BOOK CHAPTER | Signal Attacks

Mitigating Electromagnetic Side-Channel Attacks

Amankwah Attah
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: attagate@gmail.com

ABSTRACT

By providing new sources of electronic evidence, the Internet of Things (IoT) has opened up new possibilities for digital forensics. Obtaining electronic data from IoT, on the other hand, is a difficult process for a variety of reasons, including the use of various types of standard interfaces, the use of light-weight data encryption, such as elliptic curve cryptography (ECC), and so on. The use of electromagnetic side-channel analysis (EM-SCA) to obtain forensically valuable electronic data from IoT devices has been proposed. EM side-channel analysis is a technique for eavesdropping on the operations and data handling of computing devices using unintentional electromagnetic emissions. However, successful EM-SCA attacks on IoT devices require expert knowledge and specialized tools that are not available to most digital forensic investigators. The electromagnetic side-channel (EM-SC) is one of several types of side-channel approaches for extracting usable electronic data from IoT devices. This paper with focus on Electromagnetic side-channel (EM-SC), the positive and negative usage and how to mitigate the negative usage.

Keywords: Electromagnetic, Side-channels, digital forensics, IOT, electronic evidence, Africa.

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Amankwah Attah (2022): Mitigating Electromagnetic Side-Channel Attacks
SMART-IEEE-Creative Research Publications Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics.
Pp 71-76. www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P12

1. INTRODUCTION

A side-channel attack is a security exploit that aims to gather information from or influence the program execution of a system by measuring or exploiting indirect effects of the system or its hardware rather than targeting the program or its code directly. Most commonly, these attacks aim to infiltrate sensitive information, including cryptographic keys, by measuring coincidental hardware emissions. A side-channel attack may also be referred to as a *sidebar attack* or an *implementation attack [2]*. A side-channel attack does not directly attack a program or its code. A side-channel attack, on the other hand, tries to obtain information or alter the program execution of a system by measuring or exploiting the system's or its hardware's indirect effects.

Simply put, a side channel attack is a type of cryptography attack that takes use of information that is accidentally disclosed by a system.

Electromagnetic, acoustic, power, optical, timing, memory cache, and hardware vulnerabilities are all examples of side-channel attacks [6]. This study will concentrate on electromagnetic side channel attacks, detailing some of the most common attacks, as well as mitigating electromagnetic side channel attacks in digital forensics, which can have both positive and negative effects on the acquisition of electronic evidence.

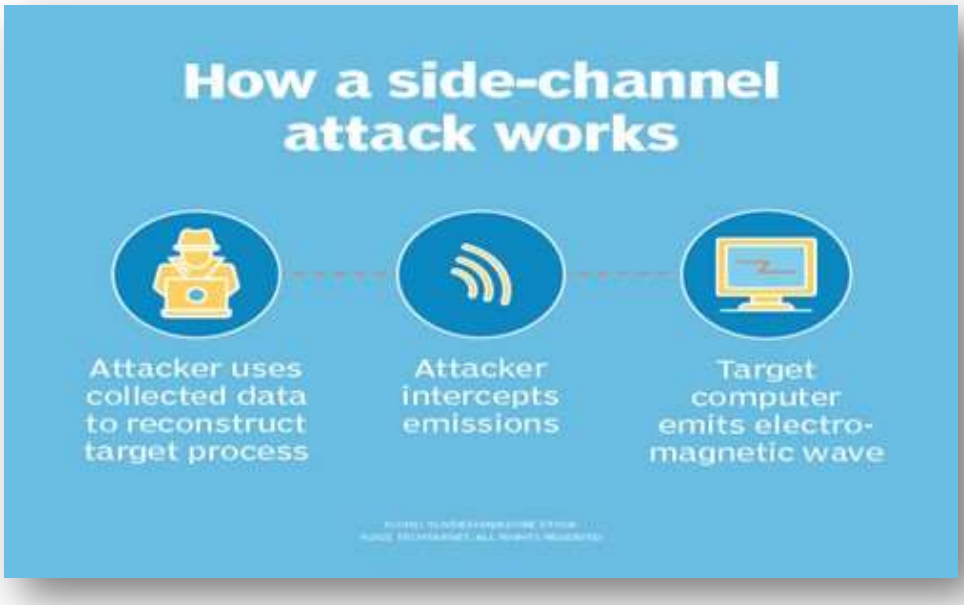

Fig.1 illustrating how side-channels attack works [3]

1.1 Background To Study

Side-channel assaults have become a more sophisticated horizon in recent years, utilized to investigate a group of weaknesses on physical equipment or to divulge the secrets of a workflow, communication channel, or cipher tunnel using signals. Meltdown and Spectre are the true embodiments of this hazardous threat, exploiting microprocessor vulnerabilities and using a time-based side-channel attack. Each employs different methods to gain access to the secret data and decode it in a processor's cache, which is a section of memory meant to keep certain data close at hand for increased efficiency. An attacker can use this context to study the timing of the processor's answers and figure out what the cache is leaking, and hence the secret information.

Due to the success of EM side-channel analysis in recovering data from computing equipment, many mitigation techniques have been investigated on both the software and hardware levels. A basic software-based countermeasure that has been shown to be ineffective against EM side-channel assaults is masking variables by utilizing random values alongside operations.

Other approaches, such as randomizing algorithm operation sequences or lookup tables, avoiding instructions pairs executing adjacently that are known to emit distinguishable EM patterns, and accessing critical data with pointers rather than values, all require more research to determine their effectiveness against EM side-channel attacks [1]. Several hardware design countermeasures to these attacks have been proposed. Minimizing metal parts in a chip to reduce EM emissions, using Faraday cage-like packaging, making the chip less power consuming (which leads to fewer unintentional emissions), asynchronism (i.e., design the chip not to use a central system clock and instead operate asynchronously), and using dual line logic are all actions that hardware designers can take (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 demonstrated that during the design process of an electrical chip, mathematical modeling can be used to discover and minimize potential information leakages through EM side-channels.

2. LITERATURE REVIEW

We present literature outlook in a tabulated form below

TABLE 1: LITERATURE OUTLOOK

S/N	Authors	Works on electromagnetic side channels attack
1	(Sayakkara et al., 2019a) Facilitating Electromagnetic Side-Channel Analysis for IoT Investigation: Evaluating the EMvidence Framework	This work presents the methodology behind and an evaluation of a framework, EMvidence, that enables forensic investigators to acquire evidence from IoT devices through EM-SCA. This framework helps to automate and perform electromagnetic side-channel evidence collection for forensic purposes
2	Ashwin Lakshminarasimhan University of Massachusetts Amherst Electromagnetic Side-Channel Analysis for Hardware and Software Watermarking	This paper starts with EM side-channel analysis on FPGA for smaller designs. We insert watermarks on a Microcontroller, Smartcard and an FPGA and detect these watermarks using EM side-channel information emanated from the Design under Test. We used environments with different levels of noise interference. We compare the watermarking application using EM side-channels and Power side-channels in these different setups.
3	J. Longo, E. De Mulder, D. Page & M. Tunstall 01 September 2015 SoC It to EM: ElectroMagnetic Side-Channel Attacks on a Complex System-on-Chip	In this paper, we investigate electromagnetic-based leakage from three different means of executing cryptographic workloads (including the general purpose ARM core, an on-chip co-processor, and the NEON core) on the AM335x SoC. Our conclusion is that addressing challenges of the type above *is* feasible, and that key recovery attacks can be conducted with modest resources.

S/N	Authors	Works on electromagnetic side channels attack
4	Asanka Sayakkara University of Colombo Nhien-An Le-Khac University College Dublin Mark Scanlon University College Dublin 1. A Survey of Electromagnetic Side-Channel Attacks and Discussion on their Case-Progressing Potential for Digital Forensics	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.
5	Haider Adnan Khan Side-channel signal analysis for securing embedded and cyber-physical systems	This thesis develops methods that leverage electromagnetic (EM) side-channel signals for non-adversarial and non-intrusive monitoring of embedded and cyber-physical systems, and provides techniques for identifying anomalous/malicious program behavior by detecting deviations in EM emanations, and presents a framework for end-to-end basic-block program execution tracking by monitoring the device's EM side-channel signal.

3. RESEARCH GAPS AND FINDINGS

EM side-channel attacks are not currently commonly being used in africa 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.

4. CONCLUSION

Traditionally, digital forensics has focused on evaluating file storage, log files, network traces, and other traces left behind by suspects on digital devices [5]. On systems that require more sophisticated investigative techniques and abilities, live data forensics can be performed. As computing systems evolve from less privacy- and security-conscious platforms to hardened platforms built from the ground up with security in mind, the typical work done by digital forensic investigators must evolve as well.

One of the most significant roadblocks to effective digital forensic investigation is cryptographically protected storage systems. From a security standpoint, EM side-channel analysis has been shown to be a possible door-opener for cryptographically protected data storage and transmission, which can be developed upon and utilized for digital forensic reasons.

5. CYBER SAFETY IN AFRICA

Africa has been among the fastest growing regions in terms of cybercrime activities. The continent is also a source of significant cyberattacks targeting the rest of the world. However, a number of measures have been taken to address cyber-threats and improve cybersecurity in the continent. Many countries in the continent have developed legislation to fight cyber-threats. They have also strengthened enforcement measures. Private sector efforts have also been undertaken to strengthen cybersecurity [7].

6. RECOMMENDATION FOR POLICY AND PRACTICES

1. The Federal Communications Commission (FCC), the International ElectroTechnical Commission (IEC) and the African Governments should implement international standardization for manufactures of IoT devices. [5]
2. There should be in place a standard framework tools which will enable IoT system developers to test the robustness of their hardware against physical side channel attacks and identify information leakages. [5]

REFERENCES

1. AsankaSayakkara Forensic Science International: Digital Investigation,Volume 33, Supplement, July 2020, 301003 Facilitating Electromagnetic Side-Channel Analysis for IoT Investigation: Evaluating the EMvidence Framework, https://www.sciencedirect.com/science/article/pii/S2666281720302523
2. Debayan Das* and Shreyas Sen Department of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907, USA; shreyas@purdue.edu Correspondence: das60@purdue.edu Received: 1 October 2020; Accepted: 29 October 2020; Published: 31 October 2020 Electromagnetic and Power Side-Channel Analysis: Advanced Attacks and Low-Overhead Generic Countermeasures through White-Box Approach https://mdpi-res.com/d_attachment/cryptography/cryptography-04-00030/artic
3. Gavin Wright, side-channel attack https://www.techtarget.com/searchsecurity/definition/side-channel-attack
4. François-Xavier Standaert Université Catholique de Louvain – UCLouvain, Introduction to Side-Channel Attacks December 2010 DOI:10.1007/978-0-387-71829-3_2, https://www.researchgate.net/publication/225852558_Introduction_to_Side-Channel_Attacks
   Mark Scanlon University College DublinA Survey of Electromagnetic Side-Channel Attacks and Discussion on their Case-Progressing Potential for Digital Forensics,March 2019Digital Investigation 29(11) DOI:10.1016/j.diin.2019.03.002, https://www.researchgate.net/publication/331777625_A_Survey_of_Electromagnetic_Side-Channel_Attacks_and_Discussion_on_their_Case-Progressing_Potential_for_Digital_Forensics
5. Pedro Tavares. What is a side-channel attack. November 30, 2020, https://resources.infosecinstitute.com/topic/what-is-a-side-channel-attack/