Electromagnetic Side-Channel Attacks: Potential for Progressing Hindered Digital Forensic Analysis

Asanka Sayakkara
Forensics & Security Research Group
School of Computer Science
University College Dublin
Ireland
asanka.sayakkara@ucdconnect.ie

Nhien-An Le-Khac
Forensics & Security Research Group
School of Computer Science
University College Dublin
Ireland
an.lekhac@ucd.ie

Mark Scanlon
Forensics & Security Research Group
School of Computer Science
University College Dublin
Ireland
mark.scanlon@ucd.ie

ABSTRACT

Digital forensics is fast-growing field involving the discovery and analysis of digital evidence acquired from electronic devices to assist investigations for law enforcement. Traditional digital forensic investigative approaches are often hampered by the data contained on these devices being encrypted. Furthermore, the increasing use of IoT devices with limited standardisation makes it difficult to analyse them with traditional techniques. This paper argues that electromagnetic side-channel analysis has significant potential to progress investigations obstructed by data encryption. Several potential avenues towards this goal are discussed.

CCS CONCEPTS

•**Security and privacy → Side-channel analysis and countermeasures;** *Hardware attacks and countermeasures;*

KEYWORDS

Electromagnetic Side-channels, Unintentional Hardware Emissions, Software Defined Radio, Digital Forensics

ACM Reference format:
Asanka Sayakkara, Nhien-An Le-Khac, and Mark Scanlon. 2018. Electromagnetic Side-Channel Attacks: Potential for Progressing Hindered Digital Forensic Analysis. In *Proceedings of The International Workshop on Speculative Side Channel Analysis, Amsterdam, Netherlands, 2018 (WoSSCA),* 6 pages.
DOI: 10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

The increasing consumer reliance on electronic devices has risen to a level where it is easier for attackers to compromise the privacy and security of an individual's digital information than by any other means. Private information is stored in a wide variety of digital platforms including mobile phones, personal computers, social media profiles, cloud storage, etc. [27]. The recent emergence of Internet of Things (IoT) devices, which integrates into the fabric of everyday life, enables the digital recording of even more personal information. The field of information security deals with the challenge of keeping this sensitive data from falling into the hands of unauthorized parties. However, when criminal and illegal activities involve electronic and computing devices, law enforcement authorities require access to each suspect's private data, under warrant, in order to collect potentially pertinent evidence [29]. In this regard, the fields of information security and digital forensics are juxtaposed with each other.

Modern personal computers and mobile devices provide facility to encrypt the hard disks and other non-volatile data storage. While this functionality was first offered as an option to users on initial setup of these devices, it is increasingly the default behaviour, especially on mobile environments, such as iOS and Android [2]. While IoT devices have limited data processing power and storage capabilities, lightweight cryptographic mechanisms are utilized in many platforms. Encrypted data has long been identified as a potentially rich source of evidence. Many cases have been hampered when encrypted data was encountered [17]. With respect to IoT devices, even if encryption is not employed, the lack of standardised interfaces to access the stored data can still pose a challenge.

Side-channel analysis has been proven to be effective against many security mechanisms on computing systems. Accessing unauthorized regions of volatile and non-volatile storage, intercepting regular operations of applications and processes, and many other useful possibilities exist [22]. Among various side-channel attacks, electromagnetic (EM) side-channel analysis is an important class of attacks that does not require an attacker to have physical access to the target device. This means that passive observation of unintentional EM wave emissions from a target device opens up a window to an attacker to infer the activities being performed and the data being handled on the target [34]. Without running any specific software on the target device or without tapping into its internal hardware, EM side-channel attacks can provide a seamless access point for the attacker. Recent advances in the domain shows that such attacks are capable of retrieving sensitive data, such as encryption keys [24].

Most mobile devices and IoT devices seized for forensic investigations tend to be powered on when they are found. However, legal requirements for digital forensic investigation demand that, ideally, investigations should be performed without inadvertently, or intentionally, modifying any information. Meeting this requirement often prevents an investigator from compromising the software and hardware while acquiring evidence [9]. Due to the nature of EM side-channel analysis, it has a desirable hands-off quality from a forensic perspective and has the potential to act as a manner to unobtrusively access the internal information from a device. A variety of avenues ranging from simple activity recognition to breaking

WoSSCA, Amsterdam, Netherlands

DOI: 10.1145/nnnnnnn.nnnnnnn

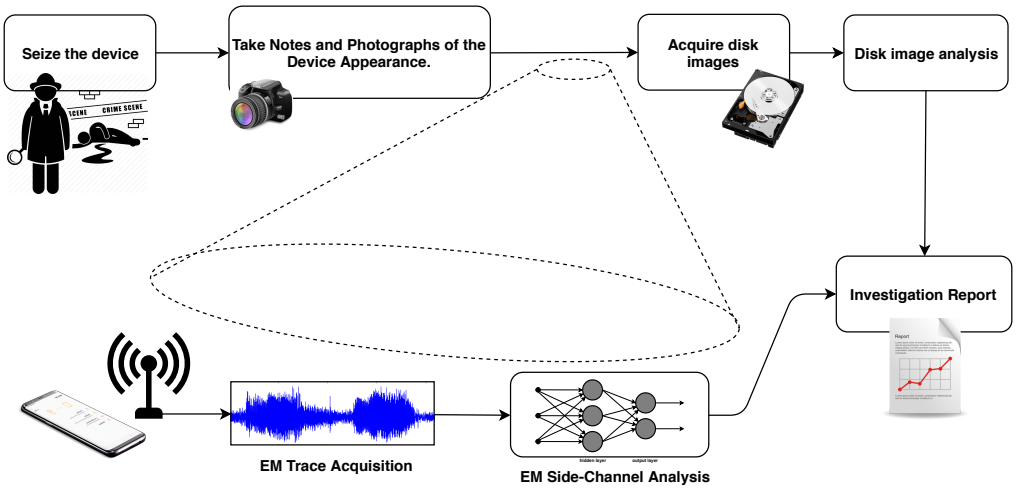

Figure 1: A typical digital forensic investigation starts with a seized device as part of a legal process. Major focus of the investigation goes to the analysis of non-volatile storage, i.e., hard disk. However, with the incorporation of EM side-channel analysis into the process, live data forensics can be performed if the device is switched on at the time it was seized.

encryption could be beneficial to a digital forensic investigator. In this work, various potential applications for EM side-channel analysis in the domain of digital forensics are discussed in.

2 DIGITAL FORENSIC ANALYSIS

A typical digital forensic investigation starts when a law enforcement encounters an electronic device in a crime scene or seized it from a person under investigation. These devices can vary from traditional personal computers and mobile devices to IoT devices, such as smart home devices and wearables. The seized devices are usually handed over to a digital forensic laboratory where specialists perform the investigation on the device [9]. Initially, pictures and notes were taken about the physical conditions of the device. For personal computers, the investigation mainly focuses on the data stored in the non-volatile memory, i.e., the hard disk or solid state drive. A forensically-sound disk image is acquired, which is analysed using specialised software tools to identify pertinent information.

The sole purpose of acquiring a disk image from the device under investigation is to prevent the investigative procedure from inadvertently making changes to the device. Popular tools such as *EnCase* and *The Sleuth Kit* are designed to extract information from disk images. In contrast to personal computers, the forensic analysis of mobile devices typically requires specialised hardware tools due to the fact that different makes and models of mobile devices has different internal structures. Even though there are various commercial tools available for mobile devices, they need to be updated each time a new device model comes into the market. The maintainers of commercial tools for forensic evidence acquisition on mobile devices are struggling to keep up with the highly dynamic ecosystem of mobile devices [2].

IoT devices have become ubiquitous in everyday life and collect a large volume of information that can be useful in a forensic investigation [19]. For example, a fitness wearable can contain highly precise information regarding the movements of the owner, which can assist in identifying where the person was at a particular point in time. Similarly, a smart TV or a smart light bulb may contain information regarding the usage patterns of the owner and might hint at the presence of the owner in a premises at a particular time. However, IoT focused digital forensic tools are extremely limited. In fact, many IoT devices are not usable in investigations due to unavailability of support from commercial vendors or open-source projects. The large variety of IoT devices in the market makes it virtually impossible to support all of them within a limited tool set.

Whenever encryption is involved in the storage of a device being investigated, forensic tools are unable to extract information [17]. From the investigator's perspective, a very limited number of workarounds are potentially viable. The obvious approach can be asking the device owner for the decryption key or password. However, if the device owner is not corporative, this approach is not viable. Another possible approach can involve seeking the assistance of the device vendor to unlock the access to data using whatever the capabilities the vendor holds. However, many recent cases indicates that even the device vendors does not have access to the encrypted data storage on devices they produce. Under these circumstances, forensic investigations may end up unable to collect the required evidence from the devices they have seized [33].

Figure 1 illustrates the workflow of actions taken in a typical digital forensic analysis of a device. The usual sequence of actions to analyse non-volatile storage has to be altered if the device uses encryption to protect data. If the device is turned on at the time it was seized, there's an opportunity to use EM side-channel analysis as a live data forensic technique on the device.

3 ELECTROMAGNETIC SIDE-CHANNELS

Passing time varying electric currents through conductors cause EM waves to radiate into the environment. As computing devices consist of electronic circuits, they unintentionally generate EM

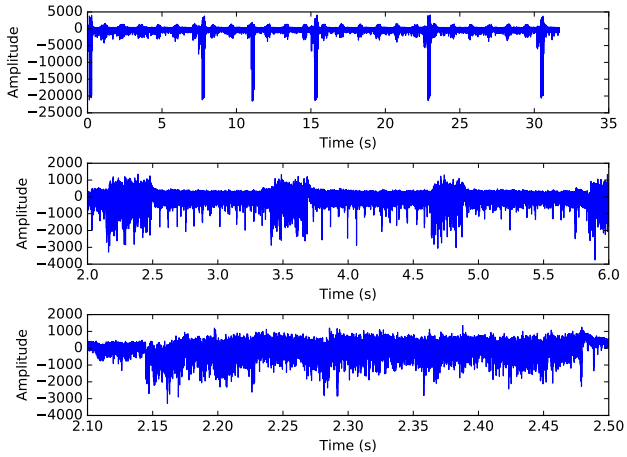

Figure 2: Waveform of the AM demodulated signal from the CPU of Raspberry Pi. The signal represents the AES encryptions performed on the device with approximately 1 second gaps.

emissions during their internal operations [10]. Depending on the exact component on a device that contributes, the resulting EM emission can unintentionally contain information about the activities associated with that component. For example, computer displays are a source of strong EM emissions that are known to facilitate reconstruction of the images being [15, 26, 32]. Similarly, central processing units (CPUs) of computers are known to provide hints on the CPU activities being performed [5]. From a digital forensic perspective, EM emissions associated with the CPU operations are of specific interest.

In order to use EM emissions as a side-channel information source for an attacker, it is necessary to capture the signals with sufficient accuracy. Professionals in radio frequency (RF) engineering and related fields uses oscilloscopes and spectrum analysers as the typical tools to measure EM emissions from electronic devices for purposes such as electromagnetic compatibility (EMC) testing. However, cheap and off-the-shelf devices, software defined radios (SDR), are getting increasingly popular among EM side-channel security researchers due to their lower cost and ease of use with configurable software components [31].

When an acquired EM signal from a target device, i.e., EM trace, is illustrated as a waveform or as a spectrogram, it is possible to visually distinguish individual operations of the CPU. Using these illustrations straightforwardly to eavesdrop on the the CPU activities is called *simple electromagnetic analysis* (SEMA). This has been widely used to demonstrate attacks to computer systems [13]. By monitoring instructions being executed on the CPU, an attacker gains several capabilities including reverse engineering unknown software, monitoring the control flow of known software, etc.

The most powerful EM emission source of a computing device is the processor, which operates with the help of fast clock pulses. For example, consider a *Raspberry Pi* device as a target that has a processor running at 1.4 GHz. Tuning an SDR to the relevant frequency near the target reveals that there is a strong EM signal at the processor clock frequency. Taking it as the carrier wave, other operations within the CPU gets modulated into it, which can be observed after demodulating the EM traces. If a target device is performing cryptographic operations, the captured EM traces can contain the information relevant to the cryptographic algorithms in some type of modulation. Figure 2 illustrates the amplitude demodulated EM traces of the target device when it was performing advanced encryption standard (AES) encryption operations. The blobs visible in the waveform across time are the signature of AES encryption blocks as modulated into the CPU clock frequency.

Differential electromagnetic analysis (DEMA) is an advanced technique to eavesdrop on critical variables being handled by algorithms running on a CPU [13, 14]. For example, when a cryptographic algorithm performs data encryption continuously over a time period using a single encryption key, the observed EM traces have a strong correlation to that specific reused encryption key. DEMA attacks utilise this correlation between the secret key and the EM traces to reduce the number of bruteforce guesses an attacker has to make in order to determine the secret key's bit pattern. It has been shown that DEMA is successful against many cryptographic algorithms including AES, RSA and many others [23, 36].

Recognising the threat of EM side-channel attacks to computer systems, various countermeasures have been proposed that involves both hardware and software modifications [23, 25, 35]. Among various software based countermeasures, two important methods are, masking variables and randomizing the operations of algorithms in order to make it difficult for an external observer to identify them. Similarly, major hardware countermeasures include minimizing the EM emission intensity by employing obfuscation techniques and the use of dual line logic. Even though proper implementation of such countermeasures can place a barrier to the attackers, many computing devices do not implement these technique – leaving the window for EM side-channel attacks open. Furthermore, it has been shown that even when such countermeasures are implemented on devices, it does not completely prevent EM side-channel attacks. They simply increase the difficultly for the attacker by requiring more observations and a larger number of EM traces to carry out the same attack procedure.

Figure 3 illustrates a forensic investigative setting for EM side-channel analysis. The device under investigation (DUI) is placed inside an EMC/Anechoic chamber to prevent external EM interference and vibrations from affecting the accuracy of the EM measurement. The signals are captured using a magnetic loop antenna connected to a software defined radio (SDR). Captured signals are converted to an Inphase and Quadrature (I/Q) data stream that is subsequently analysed on a host computer system.

4 ELECTROMAGNETIC SIDE-CHANNELS FOR FORENSICS

With the current challenges in digital forensics and the state-of-the-art of EM side-channel analysis, it is important to identify the future potential impact for digital forensics from these attacks. This section highlights some of the potential ways this impact may occur in the future under several key themes. Many of these approaches are

Figure 3: An illustration of how an EM side-channel analysis would be performed in a forensic investigative setting. Target device is placed inside an EMC/Anechoic chamber and observed using an SDR device that is connected to an EM analysis software framework.

already starting to be realised and others are ambitious predictions that can prove significantly beneficial.

4.1 More Frequent Cryptographic Operations

EM side-channel attacks require a large number of traces acquired from a target device while the device is performing cryptographic operations using a single key. It has been demonstrated that such attacks are viable under laboratory conditions. However in most PC operating systems, it is rare to find practical situations where an attacker can observe EM emissions from a device for an extended period of time (since cryptographic operations typically occur less often than in the laboratory experimental conditions). The most common encryption occurring on many personal devices are secure socket layer (SSL) based web traffic.

Encrypted storage is becoming commonplace in both desktop and mobile devices. Access to encrypted file systems causes an increased number of cryptographic CPU operations. Live data forensic techniques can help to perform investigations on such devices [12]. However, forensic investigators often encounter powered on but locked devices. As long as the device is reading and writing to the encrypted storage, EM emissions should reflect the cryptographic operations on the device. Therefore, an attacker can straightforwardly force the victim device to perform cryptographic operations in order to acquire side-channel traces for key extraction.

4.2 Combined Side-Channel Attacks

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 [1]. 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.

Sometimes, combining conventional attacks, e.g., spyware and worms, with EM side-channel attacks can provide new kinds of compound attacks that are difficult to counteract. For example, a malware running on a victim computer can aid an EM side-channel attacker to extract additional information over the EM side-channel alone. This can be achieved through running specially selected instruction sequences on the CPU to intentionally emit encoded EM signals. Yang et al. [37] illustrated a mechanism to intentionally modulate EM emissions of electronic and electromechanical devices to exfiltrate data from the device to an external receiver. This hints at the potential for employing these unintentional EM side-channels to intentionally and covertly transmit data wherever necessary.

There are two potential avenues for malware assisted EM side-channel attacks. Firstly, malicious JavaScript can be embedded in a website, using cross-site scripting (XSS) or otherwise, and read the contents of a user's screen and encode that information into deliberate CPU EM emissions. Furthermore, TEMPEST style attacks on computer monitors can be combined with other attacks to increase the attack surface for air-gapped computer equipment [11]. For example, malware running on a target computer could read local files and encode that information into the computer's video output. Image steganographic techniques can be used to hide the encoded data from the human user's view [6]. Meanwhile, a TEMPEST style attack can be performed on the computer's monitor in order to extract the video frames ultimately leaking data to the attacker.

4.3 File Signatures

Many types of digital multimedia content including images, audio, and video files are stored in a compressed format for efficient storage and distribution [3]. As a result, when a computer starts playing an audio/video file in a specific format, e.g., MPEG-2 Audio Layer III, AAC, MPEG-4, etc., or attempts to display a compressed image format, e.g., JPEG, GIF, etc., corresponding decompression software has to process the content. Since the software's execution path will be governed by the media file content, the instruction execution sequence will also depend on the media file. Therefore, it is possible that the CPU might emit EM patterns unique to a specific file being handled. This could potentially lead to the ability to identify the files being handled by a device.

While there have been attempts to make EM emission signatures for hardware devices and specific software running on them for profiling purposes, such as RF-DNA technique [8], the possibility of profiling specific media files using the EM emission caused by them is a potential avenue for future exploration. Searching for a known file, such as known illegal content, in a target device is a challenge that the digital forensics community has been attempting to solve in efficient and effective ways as manual comparison is often overly arduous for the expert investigators [18]. When a

device is handling a file, passive observations of EM emissions can help to profile the file being handled by the device. This can be later be compared with a known set of file signatures to confirm the access or processing of a specific file on the target device.

4.4 Packet Analysis at Network Devices

There are a wide variety of special purpose computers being used in various specialised application environments including network routers and switches. There can often be an operational need to investigate a live network. This focuses on the data-link and IP layers in the networking stack. In such cases, it is necessary to run network analysis software tools on specific interfaces at host computers [7]. Analysing the network purely based on the traffic going through routers and switches in order to observe live events is a challenging task. 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. It has been shown that EM emissions observed from Ethernet cables can lead to identify the MAC addresses of frames being handled by networking devices [28]. In that demonstration, attackers has used a technique similar to SEMA.

When IP packets are being switched at routers, the router has to update certain fields in the packet including time-to-live (TTL) and the header checksum. After updating these fields, the router forwards the packet to the relevant network interface. If the EM emission patterns of the router forwarding a packet to an interface and processing a packet are distinguishable, there are opportunities to perform interesting analysis on routers by observing their EM emissions. Packets that contains a specific payload, such as malware that comes from or addressed to a specific host, and network based attacks, e.g., DoS attacks, might be identifiable. Similarly, an attacker could gather EM emissions from a router to eavesdrop on the data being delivered through a wired network. Such possibilities are important from a digital forensic perspective when network analysis tools cannot be attached to a live system for analysis.

4.5 Easy Access to Electromagnetic Spectrum

EM side-channel analysis attacks traditionally involve expensive hardware including RF probes, oscilloscopes, spectrum analysers, and data acquisition modules. Such devices are mostly used in EM insulated laboratory environments. Moreover the configuration and operation of these devices requires specialized domain knowledge. Information security specialists and digital forensic analysts might not have access to such hardware and might not posses the specialized knowledge required for their operation. While DIY enthusiast attempts have been made to build such tools for lower costs, such efforts come with a penalty of lower precision and accuracy. This situation places a significant barrier to the wide adoption of EM side-channel analysis.

Recent advancements in SDR hardware enables new opportunities for accessing radio spectrum for non-specialists. Affordable SDR hardware and freely available software libraries can be used to process and decode various wireless communication protocols. The ever-increasing processing power and memory capacity on personal computers supports the use of SDR software tools at high sampling rates. EM side-channel analysis attackers have recently started to use SDR tools as a more affordable alternative to the expensive RF signal acquisition hardware. Following this trend, digital forensic analysis should be possible through the leveraging of EM side-channels detected on SDR based hardware and software platforms.

4.6 Advancements in Machine Learning

Recent advances that have been made in the area of artificial intelligence (AI) 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 machine learning and deep learning based 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, image manipulation, and network anomaly detection.

EM side-channel analysis techniques, such as SEMA and spectrogram pattern observations, that previously required human intervention can be automated through the development of AI techniques. It is possible to extract better information from EM traces than the current manual observations are capable of achieving. There are several examples of existing work that has already leveraged AI techniques to recognize EM trace patterns, which strongly hints the future role that can be played by AI algorithms in EM side-channel analysis for digital forensics [4, 16, 20, 21, 30].

5 DISCUSSION AND FUTURE WORK

When digital evidence is presented to a court of law as a part of an investigation, the evidence acquisition procedure can get thoroughly questioned and challenged. This is due to the fact that legal processes follow strict procedures to ensure fairness to all parties involved. As a result, digital forensic evidence acquisition procedures are demanded to be documented and auditable. Current digital evidence acquisition procedures, practices and tools in use are time-tested to be resilient against such legal challenges. Therefore, whenever a completely new way of acquiring digital evidence is introduced, it has to be thoroughly scrutinized to face reliability challenges in a court of law.

Many of the EM side-channel attacks that have been demonstrated in the literature are performed in controlled laboratory conditions where the attacker had the choice of target device selection. Therefore, the attackers had the freedom to avoid potential pitfalls that could affect the end result. In order to make such attacks realistic and reliable enough to perform on any arbitrary device encountered, further research is necessary. Sometimes, a successful execution of an EM side-channel attack can be easier for a malicious objective while the same attack can be unreliable and insufficiently trustworthy for a digital forensic investigation. This situation hints that for EM side-channel analysis to be leveraged for digital forensic purposes, well tested tools and frameworks need to be developed so that the digital forensic community can gradually build trust with the technique.

Our future work is towards this goal of leveraging EM side-channel analysis as a reliable digital forensic practice to overcome the currently faced challenges. Due to the lack of realistic and

reliable attack demonstrations, further evaluations are necessary to confirm that various published attacks are applicable on a wide variety of devices on the market. The manner to increase the reliability of these attacks needs to be explored. Many digital forensic specialists working for law enforcement and industry may not be experienced in operating radio frequency data acquisition devices. Therefore, easily operable tools are necessary.

6 CONCLUSION

This work discussed the challenges faced by digital forensic investigators due to encrypted storage on computing devices and IoT devices with non-uniform internal designs. EM side-channel analysis techniques, which have been successfully demonstrated to leak critical information from computing devices, is considered a promising solution. Various applicable scenarios of the technique in the context of digital forensic domain are identified. While the EM side-channel analysis domain is still in its infancy to address the demanding encryption issue in digital forensics, the aforementioned application scenarios indicate that it shows strong promise to produce useful, case progressing results in the future.

REFERENCES

[1] Dakshi Agrawal, Josyula R Rao, and Pankaj Rohatgi. 2003. Multi-channel attacks. In *International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*. Springer, 2–16.

[2] Mohd Shahdi Ahmad, Nur Emyra Musa, Rathidevi Nadarajah, Rosilah Hassan, and Nor Effendy Othman. 2013. Comparison between android and iOS Operating System in terms of security. In *8th International Conference on Information Technology in Asia (CITA)*. IEEE, 1–4.

[3] Vasudev Bhaskaran and Konstantinos Konstantinides. 1997. *Image and video compression standards: algorithms and architectures*. Vol. 408. Springer Science & Business Media.

[4] Robert Callan, Farnaz Behrang, Alenka Zajic, Milos Prvulovic, and Alessandro Orso. 2016. Zero-overhead profiling via em emanations. In *Proceedings of the 25th International Symposium on Software Testing and Analysis*. ACM, 401–412.

[5] Robert Callan, Alenka Zajic, and Milos Prvulovic. 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, 242–254.

[6] Abbas Cheddad, Joan Condell, Kevin Curran, and Paul Mc Kevitt. 2010. Digital image steganography: Survey and analysis of current methods. *Signal Processing* 90, 3 (2010), 727–752.

[7] Vicka Corey, Charles Peterman, Sybil Shearin, Michael S Greenberg, and James Van Bokkelen. 2002. Network forensics analysis. *IEEE Internet Computing* 6, 6 (2002), 60–66.

[8] Randall D Deppensmith and Samuel J Stone. 2014. Optimized fingerprint generation using unintentional emission radio-frequency distinct native attributes (RF-DNA). In *Aerospace and Electronics Conference, NAECON 2014-IEEE National*. IEEE, 327–330.

[9] Xiaoyu Du, Nhien-An Le-Khac, and Mark Scanlon. 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, 573–581.

[10] Robin Getz and Bob Moeckel. 1996. Understanding and eliminating EMI in Microcontroller Applications. *National Semiconductor* (1996).

[11] Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici. 2015. GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies.. In *USENIX Security Symposium*. 849–864.

[12] Brian Hay, Matt Bishop, and Kara Nance. 2009. Live analysis: Progress and challenges. *IEEE Security & Privacy* 7, 2 (2009).

[13] Paul Kocher, Joshua Jaffe, and Benjamin Jun. 1999. Differential power analysis. In *Advances in Cryptology (CRYPTO '99)*. Springer, 789–789.

[14] Paul Kocher, Joshua Jaffe, Benjamin Jun, and Pankaj Rohatgi. 2011. Introduction to differential power analysis. *Journal of Cryptographic Engineering* 1, 1 (2011), 5–27.

[15] Markus G Kuhn and Ross J Anderson. 1998. Soft tempest: Hidden data transmission using electromagnetic emanations. In *International Workshop on Information Hiding*. Springer, 124–142.

[16] Liran Lerman, Gianluca Bontempi, and Olivier Markowitch. 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, 29–41.

[17] David Lillis, Brett Becker, Tadhg O'Sullivan, and Mark Scanlon. 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, 9–20.

[18] David Lillis, Frank Breitinger, and Mark Scanlon. 2018. Hierarchical Bloom Filter Trees for Approximate Matching. *Journal of Digital Forensics, Security and Law* 13, 1 (01 2018).

[19] Aine MacDermott, Thar Baker, and Qi Shi. 2018. IoT Forensics: Challenges For The IoA Era. In *New Technologies, Mobility and Security (NTMS), 2018 9th IFIP International Conference on*. IEEE, 1–5.

[20] Houssem Maghrebi, Thibault Portigliatti, and Emmanuel Prouff. 2016. Breaking cryptographic implementations using deep learning techniques. In *International Conference on Security, Privacy, and Applied Cryptography Engineering*. Springer, 3–26.

[21] Alireza Nazari, Nader Sehatbakhsh, Monjur Alam, Alenka Zajic, and Milos Prvulovic. 2017. EDDIE: EM-Based Detection of Deviations in Program Execution. In *Proceedings of the 44th Annual International Symposium on Computer Architecture*. ACM, 333–346.

[22] Romain Poussier, Vincent Grosso, and François-Xavier Standaert. 2015. Comparing approaches to rank estimation for side-channel security evaluations. In *International Conference on Smart Card Research and Advanced Applications*. Springer, 125–142.

[23] Jean-Jacques Quisquater and David Samyde. 2001. Electromagnetic Analysis (EMA): Measures and counter-measures for smart cards. *Smart Card Programming and Security* (2001), 200–210.

[24] C. Ramsay and J. Lohuis. *White Paper: TEMPEST attacks against AES covertly stealing keys for 200 euros*. Technical Report. Fox-IT, Netherlands. 10 pages. https://www.fox-it.com/nl/wp-content/uploads/sites/12/Tempest_attacks_against_AES.pdf

[25] Hendra Saputra, Narayanan Vijaykrishnan, M Kandemir, Mary Jane Irwin, R Brooks, Soontae Kim, and Wei Zhang. 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, 10084.

[26] Asanka Sayakkara, Nhien-An Le-Khac, and Mark Scanlon. 2018. Accuracy Enhancement of Electromagnetic Side-channel Attacks on Computer Monitors. In *The 2nd International Workshop on Criminal Use of Information Hiding (CUING), part of the 13th International Conference on Availability, Reliability and Security (ARES) (ARES '17)*. ACM, Hamburg, Germany.

[27] Mark Scanlon, Jason Farina, and M-Tahar Kechadi. 2015. Network Investigation Methodology for BitTorrent Sync: A Peer-to-Peer Based File Synchronisation Service. *Computers & Security* 54 (10 2015), 27 – 43. DOI: http://dx.doi.org/10.1016/j.cose.2015.05.003

[28] Matthias Schulz, Patrick Klapper, Matthias Hollick, Erik Tews, and Stefan Katzenbeisser. 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, 43–48.

[29] Somayeh Soltani and Seyed Amin Hosseini Seno. 2017. A survey on digital evidence collection and analysis. In *7th International Conference on Computer and Knowledge Engineering (ICCKE)*. IEEE, 247–253.

[30] Barron Stone and Samuel Stone. 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, 475.

[31] Walter HW Tuttlebee. 2003. *Software defined radio: enabling technologies*. John Wiley & Sons.

[32] Wim Van Eck. 1985. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security* 4, 4 (1985), 269–286.

[33] Eva A Vincze. 2016. Challenges in digital forensics. *Police Practice and Research* 17, 2 (2016), 183–194.

[34] Satohiro Wakabayashi, Seita Maruyama, Tatsuya Mori, Shigeki Goto, Masahiro Kinugawa, and Yu-ichi Hayashi. 2017. POSTER: Is Active Electromagnetic Side-channel Attack Practical?. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2587–2589.

[35] Marc Witteman and Martijn Oostdijk. 2008. Secure application programming in the presence of side channel attacks. In *RSA Conference*, Vol. 2008.

[36] Marc F Witteman, Jasper GJ van Woudenberg, and Federico Menarini. 2011. Defeating RSA Multiply-Always and Message Blinding Countermeasures. In *Cryptographersfi Track at the RSA Conference (CT-RSA)*, Vol. 6558. Springer, 77–88.

[37] Chouchang Jack Yang and Alanson P Sample. 2017. EM-Comm: Touch-based Communication via Modulated Electromagnetic Emissions. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, 3 (2017), 118.