using a single side-channel attack in isolation, combinations of multiple side-channel attacks directed towards a single computer system can prove more fruitful. It has been proven that power and EM side-channel analysis can be combined to achieve better results (Agrawal et al., 2003). There can be some operations of the CPU that are more clearly reflected in the device's power consumption than in the EM emission and vice versa. Similarly, malware running on a victim computer can aid an EM side-channel attacker to extract additional information (over the EM side-channel alone) by intentionally modulating data into the EM emission of the CPU or the monitor (Cheddad et al., 2010; Yang and Sample, 2017; Sayakkara et al., 2018b).

The unintentional EM emissions from computing devices can cause interference to other radio signals in the vicinity. This phenomena is evident in laptop computers, which have been shown to modulate signals from commercial AM radio stations (Entriken, 2018). IoT devices already use this interference phenomena to communicate purposefully with other devices by modulating the ambient RF signals. This is called *backscatter* communication
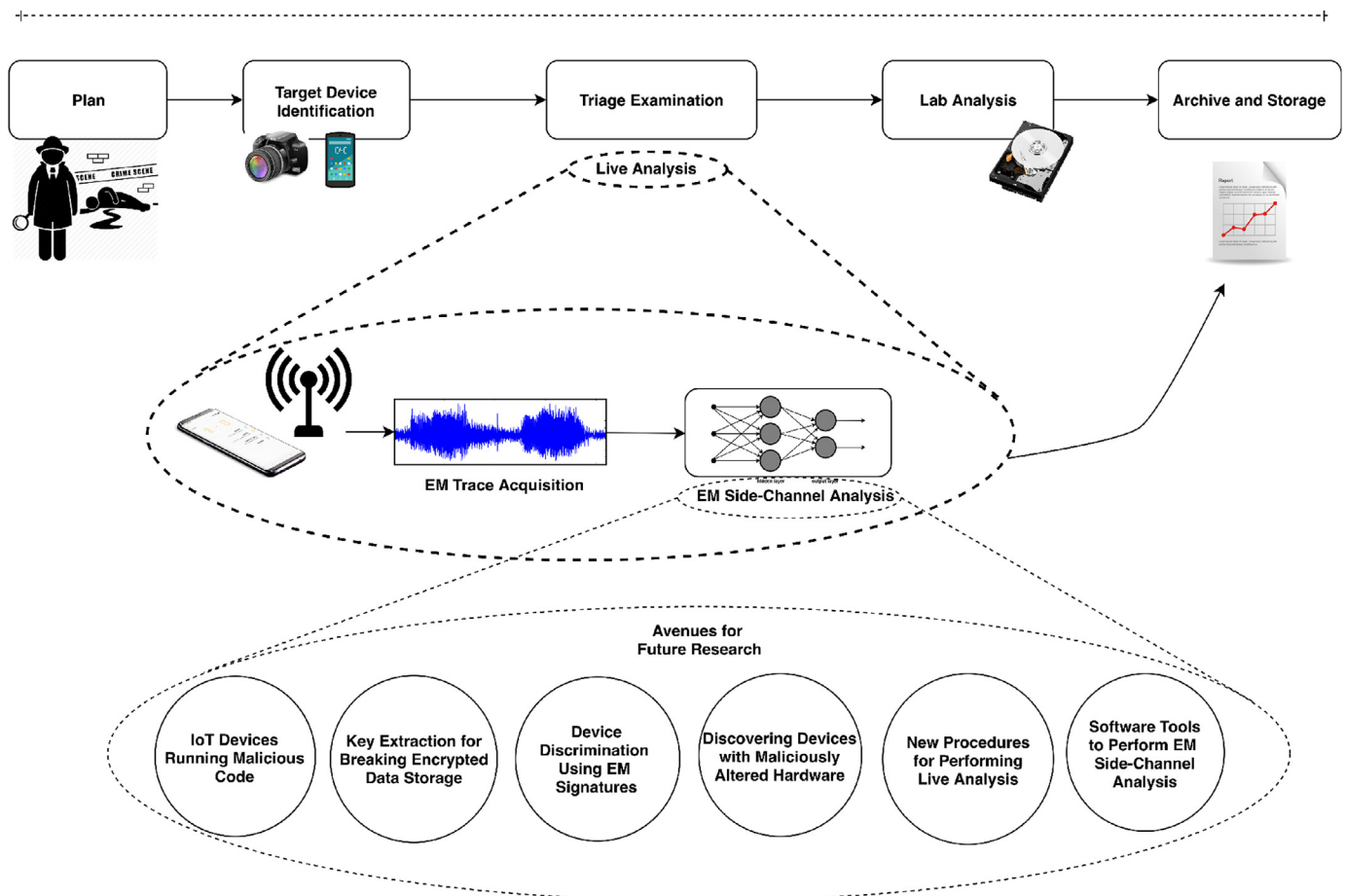

Fig. 4. Altering the traditional IoT digital evidence acquisition process (Du et al., 2017), EM side-channel analysis can help in various ways for live analysis of computing devices.

technology (Liu et al., 2017). There are various carrier wave sources that have been tested in the literature including TV transmission stations and WiFi access points (Liu et al., 2013; Kellogg et al., 2014; Bharadia et al., 2015; Zhang et al., 2016). The potential of using this backscatter phenomena to eavesdrop on internal CPU operations of IoT devices by listening to ambient RF sources warrants further exploration.

Devices deployed in wired networks, such as routers and switches, are known EM noise sources. It has been already showed that MAC addresses in Ethernet frames can be extracted by performing SEMA analysis on the EM emissions from wired routers (Schulz et al., 2016). When it is required to perform an investigation on a live wired network, it is necessary to be connected in order to inspect packets (Corey et al., 2002). In situations like this, the EM emissions of routers and switches might be able to provide an approximate picture of the workload and traffic on the network (Goudos et al., 2008).

Recent advances that have been made in the area of artificial intelligence (AI) (incorporating machine learning (ML) and deep learning (DL)) have demonstrated promising applications to many other domains across computer science. Various tasks where human intuition was required to perform decision making are now being replaced with ML/DL powered algorithms. Software libraries and frameworks are becoming increasingly available in order to assist the building of applications that have intelligent capabilities. Examples include the automated detection of malicious programs (Kolter and Maloof, 2004), image manipulation (Saboia et al., 2011), and anomaly detection in network traces (Mukkamala and Sung, 2003).

EM side-channel analysis techniques that previously required human intervention can be automated through the development of AI algorithms. Recent work by Wang et al. (2018) applied deep learning algorithms including multi-layer perceptron (MLP) and long short-term memory (LSTM) to detect anomalies in the code of simple IoT devices, e.g., Arduino and Raspberry Pi, through the power consumption side-channel. Therefore, it is potentially possible to extract better information from EM traces than the current manual observations are capable of achieving. Several examples that were discussed in previous sections already leverages AI techniques to recognise EM trace patterns, which strongly hints the future role that can be played by AI algorithms in EM side-channel analysis for digital forensics (Laput et al., 2015; Lerman et al., 2011; Callan et al., 2016; Callan, 2016; Nazari et al., 2017; Stone and Stone, 2016).

Conclusions

Traditionally, digital forensics focuses on analysing traces left behind by suspects on digital devices by inspecting file storage, log files, network traces, etc. Live data forensics can also be performed on systems that require more sophisticated investigative techniques and skills. As computing systems transform from less privacy and security concerned platforms into hardened platforms that are designed with security in mind from their inception, the typical work conducted by digital forensic investigators must change accordingly. Cryptographically protected storage systems is one of the largest challenges hindering efficient digital forensic analysis. EM side-channel analysis has been demonstrated as a potential door-opener for cryptographically protected data storage and communications from a security perspective, which can be built upon and adopted for digital forensic purposes.

This paper comprehensively analysed the literature on EM side-channel attacks with the goal of applying the technique to assist digital forensic investigations on IoT devices. While various mitigation techniques have been suggested and applied to counter against EM side-channel attacks, existing literature demonstrates that such attempts have not been successful in reducing the prevalence of this attack vector. EM side-channel analysis is still in its infancy for digital forensic applications, which demands court-admissible, forensically-sound processing when used not only for obtaining security keys but also for the detection of unintentional data leakage. However, this technique has significant potential to have a substantial impact on the field and enable the progression of otherwise stalled investigative cases involving both IoT devices, and encrypted computing devices in general.

Conflicts of interest

None.

APPENDIX

A categorisation of the literature of EM side-channel attacks and related areas are listed in Table 1.

Table 1
Categorisation of the literature on EM side-channels.

Objective	Technique	References
Acquisition of EM Emissions	SAVAT	(Callan et al., 2014; Zajic and Prvulovic, 2014; Prvulovic et al., 2017)
	FASE	(Callan et al., 2015b; Prvulovic et al., 2017)
	SDR Signal Acquisition	(Tuttlebee, 2003; Cass, 2013; Ossmann; Ettus and Braun, 2015; Blossom, 2004)
	General	(Getz and Moeckel; Ott, 2011; Jabbar and Rahman, 1991; Peeters et al., 2007; Sohaib ul Hassan)
EM as a Signature	Time/Frequency/Hilbert Transform Domains	(Yang and Sample, 2016; Stagner, 2013; Ahmed et al; Stone and Stone, 2015; Stone et al., 2015; Callan et al., 2016; Callan, 2016)
		(Nazari et al., 2017; Clark et al., 2013)
	RF-DNA	(Laput et al., 2015; Reising, 2012; Dubendorfer, 2013; Lukacs et al., 2015; Deppensmith and Stone, 2014)
	General	(Bianchi and Oakley, 2016; Yang et al., 2017; Stone and Stone, 2016)
Cryptographic Key Extraction	SEMA/Spectrum Observation	(Hayashi et al., 2013; Van Eck, 1985; Elibol et al., 2012; Kocher et al., 1999; Agrawal et al., 2003; Genkin et al., 2015a, 2015b, 2016a)
		(Genkin et al., 2016b; Belgarric et al., 2016)
	DEMA	(Kocher et al., 1999, 2011; Peeters et al., 2007; Bogdanov et al., 2015; Quisquater and Samyde, 2001; Gandolfi et al., 2001; Messerges et al., 1999; Witteman et al., 2011)
		(Sanfelix et al., 2015; Hutter et al., 2007; Kasper et al., 2009; Chari et al., 2002; Camurati et al., 2018)
Countermeasures for EM Side-Channels	Hardware Countermeasures	(Fritzke, 2012; Quisquater and Samyde, 2001; Ishai et al., 2003; Standaert et al., 2009)
	Software Countermeasures	(Callan et al., 2014; Zajic and Prvulovic, 2014; Kim et al., 2008, 2016; Chari et al., 2002; Saputra et al., 2003; Witteman and Oostdijk, 2008; Standaert et al., 2009)
Tools and Frameworks	Various	(Cass, 2013; Ossmann; Ettus and Braun, 2015; Blossom, 2004; Marinov, 2018; ChipWhisperer embedded ha, 2018; O'Flynn and Chen, 2014; Riscure, 2018)
		(Ramsay and Lohuis; Blanco et al., 2017)

References

Agrawal, D., Rao, J.R., Rohatgi, P., 2003. Multi-channel attacks. In: International Workshop on Cryptographic Hardware and Embedded Systems (CHES). Springer, pp. 2–16.

Ahmad, M.S., Musa, N.E., Nadarajah, R., Hassan, R., Othman, N.E., 2013. Comparison between android and ios operating system in terms of security. In: 8th International Conference on Information Technology in Asia (CITA). IEEE, pp. 1–4.

Ahmed, M.M., Hely, D., Barbot, N., Siragusa, R., Perret, E., Bernier, M., Garet, F., 2017. Radiated electromagnetic emission for integrated circuit authentication, IEEE Microw. Wirel. Compon. Lett. 27 (11), 1028–1030.

Barron, M.R., 2007. Creating consumer confidence or confusion? the role of product certification in the market today. Marquette Intellect. Prop. Law Rev. 11 (2), 413.

Becker, G., Cooper, J., DeMulder, E., Goodwill, G., Jaffe, J., Kenworthy, G., Kouzminov, T., Leiserson, A., Marson, M., Rohatgi, P., et al., 2013. Test vector leakage assessment (tvla) methodology in practice. In: International Cryptographic Module Conference, vol. 1001, p. 13.

Belgarric, P., Fouque, P.-A., Macario-Rat, G., Tibouchi, M., 2016. side-Channel analysis of weierstrass and koblitz curve ECDSA on android smartphones. In: Cryptographers Track at the RSA Conference. Springer, pp. 236–252.

Bharadia, D., Joshi, K.R., Kotaru, M., Katti, S., 2015. BackFi: high throughput WiFi backscatter. Comput. Commun. Rev. 45 (4), 283–296.

Bianchi, A., Oakley, I., 2016. Wearable authentication: trends and opportunities. IT Inf. Technol. 58 (5), 255–262.

Blanco, A.B., de Fuentes, J., Manzano, L.G., Encinas, L.H., Munoz, A.M., Oliva, J.R., García, I.S., 2017. A framework for acquiring and analyzing traces from cryptographic devices. In: 13th EAI International Conference on Security and Privacy in Communication Networks (SecureComm).

Blossom, E., 2004. GNU radio: tools for exploring the radio frequency spectrum. Linux J. (122), 4, 2004.

Bogdanov, A., Kizhvatov, I., Manzoor, K., Tischhauser, E., Witteman, M., 2015. Fast and memory-efficient key recovery in side-channel attacks. In: International Conference on Selected Areas in Cryptography. Springer, pp. 310–327.

Brumley, D., Boneh, D., 2005. Remote timing attacks are practical. Comput. Network. 48 (5), 701–716.

Calari U., Lampkin M.C., RFID reader, US Patent 5,621,199 (Apr. 15 1997).

Callan, R.L., 2016. Analyzing Software Using Unintentional Electromagnetic Emanations from Computing Devices. Ph.D. thesis. Georgia Institute of Technology.

Callan, R., Zajic, A., Prvulovic, M., 2014. A practical methodology for measuring the side-channel signal available to the attacker for instruction-level events. In: 47th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO). IEEE, pp. 242–254.

Callan, R., Popovic, N., Daruna, A., Pollmann, E., Zajic, A., Prvulovic, M., 2015. Comparison of electromagnetic side-channel energy available to the attacker from different computer systems. In: IEEE International Symposium on Electromagnetic Compatibility (EMC). IEEE, pp. 219–223.

Callan, R., Zajić, A., Prvulovic, M., 2015. FASE: finding amplitude-modulated side-channel emanations. In: ACM SIGARCH Computer Architecture News, vol. 43. ACM, pp. 592–603.

Callan, R., Behrang, F., Zajic, A., Prvulovic, M., Orso, A., 2016. Zero-overhead profiling via em emanations. In: Proceedings of the 25th International Symposium on Software Testing and Analysis. ACM, pp. 401–412.

Camurati, G., Poeplau, S., Muench, M., Hayes, T., Francillon, A., 2018. Screaming channels: when electromagnetic side channels meet radio transceivers. In: Proceedings of the 25th ACM Conference on Computer and Communications Security (CCS), CCS '18. ACM.

Cass, S., 2013. A $40 software-defined radio. IEEE Spectrum 50 (7), 22–23.

Chari, S., Rao, J.R., Rohatgi, P., 2002. Template attacks. In: International Workshop on Cryptographic Hardware and Embedded Systems (CHES). Springer, pp. 13–28.

Cheddad, A., Condell, J., Curran, K., Mc Kevitt, P., 2010. Digital image steganography: survey and analysis of current methods. Signal Process. 90 (3), 727–752.

ChipWhisperer Embedded Hardware Security Toolchain. https://newae.com/tools/chipwhisperer/, 2018-01-21.

Clark, S.S., Mustafa, H., Ransford, B., Sorber, J., Fu, K., Xu, W., 2013. Current events: identifying webpages by tapping the electrical outlet. In: European Symposium on Research in Computer Security (ESORICS). Springer, pp. 700–717.

Corey, V., Peterman, C., Shearin, S., Greenberg, M.S., Van Bokkelen, J., 2002. Network forensics analysis. IEEE Internet Computing 6 (6), 60–66.

Danev, B., Zanetti, D., Capkun, S., 2012. On physical-layer identification of wireless devices. ACM Comput. Surv. 45 (1), 6.

Deppensmith, R.D., Stone, S.J., 2014. Optimized fingerprint generation using unintentional emission radio-frequency distinct native attributes (rf-dna). In: Aerospace and Electronics Conference, NAECON 2014-IEEE National. IEEE, pp. 327–330.

Dhem, J.-F., Koeune, F., Leroux, P.-A., Mestré, P., Quisquater, J.-J., Willems, J.-L., 1998. A practical implementation of the timing attack. In: International Conference on Smart Card Research and Advanced Applications. Springer, pp. 167–182.

Du, X., Le-Khac, N.-A., Scanlon, M., 2017. Evaluation of digital forensic process models with respect to digital forensics as a service. In: Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS 2017). ACPI, Dublin, Ireland, pp. 573–581.

Dubendorfer, C.K., 2013. Using RF-DNA Fingerprints to Discriminate ZigBee Devices in an Operational Environment. Master's thesis. Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio.

Casey, E., Stellatos, G.J., 2008. The impact of full disk encryption on digital forensics. ACM SIGOPS - Oper. Syst. Rev. 42 (3), 93–98.

Elibol, F., Sarac, U., Erer, I., 2012. Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system. In: Proceedings of the 20th European Signal Processing Conference (EUSIPCO). IEEE, pp. 1767–1771.

Entriken, W.. System Bus Radio. https://github.com/fulldecent/system-bus-radio, 2018-01-26.

Espitau, T., Fouque, P.-A., Gérard, B., Tibouchi, M., 2017. Side-channel attacks on bliss lattice-based signatures: exploiting branch tracing against strongswan and electromagnetic emanations in microcontrollers. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM, pp. 1857–1874.

Ettus, M., Braun, M., 2015. The Universal Software Radio Peripheral (Usrp) Family of Low-Cost Sdrd, Opportunistic Spectrum Sharing and White Space Access. The Practical Reality, pp. 3–23.

Fahl, S., Harbach, M., Perl, H., Koetter, M., Smith, M., 2013. Rethinking SSL development in an appified world. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. ACM, pp. 49–60.

Fritzke, A.W., 2012. Obfuscating against Side-Channel Power Analysis Using Hiding Techniques for Aes. Master's thesis. Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio.

Gandolfi, K., Mourtel, C., Olivier, F., 2001. Electromagnetic analysis: concrete results. In: International Workshop on Cryptographic Hardware and Embedded Systems (CHES). Springer, pp. 251–261.

R. Getz, B. Moeckel, Understanding and eliminating EMI in Microcontroller Applications, National Semiconductor.

Genkin, D., Shamir, A., Tromer, E., 2014. RSA key extraction via low-bandwidth acoustic cryptanalysis. In: International Cryptology Conference. Springer, pp. 444–461.

Genkin, D., Pachmanov, L., Pipman, I., Tromer, E., 2015. Stealing keys from PCs using a radio: cheap electromagnetic attacks on windowed exponentiation. In: International Workshop on Cryptographic Hardware and Embedded Systems (CHES). Springer, pp. 207–228.

Genkin, D., Pipman, I., Tromer, E., 2015. Get your hands off my laptop: physical side-channel key-extraction attacks on pcs. Journal of Cryptographic Engineering 5 (2), 95–112.

Genkin, D., Pachmanov, L., Pipman, I., Tromer, E., 2016. ECDH key-extraction via low-bandwidth electromagnetic attacks on PCs. In: Cryptographers Track at the RSA Conference. Springer, pp. 219–235.

Genkin, D., Pachmanov, L., Pipman, I., Tromer, E., Yarom, Y., 2016. ECDSA key extraction from mobile devices via nonintrusive physical side channels. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, pp. 1626–1638.

Golmie, N., Rebala, O., Chevrollier, N., 2003. Bluetooth adaptive frequency hopping and scheduling. In: Military Communications Conference (MILCOM'03), vol. 2. IEEE, pp. 1138–1142.

Goubin, L., 2003. A refined power-analysis attack on elliptic curve cryptosystems. In: International Workshop on Public Key Cryptography. Springer, pp. 199–211.

Goudos, S.K., Rekanos, I.T., Sahalos, J.N., 2008. EMI reduction and ICs optimal arrangement inside high-speed networking equipment using particle swarm optimization. IEEE Trans. Electromagn Compat. 50 (3), 586–596.

Han, Y., Etigowni, S., Liu, H., Zonouz, S., Petropulu, A., 2017. Watch me, but don't touch me! contactless control flow monitoring via electromagnetic emanations. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM, pp. 1095–1108.

Hayashi, Y.-i., 2016. State-of-the-art research on electromagnetic information security. Radio Sci. 51 (7), 1213–1219.

Hayashi, Y.-i., Homma, N., Mizuki, T., Shimada, H., Aoki, T., Sone, H., Sauvage, L., Danger, J.-L., 2013. Efficient evaluation of em radiation associated with information leakage from cryptographic devices. IEEE Trans. Electromagn Compat. 55 (3), 555–563.

Hay B., Bishop M., Nance K., Live analysis: Progress and challenges, IEEE Security & Privacy 7 (2).

Hongxin, Z., Yuewang, H., Jianxin, W., Yinghua, L., Jinling, Z., 2009. Recognition of electro-magnetic leakage information from computer radiation with svm. Comput. Secur. 28 (1–2), 72–76.

Hoog, A., 2011. Android Forensics: Investigation, Analysis and Mobile Security for Google Android. Elsevier.

Hutter, M., Mangard, S., Feldhofer, M., 2007. Power and EM attacks on passive 13.56 MHz RFID devices. In: International Workshop on Cryptographic Hardware and Embedded Systems (CHES), vol. 7. Springer, pp. 320–333.

Ishai, Y., Sahai, A., Wagner, D., 2003. Private circuits: securing hardware against probing attacks. In: Annual International Cryptology Conference. Springer, pp. 463–481.

ISO/IEC 17825:2016. Testing Methods for the Mitigation of Non-invasive Attack Classes against Cryptographic Modules. https://www.iso.org/obp/ui/#iso:std:iso-iec:17825:ed-1:v1:en, 2018-01-21.

ISO/IEC TS 30104:2015. Physical Security Attacks, Mitigation Techniques and Security Requirements. https://www.iso.org/standard/56890.html, 2018-01-21.

Iyer, V., Hermans, F., Voigt, T., 2015. Detecting and avoiding multiple sources of interference in the 2.4 GHz spectrum. In: 12th European Conference on Wireless Sensor Networks (EWSN). Springer, pp. 35–51.

Jabbar, M., Rahman, M.A., 1991. Radio frequency interference of electric motors and associated controls. IEEE Trans. Ind. Appl. 27 (1), 27–31.

Kasper, T., Oswald, D., Paar, C., 2009. EM Side-Channel Attacks on Commercial Contactless Smartcards Using Low-Cost Equipment. Information Security Applications, pp. 79–93.

Kellogg, B., Parks, A., Gollakota, S., Smith, J.R., Wetherall, D., 2014. Wi-Fi backscatter: internet connectivity for RF-powered devices. In: ACM SIGCOMM Computer Communication Review, vol. 44. ACM, pp. 607–618.

Kim, C., Schläffer, M., Moon, S., 2008. Differential side channel analysis attacks on FPGA implementations of ARIA. ETRI J. 30 (2), 315–325.

Kim, T., Lee, S., Choi, D., Yoon, H., 2016. Protecting secret keys in networked devices with table encoding against power analysis attacks. J. High Speed Netw. 22 (4), 293–307.

Kocher, P.C., 1996. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In: Annual International Cryptology Conference. Springer, pp. 104–113.

Kocher, P., Jaffe, J., Jun, B., 1999. Differential power analysis. In: Advances in Cryptology (CRYPTO '99). Springer, 789–789.

Kocher, P., Jaffe, J., Jun, B., Rohatgi, P., 2011. Introduction to differential power analysis. Journal of Cryptographic Engineering 1 (1), 5–27.

Kolter, J.Z., Maloof, M.A., 2004. Learning to detect malicious executables in the wild. In: Proceedings of the 10th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, pp. 470–478.

Laput, G., Yang, C., Xiao, R., Sample, A., Harrison, C., 2015. Em-sense: touch recognition of uninstrumented, electrical and electromechanical objects. In: Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology. ACM, pp. 157–166.

Lerman, L., Bontempi, G., Markowitch, O., 2011. Side channel attack: an approach based on machine learning. In: Proceedings of 2nd International Workshop on Constructive Side-Channel Analysis and Security Design (COSADE). Schindler and Huss, pp. 29–41.

Lillis, D., Becker, B., O'Sullivan, T., Scanlon, M., 2016. Current challenges and future research areas for digital forensic investigation. In: The 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016). ADFSL, Daytona Beach, FL, USA, pp. 9–20.

Liu, V., Parks, A., Talla, V., Gollakota, S., Wetherall, D., Smith, J.R., 2013. Ambient backscatter: wireless communication out of thin air. Comput. Commun. Rev. 43 (4), 39–50.

Liu, F., Yarom, Y., Ge, Q., Heiser, G., Lee, R.B., 2015. Last-level cache side-channel attacks are practical. In: IEEE Symposium on Security and Privacy. IEEE, pp. 605–622.

Liu, W., Huang, K., Zhou, X., Durrani, S., 2017. Full-duplex backscatter interference networks based on time-hopping spread spectrum. IEEE Trans. Wirel. Commun. 16 (7), 4361–4377. https://doi.org/10.1109/TWC.2017.2697864.

Lukacs, M.W., Zeqolari, A.J., Collins, P.J., Temple, M.A., 2015. rf-dna fingerprinting for antenna classification. IEEE Antennas Wirel. Propag. Lett. 14, 1455–1458.

Marinov, M.. TempestSDR Remote Video Eavesdropping Using a Software-Defined Radio Platform. https://github.com/martinmarinov/TempestSDR, 2018-02-01.

Maxwell, J.C., 1865. A dynamical theory of the electromagnetic field. Phil. Trans. Roy. Soc. Lond. 155, 459–512.

Messerges, T.S., Dabbish, E.A., Sloan, R.H., 1999. Investigations of power analysis attacks on smartcards. Smartcard 99, 151–161.

Mukkamala, S., Sung, A.H., 2003. Identifying significant features for network forensic analysis using artificial intelligent techniques. International Journal of Digital Evidence 1 (4), 1–17.

Nazari, A., Sehatbakhsh, N., Alam, M., Zajic, A., Prvulovic, M., 2017. EDDIE: EM-based detection of deviations in program execution. In: Proceedings of the 44th Annual International Symposium on Computer Architecture. ACM, pp. 333–346.

Nie, N.H., Erbring, L., 2000. Internet and Society, vol. 3. Stanford Institute for the Quantitative Study of Society, pp. 14–19.

Ossmann, M.. Software Defined Radio with Hackrf, Great Scott Gadgets. https://greatscottgadgets.com/sdr.

Ott, H.W., 2011. Electromagnetic Compatibility Engineering. John Wiley & Sons.

O'Flynn, C., Chen, Z.D., 2014. ChipWhisperer: an open-source platform for hardware embedded security research. In: International Workshop on Constructive Side-Channel Analysis and Secure Design. Springer, pp. 243–260.

O'Malley, S.J., Choo, K.-K.R., 2014. Bridging the air gap: inaudible data exfiltration by insiders. In: 20th Americas Conference on Information Systems (AMCIS). Association for Information Systems.

Peeters, E., Standaert, F.-X., Quisquater, J.-J., 2007. Power and electromagnetic analysis: improved model, consequences and comparisons, Integration. the VLSI Journal 40 (1), 52–60. https://doi.org/10.1016/j.vlsi.2005.12.013.

Prvulovic, M., Zajić, A., Callan, R.L., Wang, C.J., 2017. A method for finding frequency-modulated and amplitude-modulated electromagnetic emanations in computer systems. IEEE Trans. Electromagn Compat. 59 (1), 34–42.

Quisquater, J.-J., Samyde, D., 2001. Electromagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards. Smart Card Programming and Security, pp. 200–210.

Ramsay, C., Lohuis, J.. White Paper: TEMPEST Attacks against AES Covertly Stealing Keys for 200 Euros, Tech. Rep., Fox-IT, Netherlands. https://www.fox-it.com/nl/wp-content/uploads/sites/12/Tempest_attacks_against_AES.pdf.

Reising, D.R., 2012. Exploitation of RF-DNA for Device Classification and Verification Using GRLVQI Processing. Master's thesis. Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio.

Riscure. Inspecture SCA: Side-Channel Analysis Tool for Embedded Systems. https://www.riscure.com/security-tools/inspector-sca/, 2018-01-21.

Saboia, P., Carvalho, T., Rocha, A., 2011. Eye specular highlights telltales for digital forensics: a machine learning approach. In: 18th IEEE International Conference on Image Processing (ICIP). IEEE, pp. 1937–1940.

Sanfelix, E., Mune, C., de Haas, J., 2015. Unboxing the White-Box Practical Attacks against Obfuscated Ciphers, Black Hat Europe.

Saputra, H., Vijaykrishnan, N., Kandemir, M., Irwin, M.J., Brooks, R., Kim, S., Zhang, W., 2003. Masking the energy behavior of des encryption. In: Proceedings of the Conference on Design, Automation and Test in Europe-Volume 1. IEEE Computer Society, p. 10084.

Sayakkara, A., Le-Khac, N.-A., Scanlon, M., 2018. Electromagnetic side-channel attacks: potential for progressing hindered digital forensic analysis. In: Proceedings of the International Workshop on Speculative Side Channel Analysis (WoSSCA 2018). ACM, Amsterdam, Netherlands. https://doi.org/10.1145/3236454.3236512.

Sayakkara, A., Le-Khac, N.-A., Scanlon, M., 2018. Accuracy enhancement of electromagnetic side-channel attacks on computer monitors. In: Proceedings of the 13th International Conference on Availability, Reliability and Security, ARES 2018. ACM, New York, NY, USA. https://doi.org/10.1145/3230833.3234690, 15: 1–15:9. http://doi.acm.org/10.1145/3230833.3234690.

Schulz, M., Klapper, P., Hollick, M., Tews, E., Katzenbeisser, S., 2016. Trust the wire, they always told me!: on practical non-destructive wire-tap attacks against ethernet. In: Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks. ACM, pp. 43–48.

Smith, S.W., 1997. The Scientist and Engineer's Guide to Digital Signal Processing. California Technical Publishing. Ch. 28.

N. Sohaib ul Hassan, Em side channel analysis on complex soc architectures, MSc thesis, Tampere University of Technology.

Soltani, S., Seno, S.A.H., 2017. A survey on digital evidence collection and analysis. In: 7th International Conference on Computer and Knowledge Engineering (ICCKE). IEEE, pp. 247–253.

Souvignet, T., Frinken, J., 2013. Differential power analysis as a digital forensic tool. Forensic Sci. Int. 230 (1–3), 127–136.

Spreitzer, R., Moonsamy, V., Korak, T., Mangard, S., 2018. Systematic classification of side-channel attacks: a case study for mobile devices. IEEE Communications Surveys & Tutorials 20 (1), 465–488.

Stagner, C.B., 2013. Detecting and Locating Electronic Devices Using Their Unintended Electromagnetic Emissions. Missouri University of Science and Technology.

Standaert, F.-X., Malkin, T., Yung, M., 2009. A unified framework for the analysis of side-channel key recovery attacks. In: Eurocrypt, vol. 5479. Springer, pp. 443–461.

Stojkoska, B.L.R., Trivodaliev, K.V., 2017. A review of internet of things for smart home: challenges and solutions. J. Clean. Prod. 140, 1454–1464.

Stone, B.D., Stone, S.J., 2015. Radio frequency based reverse engineering of microcontroller program execution. In: National Aerospace and Electronics Conference (NAECON), 2015. IEEE, pp. 159–164.

Stone, B., Stone, S., 2016. Comparison of radio frequency based techniques for device discrimination and operation identification. In: 11th International Conference on Cyber Warfare and Security: ICCWS2016. Academic Conferences and Publishing Limited, p. 475.

Stone, S.J., Temple, M.A., Baldwin, R.O., 2015. Detecting anomalous programmable logic controller behavior using rf-based hilbert transform features and a correlation-based verification process. International Journal of Critical Infrastructure Protection 9, 41–51.

Tuttlebee, W.H., 2003. Software Defined Radio: Enabling Technologies. John Wiley & Sons.

van de Wiel, E., Scanlon, M., Le-Khac, N.-A., 2018. Enabling non-expert analysis of large volumes of intercepted network traffic. In: Peterson, G., Shenoi, S. (Eds.), Advances in Digital Forensics XIV. Springer International Publishing, Cham, pp. 183–197.

Van Eck, W., 1985. Electromagnetic radiation from video display units: an eavesdropping risk? Comput. Secur. 4 (4), 269–286.

Wakabayashi, S., Maruyama, S., Mori, T., Goto, S., Kinugawa, M., Hayashi, Y.-i., 2017. Poster: is active electromagnetic side-channel attack practical?. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM, pp. 2587–2589.

Wang, X., Zhou, Q., Harer, J., Brown, G., Qiu, S., Dou, Z., Wang, J., Hinton, A., Gonzalez, C.A., Chin, P., 2018. Deep learning-based classification and anomaly detection of side-channel signals. In: Cyber Sensing 2018, vol. 10630. International Society for Optics and Photonics, p. 1063006.

Witteman, M., Oostdijk, M., 2008. Secure application programming in the presence of side channel attacks. In: RSA Conference, vol. 2008.

Witteman, M.F., van Woudenberg, J.G., Menarini, F., 2011. Defeating RSA multiply-always and message blinding countermeasures. In: Cryptographers Track at the RSA Conference (CT-RSA), vol. 6558. Springer, pp. 77–88.

Wolfe, H., 2003. Setting up an electronic evidence forensics laboratory. Comput. Secur. 22 (8), 670–672.

Xu, R., Zhu, L., Wang, A., Du, X., Choo, K.-K.R., Zhang, G., Gai, K., 2018. Side-channel attack on a protected rfid card. IEEE Access, 1–1.

Yang, C., Sample, A.P., 2016. Em-id: tag-less identification of electrical devices via electromagnetic emissions. In: IEEE International Conference on RFID (RFID). IEEE, pp. 1–8.

Yang, C.J., Sample, A.P., 2017. EM-comm: touch-based communication via modulated electromagnetic emissions. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 1 (3), 118.

Yang, K., Hicks, M., Dong, Q., Austin, T., Sylvester, D., 2017. Exploiting the analog properties of digital circuits for malicious hardware. Commun. ACM 60 (9), 83–91.

Yilmaz, B.B., Callan, R.L., Prvulovic, M., Zajić, A., 2018. Capacity of the em covert/side-channel created by the execution of instructions in a processor. IEEE Trans. Inf. Forensics Secur. 13 (3), 605–620.

Zajic, A., Prvulovic, M., 2014. Experimental demonstration of electromagnetic information leakage from modern processor-memory systems. IEEE Trans. Electromagn Compat. 56 (4), 885–893.

Zankl, A., Seuschek, H., Irazoqui, G., Gulmezoglu, B., 2018. Side-channel attacks in the internet of things: threats and challenges. In: Solutions for Cyber-Physical Systems Ubiquity. IGI Global, pp. 325–357.

Zdziarski, J., 2008. iPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets. O'Reilly Media, Inc.

Zhang, Y., Juels, A., Reiter, M.K., Ristenpart, T., 2014. Cross-tenant side-channel attacks in paas clouds. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, pp. 990–1003.

Zhang, P., Bharadia, D., Joshi, K., Katti, S., 2016. Hitchhike: practical backscatter using commodity wifi. In: Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems. ACM, pp. 259–271.