Leveraging Electromagnetic Side-Channel Attacks for Digital Forensics

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

Forensics and Security Research Group,
School of Computer Science,
University College Dublin,
Ireland
asanka.sayakkara@ucdconnect.ie, {an.lekhac, mark.scanlon}@ucd.ie

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. [6]. 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 [7]. 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 device's main storage 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 [1]. While IoT devices have limited data processing power and storage capabilities, lightweight cryptographic mechanisms, such as elliptic curve cryptography, are often utilised 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 [3]. 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 significant challenge.

2 Electromagnetic Side-Channel Attacks to the Rescue

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, alongside many other promising possibilities for the approach [4]. Among various side-channel attacks, electromagnetic (EM) side-channel analysis is an interesting category 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 [8]. Without running any specific software on the target device, and without tapping into its internal hardware, EM side-channel attacks can provide a seamless access point for the attacker. Recent advances in the domain show that such attacks are capable of retrieving sensitive data or inferring the data being processed, such as encryption keys [5].

Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

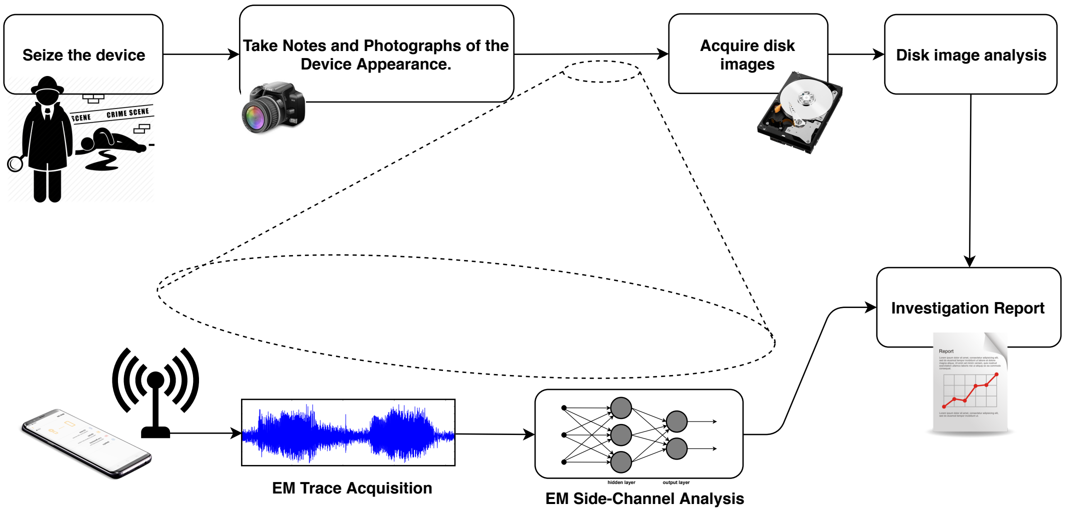

Figure 1 A significant proportion of typical digital forensic investigations is focused on non-volatile storage, i.e., hard disks. However, with the incorporation of EM side-channel analysis into the process, live data forensics can be performed if the device is seized powered on.

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 [2]. 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. Figure 1 illustrates the workflow of actions taken in a typical digital forensic analysis of a device and where the EM side-channel analysis may fit in for cases involving encrypted content, or bespoke filesystems, protocols and hardware.

3 Potential Research Avenues

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.

- **More Frequent Cryptographic Operations**
  Encrypted storage is becoming commonplace in both desktop and mobile devices which makes access to encrypted file systems causes an increased number of cryptographic CPU operations. It increases the opportunity to perform EM side-channel attacks.
- **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
- **Backscatter Side-Channels**
  Internal operations of electronic circuits (including CPUs) could demonstrate the backscatter effect on ambient RF sources during their operation. The potential of using externally generated RF signals near a target CPU and whether internal CPU operations modulate the RF signal in some predictable manner requires further exploration.

- **File Signatures**
  When a computer is handling media files which are mostly in compressed formats, it is possible that the EM emissions from the CPU can contain the distinguishable signatures of the files. This could potentially lead to the ability to identify the files being handled by a device.
- **Packet Analysis at Network Devices**
  There can often be an operational need to investigate a live wired network without physically tapping into the hardware. If the EM emission patterns of networking devices forwarding and/or processing packets are distinguishable, there are opportunities to perform interesting analysis on routers by observing their EM emissions.
- **Easy Access to Electromagnetic Spectrum**
  Recent advancements in SDR hardware enables new opportunities for accessing radio spectrum for non-specialists. Digital forensic analysis should be possible through the leveraging of EM side-channels detected on SDR based hardware and software platforms.
- **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 EM side-channel analysis techniques that previously required human intervention can be automated through the development of AI techniques.

References

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

2 Xiaoyu Du, Nhien-An Le-Khac, and Mark Scanlon. 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)*, pages 573–581, Dublin, Ireland, 06 2017. ACPI.

3 David Lillis, Brett Becker, Tadhg O'Sullivan, and Mark Scanlon. Current Challenges and Future Research Areas for Digital Forensic Investigation. In *The 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016)*, pages 9–20, Daytona Beach, FL, USA, 05 2016. ADFSL.

4 Romain Poussier, Vincent Grosso, and François-Xavier Standaert. Comparing Approaches to Rank Estimation for Side-channel Security Evaluations. In *International Conference on Smart Card Research and Advanced Applications*, pages 125–142. Springer, 2015.

5 C. Ramsay and J. Lohuis. White Paper: TEMPEST attacks against AES covertly stealing keys for 200 euros. Technical report, Fox-IT, Netherlands.

6 Mark Scanlon, Jason Farina, and M-Tahar Kechadi. Network Investigation Methodology for BitTorrent Sync: A Peer-to-Peer Based File Synchronisation Service. *Computers & Security*, 54:27 – 43, 10 2015.

7 Somayeh Soltani and Seyed Amin Hosseini Seno. A Survey on Digital Evidence Collection and Analysis. In *7th International Conference on Computer and Knowledge Engineering (ICCKE)*, pages 247–253. IEEE, 2017.

8 Satohiro Wakabayashi, Seita Maruyama, Tatsuya Mori, Shigeki Goto, Masahiro Kinugawa, and Yu-ichi Hayashi. Poster: Is active electromagnetic side-channel attack practical? In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 2587–2589. ACM, 2017.