Electromagnetic interference and Information security : characterization, exploitation and forensic analysis

José Lopes Esteves

HESAM UNIVERSITÉ

le cnam

ÉCOLE DOCTORALE SCIENCES DES METIERS DE L'INGÉNIEUR

THÈSE

présentée par **José LOPES ESTEVES**

soutenue le **06 juin 2023**

pour obtenir le grade de **Docteur d'HESAM Université**

préparée à

Agence Nationale de la Sécurité des Systèmes d'Information

et au

Conservatoire National des Arts et Métiers

Discipline **Sciences de l'Ingénieur**
Spécialité **Informatique**

Electromagnetic interference and information security: characterization, exploitation and forensic analysis

THÈSE dirigée par :
Pierre PARADINAS

Jury

Mme. Samia BOUZEFRANE,	Professeure, CEDRIC, CNAM	Présidente
M. Aurélien FRANCILLON,	Professeur, S3, EURECOM	Rapporteur
Mme. Virginie DENIAU,	Directrice de recherche, Université Gustave Eiffel	Rapportrice
M. Jean-Philippe PARMANTIER,	Adjoint scientifique, DEMR, ONERA	Examinateur
Mme. Karine HEYDEMANN,	Maîtresse de conférences, LIP6, Thales	Examinatrice
M. Chaouki KASMI,	Directeur scientifique, DERC, TII	Invité
M. Philippe VALEMBOIS,	Chef de laboratoire, LSF, ANSSI	Invité
M. Pierre PARADINAS,	Professeur, CEDRIC, CNAM	Directeur de thèse

THÈSE

Acknowledgements

Ce travail de thèse touche à sa fin. Cela aura été une aventure, une expédition, une épopée dont les épreuves et les bénéfices vont bien au delà de ce que j'aurais pu anticiper tout au long de ce projet. Ce qui aurait semblé n'être qu'une formalité à première vue s'est avéré un long parcours semé d'embûches, pendant lequel un ensemble de forces extérieures et intérieures ont mené des opérations de déni de service sur le protagoniste, qui s'est vite aperçu qu'il était lui-même son plus redoutable adversaire.

Le mémoire de thèse est la concrétisation simultanée d'un travail individuel, parfois même solitaire, et de contributions collectives mobilisant un grand nombre de personnes qui, volontairement ou non, consciemment ou non, directement ou indirectement, ont œuvré pour que ce projet soit possible. Réciproquement, il se peut que des personnes y aient contribué indépendamment de ma volonté ou sans que je n'en aie pleinement conscience. Je tiens ici à leur exprimer ma profonde gratitude.

Comme le veut la tradition, je commence par adresser mes plus sincères remerciements aux membres du jury qui ont accepté de me faire l'honneur de mobiliser de leur temps, de leur expérience, de leur énergie et de leur expertise au service de l'évaluation de mon travail.

Un grand merci à Virginie DENIAU d'avoir accepté d'être rapportrice sans une nanoseconde d'hésitation et d'avoir procédé à une analyse minutieuse de ma production écrite et orale, avec une grande rigueur scientifique et une exigence de précision qui m'ont, certes, donné du fil à retordre mais également l'opportunité d'exposer mes idées, mes approches expérimentales, mes doutes.

J'exprime également mon infinie reconnaissance à Aurélien FRANCILLON de s'être impliqué en tant que rapporteur et pour le soutien récurrent et bienveillant qu'il m'a apporté pendant toute la durée de ce projet, avec une capacité d'émerveillement qui lui permet de déceler de la valeur et de l'intérêt chez l'autre et de tout transformer en quelque chose de positif.

Je remercie Karine HEYDEMANN et Jean-Philippe PARMANTIER d'avoir participé à ma soutenance et de m'avoir permis de percevoir l'espace d'un instant comment le travail que j'ai défendu pouvait se bonifier par diffusion à travers leur regard, leur expérience, leur vision.

L'accompagnement du Conservatoire National des Arts et Métiers a été crucial, et notamment à travers la mobilisation de Samia BOUZEFRANE qui a présidé mon jury et Pierre PARADINAS qui m'a guidé durant toute la phase finale de la rédaction et de la soutenance. Pour m'accompagner dans ce contexte nouveau de la VAE, il faut je pense une bonne dose d'ouverture, d'optimisme et aimer relever des défis. Je me dois évidemment de les associer à la réussite de ce projet.

Ce projet aurait certainement pu durer éternellement sans l'intervention de Philippe VALEMBOIS qui a su me mettre dans les meilleures dispositions possibles pour avancer sereinement, aménager ma charge de travail et me pousser à me dépasser, à apprivoiser mes angoisses et à m'autoriser une certaine indulgence, nécessaire dans des entreprises de cette envergure. Je le remercie pour son soutien et de m'accorder sa confiance.

Il m'est difficile d'exprimer des remerciements à la hauteur de ce que je ressens à l'endroit de Chaouki KASMI et de sa contribution à ce projet. Chaouki KASMI m'a entrainé dans son sillage et j'ai acquis une grande partie de mes compétences, de ma méthodologie, de mes connaissances en le côtoyant quotidiennement pendant plusieurs années. Cela aura été une collaboration très agréable, amusante, extrêmement fructueuse et efficace, que ce soit en conférence lors de nos présentations en binôme, dans les phases de rédaction, ou dans les phases expérimentales, dont certaines se sont ponctuées par un "Mais c'est un truc de ouf, mec!" que je n'oublierai jamais.

La réalisation sur le plan administratif de ce projet a également mobilisé plusieurs personnes, à

l'ANSSI et au CNAM. Je remercie dans le désordre Emmanuel DUPONCHELLE, José ARAUJO, Eric SALIBA, Aline GOUGET-MORIN, Renaud LABELLE, Vincent STRUBEL et Guillaume POUPARD qui ont soutenu mon initiative et qui m'ont autorisé à m'engager dans cette démarche de doctorat.

Je remercie l'ensemble des services du CNAM chargés du traitement et de l'accompagnement des doctorants et des VAE, en particulier Marie-Camille BORGETTO, David LOAREC, Merry MENDY, Laetitia BOUISSET BONORA, Gwladys MÉDÉLICE, Claire RYCKMANS. Je remercie également Jean-Louis LANET et Marcos RUBINSTEIN d'avoir accepté de rapporter mon dossier de candidature au CNAM.

J'ai été assez peu en contact avec des équipes de recherche au CNAM, juste assez pour adresser mes sincères remerciements à Stefano SECCI, Nour YELLAS de l'équipe ROC du laboratoire CEDRIC pour leur aide lors de la préparation de la soutenance.

A l'ANSSI, le soutien de mes collègues a été très important tout au long de ma demarche. Les membres du laboratoire de la sécurité des technologies sans fil, ceux en poste comme les anciens, ont été les plus impliqués, ont participé aux phase de recherche, aux phases de relecture et de corrections. Lorsque l'on est entouré par autant de personnes aussi compétentes, pédagogues, patientes et disponibles, tout projet recherche est facilité. Un grand merci à Emmanuel DUPONCHELLE, Benoit MICHAU, Christophe DEVINE, Pierre-Michel RICORDEL, Loïc MAZET, Eric DA SILVA, Xavier LE VILLAIN, Patrick SALLES, et une mention spéciale pour leur engagement plus significatif à Tristan CLAVERIE, Emmanuel COTTAIS et Valentin HOUCHOUAS, sans oublier le chef que j'ai déjà remercié un peu plus haut. Je remercie aussi Guenaël RENAULT, Guillaume BOUFFARD, louis DUBOIS et Ange MARTINELLI pour leurs conseils précieux.

Je tiens également mentionner la contribution de certains collègues de la communauté scientifique qui m'ont inspiré par leurs travaux, encouragé, exprimé leur soutien, leur intérêt pour mes travaux de recherche et qui ont par conséquent renforcé mon engagement scientifique. Merci donc à Christian CAREL, Tristan DUBOIS, Christian VOLLAIRE, Christophe GUIFFAUT, François TORRES, Clovis POUANT, Philippe MAURINE, Guillaume MEJECAZE, Guillaume ANDRIEU, Michael SUHRKE, Alexander SUKHOV, Felix VEGA, Nicolas MORA, Frédéric RAYNAL, Philippe TEUWEN, Adrian THILLARD, Ryad BENADJILA, Antriksh SHAH, Thomas TROUCHKINE, Bertrand GERFAULT, Samuel LEMAN, Christophe GRANSART, Matthieu RIVAIN, David EL-BAZE, Amir HASHEMI-KERMANI, Richard PERDRIAU, Vincent GUYOT, Philippe BESNIER, Florian LEBOURDAIS et les copains de NinjaLab Victor LOMNÉ et Thomas ROCHE.

Je remercie infiniment ma famille et mes proches, et leur dédie ce manuscrit.

Abstracts

English

Electronic devices have become ubiquitous in all sectors of our lives, from military to civilian, from critical infrastructures to our homes, our cars, our pacemakers. This widespread comes with increasing needs for the security of the information manipulated by electronic devices. The work in this thesis was focused on the effects of intentional electromagnetic interference (IEMI) on electronic devices and their impact on information security. Approaches for studying these effects through an electromagnetic compatibility (EMC) prism are not tailored to enable information security assessments. An effect assessment methodology involving software-level fault models is proposed and applied to several electronic devices. A key benefit of this methodology is the straightforward possibility to derive impacts on information security, as well as to design countermeasures, detection and forensics strategies.

Exploitability analysis is also facilitated and, as an outcome, new ways of exploiting IEMI effects were uncovered. An original attack was designed targeting a smartphone involving IEMI to obtain a remote, stealthy, unauthorized use of voice assistants by exploiting the susceptibility of the audio front-end. A new threat model was discovered and demonstrated, consisting in an exploitation of IEMI for the establishment of covert communication channels. A new threat model was explored, *electromagnetic watermarking*, which exploits specific IEMI effects to introduce information into a remote non-cooperating target. A practical application was proposed to provide a forensics tracking capability in a framework of counter unmanned aerial systems (C-UAS).

Keywords: IEMI, EMFI, fault, EMI, forensics, attacks, electromagnetic watermarking, covert channel, sensor security, information security

Français

Les équipements électroniques sont devenus omniprésents dans tous les secteurs de nos vies, du militaire au civil, des infrastructures critiques à nos maisons, nos pacemakers. Cette prolifération introduit de nouveaux besoins de sécurité de l'information manipulée par ces équipements. Le travail valorisé dans cette thèse s'est focalisé sur les effets des interférences électromagnétiques intentionnelles (IEMI) et leur impact sur la sécurité de l'information. Des approches existantes pour l'étude de ces effets par le prisme de la compatibilité électromagnétique (CEM) ne sont pas adaptées à des analyses en sécurité de l'information. Une méthodologie d'analyse des effets reposant sur des modèles de faute au niveau logiciel est proposée et appliquée à différents équipements. Un avantage clé de cette approche est la possibilité de dériver les potentiels impacts pour la sécurité de l'information traitée par la cible et de concevoir des contremesures et des stratégies de détection ou d'investigation numérique.

L'analyse de l'exploitabilité des effets est ainsi facilitée et a donné lieu à l'identification de nouvelles façons d'exploiter les effets des IEMI dans des attaques. Une attaque originale ciblant un smartphone a été réalisée, fournissant à l'attaquant un accès distant, silencieux à un assistant vocal en exploitant la susceptibilité des étages d'entrée audio. Un nouveau modèle de menace permettant l'établissement d'un canal de communication caché par IEMI a été proposé. Un nouveau modèle de menace, appelé *watermarking électromagnétique*, est également exploré. Il exploite certains effets des IEMI pour implanter de l'information dans une cible distante non-coopérative. Une application pratique du watermarking électromagnétique en investigation numérique pour la lutte anti-drones est également envisagée.

Mots-clé: Interférences ElectroMagnétiques Intentionnelles, sécurité électromagnétique, attaque par injection de faute, watermarking électromagnétique, canaux cachés, sécurité des capteurs, sécurité de l'information, sécurité matérielle

Contents

List of Figures

List of Tables

Forewords

In 2023, societies are relying heavily on electronic devices and their widespread is still growing fast. All sectors are concerned, both civilian and military. Individuals communicate with smartphones, produce and acquire knowledge on the internet, use computers, smart TVs and buy essentials with smartcards. The automotive industry has been continuously integrating more electronic devices and nowadays cars are comparable to Internet-connected computers on wheels. This trend is global and this is perfectly reflected by the development of the internet of things (IoT) and industrial IoT in as many segments as smart cities, building automation, smart grid and energy production and distribution, healthcare and telemedicine, electric and connected transportation.

Therefore, the resilience and the efficiency of critical services and critical infrastructure are relying on electronic devices. This naturally comes with growing needs of information security, which are also changing fast. Indeed, technology usage is evolving, cloud and edge computing come with new trust issues, placing sensitive data and computation on hardware resources potentially owned by or accessible to attackers. Furthermore, it is more and more common to see generic commercial off the shelf (COTS) products replacing dedicated hardened devices in critical contexts in industrial or military ecosystems.

In this context, the likelihood of some threats becomes higher. In particular, several threats involve a physical interaction with electronic devices, locally or remotely. One class of physical attacks leverages physical properties of a target device or its environment to impact the security of the information processed or stored. In the case of electromagnetic (EM) perturbations, as intentional electromagnetic interference (IEMI), the physical property is the EM environment of the target and the attacker is considered active, with the ability of imposing EM energy to the target. When this energy reaches conductive parts of the target, physical effects may occur as parasitic currents and voltages.

These physical effects can then propagate into logical effects, impacting the function of the target or the processed information. When it comes to cybersecurity risks related to these threats, studying these effects is necessary to understand their conditions of occurrence, to identify if they may lead to compromising the security the information, to develop detection methods and countermeasures.

Research on electromagnetic compatibility (EMC) already focused for several decades on characterizing those physical effects and limiting their functional impact. Unfortunately, EMC methods are not exactly tailored to answer cybersecurity questions, they focus on functional impacts rather than impacts on information. Failure criteria are generally related to the availability of the main functions of the target, and the exploitability analysis of the effects is not straightforward.

Research on electromagnetic fault injection (EMFI) focused for several decades on the impacts of those physical effects on intergated circuit (IC) from a cybersecurity perspective. Assessment approaches are based on fault models and allow for analyzing the exploitability and designing detection methods and countermeasures. However, these approaches focused on ICs are hardly transposable to complex systems and the threat models considered are significantly different from IEMI.

This thesis is dedicated to the study of effects of IEMI on electronic devices to assess their impacts on the security of the information processed. The main contributions are:

- An effect characterization method based on a software instrumentation of the target specifically designed to test against fault models, enabling an easier assessment of the exploitability and more suitable for detection and forensics;

- A new exploitation of IEMI effects on smartphones, resulting in a remote and stealthy unauthorized use of voice assistants;

- The exploration of a new threat model allowing an attacker to establish a covert communication channel with a software implant on a remote target with IEMI;

- The proposition of a new threat model called electromagnetic watermarking, allowing to introduce information remotely into non cooperative targets by exploiting specific effects of IEMI, and its practical application in the framework of counter unmanned aerial systems (C-UAS) providing forensics tracking capabilities.

Chapter 1 provides an overview of EMC and information security (InfoSec), and an introduction to EM security. EMC is about assessing both the EM emissions and the susceptibility of electronic systems in order to guarantee their ability to coexist without disrupting each other. InfoSec is about ensuring that sensitive information is properly protected in terms of confidentiality, integrity and availability. EM security focuses on the threats for the information processed by electronic devices which are caused by EM emissions and susceptibility. It is shown that threats related to emissions mostly impact confidentiality and threats related to susceptibility, including IEMI, can impact the

availability or the integrity of information. A brief state of the art of EM security is proposed with a emphasis on the different threat models.

Chapter 2 summarizes two EM perturbation approaches targeting the susceptibility of the targets, namely EMFI and IEMI. While EMFI is an attack technique studied in a cybersecurity perspective which targets ICs, IEMI is studied in an EMC context and can target more complex systems. Both approaches are described in terms of injection vectors, common waveforms, threat models, vulnerability assessment methodologies and hardening techniques. Overall, this comparison shows that IEMI effect assessment methods are not suitable for InfoSec analysis and that EMFI methods, which are intrinsically InfoSec oriented, rely on fault models for characterizing the vulnerability of targets.

In chapter 3, an IEMI effect assessment approach using fault models at the operating system layer is proposed. This approach, called the systemic approach, consists in placing the observation of effects at a software viewpoint as perceived by the operating system. The systemic approach appears to be promising for IEMI susceptibility testing, via a software instrumentation of the target. The software instrumentation can also be destined to perform a real-time detection of IEMI attacks at the system scale, or at networks scale if several nodes implement the detection. Benefiting from the use of fault models, exploitability analysis also becomes easier by inferring the propagation of the effects on layers above the operating system, i.e., applications. To illustrate the approach, a desktop computer is instrumented and a few observed effects are given.

Chapter 4 presents a new attack targeting voice assistants on smartphones with IEMI. Voice assistants are ubiquitous and democratized the vocal hands-free use of electronic devices. The user interaction interface, namely the audio input front-end, is the target of IEMI, both conducted and radiated. The result is a remote, stealthy and unauthorized access to the voice assistants and the rich, sometimes sensitive, functionalities they expose.This is the first IEMI attack on smartphones and the first exploitation of voice assistants targeting the sensor with a physical attack.

Chapter 5 introduces a new threat model for IEMI leading to the establishment of a covert communication channel. Covert channels are introduced and a focus is made on air gap covert channels. The possibility of exploiting the EM susceptibility of an air gapped computer to set up an inbound covert channel is demonstrated. Relevant elements for security analysis are identified and an approach for determining an upper bound of the potential impact is given. A practical realization of this attack is performed by exploiting the susceptibility of a desktop computer thermal diode.

Chapter 6 introduces a new threat model for IEMI called electromagnetic watermarking (EMW). It consists in exploiting specific effects to introduce information remotely into non cooperative targets. Effects suitable for EMW must propagate to the logical layer and interact with a storage mechanism

intrinsic to the target. This new class of attack is modeled as an IEMI covert channel and a storage channel and relevant elements for security analysis are defined. The methodology for designing such attacks is detailed. A practical application of EMW is proposed in the context of forensics and C-UAS.

Introduction and problem statement

Chapter 1

Electromagnetic security

Contents

1.1 Chapter overview

This chapter provides an overview of EMC and InfoSec, and an introduction to EM security. EMC is about assessing both the EM emissions and the susceptibility of electronic systems in order to guarantee their ability to coexist without disrupting each other. InfoSec is about ensuring that sensitive information is properly protected in terms of confidentiality, integrity and availability.

EM security focuses on the threats for the information processed by electronic devices which are caused by EM emissions and susceptibility. A brief state of the art of EM security is proposed with a emphasis on the different threat models. The contributions of this thesis are positioned in this landscape of threat models.

This chapter is organized as follows: in section 1.2, the main principles of InfoSec are recalled, from the CIA triad to security evaluation and forensics. Section 1.3 is dedicated to general definitons about EMC, emission and susceptibility. Then, section1.4 introduces EM security via the prism of threat models. Threats exploiting EM emissions are presented and impact mostly the confidentiality of the information processed by the target. Threats exploiting EM susceptibility are presented and impact mostly the availability and the integrity of the information processed by the target.

1.2 Information security

InfoSec regroups several technical fields aiming at protecting information during their lifecycle into an information system and managing risks related to information compromise. The ISO/IEC 27000 [ISO18] standard family provides a framework for setting up and operating information security management systems. In these standards, information security is defined as follows: “Information security ensures the confidentiality, availability and integrity of information. It is achieved through the implementation of an applicable set of controls, including policies, processes, procedures, organizational structures, software and hardware to protect the identified information assets. This requires the management of risk and encompasses risks from physical, human and technology related threats with all forms of information.” The main steps of establishing an information security management system are summarized in [ISO18, Section 4.5]:

- Identify information assets and their associated information security requirements;
- Assess information security risks and treat information security risks;
- Select and implement relevant controls to manage unacceptable risks;

- Monitor, maintain and improve the effectiveness of controls associated with information assets.

1.2.1 Information security requirements

The agence nationale de la sécurité des systèmes d'information (ANSSI) (the national cyber security agency of France) has issued a guidance methodology for information security risk management which tries to unify several standards related to information security and risks management. Identifying information security requirements for each asset is again described as determining security needs in terms of confidentiality, integrity and availability [ANS10]. However, those terms are rarely precisely defined in information security related literature and can sometimes be misinterpreted or confusing. Hereafter, the definitions given in [ISO18] are recalled and discussed.

Confidentiality is the property that the information is not made available or disclosed to unauthorized individuals, entities or processes.

Availability is the property of being accessible and usable on demand by an authorized entity.

Integrity is the property of accuracy and completeness.

First, the concept of authorized entity has to be more precisely defined as there is a lack of coherence between the definition of confidentiality and availability. In fact, here an authorized entity could be any part of the information system (individuals, processes, computer programs...) which processes (creates, relays, modifies, replicates...) information. The authorization implicitly involves a security policy, in which information flows are identified and rights of each entity on these information flows are defined.

In [And20], confusion between confidentiality, privacy and secrecy is discussed, showing that the above definition of confidentiality is close to the concept of secrecy. A confusion between integrity and authenticity is also discussed and it appears that in the cryptography and protocol security communities, the notion of integrity encompasses a guarantee of the authenticity of the information as well. In the Common Criteria (CC) standard which provides guidelines for security evaluation, confidentiality, integrity, availability are considered three categories of protection relating to, respectively, unauthorized disclosure, modification or loss of use [Cri17a, p.11]

Thus, it seems more clear and accurate to consider the following definitions:

- Confidentiality is the property that information is disclosed only to authorized entities according to the security policy;

- Availability is the property that information is accessible and usable on demand by any authorized entity according to the security policy;

- Integrity is the property that information is complete, accurate, and has been modified only by authorized entities according to the security policy.

1.2.2 Security evaluation

An information system nowadays most generally involves information technology (IT) systems made of several computers or embedded systems which generate and process information and share data using communication protocols. In order to protect information, IT systems can enclose several protective measures which can be viewed as a set of security functions: access control, intrusion detection, data encryption, message authentication in a communication, etc. Assessing security risks and choosing the right countermeasures requires a good understanding of the security functions implemented or deployed and more especially their limitations. In other words, for each security function, it is necessary to determine what it protects, from what kind of attacks and in which operational conditions. It is also relevant to identify if and how the security function can be circumvented (attacked). This is the main technical purpose of security evaluations of IT products.

Several methodologies for evaluating the security of IT products exist, among which the CC (Common Criteria for Information Technology Security Evaluation) [Cri17a]. The CC is a standard aiming at permitting comparability between the results of independent security evaluations. The results of a CC evaluation are recognized among all member countries of the common criteria recognition agreement. This standard provides a security evaluation methodology [Cri17b] which defines the purpose of vulnerability analysis as determining the existence and exploitability of flaws or weaknesses in the target of evaluation in its operational environment. When a vulnerability is found, impacts on the security function and on the information security requirements of the information enforced by the security function need to be assessed. Furthermore, the attack potential [Cri17b, Annex B.3], also called the vulnerability exploitation rating [ANS20] has to be determined. This concept reflects the so-called attacker profile which quantifies the strength the attacker needs to have in order to be able to exploit the vulnerability. Several criteria can be considered for this quantification, such as the attacker's expertise level, the required equipment, the time needed to identify the vulnerability and to exploit, the amount of knowledge of the target...

Generally, a maximum attack potential is defined when the scope of a security evaluation is described. It can be imposed by the standard (as in [ANS20]), specified in the security target (document describing the evaluated perimeter in CC evaluations) or determined by the analyst according to the intended use of the product and its operational environment. The terms threat model are also commonly used in analyses of security mechanisms. The threat model reflects the maximum attack

potential considered in the analysis by defining the attacker's capabilities and the actions it is allowed to perform.

1.2.3 Digital forensics and incident response

Achieving absolute security, in the sense that the target system can resist to any attacker profile and any threat (even the exploitation of unknown vulnerabilities) is not realistic. Thus, any information system can (and will probably) be compromised. Having the ability to properly respond to security incidents allows to both limit the damage of a successful attack and also recover from the associated damage. This is the main purpose of digital forensics and incident response (DFIR) [Joh20].

Each incident starts with the first time the targeted organization becomes aware of an event or series of events indicative of malicious activity. This step of DFIR is called the detection phase. The awareness of these events can be the result of the use of specific monitoring tools (e.g. network probes, intrusion detection systems...) or come from internal or external sources noticing suspicious activity.

After detection, the suspicious events need to be analyzed to determine if they qualify as potential incident. This is the beginning of the analysis phase. In this phase, evidence is collected from impacted systems and examined. The ultimate goal is to determine the root cause of the incident and reconstruct the actions of the attacker.

Then come the containment phase, aiming at restricting the ability of the attacker to further compromise the information system, and the recovery phase consisting in removing the threat actor from the information system and restoring it in a safe state. The post incident step is dedicated to the documentation of the incident and its assimilation into the InfoSec policies, technical measures and organizational processes.

1.3 Electromagnetic compatibility

EMC is defined as the ability of an equipment or system to function satisfactorily in its electromagnetic environment without introducing intolerable electromagnetic disturbances to anything in that environment [ISO92]. The electromagnetic environment refers to the totality of electromagnetic phenomena existing at a given location. An electromagnetic disturbance can be any electromagnetic phenomenon which may degrade the performance of a device, equipment or system, or adversely affect living or inert matter. In other words, a system is electromagnetically compatible with its environment if it satisfies three criteria [Pau06]:

- It does not cause interference with other systems;
- It is not susceptible to emissions from other systems;
- It does not cause interference with itself.

From these definitions it can be derived that EMC is a constraint electrical and electronic equipment are subject to, more than a science or a set of techniques. In order to reach this constraint, EMC relies mostly on two scientific domains: electromagnetism and electronics [Bou98].

An EMC problem is therefore concerned with the generation (by a source), the transmission (through a coupling path) and the reception (by a receiver) of electromagnetic energy, as illustrated in Figure 1.1.

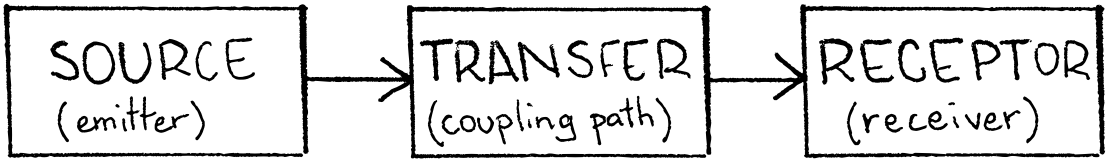


Figure 1.1 – The EMC problem (adapted from [Pau06])

This decomposition suggests three main approaches of preventing an EMC problem to occur:

- Suppress the emission at its source;
- Make the coupling path inefficient;
- Make the receiver less susceptible to the emission.

1.3.1 Emission and susceptibility

Absolute EMC for a system is impossible to ensure [ISO92] and a more reasonable way to tackle this problem is to tend to guarantee the compatibility with high probability within some arbitrary bounds representative of a target electromagnetic environment. Those bounds can be chosen to adequately fit to specific needs of a project (e.g. the design of a product) or imposed by regulation (e.g. for commercializing that product). In the end a system has to be tested for ensuring that its emission level stays below a reference emission limit and that its immunity level stays over a reference immunity limit.

Immunity is the contrary of susceptibility defined as the ability of a device, equipment or system to perform without degradation in the presence of an electromagnetic disturbance.

Electromagnetic emission and electromagnetic susceptibility are considered as the two key aspects of EMC and are illustrated in Figure 1.2.

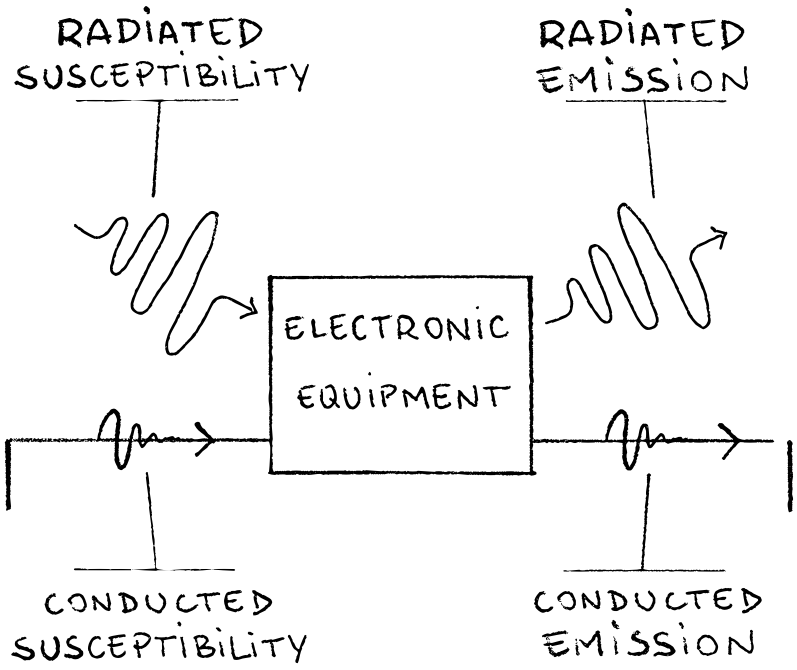


Figure 1.2 – Illustration of EMC emission and susceptibility, both for radiated and conducted paths

1.3.2 Coupling path

The transfer of electromagnetic energy between a noise source and a receiving system is considered to occur in two complementary forms [OTL14]. Sometimes, this energy is completely guided along the coupling path by direct conduction, for example through a PCB trace or a cable. In this case, the problem concerns the conducted emission of the source and conducted susceptibility of the receiver.

In all other cases, free space propagation of the electromagnetic energy radiated from time varying currents in the source occurs. This radiated energy can be collected by the receiver's conducting structures somehow acting as intentional (for radio front ends) or unintentional antennas. In this case, the problem concerns the radiated emission of the source and radiated susceptibility of the receiver.

1.3.3 Sources and electromagnetic environments

Generally speaking, sources of electromagnetic disturbances considered in EMC can be of any kind: natural or artificial, intentional or unintentional. Examples of common sources for consumer electronic devices are give below:

- Natural: electro-static discharge (ESD), lightning, cosmic noise;

- Artificial:
  - Unintentional: power supply switching noise, electric motor noise, radar, radio frequency (RF) communication;
  - Intentional: high altitude electromagnetic pulse (HEMP), IEMI.

For each source, the characteristics of the generated electromagnetic disturbances can sometimes be measured. Furthermore, EMC standards provide typical profiles for susceptibility testing: the standard electromagnetic environments. Electromagnetic environments define incoming perturbation signals by providing the considered coupling paths and information about the signal characteristics as seen by the receiving device. As for an example, high power electromagnetic (HPEM) environments are defined as follows [ISO05]: high-power conditions are achieved when the peak electric field exceeds $100\,\mathrm{V \cdot m^{-1}}$, corresponding to a plane-wave free-space power density of $26.5\,\mathrm{W \cdot m^{-2}}$. The HPEM environment can be:

- Radiated or conducted;
- A single pulse envelope with many cycles of a single frequency (an intense narrowband signal that may have some frequency agility and the pulse envelope may be modulated);
- A burst containing many pulses, with each pulse envelope containing many cycles of a single frequency;
- An ultrawideband transient pulse (spectral content from tens of MHz to several GHz);
- A burst of many ultrawideband transient pulses.

Those different signals are then described in detail in time and frequency domains along with the necessary information in order to enable immunity testing against these electromagnetic environments. Defining electromagnetic environments helps specifying to which sorts of noise signals a system is supposed to be immune. On the other hand, it also permits making assumptions about the characteristics of the probable sources of such signals.

1.4 Electromagnetic security

EMC and InfoSec have very distinct goals. While in EMC the idea is to ensure a world of compliance and self-respect for all electric or electronic systems, although the immunity to the most probable electromagnetic environments is also looked for, InfoSec introduces an attacker in the equation which

has by definition no reason to respect or comply. Furthermore, the attacker will benefit from the fact that his targets comply and follow the rules and will generally follow the weakest link to attack, which is unrelated to the most probable one.

However, some phenomena corresponding to an EMC problem can be intentionally exploited by an attacker and therefore become threats for InfoSec. Electromagnetic security (EMSEC) can be defined as a subset of InfoSec considering the threats for the security of information processed by an electronic system and which come from electromagnetic interaction between the system and its electromagnetic environment. In this perspective, emission problems are considered potential threats for the confidentiality and susceptibility problems can lead to compromising the integrity or the availability of the information processed by the system. This relationship is schematized in Figure 1.3.

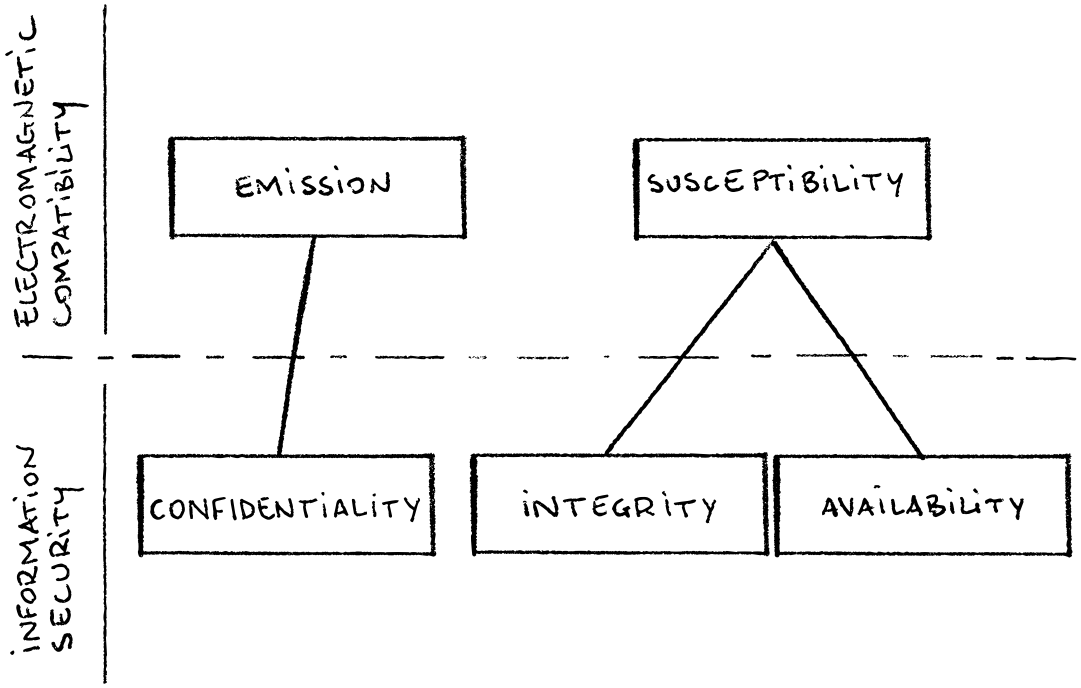


Figure 1.3 – Relationship between the EMC problem and threats for InfoSec

1.4.1 Threats from electromagnetic emission

In an information system composed of electronic devices, the way information is processed (generated, displayed, stored, modified, transmitted...) involves time varying currents, which in turn induce radiated or conducted electromagnetic emissions. If sensitive information (i.e. which has to be protected) is processed, its security might be threatened by an attacker which is able to collect the related emissions. The study of such threats can be called emissions security (and is sometimes also

abbreviated EMSEC) [And20, Chap. 19]. Those spurious electromagnetic emissions related to the processing of sensitive information are sometimes referred to as compromising emanations. Those threats are hereafter classified in three threat models which differ in either the attacker's control of the emission or the post-processing made to compromise information.

TEMPEST: electromagnetic eavesdropping

During World War II, Bell Telephone Laboratories noticed that the electrical activity of US Army encryption systems generated spikes on an oscilloscope in a distant part of their lab [Boa73]. Further investigations led Bell engineers to demonstrate the possibility to recover the plaintexts from those parasitic emissions and the US military started taking this new threat, named TEMPEST, in account for designing their new secure teletypewriters.

In the TEMPEST threat model, a target system, during its normal operation, generates compromising emanations. The attacker is supposed to be able to collect those compromising emanations and his main goal is to reconstruct the sensitive information that is being processed, as shown in Figure 1.4.

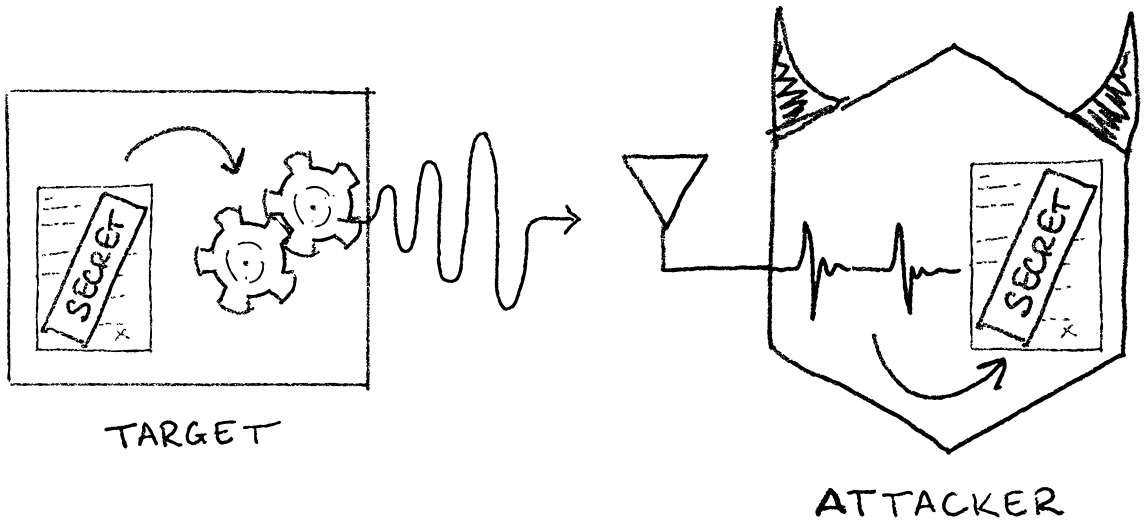


Figure 1.4 – A threat model for TEMPEST

One of the earliest scientific publication related to TEMPEST threats for computers came to public attention in 1985 and it was shown how to reconstruct the video stream processed by cathodic ray tube displays (CRT) by collecting and processing the radiated compromising emanations in the ultra high frequency (UHF) frequency band from a distance of several hundreds meters [van85]. Since then, analog and digital data processing and telecommunication technologies have been evaluated against this kind of threat. Digital video display units have also been considered in [Kuh03, Kuh13, Kuh05], showing that new generations of flat-panel LCD displays were less likely to be sources of

compromising emissions than the cables transporting analog (video graphics array (VGA)) or digital (digital visual interface (DVI)) video signals. high-definition multimedia interface (HDMI) interfaces have also been analyzed in [RD18] and again, the main source of parasitic signal identified was a poorly shielded cable. Displays from tablet computers have also been show vulnerable to TEMPEST attacks, and in [HHM+14] the video image is reconstructed at a 2 m distance with a compact attacker setup involving a laptop, a software defined radio (SDR) receiver and an small antenna. An example of TEMPEST video interception is given in Figure 1.5. Together with the video signal leakage, the touchscreen feature has also been considered in [Hoa16] and precise positioning of the touched spot on the vertical axis has been shown with a near field measurement.

(a) Original image

(b) Intercepted image

Figure 1.5 – TEMPEST exploitation example: interception of a DVI video stream [RD18]

Keyboards, as a primary communication interface between the user and electronic devices have also been scrutinized. In [VP09], parasitic signals generated by the keyboard matrix were collected, allowing keystroke recovery. Emissions coming from the PS/2 interface were also considered, both baseband and amplitude or frequency modulating the keyboard controllers clock signal [DLZ13, VP10]. PS/2 keyboards have been superseded by USB keyboards, leading to emission testing of the USB interface [NW14, PN16].

A RS-232 communication link has been studied in [Smu90] showing the presence of compromising signals generated by the amplitude modulation of the terminal's system clock by the RS-232 signal. Those signals were also present at harmonic frequencies of this unintentional carrier. In [SKH+16], the reconstruction of a 10base-T ethernet signal has been shown and the possibility of doing the same on a 100base-T signal has been shown to be highly conditioned by the signal to noise ratio at the attacker's end.

The interaction of analog audio signals and digital I2C signals with local oscillators for radio communications enclosed in a mixed signals IC has been investigated in [CYC20], demonstrating that the (lower amplitude) compromising audio emissions were modulating the radio frequency carrier and

amplified by the transmission chain.

Soft-Tempest: compromising emission based covert channels

In a declassified version of the National Security Agency (NSA) central security service regulation 90-6 [Age95] on technical security, the need for a technical security evaluation against technical (intelligence) collection threats is discussed. Among the target threat categories, TEMPEST is mentioned next to another enigmatic codename: TEAPOT. A definition of TEAPOT is given as follows: a short name referring to the investigation, study, and control of intentional compromising emanations (i.e., those that are hostilely induced or provoked) from telecommunications and automated information systems equipment [Kuh03, Age95]. Thus, it can be formalized that while TEMPEST relates to the exploitation of unintended emission from a legitimate (non compromised) system, TEAPOT introduces the notion of intentional compromising emanations, which can be interpreted as a compromise of a target system in order to whether generate (or amplify) or control compromising emanations in order to exploit them.

The seminal scientific reference of attacker controlled compromising emanations focused on a software control and assigned the term "Soft-Tempest" to this threat scenario [KA98]. The electromagnetic emission from CRT display units was exploited by an attacker software controlling the video stream in order to generate an amplitude modulated leakage of an arbitrary audio signal. A remote attacker could then receive and demodulate the compromising emanation and listen to the audio with an amplitude modulation (AM) radio.

In a way, Soft-Tempest can be considered as an attacker software controlled exploitation of spurious electromagnetic emission to create an outbound covert communication channel. The threat model can be formulated as follows: the attacker succeeded in introducing a software implant into the target system, which generates and/or controls compromising emanations in order to modulate information on a half duplex outbound electromagnetic covert channel. The compromising emanations can then be collected by the attacker which, knowing the covert channel transmission characteristics (carrier frequency, modulation, channel coding, etc.) can reconstruct the covertly exfiltrated information. This threat model is illustrated in Figure 1.6. Theoretically, any source of compromising emission could be used for Soft-Tempest, as there is by definition a correlation between the processed information and the emitted signals. Therefore, the only requisite is that the attacker software can be the origin of the aforementioned information. However, Soft-Tempest can also exploit any source of radiated or conducted emission in the EMC viewpoint and which can be modulated from software interfaces. In that sense, any emission source which can be modulated from a software interface should be consid-

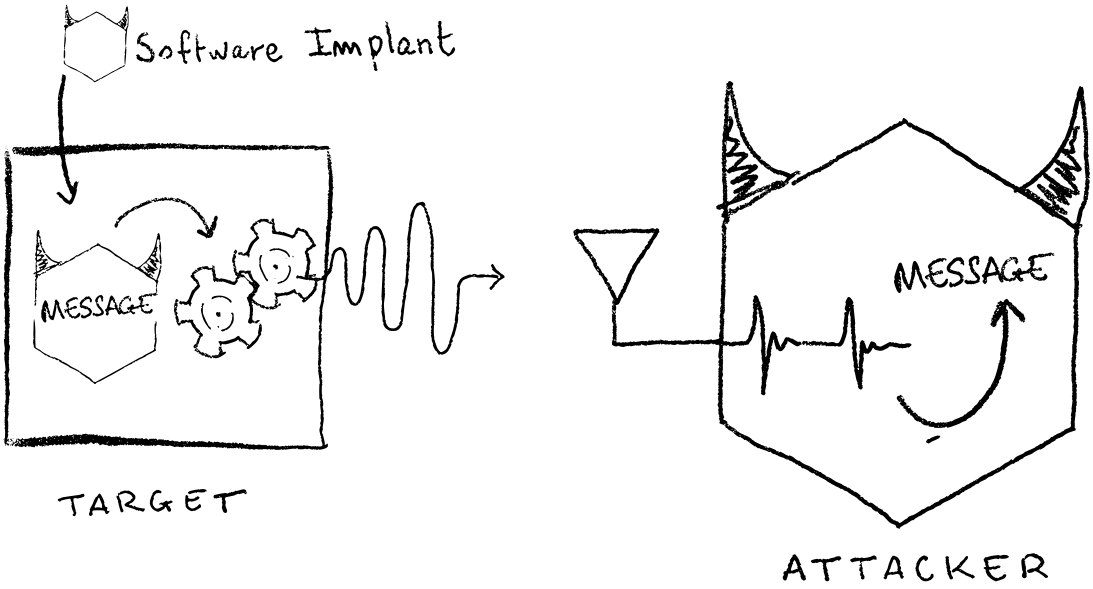


Figure 1.6 – A threat model for Soft-Tempest

ered as potentially compromising emission source in all scenarios where a malicious software implant is envisioned.

Most Soft-Tempest studies focused on exploiting known compromising emission sources via software to create so-called exfiltration covert channels. A few years after [KA98], a famous public example crafting video streams and exploiting the video display units compromising emissions to generate an AM stream of *Für Elise* (Ludwig van Beethoven) has been released [Thi01], the leakage carrier frequencies depending on the video display configuration. In [Cui12], a malicious firmware is flashed into a Cisco VoIP phone and a covert exfiltration channel is created by repurposing the phone off-hook switch wire as an antenna. This concept of an attacker creating a source of emissions by repurposing the hardware resources from a software interface has been further investigated in [Cui15] and called a *funtenna*. A work similar to [Thi01] exploited compromising emissions from video streams to generate a frequency modulation (FM) radio covert channel [GKKE14]. A malware generating a specially crafted sequence of CPU to DDR random access memory transactions was shown to induce emissions around the IO bus clock frequency which could be AM modulated into an exfiltration channel. An interesting study on the control of radiated emissions of an unshielded USB cable during the copy of a specially crafted file from a host computer to a USB drive has shown the possibility of an electromagnetic covert channel consisting of the AM modulation of a carrier at subharmonic frequencies of the USB frequency [GME16]. Low frequency magnetic fields induced by a CPU activity have been modulated by increasing or decreasing the CPU load in [Gur21, GZE20], creating a few bits per second magnetic covert channel for an attacker at 1 meter. The exact same technique also has shown

to generate conducted emissions on the power supply and a FM covert channel with carriers of a few kHz has been proposed in[GZBE20]. The investigation of Soft-Tempest generated compromising emanation with radio frequency transmitters has highlighted the possibility of those parasitic signals to modulate the local oscillators and be amplified by the front-end [LECK19]. This threat has been called the Second-Order Soft-Tempest [LECK18] where the frequencies of the covert channel are modified and the reception range for the attacker is increased. A very creative practical exploitation of Soft-Tempest has been proposed in [Cam20] by proposing applying 1-bit modulation techniques in order to widen the range of possible modulations for the compromising emissions. Experimental results have shown the possibility to control the emission modulation to achieve classical AM, FM and phase modulation (PM) but also LoRa modulation (LoRa), orthogonal frequency division multiplexing modulation (OFDM), chirp spread spectrum modulation (CSS) and direct sequence spread spectrum modulation (DSSS) modulations.

Side-channel attacks: passive physical cryptanalysis

Cryptanalysis is the science of attacking cryptographic primitives (ciphers, hash functions...) and cryptosystems. Two approaches can be distinguished: theoretical cryptanalysis, where those are viewed as mathematical objects, and physical cryptanalysis where the target primitives and cryptosystems are attacked by taking the external environment where the mathematical object evolves [Roc10]. Measuring conducted or radiated emissions from an electronic device while it is performing cryptographic operations are examples of exploiting this external environment. Physical cryptanalysis by measuring conducted emissions has been first proposed and applied on the DES cipher in [KJJ99], and is called a power side channel attack (SCA). Considering radiated emissions was introduced in [GMO01], where DES, COMP-128 and RSA primitives have been attacked. It is referred to as an electromagnetic SCA. Since then, attacks have been proposed against several implementations of the mostly deployed cryptographic primitives used for encryption, authentication or signature, such as ECDSA [RLMI21], AES [ROSW16], MILENAGE [DSPT18], on different computing platforms ranging from smartcards and RFID smartcards [OP11] to laptops [GPT15] and smartphones [LKMM21].

The threat model (Figure 1.7), from a cryptology viewpoint, is a *grey box* model, as the attacker can observe or manipulate inputs or outputs of the cryptosystem, but also get insight on the internal state of the target by analyzing its emissions [Lom10]. The main goal is mostly restricted to cryptanalysis and recovering the secret key. Generally, the attacker is in close physical proximity with the IC performing the cryptographic computations, but recent work has also shown possible extended

range attacks exploiting parasitic propagation through network cables [GPT15] or amplification by a RF front-end located in the same mixed-signal IC [Cam20].

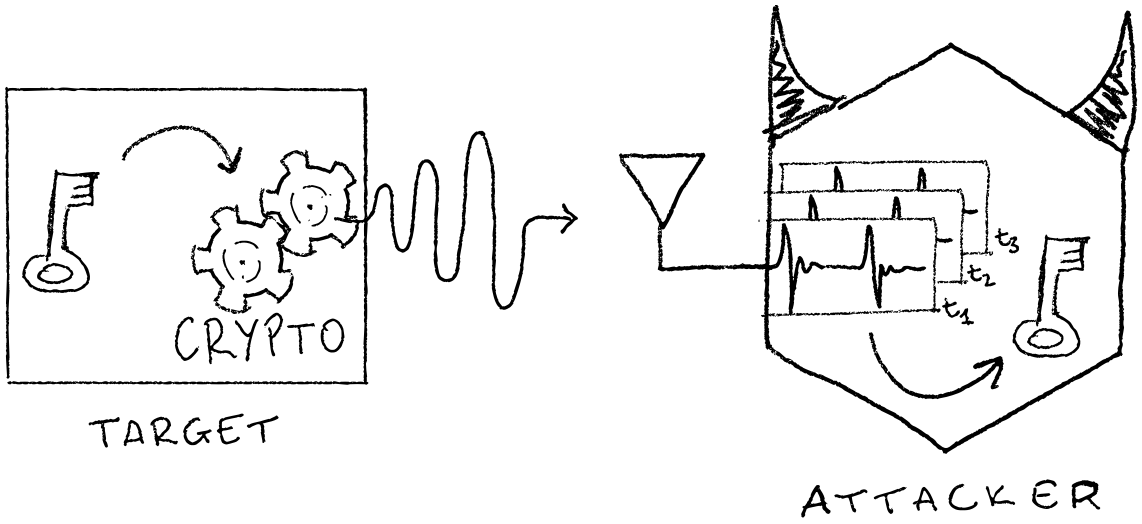


Figure 1.7 – Side channel analysis: threat model

Most attacks require the collection of a large amount of compromising emission measurements. The cryptographic material recovery may involve signal processing techniques (filtering, time synchronization...) and a statistical analysis to identify the secrets which would generate the measured leakage with the highest probability according to a reference theoretical or experimental leakage profile.

1.4.2 Threats from electromagnetic susceptibility

Elements composing an information system can be electric or electronic devices which intrinsically involve electric, electronic or electromagnetic interactions to operate. They are therefore composed of several conductive parts, enclosures, power and communication cables, connectors, wires, printed circuit board (PCB) power planes and transmission lines, IC pads, bonding wires, antennas, etc. The presence of time varying electromagnetic fields around those conductive parts may induce parasitic currents and voltages [Sch02]. These phenomena can be exploited by an attacker in order to introduce unwanted signals into a target device and trigger unpredicted behavior.

The introduction of parasitic signals into a system can result in impacts on the availability of the information it processes if the system is disrupted or if communication with other systems is made impossible. Impacts on integrity can also occur if the parasitic signals alter functional signals in way that the information they convey is also altered and (mis)interpreted. Moreover, when processing units

are disturbed, data, instructions and execution flows can also be altered, leading to specific threats on programs enforcing security functions.

Electromagnetic perturbation attacks being the main topic of this thesis, an in depth description as well as new threat scenarios will be provided in the following Chapters. In this Section, only an overview of the threat models exploiting electromagnetic susceptibility to impact information security is given, with an emphasis when new contributions are made.

Denial of service and jamming

Destructive (and permanent) effects of parasitic signals induced on systems have been reported on several targets. Thermal effects or electrical dielectric breakdowns can occur and cause damage on semiconductor components and PCBs such as melted traces, bond wire destruction, flashover effects [GHS20]. Such effects are very likely to imply a functional failure of the whole or at least part of the system. A recent study on power supplies has confirmed those observations, showing physical damage on discrete components (e.g., resistors), ICs, PCB traces [Mej19]. Of course, without a proper power supply, many systems may stop functioning. Physical damage of RF front-ends has also been observed, the receiver low noise amplifier (LNA) being reported as one of the weakest elements [Gir18, GHS20]. In that case, communication is simply made impossible. Computers have also been studied in [Hoa07] and has highlighted the possibility of peripheral damage, functional damage or permanent damage of the tested devices. Repeatedly shutting down the target or triggering reboots can also result in a functional denial of service until the system has booted and the application environment is back up and running.

Non destructive transient effects on conductive parts involved in communication, such as cables, PCB tracks or RF front ends can introduce noise signals and reduce the efficiency of the communication protocol. Examples of such effects have been reported on network cables [BL04, KSG15b, KSG15a]. In the radiated case, if the noise is in the same frequency band (i.e. in-band) as the legitimate communication signal, it can be viewed as a classical RF jamming problem. In both cases, the communication is jammed during the activation of the noise source.

Finally, the possibility of exploiting functional weaknesses of power amplifiers in RF transmitters has been proposed in [CLEHK17], where an attacker introduces parasitic signals during the measurement of output distortion, resulting in a false pre-distortion processing and thus in a temporary jamming of the output signal. In that case, the attacker signal is present only during the measurement and the jamming is effective until the next measurement phase.

Signal injection

The electromagnetic susceptibility of a target system can be exploited to introduce parasitic signals specifically crafted in order to get them interpreted by the system. In this threat category, the induced parasitic signal can be in-band and share the same characteristics as the expected legitimate signal or it can be out-of-band (OOB) and be transformed into or interpreted as an in-band signal by the target [GR19]. The possibility of inducing an RF signal into an ultrasonic front-end in order to attack an ultrasound based distance bounding protocol has been mentioned in [RCHC09]. A formalization of such attack vector has been proposed in [KBC+13], where in-band parasitic signals were successfully interpreted by cardiac implantable devices with severe consequences as pacing inhibition and defibrillation. Radiated OOB AM signals targeting analog microphones shown to be first demodulated and brought in-band and then interpreted by a Bluetooth headset and a webcam, opening the possibility of exploitation scenarios such as injecting voice or noise during a phone call.

Magnetic wheel speed sensors from Anti-lock Braking System (ABS) are disrupted and spoofed in [SMTS13] using a flat PCB coil to produce a continuous wave (CW) magnetic field at specific frequencies. As a result of this in-band front-door injection, car breaks can be impacted significantly enough to envision life-threatening outcomes.

Perturbation of sensors and actuators has been investigated in [Sel18]. On analog sensors, previous results were confirmed showing that modulated signals can be demodulated by non-linearity in the victim circuit. On digital sensors, the study focused on the reading errors of a microcontroller general purpose input/output (GPIO) while an attacker introduced CW and sawtooth parasitic signals into a jumper cable. Bit flips were observed in both cases, but a deterministic control of the resulting values was better achieved with a sawtooth synchronized with rising and falling edges of the victim circuit sampling clock. A pulse width modulation (PWM) driven servo-motor has been analyzed while parasitic signals were injected in the cable transmitting the PWM control signal. It has been observed that a pulsed sinusoidal interference signal could introduce a DC offset leading to an increase of the PWM pulse width if injected during a high state, thus increasing the rotation angle of the servo-motor. Similarly, a sawtooth interference during high state could introduce a parasitic falling edge, resulting in a shortening of the PWM pulse width, thus reducing the rotation angle of the servo-motor.

Capacitive touch screens from smartphones were targeted in [MWM19] by injecting a CW signal from a copper plate hidden 5 mm behind the target. Effective signal frequencies of a few hundreds of kilo Hertz, which are target dependent, introduce fake touch events which are exploited to force

clicks on confirmation buttons without user interaction.

Fault attacks

EMFI is a discipline dedicated on the investigation of attacks on ICs and exploiting their EM susceptibility. Conducted EMFI is often referred to as glitching and generally targets power or clock pins. Radiated EMFI is generally a near-field interaction with an EM probe placed a few millimeters over the target. These threat models imply that the attacker is assumed to have a physical access to the target IC, with the possibility to adapt its environment (e.g., removing filters) and to synchronize to the target activity. In most scenarios, the attacker is also able to interact with the target, provide inputs, trigger specific processing and get access to the result. With EMFI, attackers have been mostly impacting the integrity of data and processing, opening the way to several exploitation scenarios.

The active counterpart to side channel analysis consists in using EMFI to corrupt cryptographic operations to perform a cryptanalysis and recover secret keys [Riv09]. Several cryptosystems have been considered, in both encryption and digital signature contexts, such as DES [BS97], AES [DDRT13], RSA [BDL97] or elliptic curve cryptography [BMM00].

Random number generation is a cornerstone of many cryptographic protocols. True Random Number Generator (TRNG) are components dedicated to the production of random number sequences. Using EMFI against TRNGs to bias the random number production has been proposed [Had15, HKLEH16, MAB+18].

Processing corruption with EMFI has led to several exploitation scenarios benefiting from an alteration of the execution flow, such as instruction skip. As a result, privilege escalation on a rich operating system (Linux) has been show possible in [GAP+20, TM17]. Attacks targeting verifications for secure boot were also demonstrated on several System on chip (SoC), allowing attackers to load unsigned firmware [Res19, pdn17, TSW16]. Protections present en SoCs to secure access to debugging and programming interfaces were also bypassed with EMFI [BFP19, Res20]. Finally, memory leaks were also obtained with EMFI, probably corrupting length verification during the forge of a response packet of the universal serial bus (USB) protocol, and resulting in a response returning much more data than necessary [O'F19, Sco16].

1.5 Conclusion

InfoSec and EMC seem to be completely unrelated research and engineering topics. The former is the art of protecting sensitive information during its lifecycle against threats which are incarnated by

an attacker. Security analysis consists in the identification of vulnerabilities and the determination of the impacts of their exploitation and the abilties an attacker needs to have to be able to exploit. DFIR is the part of InfoSec which is related to the detection of attacks, live or during digital investigation, the remediation and the recovery. EMC is the art of ensuring a peaceful and respectful coexistence of electrical and electronic systems with regards to the electromagnetic noise generated by their activity. This is achieved by controlling the emissions and the susceptibility of such systems against thresholds which reflect the most probable situations those can be confronted to.

However, when information is processed by electrical or electronic devices, the physical phenomena originating EMC problems can also become InfoSec threats. The study of such threats and their exploitation to compromise information security belongs to the field of electromagnetic security. An overview of threats considered in electromagnetic security is depcted in Figure 1.8.

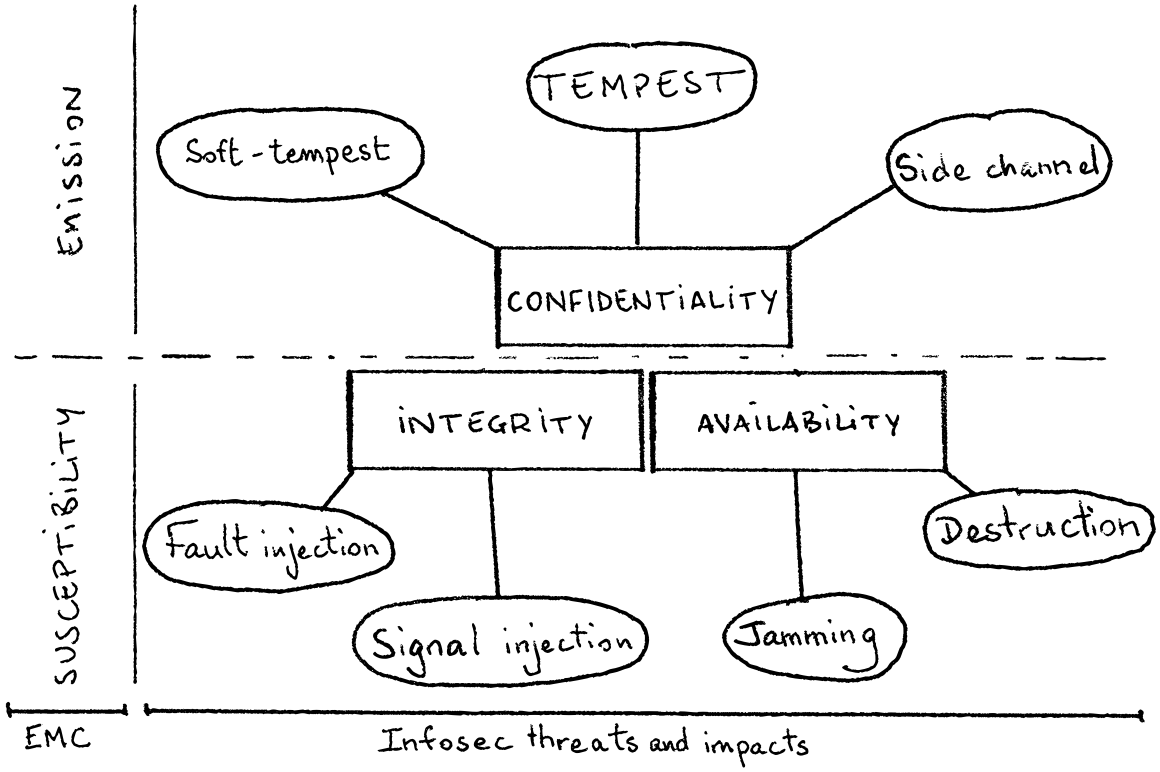


Figure 1.8 – Summary of electromagnetic security threats

Such threats are the focus of this thesis, and more specifically threats coming from the electromagnetic susceptibility of electronic devices. Those have been introduced in this chapter and each corresponding threat model has been explained in order to give an understanding of how an attacker can exploit the susceptibility of a device in order to compromise the security of the information processed. Impacts on information availability can be achieved mostly by jamming or physical destruction. Integrity can be impacted and lead to signal injection and fault injection.

For threats involving the exploitation of the susceptibility of a target, a security analysis requires a susceptibility analysis considering electromagnetic environments reflecting an attacker. EMC standards defined such electromagnetic environments as IEMI. In InfoSec, most effort to understand and take those threats into account came from studies on fault injection and sensor security. A comparison on IEMI and fault injection is the subject of Chapter 2, with the ambition of understanding how to characterize the susceptibility of a target and how to determine the possible exploitation of the problems identified. This characterization could also lead to detection techniques which could be useful for DFIR.

1.6 References

[Age95] National Security Agency. NSA/CSS Regulation 90-6: Technical Security Program. Technical report, National Security Agency, 1995. 18

[And20] Ross J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley Publishing, 2 edition, 2020. 9, 16

[ANS10] ANSSI. EBIOS: Expression des Besoins et Identification des Objectifs de Sécurité - méthode de gestion des risques. Standard, Agence Nationale de la Sécurité des Systèmes d'Information, Paris, France, 2010. 9

[ANS20] ANSSI. Criteria for evaluation in view of a first level security certification. Standard ANSSI-CSPN-CER-P-02_v4.0, ANSSI, 2020. 10

[BDL97] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the importance of checking cryptographic protocols for faults (extended abstract). In Walter Fumy, editor, *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding*, volume 1233 of *Lecture Notes in Computer Science*, pages 37–51. Springer, 1997. 24

[BFP19] Claudio Bozzato, Riccardo Focardi, and Francesco Palmarini. Shaping the Glitch: Optimizing Voltage Fault Injection Attacks. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 199–224, 2019. 24

[BL04] M. G. Backstrom and K. G. Lovstrand. Susceptibility of electronic systems to high-power microwaves: Summary of test experience. *IEEE Transactions on Electromagnetic Compatibility*, 46(3):396–403, 2004. 22

[BMM00] Ingrid Biehl, Bernd Meyer, and Volker Müller. Differential Fault Attacks on Elliptic Curve Cryptosystems. In Mihir Bellare, editor, *Advances in Cryptology — CRYPTO 2000*, pages 131–146, Berlin, Heidelberg, 2000. Springer. 24

[Boa73] David G. Boak. History of U.S. Communication Security (Volumes I and II). Lectures, National Security Agency, 1973. 16

[Bou98] Jean-Claude Boudenot. La compatibilité électromagnétique et nucléaire. In *La compatibilité électromagnétique et nucléaire*. Ellipses, Paris, DL 1998. 12

[BS97] Eli Biham and Adi Shamir. Differential fault analysis of secret key cryptosystems. In Burton S. Kaliski, editor, *Advances in Cryptology — CRYPTO '97*, pages 513–525, Berlin, Heidelberg, 1997. Springer. 24

[Cam20] Giovanni Camurati. *Security Threats Emerging from the Interaction between Digital Activity and Radio Transceivers*. PhD thesis, 2020. 20, 21

[CLEHK17] Emmanuel Cottais, José Lopes Esteves, Valentin Houchouas, and Chaouki Kasmi. Effects of intentional electromagnetic interference on an adaptive predistortion algorithm. In *Electromagnetic Compatibility-EMC EUROPE, 2017 International Symposium On*, pages 1–6, Angers, France, 2017. IEEE. 22

[Cri17a] Common Criteria. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model. Standard Version 3.1 Revision 5, 2017. 9, 10

[Cri17b] Common Criteria. Common Methodology for Information Technology Security Evaluation - Evaluation methodology. Standard Version 3.1 Revision 5, 2017. 10

[Cui12] Ang Cui. Hacking Cisco Phones. In *29th Computer Chaos Club Congress*, Hamburg, Germany, 2012. 19

[Cui15] Ang Cui. Emanate Like a Boss: Generalized Covert Data Exfiltration with Funtenna. In *Black Hat USA 2015*, Las Vegas, 2015. 19

[CYC20] Jieun Choi, Hae-Yong Yang, and Dong-Ho Cho. TEMPEST Comeback: A Realistic Audio Eavesdropping Threat on Mixed-signal SoCs. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, CCS '20, pages 1085–1101, New York, NY, USA, 2020. Association for Computing Machinery. 17

[DDRT13] A. Dehbaoui, J. M. Dutertre, B. Robisson, and A. Tria. Investigation of near-field pulsed EMI at IC level. In *2013 Asia-Pacific Symposium on Electromagnetic Compatibility (APEMC)*, pages 1–4, 2013. 24

[DLZ13] Yu-Lei Du, Ying-Hua Lu, and Jin-Ling Zhang. Novel Method to Detect and Recover the Keystrokes of Ps/2 Keyboard. *Progress In Electromagnetics Research*, 41:151–161, 2013. 17

[DSPT18] Christophe Devine, Manuel San Pedro, and Adrian Thillard. A Practical Guide to Differential Power Analysis of USIM Cards. In *Symposium Sur La Sécurité Des Technologies de l'Information et Des Communications (SSTIC)*, Rennes, France, 2018. 20

[GAP+20] Clément Gaine, Driss Aboulkassimi, Simon Pontié, Jean-Pierre Nikolovski, and Jean-Max Dutertre. Electromagnetic Fault Injection as a New Forensic Approach for SoCs. In *2020 IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 1–6, 2020. 24

[GHS20] Dave Giri, Richard Hoad, and Franck Sabath. *High-Power Electromagnetic Effects on Electronic Systems*. Artech House, 2020. 22

[Gir18] Maxime Girard. *Recherche de Vulnérabilités Des Étages de Réception Aux Agressions Électromagnétiques de Forte Puissance : Cas d'un LNA AsGa*. PhD thesis, Bordeaux, 2018. 22

[GKKE14] M. Guri, G. Kedma, A. Kachlon, and Y. Elovici. AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies. In *2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE)*, pages 58–67, 2014. 19

[GME16] Mordechai Guri, Matan Monitz, and Yuval Elovici. USBee: Air-gap covert-channel via electromagnetic emission from USB. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, pages 264–268. IEEE, 2016. 19

[GMO01] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic Analysis: Concrete Results. In Çetin K. Koç, David Naccache, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems — CHES 2001*, Lecture Notes in Computer Science, pages 251–261, Berlin, Heidelberg, 2001. Springer. 20

[GPT15] Daniel Genkin, Itamar Pipman, and Eran Tromer. Get your hands off my laptop: Physical side-channel key-extraction attacks on PCs. *Journal of Cryptographic Engineering*, 5(2):95–112, 2015. 20, 21

[GR19] Ilias Giechaskiel and Kasper Bonne Rasmussen. SoK: Taxonomy and Challenges of Out-of-Band Signal Injection Attacks and Defenses. *arXiv:1901.06935 [cs]*, 2019. 23

[Gur21] Mordechai Guri. MAGNETO: Covert channel between air-gapped systems and nearby smartphones via CPU-generated magnetic fields. *Future Generation Computer Systems*, 115:115–125, 2021. 19

[GZBE20] Mordechai Guri, Boris Zadov, Dima Bykhovsky, and Yuval Elovici. PowerHammer: Exfiltrating Data From Air-Gapped Computers Through Power Lines. *IEEE Transactions on Information Forensics and Security*, 15:1879–1890, 2020. 20

[GZE20] Mordechai Guri, Boris Zadov, and Yuval Elovici. ODINI: Escaping Sensitive Data From Faraday-Caged, Air-Gapped Computers via Magnetic Fields. *IEEE Transactions on Information Forensics and Security*, 15:1190–1203, 2020. 19

[Had15] Patrick Haddad. *Caractérisation et Modélisation de Générateurs de Nombres Aléatoires Dans Les Circuits Intégrés Logiques.* PhD thesis, Université Jean Monnet, Saint Etienne, 2015. 24

[HHM+14] Yuichi Hayashi, Naofumi Homma, Mamoru Miura, Takafumi Aoki, and Hideaki Sone. A Threat for Tablet PCs in Public Space: Remote Visualization of Screen Images Using EM Emanation. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, pages 954–965, New York, NY, USA, 2014. ACM. 17

[HKLEH16] Patrick Haddad, Chaouki Kasmi, José Lopes Esteves, and Valentin Houchouas. Electromagnetic Harmonic Attack on Transient Effect Ring Oscillator based True Random Generator. In *Hardwear.Io*, The Hague, Netherlands, 2016. 24

[Hoa07] Richard Hoad. *The Utility of Electromagnetic Attack Detection to Information Security*. PhD thesis, University of Glamorgan, 2007. 22

[Hoa16] Richard Hoad. Identifying Some Radiated EMSEC Vulnerabilities of Tablet Personal Computers. In *European Electromagnetics International Symposium EUROEM 2016*, London, UK, 2016. 17

[ISO92] ISO/IEC. Electromagnetic compatibility (EMC) - Part 1-1: General - Application and interpretation of fundamental definitions and terms. Standard ISO/IEC 61000-1-1:1992, International Organization for Standardization, Geneva, CH, 1992. 11, 12

[ISO05] ISO/IEC. Electromagnetic compatibility (EMC) - Part 2-13: Environment - High-power electromagnetic (HPEM) environments - Radiated and conducted. Standard ISO/IEC 61000-2-13:2005, International Organization for Standardization, Geneva, CH, 2005. 14

[ISO18] ISO/IEC. Information technology — Security techniques — Information security management systems. Standard ISO/IEC 27000:2018, International Organization for Standardization, 2018. 8, 9

[Joh20] G. Johansen. *Digital Forensics and Incident Response: Incident Response Techniques and Procedures to Respond to Modern Cyber Threats, 2nd Edition*. Packt Publishing, 2020. 11

[KA98] Markus G Kuhn and Ross J Anderson. Soft tempest: Hidden data transmission using electromagnetic emanations. In *International Workshop on Information Hiding*, pages 124–142. Springer, 1998. 18, 19

[KBC+13] Denis Foo Kune, John Backes, Shane S. Clark, Daniel Kramer, Matthew Reynolds, Kevin Fu, Yongdae Kim, and Wenyuan Xu. Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors. In *2013 IEEE Symposium on Security and Privacy*, pages 145–159, 2013. 23

[KJJ99] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In Michael Wiener, editor, *Advances in Cryptology — CRYPTO' 99*, Lecture Notes in Computer Science, pages 388–397, Berlin, Heidelberg, 1999. Springer. 20

[KSG15a] M. Kreitlow, F. Sabath, and H. Garbe. Analysis of IEMI effects on a computer network in a realistic environment. In *2015 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, pages 1063–1067, 2015. 22

[KSG15b] M Kreitlow, F Sabath, and Heyno Garbe. A test method for analysing disturbed ethernet data streams. *Advances in Radio Science 13 (2015)*, 13:149–153, 2015. 22

[Kuh03] Markus G. Kuhn. Compromising emanations: Eavesdropping risks of computer displays. Technical Report UCAM-CL-TR-577, University of Cambridge, Computer Laboratory, 2003. 16, 18

[Kuh05] Markus G. Kuhn. Electromagnetic Eavesdropping Risks of Flat-panel Displays. In *Proceedings of the 4th International Conference on Privacy Enhancing Technologies*, PET'04, pages 88–107, Berlin, Heidelberg, 2005. Springer-Verlag. 16

[Kuh13] Markus G Kuhn. Compromising emanations of LCD TV sets. *IEEE Transactions on Electromagnetic Compatibility*, 55(3):564–570, 2013. 16

[LECK18] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. Second Order Soft-Tempest in RF Front-Ends: Design and Detection of Polyglot Modulations. In *Electromagnetic Compatibility-EMC EUROPE, 2018 International Symposium On*, Amsterdam, Netherland, 2018. IEEE. 20

[LECK19] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. Second Order Soft Tempest: From Internal Cascaded Electromagnetic Interactions to Long Haul Covert Channels. In *Radio Science Conference (URSI AP-RASC), 2019 URSI Asia Pacific*, New Dehli, India, 2019. IEEE. 20

[LKMM21] Oleksiy Lisovets, David Knichel, Thorben Moos, and Amir Moradi. Let's take it offline: Boosting brute-force attacks on iPhone's user authentication through SCA. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2021(3):496–519, 2021. 20

[Lom10] Victor Lomne. *Power and Electro-Magnetic Side-Channel Attacks : Threats and Countermeasures*. These de doctorat, Montpellier 2, 2010. 20

[MAB+18] M. Madau, M. Agoyan, J. Balasch, M. Grujić, P. Haddad, P. Maurine, V. Rožić, D. Singelée, B. Yang, and I. Verbauwhede. The Impact of Pulsed Electromagnetic Fault Injection on True Random Number Generators. In *2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 43–48, 2018. 24

[Mej19] Guillaume Mejecaze. *Analyse des destructions d'alimentations électroniques soumises à un courant impulsionnel fort niveau*. PhD thesis, Université de Bordeaux, 2019. 22

[MWM19] Seita Maruyama, Satohiro Wakabayashi, and Tatsuya Mori. Tap 'n Ghost: A Compilation of Novel Attack Techniques against Smartphone Touchscreens. In *2019 IEEE Symposium on Security and Privacy (SP) (SP)*, 2019. 23

[NW14] Leszek Nowosielski and Marian Wnuk. Compromising Emanations from USB 2 Interface. In *PIERS Proceedings*, 2014. 17

[O'F19] Colin O'Flynn. MIN()imum failure: EMFI attacks against USB stacks. In *13th USENIX Workshop on Offensive Technologies (WOOT 19)*, Santa Clara, CA, 2019. USENIX Association. 24

[OP11] David Oswald and Christof Paar. Breaking mifare DESFire MF3ICD40: Power analysis and templates in the real world. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 207–222. Springer, 2011. 20

[OTL14] Sjoerd Op 'T Land. *La Modélisation de l'immunité Des Circuits Intégrés Au-Delà de 1 GHz*. PhD thesis, 2014. 13

[Pau06] Clayton R Paul. *Introduction to Electromagnetic Compatibility*, volume 184. John Wiley & Sons, 2006. 11, 12

[pdn17] plutoo, derrek, and naehrwert. Console Security - Switch. In *34th Computer Chaos Club Congress*, Leipzig, Germany, 2017. 24

[PN16] R. Przesmycki and L. Nowosielski. USB 3.0 interface in the process of electromagnetic infiltration. In *2016 Progress in Electromagnetic Research Symposium (PIERS)*, pages 1019–1023, 2016. 17

[RCHC09] Kasper Bonne Rasmussen, Claude Castelluccia, Thomas S. Heydt-Benjamin, and Srdjan Capkun. Proximity-based access control for implantable medical devices. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, pages 410–419, New York, NY, USA, 2009. Association for Computing Machinery. 23

[RD18] Pierre-Michel Ricordel and Emmanuel Duponchelle. Risques associés aux signaux parasites compromettants : Le cas des câbles DVI et HDMI. In *Symposium Sur La Sécurité Des Technologies de l'Information et Des Communications (SSTIC)*, Rennes, France, 2018. 17

[Res19] Limited Results. Fatal Fury On ESP32 Time To Release HW Exploits. In *Black Hat Europe 2019*, London, UK, 2019. 24

[Res20] Limited Results. Debug Resurrection On nRF52 Series. In *Black Hat Europe 2020*, 2020. 24

[Riv09] Matthieu Rivain. Differential Fault Analysis on DES Middle Rounds. In *Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems*, CHES '09, pages 457–469, Berlin, Heidelberg, 2009. Springer-Verlag. 24

[RLMI21] Thomas Roche, Victor Lomné, Camille Mutschler, and Laurent Imbert. A side journey to titan. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 2021. 20

[Roc10] Thomas Roche. *Dimensionnement et intégration d'un chiffre symétrique dans le contexte d'un système d'information distribué de grande taille.* PhD thesis, Université Joseph-Fourier - Grenoble I, 2010. 20

[ROSW16] Eyal Ronen, Colin O'Flynn, Adi Shamir, and Achi-Or Weingarten. IoT Goes Nuclear: Creating a ZigBee Chain Reaction. Technical Report 1047, 2016. 20

[Sch02] R. Schmitt. *Electromagnetics Explained: A Handbook for Wireless/ RF, EMC, and High-Speed Electronics*. EDN Series for Design Engineers. Elsevier Science, 2002. 21

[Sco16] Micah Scott. A USB Glitching Attack. In *PoC||GTFO, 2(0x13)*, number 2 in PoC||GTFO,, pages 30–37. 2016. 24

[Sel18] Jayaprakash Selvaraj. *Intentional Electromagnetic Interference Attack on Sensors and Actuators*. PhD thesis, Iowa State University, 2018. 23

[SKH+16] Matthias Schulz, Patrick Klapper, Matthias Hollick, Erik Tews, and Stefan Katzenbeisser. Trust The Wire, They Always Told Me!: On Practical Non-Destructive Wire-Tap Attacks Against Ethernet. In *WiSec '16. Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pages 43–48, United States, 2016. Association for Computing Machinery. 17

[SMTS13] Yasser Shoukry, Paul Martin, Paulo Tabuada, and Mani Srivastava. Non-invasive Spoofing Attacks for Anti-lock Braking Systems. In Guido Bertoni and Jean-Sébastien Coron, editors, *Cryptographic Hardware and Embedded Systems - CHES 2013*, Lecture Notes in Computer Science, pages 55–72, Berlin, Heidelberg, 2013. Springer. 23

[Smu90] Peter Smulders. The threat of information theft by reception of electromagnetic radiation from RS-232 cables. *Computers & Security*, 9(1):53–58, 1990. 17

[Thi01] Erik Thiele. Tempest for Elisa. www.erikyyy.de/tempest, 2001. 19

[TM17] N. Timmers and C. Mune. Escalating Privileges in Linux Using Voltage Fault Injection. In *2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 1–8, 2017. 24

[TSW16] Niek Timmers, Albert Spruyt, and Marc Witteman. Controlling PC on ARM using fault injection. In *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2016, Santa Barbara, CA, USA, August 16, 2016*, pages 25–35. IEEE Computer Society, 2016. 24

[van85] Wim van Eck. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security*, 4(4):269–286, 1985. 16

[VP09] Martin Vuagnoux and Sylvain Pasini. Compromising Electromagnetic Emanations of Wired and Wireless Keyboards. In *Proceedings of the 18th Conference on USENIX Security Symposium*, SSYM'09, pages 1–16, Berkeley, CA, USA, 2009. USENIX Association. 17

[VP10] Martin Vuagnoux and Sylvain Pasini. An improved technique to discover compromising electromagnetic emanations. In *2010 IEEE International Symposium on Electromagnetic Compatibility*, pages 121–126, 2010. 17

Chapter 2

Electromagnetic Perturbation Techniques

Contents

2.1 Chapter overview

In this chapter, a focus is made on non-ionizing electromagnetic interactions with electronic systems which result in functional faults which can have an impact on the security of the information processed. This topic has been studied mainly by two research communities with different mindsets and approaches. EMC researchers focused on the intentional malicious exploitation of the susceptibility of electronic systems under the name of IEMI. Cryptography researchers started to consider the possibility to fault electronic systems in order to break cryptographic implementations and called it EMFI. EMFI and IEMI are described and compared in order to clearly identify discrepancies, common points and hopefully bring up a conceptual basis which will help both communities to better understand each other and collaborate. Regarding the study of effects, it appears that the EMFI approach is focused on ICs and tailored for the assessment of information security impacts and exploitation. Besides, IEMI considers a wider range of targets and threat models but inherits from high power EMC approaches which focus mainly on functional availability impacts. Overall, this comparison shows that between EMFI and IEMI, there is room for new intermediary threat models requiring less power and still allowing for synchronization. Furthermore, methods from EMFI that bring easier information security assessment could be transposed and adapted to IEMI.

2.2 Intentional Electromagnetic Interference

Part of the research in the field of EMC is dedicated to the understanding of the effects on electric or electronic devices which are caused by EM interaction with their environment. The need for test procedures for the management of electromagnetic interference (EMI) has been in the scope of several standards committees since the early 1930s [Hoa07]. At this time, sources of interference were unintentional, both natural (e.g., lightning and ESD) and artificial (e.g., radio transceivers).

However, the potential offensive exploitation of such effects has gained interest, especially since the observations of collateral damage during the operation Starfish, a high altitude nuclear test in 1962 [Wik23] which created a HEMP. Effects on electric and electronic devices were reported, such as input circuit troubles in radio receivers and street light failures, on the Hawaiian island of Oahu, at merely 1400 km from the detonation [Vit89]. The evolution of technology used for radars and their proliferation also introduced new sources of EMI, with potentially critical impacts as in the U.S.S. Forrestal case. A landing airplane was illuminated by a radar and an EMI triggered the uncommanded release of ammunition, according to a report from national aeronautics and space admin-

istration (NASA) [LA95]. In order to evaluate equipment immunity against such EM environments, research was driven to build simulators focusing on the reproduction of these categories of waveforms.

In 1999, the international union of radio science (URSI) published a resolution on criminal activities using electromagnetic tools raising awareness about the likelihood of offensive use of EMI and the need of scientific investment on protection and test methods [URS99]. The same year, the international electrotechnical commission (IEC) SC 77C subcommittee had added this topic in its standardization program [LEKA+21].

IEMI was officially defined in 2005 as follows [ISO05]:

"Intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purposes."

The terms *intentional malicious* explicitly introduce an attacker, which is quite uncommon and surprising in a set of standards concerning the *compatibility* of equipment. The terms *disrupting, confusing or damaging* refer to functional safety and reliability issues. Together with the concept of an attacker, they also refer to information security issues, mostly on the availability of the information processed by the target system.

Furthermore, the definition encompasses the use of jammers, which are designed to overload antenna receiver circuits [ISO20]. As a result, this new EMC field intersects with other technical fields such as electronic warfare, wireless communication, functional safety, information security and risk management.

This historical introduction to IEMI and the standard definition uncovers slightly the diversity and the complexity of the physical interactions, the targeted systems or the attack scenarios that can be considered in this field.

2.2.1 IEMI interaction model

Starting from the standard definition, IEMI can be modeled as shown in Figure 2.1, which provides a simplified version of the EM interaction model in [GHS20] and the electromagnetic pulse (EMP) interaction models from [GT94, Lee86].

The attacker is in possession of a *source* which is able to generate electromagnetic energy destined to the target electric or electronic system. This electromagnetic energy, to reach the target, is subject to a *propagation* which can be radiated or conducted. It refers to the movement of currents, charges and/or electric and magnetic fields. Then the physical interaction with the conductive parts of the target, referred to as a *coupling*, occurs. The coupling produces physical effects, parasitic currents or

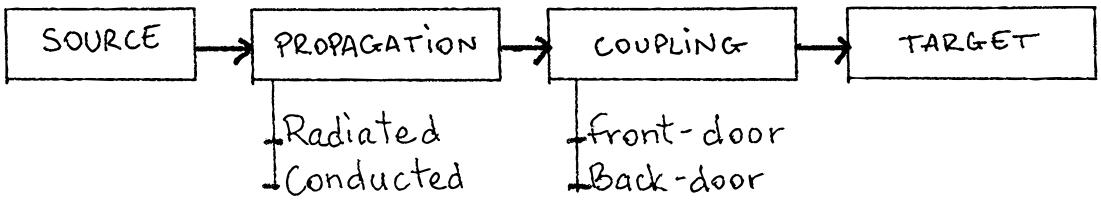


Figure 2.1 – A model for IEMI (adapted from [Lee86])

voltages which, by reaching systems or components, can introduce physical or logical impacts.

Depending on the complexity of the target topology, cascaded interactions might be considered, introducing other coupling, penetration and propagation steps [GT94].

Front-door coupling

When the IEMI signal couples through an interface intended to interact with the external EM environment, the coupling is called *front-door coupling*. Such interfaces are mostly antennas or sensors, which cannot be protected by shielding without loss of functionality. Therefore, front-door coupling efficiency is both space dependent, due to the antenna radiation pattern, and frequency dependent, due to the antenna reflection coefficient [Van16].

First order front-door coupling, or in-band font-door coupling, refers to situations where the IEMI frequency coincides with the working frequency of the interface. For an RF front-end, a first order front-door coupling will involve an IEMI signal in the target passband.

Second order front-door coupling, or out-of-band front-door coupling, refers to situations where the IEMI signal frequency does not coincide with the working frequency of the interface.

First order front-door coupling is generally assumed to have a much better coupling efficiency than second order front-door coupling [GHS20].

Back-door coupling

When the IEMI signal couples through cables, apertures or imperfections of the enclosure, the coupling is called *back-door coupling*. Back-door coupling interfaces can generally be shielded without performance degradation. For example, a field-to-cable coupling into a low voltage power supply cable of a smartphone [KLE15] is considered back-door. For back-door coupling, main points of entry are conducted penetrations and large apertures [MP16].

2.2.2 Considerations for threat models

From an InfoSec point of view, the IEMI interaction model can be used as a basis from threat modelling. The source is a significant point for the determination of the attacker profile. It reflects the financial, technical, technological power of the attacker because of the costs and skills needed to design, build, operate and maintain the source. It also reflects the attackers operational agility which is related to the source portability (volume, weight, energy source, etc.). Finally, the IEMI environments that the source can generate also contribute to the attacker profile determination.

After being emitted, the propagation, penetration and coupling are inherent to the operational environment topology and also the target topology.

Finally, the physical effects are the result of an EM vulnerability, which reflects the possibility of occurrence of the parasitic currents, voltages, EM fields in the target. Their propagation to the upper layers and the impacts on the information manipulated by the target are specific to the target. Therefore, IEMI attacks can be considered as always being targeted attacks. To determine the potential consequences of effects on the security of the information manipulated by the target, it is necessary to detect and identify impacts on logical layers and to analyse their exploitability, i.e. the potential scenarios where those impacts threaten the confidentiality, integrity, or availability of the information.

2.2.3 Standard waveforms and EM environments

The EM environments for IEMI are defined and classified in [ISO05, ISO20]. Unlike other intentional or unintentional EM environments considered in this standard, one important specificity of IEMI environments is that they encompass a wide variety of waveforms. This makes the definition of the potential threats, the associated sources, the EMC problem formulation, the InfoSec problem formulation, the choice and the design of countermeasures very complex. Due to this wide range of possibilities, the IEMI environments are classified according to source signal characteristics. The band ratio (br) is the ratio of the high and low frequencies (resp. f_h and f_l) between which there is 90% of the energy [GHS20]:

$$br = \frac{f_h}{f_l} \tag{2.1}$$

The classification of IEMI environments according to the band ratio is given in Table 2.1.

Typical examples of hypoband 2.2, mesoband 2.3 and hyperband 2.4 environments are given in the time and frequency domains.

Considering these definitions, IEMI environments include or overlap several other high power

Table 2.1 – Frame format for the covert communication

Band type	**Band ratio** (br)
Hypoband	$br \leq 1.01$
Mesoband	$1.01 < br \leq 3$
Sub-hyperband	$3 < br \leq 10$
Hyperband	$10 < br$

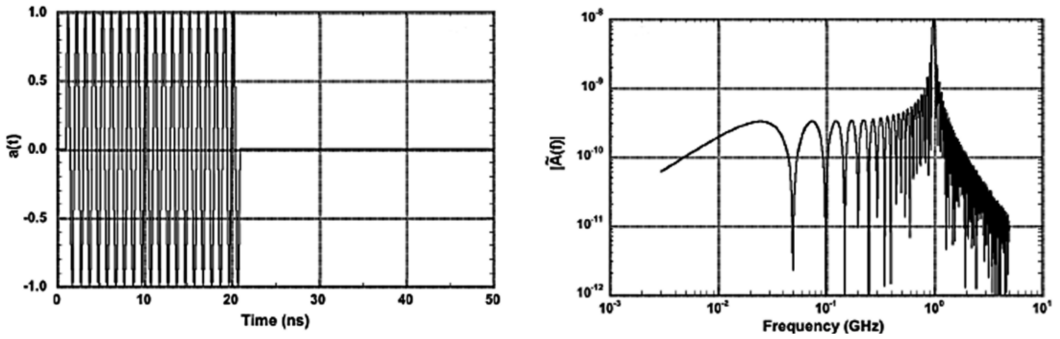


Figure 2.2 – Example of typical hypoband IEMI environment in time (left) and frequency (right) domains (from [ISO05])

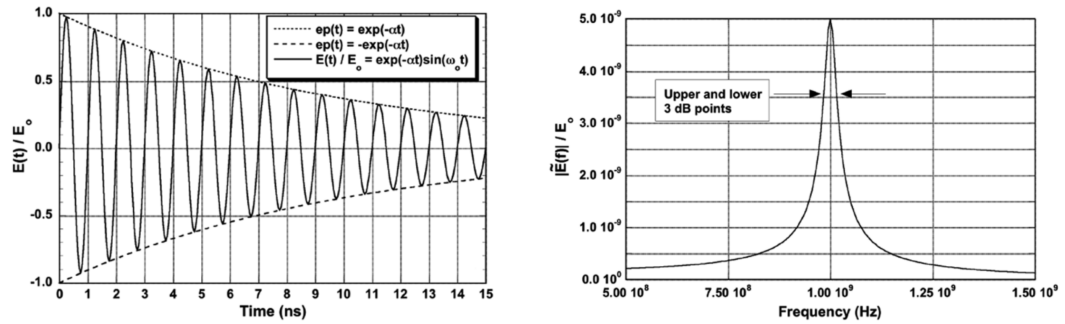


Figure 2.3 – Example of typical mesoband IEMI environment in time (left) and frequency (right) domains (from [ISO05])

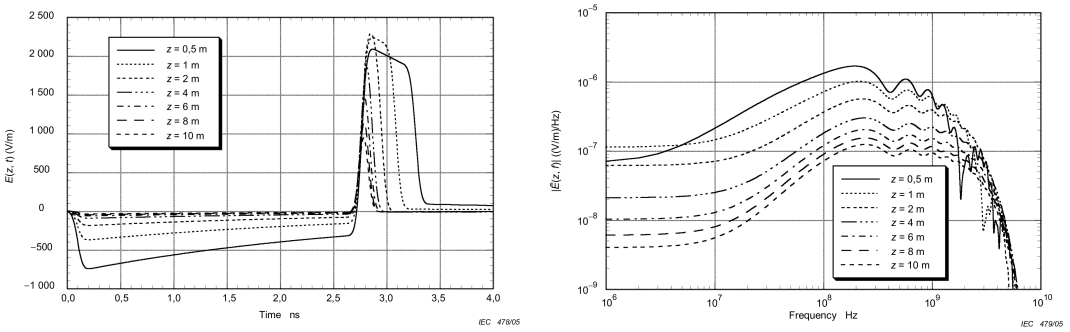


Figure 2.4 – Example of typical hyperband IEMI environment in time (left) and frequency (right) domains (from [ISO05])

EM environments from the EMC standard. This further confirms the multiplicity of the threats that are considered and the complexity of testing and decision making when it comes to solving an IEMI problem. Figure 2.5 places IEMI environments into the spectrum relatively to other high power environments defined in [ISO05], such as lightning, EMI for COTS devices, ESD, HEMP and high intensity radiated field (HIRF).

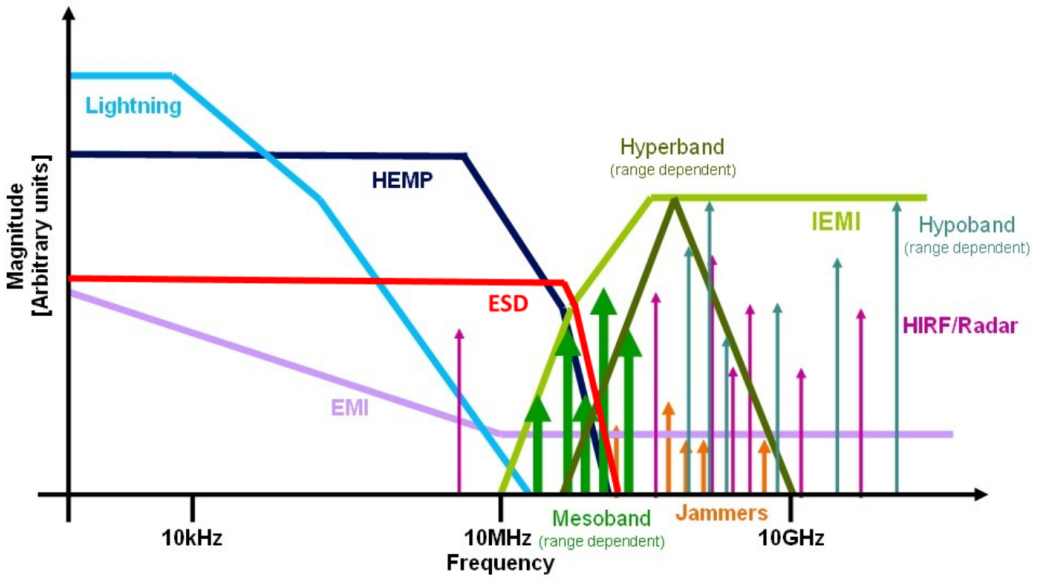


Figure 2.5 – Spectral view of the classification of IEMI environments with other high power EM environments (from [ISO05])

2.2.4 Sources

When it comes to analyzing risks related to IEMI, the signal source the attacker possesses are a dimensioning factor regarding several aspects. In [MP16], existing IEMI sources are analyzed and classified according to several criteria reflecting what is at stake both from a technology viewpoint and from a risk analysis viewpoint.

The source is a significant point that defines the attacker profile, its capabilities on financial, technical grounds, regarding the access to certain technology. Indeed, some sources are not readily available for sale or exist only in very few units. Some solid scientific background might be necessary to build, maintain or operate such sources. For example, in [ISO20], a source category referred to as "simulators" designates sources that are unique and that were built for research purposes, such as the UK Orion hypoband source [GHS20], capable of generating 350 MW CW signals in 1–3 GHz.

[ISO20] defines several technical capability groups:

- Novice: individuals or small groups with minimal financial or technical support;

- Skilled: moderately well-funded adversaries with training and expertise in relevant technology;
- Specialist: well-funded adversaries with post-graduate level training and access to substantial research capabilities, resources and funding.

The characteristics of the signal that can be produced are also an important point when considering sources. Primary parameters are the frequency range, the IEMI environment class, the peak and average power, the pulse width, the pulse repetition frequency, the burst length. These impact other parameters such as the source mobility, the technical complexity, the cost, the characteristics of the antenna or the conducted injection method and the operating range. The technical complexity and the cost are taken into account in the attacker profile. The source mobility and the characteristics of the antenna or the conducted injection method are dimensioning factors regarding the operational deployment and use of the source. Same goes for the range, which depends on the source signal characteristics and the propagation path characteristics between the source and the target.

In [MP16], the mobility is quantified as the "portability level", which can take the following values: pocket, briefcase, motor vehicle, trailer. Overall, among the existing sources considered in the survey, conducted sources are generally smaller than radiated sources. Radiated sources which have a portability level that can be carried by an individual produce an EM field with a far voltage[1] inferior to 1 kV.

An interesting trend was also observed in [MP16] regarding the source class produced over time. First interest was clearly directed to high power hyperband sources and after 2010, research was published about the production of mostly mesoband sources, which might indicate that the focus of the community shifted from means to transfer the maximum amount of energy to any target to sources with more agility that can generate the most efficient IEMI environment for a specific target, with the opportunity to obtain more subtle effects.

2.2.5 Targets

A specificity of the standards related to IEMI is the wide range of scales for the considered targets. This point is well illustrated in [GHS20] with the view of a system-of-systems hierarchy. The systems which can be considered as a target for IEMI threats range from electronic components (e.g., diode, transistor, IC) to infrastructures (e.g., building, energy transmission grid).

In [Pou15, TPR+18], the susceptibility of a Metal Oxide Semiconductor (MOS) transistor was assessed and modeled between 10 MHz and 1 GHz, showing that a rectification effect occurred above

[1] Range normalized electric field magnitude, defined in section 2.2.6 on page 43

the operating frequency of the target and that this rectification effect is caused by the nonlinear parasitic capacitances. A phase locked loop (PLL) operating in the 2.95–3.15 GHz range was tested in [Dub11] against in-band conducted IEMI, showing that the output signal produced by the PLL could be altered in frequency and in amplitude when stressed by a CW. When stressed with an AM IEMI, the low frequency modulating signal was also shown to modulate the PLL output frequency. In [OTL14], a summary of conducted immunity testing on components and simple ICs is given, showing that most studies focus on CW injection below 1 GHz. Flash memory ICs were also tested in [Ame15] against conducted injection of a sub-GHz CW during read/write operations.

The behaviour of the power network of several microcontrollers from the STM32 family against pulsed stresses and CW was tested in [Bac17], with a conducted injection on the power pins. The common mode to differential mode conversion was studied and it was observed that it was maximal when the injected signal frequency was close to the power network resonance frequency. The susceptibility of the internal analog to digital converter (ADC) of a Tiva C microcontroller was assessed with a conducted CW IEMI in [War17], with a focus on the frequencies for which the digitized parasitic signal was higher.

Beside components, PCB scale systems or electronic devices were also considered, such as radio front-ends and LNA [Van16]. In [Mej19], computer power supplies were tested against conducted signals in the low voltage power supply pins in order to identify which internal components get damaged.

Information technology (IT) network equipment, such as wired or wireless routers were tested in [BL04, KSG15b, KSG15a, SN06], focusing on the impacts on the network traffic performance. Desktop computers were also tested, as in [GHS20, Hoa07, SN06], where susceptibility criterion were reboots, shutdown, mouse pointer deflection, loss of networking link.

Unmanned aerial vehicle (UAV) were tested in [CZCW18, KLHY22, LE19, LECK18, LLLS20, ZZC+20], with susceptibility analyses of the front-door (on data and control wireless links) and back-door coupling of CW or wide band pulses. The susceptibility criteria were mostly the impacts on the course on the targets.

Even bigger scale systems of systems are concerned by susceptibility testing against IEMI, such as cars, planes, missiles, but results on such targets made in a military context usually stay confidential. Without providing details on the test setup, effects observed on a 1993 car engine were reported in [BL04]. Car engine stopped when submitted to radiated pulsed CW with a carrier in the 1.3–3 GHz frequency range, a 5 µs duration and a 200 Hz pulse repetition frequency. Conducted IEMI was performed at a building scale, with an injection into the low voltage power network trans-

former [PZRI04]. In [MNTB07] pulses rising time are less than 1 ns with a maximum amplitude of 450 V. It was highlighted that: the injected power can propagate at large distance into the low voltage power network. This was also reported in the standard [ISO05]. In [GP14], the radiated penetration and propagation of signals in the 2–4 GHz frequency range generated by a 2 MW FPS-6 radar through and across buildings is studied, showing that some electronic devices could suffer disturbances over nearly 3 km.

2.2.6 Characterization of the susceptibility of a target

Studying the susceptibility of a target against IEMI can be a very challenging task. Following the definition of the EMC susceptibility, the main goal is to assess "the possibility of a degradation to the performance of a device, equipment or system in the presence of an electromagnetic field", and in this case, the characteristics of the EM field are defined by the IEMI environment.

However, difficulties arise in practice because of the following:

- The EM environment is only completely defined from the operational context;
- The performance degradation criterion are defined on main functional mission, therefore are not intrinsic to the target;
- The observation of effects.

According to [ISO20], preliminary steps are necessary to dimension the EMC problem that will be studied during susceptibility testing. The steps for tailored test specification are given hereafter:

- Understand the IEMI threat environment;
- Measure the protection level by obtaining transfer functions;
- Predict induced signals at the location of the target;
- Create envelope predictions;
- Assess immunity of target: inject predicted induced waveforms.

For the determination of the IEMI environments that will be considered during the tests, the difficulty comes from the fact that with IEMI, unlike other EMC phenomena, assumptions cannot be made about a general or average disturbance level. It is therefore necessary to choose or to determine, according to the operational deployment of the target, the IEMI source parameters and the protection level of the target (range between source and target, propagation channel loss). For source parameters,

the standard suggests an approach based on the expected attacker profiles via the technical capability groups and provides a correspondence table with source characteristics, especially signal intensity, as shown in Table 2.2. Signal intensity represents the *far voltage* V_{var}, which is a range normalized magnitude of the electric field and expressed as follows:

$$rE_{far} = V_{far} \tag{2.2}$$

where E_{far} is the far-field magnitude measured at distance r from the source [ISO20].

Table 2.2 – High power radiated IEMI source by capability group (from [ISO20]

Category	**Source type**	**Source name or technology type**	V_{far} (V)
Novice	Hyperband	ESD gun	5000
	Hypoband	Microwave oven magnetron	2000
Skilled	Hyperband	Commercial solid state pulser	60 000
	Mesoband	Commercially available pulser	120 000
	Hypoband	Radar	450 000
Specialist	Hyperband	Military demonstrator	5 300 000
	Mesoband	Military demonstrator	500 000
	Hypoband	Military demonstrator	30 000 000

Regarding the protection level of the target, an estimation or a measurement of the overall attenuation between the source and the target must be done. The determination of transfer functions represent the channel effects on the source waveform of the cascaded propagation, coupling and penetration between the source and the target.

The immunity assessment of the target consists in confronting the target with the chosen EM environment and measuring the impact on the target according to failure criteria. Those failure criteria are difficult to define and they are usually not intrinsic the target, but instead they depend on the final operational context where the target will be deployed. For ICs, the criteria can be related to a measured electrical signal produced by the target, such as a jitter or a voltage variation of a digital signal [BDRS06]. For experimental reasons, failure criteria that can be measured in real time are more convenient for automated testing.

Observed effects are then classified in order to provide a common basis of comparison and to enable a risk based approach necessary to choose the right level of protection [ISO04]. The different classification schemes for effects are summarized in [Mej19] and will be briefly introduced hereafter.

A first classification of effects has been proposed in [Sab08] based on the potential physical cause of failure (Table 2.3). This classification is considered useful because it may help understand the physical phenomena related to the way energy couples into the target. It is mostly dedicated to

impacts on functional availability that can be easily (visually) observed [Mej19]. However, when the cause of failure cannot be easily observed, which is often the case for logical effects, effects fall into category U and the classification is ineffective.

Table 2.3 – Classification of IEMI effects by physical cause [Sab08]

Category	Effect	Description
U	unknown	unable to determine due to effects on another component or not observed
N	No effect	No effect occurs
I.1	Noise	Raised noise level on signal or power lines
I.2	Bit flip	Injected signal alternate bits in data stream
I.3	Failure	Malfunction of the system
I.4	Break down	Hang up or crashing of software
D.1	Latch up	Injected signal causes latch up in semiconductor components
D.2	Flashover	On chip flashover
D.3	On chip wire melting	Wires on chip are melted by injected energy
D.4	Bond wire destruction	Wires on PCB, bond wires in semiconductor devices are melted by injected energy

In [Sab08] , a classification of effects according to their duration relatively to the IEMI is proposed, and reminded in table 2.4.

Table 2.4 – Classification of IEMI effects by duration [Sab08]

Category	Duration	Description
U	Unknown	No effect occurs or the duration has not been observed (e.g., observer was unable to determine duration due to effects on another component)
E	During exposure only	Observed effect is present only during exposure to the EM environment, system functionality is completely available when environment has vanished
T	Some time after exposure	Effect is present some time after the EM environment has vanished
H	Resistant until human intervention	Effect is persistent until human intervention, the system is not able to recover to normal operation
P	Permanent until replacement of hardware or software	Effect has damaged hardware to the point that it must be replaced or software to the point that it must be reloaded

According to [Mej19], this classification is based on an objective criteria, seemingly independently from the system functional operation. However, the classification is based on the ability of the target to “recover to normal operation” or on the availability of the “the system functionality”.

In [Sab08] and [ISO09], a classification of effects based on their criticality on the main mission

Table 2.5 – Classification of IEMI effects by criticality [Sab08]

Level	Effect	Description
U	Unknown	Unable to determine due to effects on another component or not observed
N	No effect	No effects occurs or the system can fulfill his mission without disturbances
I	Interference	The appearing disturbance does not influence the main mission
II	Degradation	The appearing disturbance reduces the efficiency and capability of the system
III	Loss of main function	The appearing disturbance prevents that the system is able to fulfill its main function or mission

of the target is proposed (Table 2.5). This classification is convenient for service-based system-level risk assessment of the operational deployment of the target [MP16].

Overall, the different classification methods are mostly dependent on the operational context where the target is destined to evolve. The failure criteria that might be chosen for susceptibility testing will therefore not reflect an intrinsic vulnerability of the target. Furthermore, both the IEMI environment selection and the effects observation are dependent on the operational context. Finally, failure criteria are focused on the availability of the target main function.

2.2.7 Exploitation

In this section, a focus is made on the exploitation of IEMI effects on a target device. An overview of the type of achievements that can be obtained by an attacker with IEMI impacting the security of the information manipulated by the target.

Destruction, denial of service

Several studies were dedicated to the determination of breakdown, burnout, destruction thresholds for different types and generations of electronic components [BL04, GHS20, Hoa07, Int78, SN06]. In [Mej19], switch mode power supplies were tested against conducted high power (> 12 kW) hyperband signals in order to determine the destruction sequence of the components, showing that most impacted components were the fuses, the diodes, the PWM controller and the Metal Oxide Semiconductor Field Effect Transistor (MOSFET). Figure 2.6 shows some destructive effects observed.

In [PS11], the functional performance of several IT network equipment was tested against high power (> 200 kW) hypoband and hyperband radiated IEMI. Ethernet routers with different cables and Wi-Fi routers showed impacts of I, II and III criticality levels (see Table 2.5), resulting mostly in a degradation or an interruption of the network traffic.

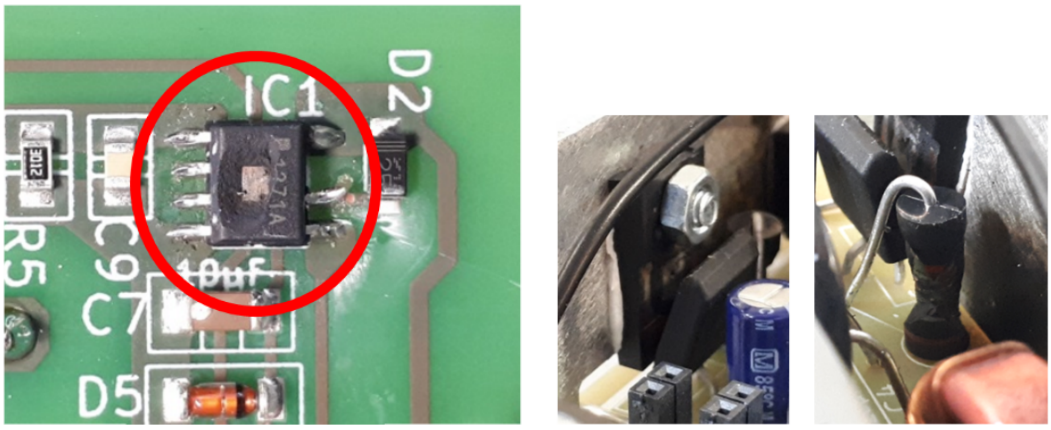


Figure 2.6 – Example of destructive effects on components of a switched mode power supply [Mej19]

.

In [ASP+14], electronic passport readers for automated border controls were tested against 1 µs pulsed signals with 1 kHz repetition rate at 150–3425 MHz for backdoor coupling, and 13.56 MHz for front door coupling. Effects were classified by criticality as in Table 2.5. Interference type effects reported included impacts on the image reading (no picture, failure in image recognition, failure in reading the machine-readable zone of the passport). Upset type effects included communication interruption on USB and radio frequency identification (RFID).

Denial of service on RF front-ends

A PLL was sudied in [Dub11] and the impact of its susceptibility when used as an oscillator in a quadrature phase shift keying (QPSK) radio receiver was assessed. Effects on the PLL were impacting the output signal frequency, phase and amplitude, resulting in demodulation errors. In case of a hypoband CW IEMI, impacts were significant when the CW frequency was close to the PLL output frequency (in this case 3 GHz). In case of hypoband AM CW, longer pulses and higher pulse repetition frequencies gave better results.

A 2.4 GHz radio front-end was studied in [PRC17], with a focus on effects impacting the LNA and the power amplifier (PA). It was illuminated by a $3\,\mathrm{kV \cdot m^{-1}}$ 60 GHz pulsed CW (hypoband) with a pulse repetition rate of several kHz. The observed effect was a reduction of the amplitude or an extinction of the output signal during the pulses.

In [Van16], first order front door coupled hypoband CW IEMI effects on a TETRA receiver, leading to a saturation of the front-end and a decrease of the receivers sensitivity. Second order front door effects are also studied, showing that non-linear interaction (harmonic distortion, cross modulation, intermodulation) with the LNA and desensitization due to a high power interferer could

decrease the signal to noise ratio (SNR) and degrade the demodulation efficiency.

The signals re-radiated by RF front-ends when illuminated with IEMI were also investigated in [Mar18]. It was observed that the targets re-emitted signals containing non-linear distortion (harmonic and intermodulation products) when illuminated by hypoband mono tone or two-tone CW signals. It was suggested to use non linear radar (H2 and IM3) signals to detect RF front end characteristics such as operating frequency and bandwidth.

Signal injection in communication interfaces

Signal injection in wired baseband communication cables was investigated in [DMGM22] target universal asynchronous receiver transmitter (UART) and I2C. Hypoband signals with a 65 MHz fundamental frequency were introduced by near field coupling using a signal generator, a 20 W amplifier and a small Vivaldi antenna at 10 cm. It was shown that an attacker was able to perform bit sets and bit resets in the serial communication frames if a prior synchronization was possible (e.g., by exploiting the EM emission of the serial communication) and cables were not twisted. A similar work was proposed in [JCK+23], where the susceptibility of serial communication buses (I2C and SPI) between sensors and a SoC has been investigated, resulting in a random alteration of the transmitted data frames.

Signal injection in wired RF communication was also investigated. In [KBSM22] and [NSFG21], the possibility to disrupt power line communication (PLC) communications remotely with IEMI was shown. In [GP22], J2497, an in-vehicle UART over PLC communication protocol operating from 100–400 kHz was studied, and the possibility of remotely introduce frames into truck cables was demonstrated, using a software defined radio transmitter and a loop antenna to replay frames, needing 10 W at 45 cm.

Attacks on sensors and actuators

Both analog and digital sensors have been scrutinized under IEMI environments. Despite not being restricted to EM interactions, a very complete survey on signal injection into sensors is given in [GR19]. Most studies do not precisely identify if the observed effects are due to parasitic activity into the communication interfaces (post-transducer attack [KBM22]) or into the sensing unit (pre-transducer attack [KBM22]). However, a very thorough analysis of the different threats from IEMI against analog sensors is given in [KBC+13]. In particular, in order to introduce a parasitic signal with the characteristics of a target legitimate signal, a baseband IEMI or a modulated IEMI can be used (e.g., in Figure 2.7).

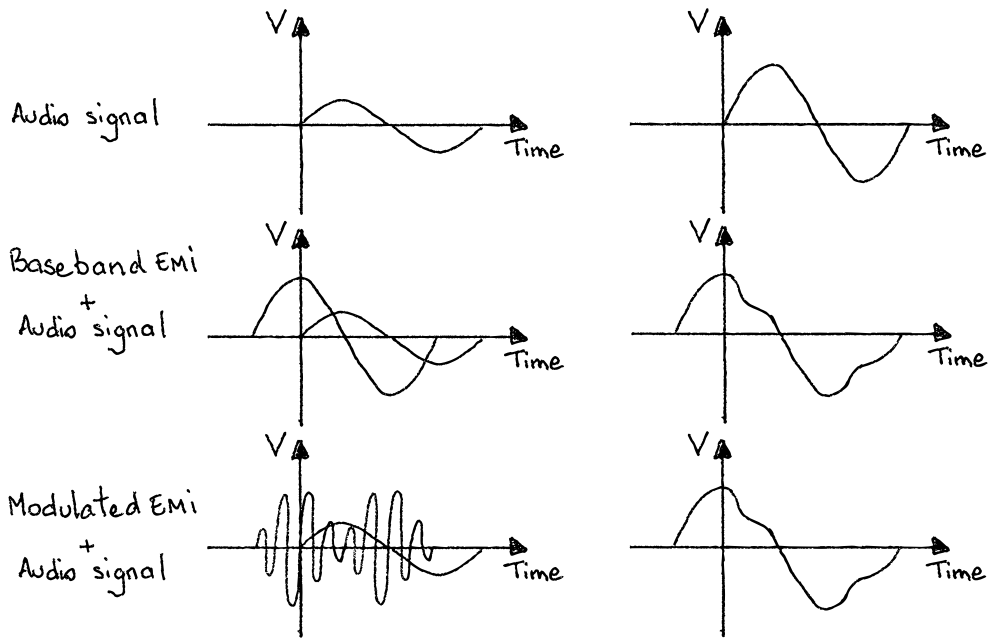


Figure 2.7 – Illustration of a baseband and a modulated EMI targeting a legitimate audio signal and the resulting amplified signal (right) [KBC+13]

The modulated IEMI can be demodulated in the target by non-linear behaviour of components, by filters or by distortion caused by ADCs. As a result, the modulator signal gets interpreted by the digital logic reading the sensor values. With a modulated signal, the carrier frequency can be chosen so as to maximize the coupling efficiency. Several sensors are then targeted in practice, such as an analog microphone in a webcam which was targeted by an AM IEMI with a carrier around 825 MHz and an audio modulator signal (an actual song). An analog microphone enclosed in a Bluetooth headset was also targeted with the same signal, but with a carrier frequency around 1.175 GHz. In both cases, the attack success criterion was the good recognition of the song by an online music recognition service. Analog microphones have also been attacked with IEMI in [DAY22, KLE15, LEK18, XHJ+21].

Optical sensors are studied in [KBM22], demonstrating the possibility to introduce an arbitrary image, with some quality limitations (e.g., colors), by a post-transducer interaction via a 190 MHz 100 mW AM IEMI. However, frame injection required a synchronization to the sensor activity. An exploitation without synchronization was also proposed, by introducing enough noise to degrade an automated barcode recognition on the optical stream.

Interaction with smartphone capacitive touchscreens was also investigated, showing the possibility of injecting arbitrary touch events with varying precision [JJW+22, MWM19, SZZ+22, WMY+22]. In [JJW+22], a conducted CW IEMI (hypoband) introduced through the USB charging cables of tar-

get smartphones is used, at a frequency close or related to the internal touchscreen excitation signal and with amplitudes of nearly 100 V (e.g., 300 kHz and 99 V on a Google Nexus 7). Again, a synchronization is necessary to inject arbitrary touch events, which precision depend on the exact moment and duration of the injection, and the exploitation of EM emission is proposed to this end. Without synchronization, random touch events or a disruption of the touch event detection are still achieved.

In [DSM+22], the possibility of injecting a signal into a PWM link between a SoC and an actuator (servomotor) is investigated. It is shown that an AM hypoband IEMI with a modulator signal corresponding to the intended PWM signal resulted in a good interpretation of the modulator signal by the actuator. A full control of the rotation of the actuator was achieved without the need of a synchronization, in contrary of previous work (e.g., [Sel18]). A radiated test on a custom target setup mounted on a Cessna 150 UAV showed a successful IEMI at 25 cm distance with a custom antenna, a 20 W amplifier and a 62 MHz carrier frequency, with a modulator of a few kHz.

2.2.8 Countermeasures

In InfoSec, countermeasures can have the following goals:

- Correcting the vulnerability: the root cause of the vulnerability is eliminated;
- Reducing the attack surface: remove the access to a path enabling exploitation;
- Increasing attacker profile: the preconditions and the effort level necessary to exploit the vulnerability are increased;
- Reducing impacts: the gain for the attacker gets more limited;
- Detecting the attack.

An overview of protective measures against IEMI is provided in [ISO04]:

- EM protection applied to the system of concern: minimization of coupling of external EM fields and increasing the effective shielding;
- Fault tolerant design of hardware and software;
- External monitoring;
- Physical security of the system: to increase distance between source and target;
- Redundancy.

Shielding and filtering

The EM protection of the target acts on the coupling, penetration and propagation of the attacker signal, and can be viewed as way of elevating the attacker profile and reducing the attack surface. If the protection level is higher, the signal power might need to be higher and so does the complexity of the source.

Some parts of the system cannot be shielded, such as front door interfaces. In this case, some filtering can still be applied to reject out of band interference [ISO04].

Zoning

To compensate the impact of shielding on the source, the attacker might need to reduce the distance with the target. To counter this comes the physical security of the system, which aims at keeping the potential attacker at a distance, with proper zoning and physical access control. Zoning is a countermeasure which consists in segmenting a physical site into several zones based on their protection level, both EM and physical.

Fault tolerance

Fault tolerant hardware and software aims at reducing the impacts of physical and logical effects on the target and correcting the vulnerability. An example is proposed in [KBC+13], adding a differential comparator in the target PCB to remove common mode interference. The same strategy is proposed in [JJW+22] via the insertion of a common mode choke.

Redundancy

Redundancy can be viewed as a way to both reduce the impacts and increase the attacker profile. Impact reduction comes from the fact that if one system is attacked with impacts on the availability or the integrity, another system out of reach is supposed to still work properly. The existence of the other systems forces the attacker to compromise multiple targets. In [GR19], in a sensor security context, a sensor redundancy approach is evoked, in the form of a duplication of sensors of the same type but with different vulnerabilities and of a sensor fusion, attenuating the impacts of an attack on one sensor.

External monitoring

External monitoring is one form of detection and will be discussed in the next section.

2.2.9 Detection and forensics

As recommended in the standard [ISO09], an external monitoring can be operated in order to detect in real time. It allows to "search for the disturbing source" if an attack is detected. Even if it is not stated in the standard, such device can also be useful for forensic analysis if a recording of events can be stored and read later.

Following this recommendation, several devices were built for the detection of HPEM and IEMI. ToTEM ® [EWHR22, HRP+22] is a radiated threat detector operating in the 10 MHz to 10 GHz frequency range with 100 MHz instantaneous bandwidth. It provides a logging system recording 10^6 event, time, date and magnitude log entries. In [DFK+14], technical requirements for an IEMI detector are identified. The French commissariat à l'énergie atomique et aux énergies alternatives (CEA) has also proposed a detecting device [RJL+22] composed of 8 high dynamic range RF receiving channels combined to protection components to resist to high level EM fields. The whole covered frequency range is 0.1–8 GHz. The analysis of received waveforms is performed in the device, determining signal level ($V \cdot m^{-1}$ to tens of $kV \cdot m^{-1}$), repetition rate, pulse width, impacted frequency channels.

The detection can also be performed by the target device. In [TTPH21], the use of a dummy sensor is proposed. If a signal appears from the dummy sensor, it is likely to be a post-transducer injection. In [ZR20], it is proposed to add a varying bias voltage on the sensor output, which can not be predicted by the attacker. If the sensor output does not contain the same bias, it is likely to be a sign of a post-transducer injection. The same idea was proposed in the case of active emitter-receiver based sensors, where the emitter could modulate a challenge that should be captured by the receiver part of the sensor when no post-transducer injection occurs.

2.3 Electromagnetic fault injection

Since the first observation of functional faults on components operating in extreme environments, significant effort has been made to understand the interactions of the most probable physical perturbation sources and to improve reliability and functional safety. Controlling the physical environment of a system in order to introduce perturbations which can be exploited to circumvent security functions has been considered nearly twenty years later [Dum20]. Fault injection in InfoSec seems to inherit both from research on fault-tolerant and radiation hardened ICs conception and research on the security of cryptographic primitives deployed in secure computation platforms (e.g., secure elements, smartcards, etc.). This might explain why the focus was made on attacking and hardening

components implementing cryptographic algorithms.

2.3.1 Injection vectors

Several physical media were considered as potential perturbation sources, as synthesized in Fig. 2.8 (adapted from [Tro21]).

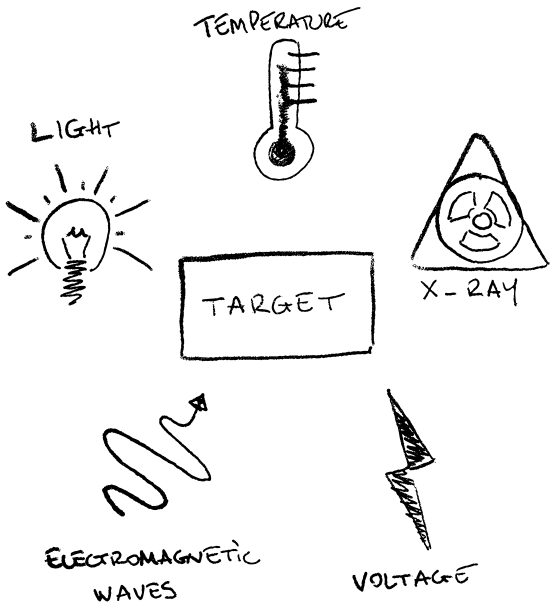


Figure 2.8 – Physical perturbation sources (adapted from [Tro21])

Fault attacks by controlling temperature [HS14], by focusing light [Sko10, VTM+17] or even an X-ray beam [ABC+17] have been proposed and successfully used on several memory technologies and processing units. These are however out of the scope of this thesis.

The term EMFI, also called electric field transient glitch [KK99] usually refers to radiated susceptibility exploitation of a target IC and will therefore be considered as radiated EMFI in what follows. Similarly, although usually considered as different from EMFI, voltage and clock glitch injection are in fact conducted susceptibility exploitation of a target IC and will be categorized as conducted EMFI.

Conducted fault injection

ICs interact with external entities through electrical input/output (IO) interfaces called pins. Interactions can be classified regarding the signal characteristics as follows:

- Power / ground: pins dedicated to provide electrical energy needed by the IC to operate. There

can be several power domains which can have different electrical properties and be routed to different areas of the IC;

- Clock: pins used to provide timing references to the IC. Again, several clock domains can coexist;
- Analog IOs: convey analog signals, such as information from analog sensors or to analog actuators. Input signals are usually digitized with an ADC block;
- Digital IOs: convey digital signals usually in the form of a digital communication protocol;
- RF IOs: convey radio frequency signals (i.e. signals which have been transposed to a carrier frequency).

Conducted fault injection consists in imposing a stimulus to a target through a cable or a PCB trace towards one or several IO interfaces. This means the attacker has physical access to and can tamper with the PCB so as to increase probability of success. Usually, filtering elements such as decoupling capacitors are removed [O'F17]. The most targeted interfaces, which also are considered as the most efficient for triggering faulty behavior are the power/ground pins and the clock pins [AK96].

By controlling the clock pin, an attacker can decide to permanently or briefly increase (overclocking) or decrease (underclocking) the clock frequency, but also to modify the duty cycle of the clock signal to introduce locally early or late transitions. By controlling the power signals, an attacker can decide to permanently or briefly increase or decrease the voltage, or even introduce transient short circuits. In synchronous circuits, such clock or power supply variations can generate the desynchronization of parts of the circuit and introduce timing constraint violations and logical faults [Zus14].

Attack waveforms can vary, depending on the target system and the injection technique, but the most common waveforms are pulses and harmonic (CW) signals. Two main strategies are commonly used: direct injection of a faulty signal and injection of a perturbation on an existing signal. In [Zus14], faulty clock signals (overclocking and frequency glitching) are generated by a field programmable gate array (FPGA), while power glitches are generated by wide band pulse generators that can be configured with a direct current (DC) offset at the nominal power voltage. The target operates at 1.2 V and the generated pulses are over ten times the nominal voltage, but only a residual parasitic signal of about 1 V is really coupled according to measurements performed with a digital voltmeter implemented on the target. In [O'F17], a low cost voltage glitch injection setup called a crowbar circuit is proposed. Using a high speed MOSFET controlled by a FPGA or a microcontroller the target power line is shorted to ground. As a result, the power line ends up ringing around the nominal volt-

age in a kind of damped sine shape. Several low-cost glitching platforms and tools have been built around this idea, such as the Chipwhisperer (250$) [New17], the PocketGlitcher (30€) [Res20c], the IceStickGlitcher [Res20a] and several other easily accessible platforms. This technique has been derived in [Res19, Res20b] using a high speed switch so that the signal is briefly switched from a nominal voltage to a target glitch voltage.

Other interesting approaches regarding the injection platforms and the attack waveforms have been proposed. In [TM17], a FPGA combined with a digital to analog converter (DAC) are used to provide an arbitrary power supply signal from −4–4 V with a 4 ns pulse resolution. This setup is used to escalate privileges on a Linux system running on a 1 GHz ARM Cortex-A9 SoC. A better control of the pulse shape has been investigated in [BFP19] and they propose to use a digital arbitrary signal generator as a primary source of pulse combined with an amplifier in order to find efficient pulse waveform parameters (rise and fall times, amplitude, etc.). Injection of RF signals has been investigated in [Ame15] with a custom injection PCB allowing mixing the nominal signal with an harmonic perturbation signal. Signals between 1 MHz and 1 GHz have been mixed with voltage and clock signals to attack several SPI flash memory ICs. Harmonic signal injection on power interfaces have also been shown to be effective against several types of TRNG. In [Had15], a digital arbitrary signal generator is used to provide a FPGA implementation of a TRNG with a power signal composed of an harmonic component at a specifically chosen frequency and amplitude and a DC component of the nominal 1.2 V. It is shown that when the frequency of the harmonic component is close to the TRNG frequency, the output of the TRNG can be biased.

Body biasing

In [MTOL12] a new fault injection vector named forward body biasing injection (FBBI) is proposed. It can be viewed as a conducted voltage injection into the substrate of an IC to introduce a static bias of a few tens of Volts to modulate threshold voltages of transistors. In this first work on FBBI, a laboratory grade voltage pulse injection setup is used with a probe made of a thin thingsten rod (20 µm diameter) which is in contact of the substrate of a decapped IC. This technique has also been applied on ICs which package exposes the raw substrate, such as wafer level chip-scale packaging (WLCSP) [O'F21b]. A low-cost pulse generation device [O'F21a] is used to inject faults on a STM32F415OG with 0.1–10 V pulses.

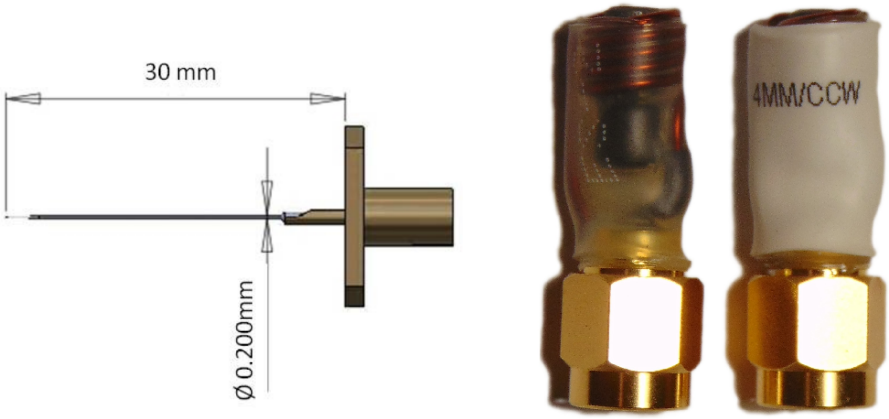
Radiated fault injection

The exploitation of the radiated susceptibility of an IC for inducing faults has been considered for a long time in the context of dependability and reliability [HTI97]. Using such techniques for InfoSec purposes has been proposed as an alternative to conducted glitching techniques as soon as 1999 [KK99], without however explicit practical results. The most commonly referenced as a seminal paper (e.g. [DDR+12, Dum20, Mad19, SH07]) on radiated EMFI with applications in InfoSec is [QS02]. Using a camera flash-gun to inject a high-voltage into the coil of a self-made probe, eddy currents were generated on the surface of the target IC leading to faulty computations and transient faults into transistors and memory cells [SH07].

Radiated fault injection consist in imposing a stimulus to a target through a contactless electromagnetic interaction in order to generate spurious electrical activity inside the target electronics or microelectronics. The attacker has physical access to the target external envelope and usually proceeds by placing an injection probe close enough to the target to ensure an efficient near field EM coupling of the signal fed to the probe into the target's conductive layers. Relevant injection parameters for this kind of interaction are the position of the probe relatively to the target, the probe EM characteristics and the characteristics of the signal fed into the probe.

Regarding the position of the probe, it is usually considered that the coupling efficiency is better the closer the probe is from the target's conductive layers. However, in [SH07], the probe is a spark gap and when it is too close to the target, the spark couples directly into the target leading to physical damage. More generally, a least effective coupling can be compensated by an increase of the injected signal amplitude. The effects of EMFI have been shown to be dependent on the location of the probe over the target [DDRT13], therefore a precise and reproducible positioning of the probe is usually achieved with a motorized x-y positioning bench.

Two different kinds of probes are mostly used for EMFI, as shown in Figure 2.9, providing different coupling mechanisms. Inductive coupling is achieved using a loop probe (also sometimes called a magnetic probe [DDR+12]) and impacts conductive loops in the target. Capacitive coupling occurs when using a monopole probe (also called electric probe) and impacts conductive surfaces. In [Ala09], both probe types are compared on a custom test IC (CESAME by ST Microelectronics) for injecting CW signals between 10 MHz and 1 GHz . The most efficient probe orientation observed for the loop probe is when the loop surface is parallel to the IC. The monopole probe was found more efficient when oriented orthogonally to the IC surface. In this study, the efficiency of the monopole probe was interestingly found better than the loop probe.



(a) Capacitive coupling probe [MPT+11] (b) Inductive coupling probes [LEHBT21]

Figure 2.9 – Example probes for radiated near-field EMFI

Similarly to conducted fault injection, signals fed into the probes are usually harmonic (composed of a single frequency CW) or single pulses. Harmonic injection is optimized by tuning the CW amplitude and frequency, which may depend on the target physical (electrical) topology and on the targeted function. The CESAME custom test IC implementing a ring oscillator is perturbated by an near-field capacitive EMFI in [MPT+11]. A 1 GHz CW between −20 dBm (10 nW) and 8.22 dBm (7 mW) is injected and results in an output frequency shift of the ring oscillator by an offset proportional to the injected power level. Ring oscillators were further investigated in [BBA+12], with the same injection setup, on a FPGA implementation. In this case, injected signal frequency was chosen close to the ring oscillators output frequency with a power set successively to 34 nW, 340 µW, 1 mW, 3 mW. Harmonic EMFI setups generally consist in a CW signal generator, an amplifier, a directional coupler for the measurement of forward and backward power and a near field probe [Ala09].

Pulsed EMFI is performed with barely the same setup. The signal source is usually a high voltage pulse generator which delivers the injection signal to the near field probe. Pulse generators can be laboratory grade equipment, such as the Keysight 33509B used in [CB19] but low cost equipment has also been proposed recently. In [AH20], an overview of laboratory grade and home made pulse generation devices is given. The design of a finely tunable pulse generation electronic device is proposed, which can be USB powered and provides pulses up to 1200 V and total width of 400 ns.

Software-based injection

Lately, several studies have shown the possibility to obtain physical faults by software-only interactions. An attack class has been called Rowhammer and targets dynamic random access memory (DRAM) components. By keeping DRAM memory lines activated by repeated reads at high frequency, the capacitors of adjacent lines can discharge faster than the target refresh time. This leads

to bit-flips in the data stored in these adjacent lines [Tro21]. This class of attacks has been proposed in [Goo15, SD15] demonstrating privilege escalation on the Linux kernel. A remote exploitation from Javascript code has been proposed in [GMM16].

Another approach takes advantage of the possibility for an attacker executing low privilege software to interact with internal energy management engines in modern SoCs, which implement a feature called dynamic voltage and frequency scaling which allows to finely control the operating voltage and frequency of each core. In [TSS17], the power management subsystem of an ARM IC has been leveraged to modify the operating frequency of a core and obtain faults, leading to a compromise of the security of ARM trusted execution environment. The same approach has been transposed to compromise the Intel secure enclave (SGX) in [MOG+20], where the faults are obtained by reducing the operating voltage of one of the cores.

For some SoC, the energy management engine can also expose a (hardware) communication interface allowing for configuration from another IC. This feature is exploited in [CVM+21] on Intel platforms targeting the SGX, with faults caused by dropping the nominal 1 V voltage by 200 mV. In [BJKS21], on AMD for compromising the secure encrypted virtualisation mechanism with roughly the same undervoltage characteristics.

2.3.2 Considerations for threat models

EMFI can be achieved by several injection methods and therefore, the threat models can vary slightly. The targets are always an IC implementing a software or hardware security feature. The attacker is therefore assumed to have a direct physical access to the target IC providing a full control of the electromagnetic environment, whether conducted (on the IC IO interfaces) or radiated (usually in the near-field).

Targets

Microcontrollers were among the first investigated targets because of their widespread in smart cards [SH07]. Effects of voltage glitching on a MSP430 have been studied in [BFP19] to bypass code readout protections and [DDR+12] attacked a software implementation of AES on a 3.6 MHz AVR microcontroller unit (MCU).

FPGA components have also been extensively used for fault injection testing. Several random number generation circuits have been implemented on FPGA and attacked [BBA+12, HKLEH16, Mad19, MAB+18]. Hardware cryptographic algorithms were also tested on FPGA against EMFI, as in [ZDCT13, DDRT12] where hardware implementations of AES were attacked on Xilinx Spartan

3. In [O'F17], intrinsic functionality of a Xilinx Spartan 6 has been tested and corruption of data registers and configuration registers has been shown.

Understanding and exploiting effects of EMFI on complex targets such as SoCs has also been investigated lately. Several ARM Cortex A/M devices have been studied, like the STM32F1 family [BFP19, CB19], Espressif ESP32 [Res19], Silabs EFM32 Gecko [Res21], Nordic NRF52 [Res20b], BeagleBone [Hum14], [TM17], Broadcom BCM2837 and BCM2711bo [Tro21]. Microprocessors have also been targeted such as Intel Core i3 [Tro21] and AMD Epyc Zen 3 [BJKS21].

In order to analyze specific mechanisms involved in the occurrence or the propagation of EMFI, dedicated application specific integrated circuit (ASIC) prototypes have been built and targeted [Ala09, MPT+11].

Finally, in [Ame15], Atmel AT25512 and Microchip 25LC512 flash memory ICs have been studied. State registers and stored data have been corrupted by a conducted injection of high frequency (HF) signals into power and clock pins.

Action on target

When performing EMFI on a target IC, several interactions involving the attacker and the target are usually considered as necessary and which can be significant for the definition of threat models and attack scenarios.

First, the injection vector is significant. As shown in 2.3.1, the perturbation signal can be injected from a software or a hardware interaction. Furthermore, in case of hardware interaction, the attacker is always assumed to have a direct physical access to the target's environment. In case of conducted injection the attacker is in control at PCB level and can inject stimuli directly into IOs of the IC. In case of radiated injection, approaches involve near-field coupling between the target and the injection antenna. This physical access assumption also gives the opportunity to modify the target's environment in order to increase the injection efficiency. For conducted injection, decoupling capacitors can be extracted from the PCB as in [Res19]. RF shields can also be removed to allow for positioning of the injection probe closer to the IC package.

In order to perform a characterization of a target or to prototype an attack, a feedback channel is necessary. The information needed relates to the occurrence of a fault and/or the success of the attack. As an example, in [Res20b] the feedback is simply a UART output providing debug information during the boot process of the target. In [Ala09], the amplitude and frequency of an output signal are monitored. In [TM17], the attacker has both a software access and a hardware access, the fault injection is considered successful if the software privilege escalation is achieved.

Another important aspect of EMFI threat model is the need for a synchronization between the execution of the target security function and the fault injection. When the effect of the injection is transient, it might be necessary to wisely choose the moment of injection relatively to the target's activity. The needed precision for the synchronization can vary but the right time to inject is one of the parameters that the attacker has to determine to be successful. Most of the time, it is considered that the attacker targets a logical security function (e.g. the generation of a random sequence by digital logic or the software verification on a PIN code) that can be triggered or that happens permanently. When the attacker can trigger the processing of security function, the moment of injection is usually considered as a delay from the trigger time. When physical access is assumed, the attacker can perform all kinds of measurement in order to get a better synchronization. The target's power consumption is often observed and used for synchronization [Res21], or the clock activity [ZDCT13].

2.3.3 Characterization

In order to be able to profile an attack, an attacker has to determine how the target security function reacts to the injected signal. Similarly, to understand the mechanisms involved in the fault process, a security analyst is interested in identifying the target response. Such steps are referred to as the characterization.

The main goal of this characterization is to exhibit the relationships between the injection parameters and the target response. From these observations, several outcomes can be interesting for the analyst. Determining efficient injection parameters provides information about the attacker profile, i.e. the operational preconditions and the attacker strength in terms of equipment, knowledge needed to obtain specific faults. Determining the different ways a target reacts to fault injection provides information about the potential operational impacts and the exploitability, i.e. the ways an attacker can use the effects of faults to circumvent security functions. Analyzing how injection parameters relate to the target's reaction provides information about the mechanisms involved in the fault injection phenomena, the physical interaction of the injected signal with the target, the cascaded propagation of effects within the target and across layers, from the hardware to the software.

Many challenges arise during the characterization. First, characterizing the injection involves a wide set of parameters to settle [Mad19]:

- the injection type (conducted, radiated)
- the waveform type (pulse, CW, modulation)
- the waveform amplitude

- the waveform repetition rate
- the waveform spectral characteristics (e.g. pulse width, rise and fall time)
- the injection probe
- the position of the probe (injection interface or 3D position over the IC)
- the injection moment relatively to the target's activity

The injection type, waveform characteristics and the injection probe are usually limitations related to the equipment available to the analyst and are therefore often fixed constraints. The position of the probe in the radiated case is usually determined by performing several experiments at different positions over the target and resulting in a fault cartography. This kind of heat map provide a statistical viewpoint about the positions providing the highest probability of obtaining a fault, as illustrated in Fig. 2.10.

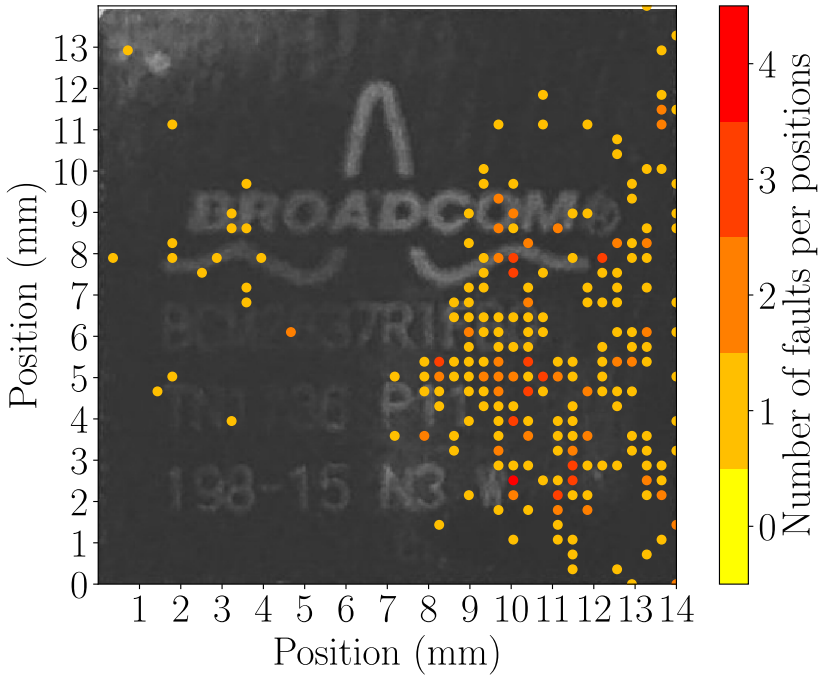


Figure 2.10 – Fault cartography of a BCM2837 from [Tro21]

As this step can be time consuming, a strategy for accelerating this process based on the reciprocity principle in electromagnetism was proposed in [Mad19]. The idea is to perform a cartography of the EM emissions of the target and to focus on the most active positions during the fault cartography. More precisely, it was proposed to focus on areas with high EM emissions at the clock frequency harmonics, based on the hypothesis that D-type flip-flops are likely to be the most sensitive elements to fault injection. This approach, however, tends to discard positions where emissions are low but

which are likely to whether allow an efficient coupling of signals at other frequencies or convey a parasitic signal to sensitive parts of the IC.

Another technical and scientific challenge in this process relates to the observation of the fault occurrence. Indeed, in order to determine which are the effects of the fault injection on the target, one needs to set up a measurement method. But on the other hand, to set up a measurement method, it is necessary to know what kind of effects are expected. This is where fault models are considered.

Fault models

The fault model of a target is the set of the possible types of faults that can occur on this target related to their probability of occurrence [PCNM15]. Among the fault zoology on the most elementary informational elements in the logical layer, the most commonly considered parameters are [KSV13]:

- the fault size: bit-level, word-level
- the effect: stuck-at fault, bit-flip, set, reset, randomization
- the duration: transient, permanent

The fault model also tends to capture the elements that are affected by the fault occurrence. However, complex digital devices have an architecture with many abstraction layers and impacts of faults can be interpreted differently depending on the considered layer [Tro21, YSW18] as illustrated in Figure 2.11.

In [Mad19], fault models are categorized according to a simplified view of these abstraction layers: software fault models and hardware fault models. Hardware fault models are focused on the effect of the parasitic signals on the digital logic. Several studies have considered that the voltage variations due to the EM perturbation were modifying the propagation time of signals through the digital logic. As an outcome, timing constraint violations were believed to be the root cause of the faults obtained on the upper layers [O'F17, Zus14, ZDC+12]. This fault model has been reconsidered by recent work [OGM17] and another perturbation mechanism at the digital logic layer has been considered: the sampling fault model [Dum20, DLM19]. In this model, a maximal susceptibility window located around the clock rising edges is considered as the moment when the D-type flip-flops are the most likely to sample an erroneous value in the presence of parasitic signals on their power, clock or input ports.

Software fault models focus on the impact of EMFI on software execution. In [KSV13], the main categories are listed and an up-to-date exhaustive state of the art is provided in [Tro21].

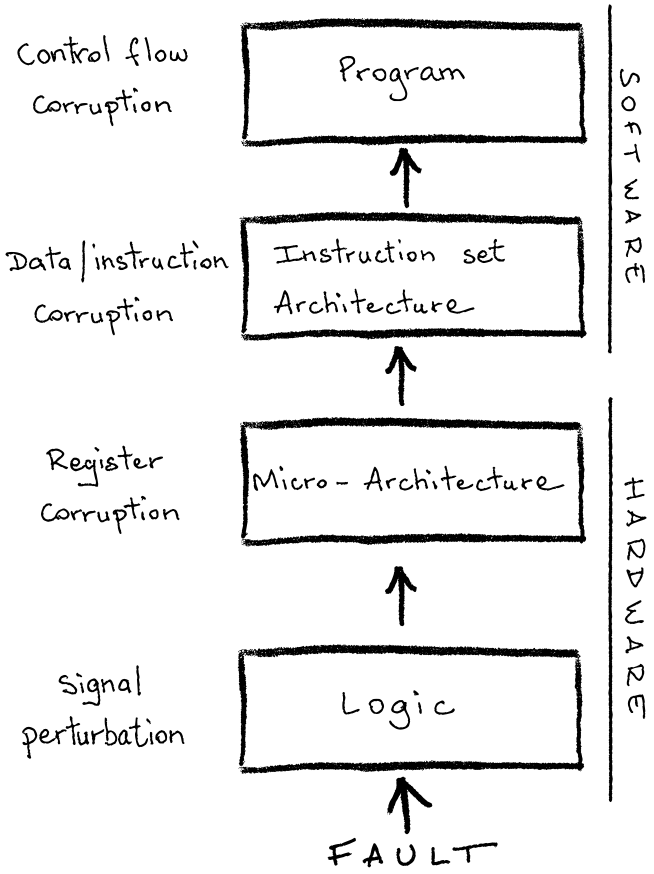


Figure 2.11 – Fault propagation and effects (adapted from [Tro21])

- Effects on storage: data and instructions may be stored in both volatile and non volatile memory and their integrity can be compromised
- Effects on data processing: data can be impacted during software computation, resulting in erroneous intermediate or final result
- Effects on control flow: instructions can be modified or skipped

Fault models are a very useful approach to help understand the complex mechanisms involved in the propagation of the physical stimuli to the informational layers, to design countermeasures and to analyze the exploitability of the faults on specific software.

The characterization process complexity can usually be reduced to an exploration of known fault models using dedicated testing software on the target. Storage fault models are usually tested with software which repeatedly writes and reads data in memory and verifies data integrity. Faults can occur during read/write operations or be performed on static data. This approach has been followed in [O'F17] on FPGA configuration data and [Ame15] on flash memory IC. Effects on data processing and control flow are more challenging to discriminate and test. Test software with a lot of *nop* equivalent instructions can be used [Tro21], programs which increment counters within cascaded loops are also pretty common [O'F17] and a proof of concept code snippet of a PIN code verification (usually called "verifyPIN") can be considered as the "hello world" (e.g. in [CB19]) of fault characterization.

2.3.4 Exploitation

In this section, a focus is made on the exploitation of faults by an attacker on a target device. More precisely, an overview of the type of achievements that can be obtained by an attacker, i.e. the security functions that can be circumvented, using the logical impacts of a fault injection.

Different approaches will be emphasized here: a practical approach and a more theoretical one. Indeed, a pragmatic attacker can perform the characterization directly on the security function he is trying to evaluate. In this case, the goal is no longer to obtain fault models but rather to tune the injection parameters to perform an attack. On the other hand, it is also possible to design attacks on security functions based on fault models, an approach which is both more generic and theoretical. Sometimes, this approach is practically validated against a real target.

Physical cryptanalysis

Interestingly, early works mentioning the exploitation of hardware faults in an information security context were theoretical and focused on physical cryptanalysis. The physical cryptanalysis using

faults is called fault analysis and can be defined as a class of implementation attacks that consists in disturbing cryptographic computations to recover secret keys [Riv09]. Attacks have been proposed on several symmetric and asymmetric cryptographic primitives. In [BS97], a differential fault analysis (DFA) is applied to DES. The main principle is to infer information about the secret key by exploiting differences between correct and faulty ciphertexts of the same plaintext, based on the assumption on a fault model. AES has also been extensively exploited by DFA, as practically demonstrated in [DDRT13] on an FPGA implementation. The first attack on RSA was called the "Bellcore attack" [BDL97], which allows to break a specific implementation of RSA (RSA-CRT) with a single faulty computation. Fault analysis was also applied to elliptic curve cryptosystems [BMM00].

TRNG biasing

Random number generation, and more precisely hardware implementations of TRNG have been successfully attacked with EMFI. The expected result for the attacker is the introduction of a bias in the random sequence produced reducing its entropy. An explicit illustration of such attacks can be found in [BBA+12], where the implementation of a ring-oscillator based TRNG on a FPGA is attacked with a near-field harmonic signal. In this study, the bias of the random sequence could be controlled in such a way to write the COSADE conference name, as shown in Fig. 2.12.

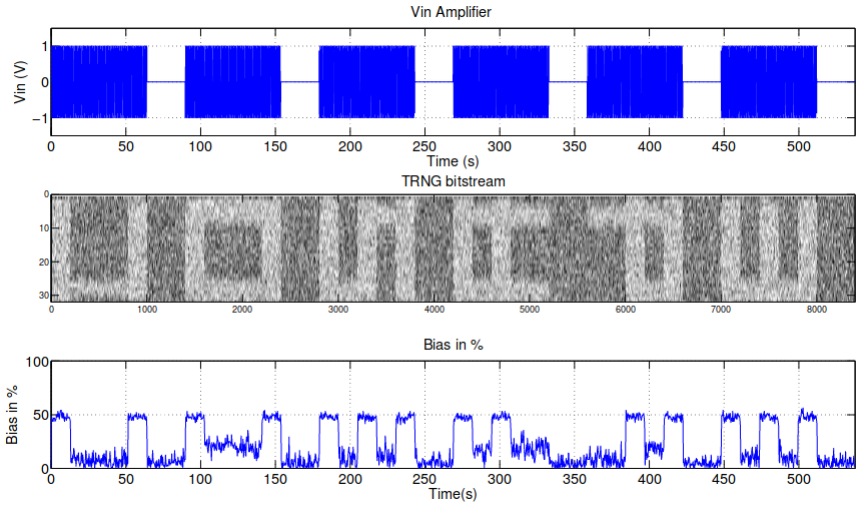


Figure 2.12 – Controlling the entropy of a TRNG with harmonic EMFI [BBA+12]

The threat of pulsed EMFI against a delay chain TRNG has been evaluated in [MAB+18] and resulted in the demonstration of an attack on a masked implementation of AES, which protects against side channel attacks using the TRNG as a source of randomness.

Privilege escalation

Recent work focused on EMFI targeting complex SoCs. Such targets have the capacity to run rich multi-application and multi-user operating systems enforcing specific security functions. A privilege escalation is an attack which aims at bringing the execution of a process from a lower privilege context (e.g. simple user) to a higher privilege context (e.g. administrator). In [TM17], conducted voltage fault injection is used on an ARM Cortex-A9 processor SoC running Ubuntu 16.04 and several privilege escalation attacks are shown, including the case of an unprivileged application to start a root shell. In all cases, the Linux kernel mechanism that verifies that the privilege level of the process asking to execute privileged functions is supposed to be corrupted, with overall success rate less than 0.1%. A radiated EMFI has been used by [GAP+20] to corrupt password verification on a Linux running on a ARM Cortex-53 based SoC.

Secure boot bypass

Secure boot is a security function which aims at providing trust in the application layer code that is executed by performing verification on the authenticity of the code loaded and executed during all boot stages on SoCs. In [TSW16], a fault induces a corruption of a code loading stage and leads to the charge of an attacker controlled address into the program counter, leading to the execution of attacker controlled code. Other examples of secure boot bypass can be found in [Res19] on Espressif ESP32 or in [BR15, Gli22] on the XBOX360. In [pdn17], conducted EMFI on the central processing unit (CPU) power IO led to a fault skipping the verification of the authenticity of loaded code, allowing attackers to execute their own code, extract and decipher firmware and bootrom on the Nintendo Switch.

Debug access bypass

SoCs expose programming (e.g. In-System Programming (ISP)) and debug (e.g. On-Chip Debugging (OCD)) interfaces in order to allow configuration, firmware code update and prototyping. Access to those interfaces can give an attacker a significant advantage to gain access to firmware binaries, user and configuration data and sometimes full control over the code execution. Depending on the SoC model, access to those interfaces can be disabled or inhibited (e.g. in the case of Code Readout Protection (CRP)), usually by setting a specific value into a register. In [Res20b], a voltage glitch is used on an nRF52840 with the APPROTECT feature enabled, gaining full debug capabilities on the target. The same results were then obtained on other nRF52xx targets. In [BFP19], CRP is

bypassed on a STM32F103 and an STM32F373 with a conducted EMFI on power supply, leading to an extraction of the firmware binary. With the same approach, the password protected readout mechanism of a MSP430F5172 and a MSP430FR5725 was bypassed.

Memory leak

EMFI has also been exploited to trigger software bugs which resulted in leaking to the attacker portions of memory which were not supposed to be revealed. A good example of this class of exploitation is the study detailed in [O'F19] in which a Trezor hardware wallet and a solo key USB security key are attacked with radiated EMFI during the processing of the routine building the response to a standard USB command in which the response length is provided. The fault seems to bypass the length check, resulting in a response returning much more data than necessary. This way, data from adjacent memory blocks is leaked, revealing cryptographic secrets in both cases. Other examples can be found in [Sco16] and [BFP19] where voltage glitching lead to extraction of firmware binary code.

2.3.5 Countermeasures

Generally speaking, countermeasures usually belong to one of the following categories:

- Correcting the vulnerability: the root cause of the vulnerability is eliminated;
- Reducing the attack surface: remove the access to a path enabling exploitation;
- Increasing attacker profile: the preconditions and the effort level necessary to exploit the vulnerability are increased;
- Reducing impacts: the gain for the attacker gets more limited;
- Detecting the attack.

Shielding

Shielding can be used as a countermeasure against radiated EMFI. The idea is to reduce the efficiency of the coupling of the attacker's injection probe with the conductive parts of the target. The shield integrity can be monitored continuously by the target by measuring impedance changes (for passive shields) or signal integrity (for active shields). Thus the attacker is forced to compensate the coupling efficiency loss by increasing the source capacities (e.g. power amplification) or by reducing the distance between the probe and the target (e.g. decapsulation, shield removal).

Sensors

If an fault injection can be detected, it is possible to take actions to eliminate the impact of the fault (by discarding a faulty result and doing another computation) or to take protective actions (e.g. erasing secrets). Several approaches imply the implantation of analog or digital sensors into the target IC to detect fault injection or fault effects. Radiated fault injection can be detected using antennas or extra bonding wires [Dum20]. Some perturbations on power an clock signals can be detected using digital voltage monitors [ZDT+14]. Phase variations can be detected with analog phase detectors and phase locked loops [Mad19]. As D-type flip-flops have been shown to be impacted by faults according to the sampling fault model and the timing constraint violation fault model, it has been proposed to use them as the building block for a fully digital EMFI detector [ERM16]. However, as stated in [Tro21], sensors suffer many trade-offs, on the calibration, on the efficiency, on the implantation cost.

Redundancy

Redundancy is a pretty common countermeasure against faults in general, it is naturally applicable to fault attacks. The main principle here is to perform the same (critical) computation several times (usually two or three times) and to compare results or to select the correct (not faulty) result. Redundancy can be done in hardware or in software and can be done in parallel or sequentially. In hardware, this often means duplicating circuit paths or registers. This redundancy can also be applied to data, with error correcting codes for example.

Control flow integrity

As EMFI has been shown to potentially impact software execution, techniques aiming at detecting unexpected modifications of the execution flow at runtime were proposed in the context of EMFI detection. The main principle is to insert mechanisms to verify that critical steps in an algorithm have not been skipped and are executed in the right order. Approaches are based on the signature of code blocks and involve a verification to be integrated to the operating system or a virtual machine executing the code. Other approaches can be simply inserted into the code, such as the insertion of step counters. An overview of such techniques is proposed in [Mad19, Tro21]. Some effort is made to integrate some of these countermeasures during software compilation.

Exploitation-specific countermeasures

Instead of being somehow generic, countermeasures can also focus on a specific exploitation scenario. For example, infection programming focuses on countering differential fault analysis by complementing code redundancy in order to diffuse information leakage in the faulty ciphertexts[LRT12]. According to [Mad19], there is no viable infective programming scheme. Adding randomness in the execution can raise difficulty in the characterization phase and for fault injection synchronization. Using code polymorphism has been proposed to this end; e.g. in [CRL+14].

2.3.6 Forensics

Most effort about the detection of EMFI is done at runtime, as discussed in the above paragraphs. As studies are focused on component security, the determination of the occurrence of an EMFI based attack in the post exploitation phase seems to be out of focus. However, ways of using EMFI during a forensic analysis process in order to provide ways to access protected data has been considered. In [GAP+20], the possibility of benefiting from EMFI originated secure boot bypass or privilege escalation is envisioned.

2.4 Conclusion

In this chapter, an overview of EMFI and IEMI, two research fields focused on the intentional use EM perturbation on electronic devices, has been given.

EMFI is a cybersecurity discipline dedicated to the investigation of attacks and defenses on ICs. The attacker is assumed to have a physical access to the target, enabling a preparation of the target's functional environment (e.g., PCB), physical measurements and a precise synchronization to the target's activity. The EM interactions are near-field over a localized area of the target, or conducted through the IO interfaces of the IC. Attack waveforms are mostly pulses, which are believed to target digital parts, and CW, for targeting analog functions.

Fault models are used to analyze, detect, identify and classify effects of EMFI on the target from the viewpoint of a chosen observation layer (e.g., physical layer, logic, micro-architecture). Using fault models also facilitates the investigation of exploitation techniques relying on the observed effects. From an IC security viewpoint, detection is only meaningful if it is done in real time and triggers immediate protection. Thus, forensic analysis is not really considered in research on EMFI.

The study of IEMI is an EMC related field and it stems from EMC methodology. The attacker is considered as being at a variable distance from the target, potentially meters or kilometers away. This

implies a wide variety of potential sources and EM environments which increases the complexity of the dimensioning of the EMC problem. A consequence of this complexity is visible in the tailored test level derivation guidance, which requires the determination of the EM environment from the operational deployment context (i.e., the practical conditions in which the target will evolve). The failure criteria can be measured currents, voltages or EM fields on the target or effects impacting the availability of the main function of the target. This makes the standard susceptibility assessment unfit for security analysis. However, recently, in the context of sensor security, new attacks involving IEMI were proposed, with an attacker which can be closer to the target and use sources with less power. Detection is considered in the standard as a protective measure with the help of devices external to the target. Sensor security researchers proposed detection techniques included in the target.

Several perspectives arise from this comparison, regarding threat models and effects assessment methods.

The threat models in EMFI assume an attacker having literally a physical access to the target IC. Attacks may require a precise synchronization in time and a precise localization of the perturbation in space. In IEMI, the attacker is distant from the target electronic parts and several obstacles can be considered. As shown in the recent studies in sensor security involving EMI, there is room for intermediate scenarios, where the attacker is no longer in contact with the IC but still close enough to have a chance to synchronize and use low or medium power sources. This opens the way to investigation around the possibility of extending the range of EMFI.

Concerning the attack waveforms, IEMI considers a wider range of possibilities, with hypoband, mesoband and hyperband categories. EMFI considers mainly two approaches, CW and baseband pulses. It might be relevant to extend EMFI to other waveforms. Furthermore, for the characterization step, the IEMI approach consisting in identifying resonant frequencies of the target might allow for a simplification of the attack waveforms. Indeed, EMFI wide band pulses are known to impact digital logic, but it would be relevant to investigate the possibility of triggering the same effects with simpler waveforms composed of narrow band signals focusing on specific resonant frequencies. Such simplification would then enable a simpler modeling of the physical phenomena and a decrease of the source complexity.

To overcome remaining challenges such as synchronization and localization of the EM interactions, several leads could be pursued. A first exploration of the possibility to achieve a conducted EMFI via a radiated or conducted IEMI from on a product with a shielded enclosure might be interesting. For synchronization, the exploitation of EM emissions or interactions with RF front-ends might provide a way to achieve longer distances. Modifications of the physical environment of the

target, by changing the enclosure or by adding hardware implants might also be worth investigating as means to focus fields to precise areas.

Security assessment of complex targets against IEMI might also benefit from EMFI approaches. For IEMI, susceptibility testing is specific to the target functional and operational deployment scenario. Fault models used in the characterization steps against EMFI provide a generic way to model the effects on the target IC, without depending on the production software or the operational conditions in which the target will be put in. This approach, applied to IEMI susceptibility testing, might provide a basis for a better use of test results in an InfoSec analysis.

2.5 References

[ABC+17] Stéphanie Anceau, Pierre Bleuet, Jessy Clédière, Laurent Maingault, Jean-luc Rainard, and Rémi Tucoulou. Nanofocused X-Ray Beam to Reprogram Secure Circuits. In Wieland Fischer and Naofumi Homma, editors, *Cryptographic Hardware and Embedded Systems – CHES 2017*, Lecture Notes in Computer Science, pages 175–188, Cham, 2017. Springer International Publishing. 52

[AH20] Karim M. Abdellatif and Olivier Hériveaux. SiliconToaster: A Cheap and Programmable EM Injector for Extracting Secrets. In *2020 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*, pages 35–40, 2020. 56

[AK96] Ross Anderson and Markus Kuhn. Tamper resistance-a cautionary note. In *Proceedings of the Second Usenix Workshop on Electronic Commerce*, volume 2, pages 1–11, 1996. 53

[Ala09] Ali Alaeldine. *Contribution à l'étude Des Méthodes de Modélisation de l'immunité Électromagnétique Des Circuits Intégrés*. These de doctorat, Rennes, INSA, 2009. 55, 56, 58

[Ame15] Mohamed Amellal. *Electromagnetic Immunity Modeling of Components for the Obsolescence Management of Systems and Electronic Modules*. PhD thesis, INSA de Rennes, 2015. 41, 54, 58, 63

[ASP+14] Christian Adami, Michael Suhrke, Thorsten Pusch, Michael Joester, Nikita Kolosnev, Georg Neubauer, and Alexander Preinerstorfer. Investigation of the impact of various IEMI sources to electronic passport readers. In *Future Security 2014*, pages 430–436, Berlin, Germany, 2014. 46

[Bac17] Yann Bacher. *Study and Modelling of the Disturbances Produced within the STM32 Microcontrollers under Pulsed Stresses*. Theses, Université Côte d'Azur, 2017. 41

[BBA+12] Pierre Bayon, Lilian Bossuet, Alain Aubert, Viktor Fischer, François Poucheret, Bruno Robisson, and Philippe Maurine. Contactless electromagnetic active attack on ring oscillator based true random number generator. In W. Schindler and S. A. Huss, editors, *COSADE: Constructive Side-Channel Analysis and Secure Design*, volume LNCS of *Constructive Side-Channel Analysis and Secure Design*, pages 151–166, Darmstadt, Germany, 2012. 56, 57, 64

[BDL97] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the importance of checking cryptographic protocols for faults (extended abstract). In Walter Fumy, editor, *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding*, volume 1233 of *Lecture Notes in Computer Science*, pages 37–51. Springer, 1997. 64

[BDRS06] Sonia Ben Dhia, Mohamed Ramdani, and Etienne Sicard, editors. *Electromagnetic Compatibility of Integrated Circuits: Techniques for Low Emission and Susceptibility*. Springer US, Boston, MA, 2006. 43

[BFP19] Claudio Bozzato, Riccardo Focardi, and Francesco Palmarini. Shaping the Glitch: Optimizing Voltage Fault Injection Attacks. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 199–224, 2019. 54, 57, 58, 65, 66

[BJKS21] Robert Buhren, Hans-Niklas Jacob, Thilo Krachenfels, and Jean-Pierre Seifert. One Glitch to Rule Them All: Fault Injection Attacks Against AMD's Secure Encrypted Virtualization. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, CCS '21, pages 2875–2889, New York, NY, USA, 2021. Association for Computing Machinery. 57, 58

[BL04] M. G. Backstrom and K. G. Lovstrand. Susceptibility of electronic systems to high-power microwaves: Summary of test experience. *IEEE Transactions on Electromagnetic Compatibility*, 46(3):396–403, 2004. 41, 45

[BMM00] Ingrid Biehl, Bernd Meyer, and Volker Müller. Differential Fault Attacks on Elliptic Curve Cryptosystems. In Mihir Bellare, editor, *Advances in Cryptology — CRYPTO 2000*, pages 131–146, Berlin, Heidelberg, 2000. Springer. 64

[BR15] Ryad Benadjila and Mathieu Renard. Stratégies de défense et d'attaque : Le cas des consoles de jeux. In *Symposium Sur La Sécurité Des Technologies de l'Information et Des Communications (SSTIC)*, Rennes, France, 2015. 65

[BS97] Eli Biham and Adi Shamir. Differential fault analysis of secret key cryptosystems. In Burton S. Kaliski, editor, *Advances in Cryptology — CRYPTO '97*, pages 513–525, Berlin, Heidelberg, 1997. Springer. 64

[CB19] Ludovic Claudepierre and Philippe Besnier. Microcontroller Sensitivity to Fault-Injection Induced by Near-Field Electromagnetic Interference. In *APEMC 2019 - Asia-Pacific International Symposium on Electromagnetic Compatibility*, pages 1–4, Sapporo, Japan, 2019. 56, 58, 63

[CRL+14] Damien Couroussé, Bruno Robisson, Jean-Louis Lanet, Thierno Barry, Hassan Noura, Philippe Jaillon, and Philippe Lalevee. COGITO: Code polymorphism to secure devices. In *SECRYPT2014 : 11th International Conference on Security and Cryptography*, page 6p, Vienne, Austria, 2014. 68

[CVM+21] Zitai Chen, Georgios Vasilakis, Kit Murdock, Edward Dean, David Oswald, and Flavio D. Garcia. VoltPillager: Hardware-based fault injection attacks against Intel SGX Enclaves using the SVID voltage scaling interface. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 2021. 57

[CZCW18] Yazhou Chen, Dongxiao Zhang, Erwei Cheng, and Xiaojia Wang. Investigation on susceptibility of UAV to radiated IEMI. In *2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC)*, pages 718–722, 2018. 41

[DAY22] Donghui Dai, Zhenlin An, and Lei Yang. Inducing wireless chargers to voice out. In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, MobiCom '22, pages 808–810, New York, NY, USA, 2022. Association for Computing Machinery. 48

[DDR+12] A. Dehbaoui, J. M. Dutertre, B. Robisson, P. Orsatelli, P. Maurine, and A. Tria. Injection of transient faults using electromagnetic pulses -Practical results on a cryptographic system-. Technical Report 123, 2012. 55, 57

[DDRT12] Amine Dehbaoui, Jean-Max Dutertre, Bruno Robisson, and Assia Tria. Electromagnetic Transient Faults Injection on a hardware and software implementations of AES. In *FDTC 2012*, page 7, Leuven, Belgium, 2012. 57

[DDRT13] A. Dehbaoui, J. M. Dutertre, B. Robisson, and A. Tria. Investigation of near-field pulsed EMI at IC level. In *2013 Asia-Pacific Symposium on Electromagnetic Compatibility (APEMC)*, pages 1–4, 2013. 55, 64

[DFK+14] J F Dawson, I D Flintoft, P Kortoci, L Dawson, A C Marvin, M P Robinson, Mirjana Stojilovic, Marcos Rubinstein, Benjamin Menssen, Heyno Garbe, Werner Hirschi, and Loubna Rouiller. A Cost-Efficient System for Detecting an Intentional Electromagnetic Interference (IEMI) attack. In *2014 International Symposium on Electromagnetic Compatibility*, pages 1252–1256, 2014. 51

[DLM19] Mathieu Dumont, Mathieu Lisart, and Philippe Maurine. Electromagnetic Fault Injection : How Faults Occur. In *2019 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 9–16, 2019. 61

[DMGM22] Gökçen Yılmaz Dayanıklı, Abdullah Zubair Mohammed, Ryan Gerdes, and Mani Mina. Wireless Manipulation of Serial Communication. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '22, pages 222–236, New York, NY, USA, 2022. Association for Computing Machinery. 47

[DSM+22] Gökçen Yılmaz Dayanıklı, Sourav Sinha, Devaprakash Muniraj, Ryan M. Gerdes, Mazen Farhood, and Mani Mina. Physical-Layer attacks against pulse width Modulation-Controlled actuators. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 953–970, Boston, MA, 2022. USENIX Association. 49

[Dub11] Tristan Dubois. Etude de formes d'onde d'agressions électromagnétiques hyperfréquences sur la vulnérabilité de circuits électroniques. Post Doctoral, 2011. 41, 46

[Dum20] Mathieu Dumont. *Modélisation de l'injection de Faute Électromagnétique Sur Circuits Intégrés Sécurisés et Contre-Mesures*. These de doctorat, Montpellier, 2020. 51, 55, 61, 67

[ERM16] David El-Baze, Jean-Baptiste Rigaud, and Philippe Maurine. An Embedded Digital Sensor against EM and BB Fault Injection. In *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 78–86, 2016. 67

[EWHR22] Eric Easton, Cyril Wafo, Richard Hoad, and Tim Rees. Real-time Substation Shielding Compromise and HPEM Event detection. In *GLOBALEM 2022*, page 3, Abu Dhabi, UAE, 2022. 51

[GAP+20] Clément Gaine, Driss Aboulkassimi, Simon Pontié, Jean-Pierre Nikolovski, and Jean-Max Dutertre. Electromagnetic Fault Injection as a New Forensic Approach for SoCs. In *2020 IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 1–6, 2020. 65, 68

[GHS20] Dave Giri, Richard Hoad, and Franck Sabath. *High-Power Electromagnetic Effects on Electronic Systems*. Artech House, 2020. 35, 36, 37, 39, 40, 41, 45

[Gli22] GliGli. Gligli/tools. https://github.com/gligli/tools/blob/master/reset_glitch_hack/reset_glitch_hack.txt, 2022. 65

[GMM16] Daniel Gruss, Clémentine Maurice, and Stefan Mangard. Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript. In Juan Caballero, Urko Zurutuza, and Ricardo J. Rodríguez, editors, *Detection of Intrusions and Malware, and Vulnerability Assessment*, Lecture Notes in Computer Science, pages 300–321, Cham, 2016. Springer International Publishing. 57

[Goo15] Google. Project Zero: Exploiting the DRAM rowhammer bug to gain kernel privileges. https://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html, 2015. 57

[GP14] Robert Gardner and Frank Peterkin. RF DEW Scenarios and Threat Analysis. *System Design and Assessment Note SDAN*, 43, 2014. 42

[GP22] Ben Gardiner and Chris Poore. Talking PLC4TRUCKS Remotely with an SDR. In *DefCon 30*, Las Vegas, USA, 2022. 47

[GR19] Ilias Giechaskiel and Kasper Bonne Rasmussen. SoK: Taxonomy and Challenges of Out-of-Band Signal Injection Attacks and Defenses. *arXiv:1901.06935 [cs]*, 2019. 47, 50

[GT94] Dave Giri and Clayborne D. Taylor. *High-Power Microwave Systems and Effects*. A SUMMA Book. Taylor and Francis, Washington, D.C, 1994. 35, 36

[Had15] Patrick Haddad. *Caractérisation et Modélisation de Générateurs de Nombres Aléatoires Dans Les Circuits Intégrés Logiques.* PhD thesis, Université Jean Monnet, Saint Etienne, 2015. 54

[HKLEH16] Patrick Haddad, Chaouki Kasmi, José Lopes Esteves, and Valentin Houchouas. Electromagnetic Harmonic Attack on Transient Effect Ring Oscillator based True Random Generator. In *Hardwear.Io*, The Hague, Netherlands, 2016. 57

[Hoa07] Richard Hoad. *The Utility of Electromagnetic Attack Detection to Information Security*. PhD thesis, University of Glamorgan, 2007. 34, 41, 45

[HRP+22] Richard Hoad, Tim Rees, Barney Petit, Anatoly Krasavin, Grant Hainsworth, and Sam Hole. Real-time Substation Shielding Compromise and HPEM Event detection. In *GLOBALEM 2022*, page 19, Abu Dhabi, UAE, 2022. 51

[HS14] Michael Hutter and Jörn-Marc Schmidt. The Temperature Side Channel and Heating Fault Attacks. In Aurélien Francillon and Pankaj Rohatgi, editors, *Smart Card Research and Advanced Applications*, Lecture Notes in Computer Science, pages 219–235, Cham, 2014. Springer International Publishing. 52

[HTI97] Mei-Chen Hsueh, T.K. Tsai, and R.K. Iyer. Fault injection techniques and tools. *Computer*, 30(4):75–82, 1997. 55

[Hum14] Tim Hummel. *Exploring Effects of Electromagnetic Fault Injection on a 32-Bit High Speed Embedded Device Microprocessor*. 2014. 58

[Int78] Integrated Circuit Electromagnetic Susceptibility Handbook. Technical Report MDC-E1929, McDonnell Douglas Astronautics Company, 1978. 45

[ISO04] ISO/IEC. Electromagnetic compatibility (EMC) - Part 1-5: General - High-power electromagnetic (HPEM) effects on civil systems. Standard ISO/IEC 61000-1-5:2004, International Organization for Standardization, Geneva, CH, 2004. 43, 49, 50

[ISO05] ISO/IEC. Electromagnetic compatibility (EMC) - Part 2-13: Environment - High-power electromagnetic (HPEM) environments - Radiated and conducted. Standard ISO/IEC 61000-2-13:2005, International Organization for Standardization, Geneva, CH, 2005. 35, 37, 38, 39, 42

[ISO09] ISO/IEC. Electromagnetic compatibility (EMC) - Part 5-9: Installation and mitigation guidelines - System level susceptibility assessment for HEMP and HPEM. Standard ISO/IEC 61000-5-9:2009, International Organization for Standardization, Geneva, CH, 2009. 44, 51

[ISO20] ISO/IEC. Electromagnetic compatibility (EMC) - Part 4-36: Testing and measurement techniques – IEMI immunity test methods for equipment and systems. Standard ISO/IEC 61000-4-36:2020, International Organization for Standardization, Geneva, CH, 2020. 35, 37, 39, 42, 43

[JCK+23] Joonha Jang, ManGi Cho, Jaehoon Kim, Dongkwan Kim, and Yongdae Kim. Paralyzing Drones via EMI Signal Injection on Sensory Communication Channels. In *Proceedings 2023 Network and Distributed System Security Symposium*, San Diego, CA, USA, 2023. Internet Society. 47

[JJW+22] Y. Jiang, X. Ji, K. Wang, C. Yan, R. Mitev, A. Sadeghi, and W. Xu. WIGHT: Wired ghost touch attack on capacitive touchscreens. In *2022 IEEE Symposium on Security and Privacy (SP) (SP)*, pages 1537–1537, Los Alamitos, CA, USA, 2022. IEEE Computer Society. 48, 50

[KBC+13] Denis Foo Kune, John Backes, Shane S. Clark, Daniel Kramer, Matthew Reynolds, Kevin Fu, Yongdae Kim, and Wenyuan Xu. Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors. In *2013 IEEE Symposium on Security and Privacy*, pages 145–159, 2013. 47, 48, 50

[KBM22] Sebastian Köhler, Richard Baker, and Ivan Martinovic. Signal Injection Attacks against CCD Image Sensors. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '22, pages 294–308, New York, NY, USA, 2022. Association for Computing Machinery. 47, 48

[KBSM22] Sebastian Köhler, Richard Baker, Martin Strohmeier, and Ivan Martinovic. Brokenwire : Wireless Disruption of CCS Electric Vehicle Charging. In *arXiv:2202.02104 [Cs]*, 2022. 47

[KK99] Oliver Kömmerling and Markus G. Kuhn. Design principles for tamper-resistant smartcard processors. In *Proceedings of the USENIX Workshop on Smartcard Technology on USENIX Workshop on Smartcard Technology*, WOST'99, page 2, USA, 1999. USENIX Association. 52, 55

[KLE15] Chaouki Kasmi and José Lopes Esteves. IEMI threats for information security: Remote command injection on modern smartphones. *IEEE Transactions on Electromagnetic Compatibility*, 57(6):1752–1755, 2015. 36, 48

[KLHY22] Sung-Geon Kim, Euibum Lee, Ic-Pyo Hong, and Jong-Gwan Yook. Review of Intentional Electromagnetic Interference on UAV Sensor Modules and Experimental Study. *Sensors*, 22(6):2384, 2022. 41

[KSG15a] M. Kreitlow, F. Sabath, and H. Garbe. Analysis of IEMI effects on a computer network in a realistic environment. In *2015 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, pages 1063–1067, 2015. 41

[KSG15b] M Kreitlow, F Sabath, and Heyno Garbe. A test method for analysing disturbed ethernet data streams. *Advances in Radio Science 13 (2015)*, 13:149–153, 2015. 41

[KSV13] Duško Karaklajić, Jörn-Marc Schmidt, and Ingrid Verbauwhede. Hardware Designer's Guide to Fault Attacks. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 21(12):2295–2306, 2013. 61

[LA95] R. D. Leach and M. B. Alexander. Electronic systems failures and anomalies attributed to electromagnetic interference, 1995. 35

[LE19] José Lopes Esteves. Electromagnetic Watermarking: Exploiting IEMI effects for forensic tracking of UAVs. In *Electromagnetic Compatibility-EMC EUROPE, 2019 International Symposium On*, Barcelona, Spain, 2019. IEEE. 41

[LECK18] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. Unlocking the Access to the Effects induced by IEMI on a Civilian UAV. In *Electromagnetic Compatibility-EMC EUROPE, 2018 International Symposium On*, Amsterdam, Netherland, 2018. IEEE. 41

[Lee86] K. S. H. Lee. *EMP Interaction: Principles, Techniques, and Reference Data (Revised Edition)*. A SUMMA Book. Hemisphere Publishing Corporation, 1986. 35, 36

[LEHBT21] José Lopes Esteves, Valentin Houchouas, Guillaume Bouffard, and Thomas Trouchkine. Caractérisation d'antennes pour l'injection de fautes sur composants électroniques. In *Conférence Plénière Du GDR Ondes*, Lille, France, 2021. 56

[LEK18] José Lopes Esteves and Chaouki Kasmi. Remote and Silent Voice Command Injection on a Smartphone through Conducted IEMI: Threats of Smart IEMI for Information Security. *System Design and Assessment Note SDAN*, 48, 2018. 48

[LEKA+21] José Lopes Esteves, Chaouki Kasmi, Luk Arnaut, Pierre Degauque, Virginie Deniau, Dave Giri, Gabriele Gradoni, Frank Gronwald, Masashi Hayakawa, Yasuhide Hobara, Farhad Rachidi, William A. Radasky, and Marcos Rubinstein. 100 Years of URSI: The Past, Present, and Future of Commission E. In *100 Years of the International Union of Radio Science*, pages 467–498. URSI Press, Gent, Belgium, p. wilkinson, p.s. cannon, w.r. stone edition, 2021. 35

[LLLS20] Grzegorz Lubkowski, Marian Lanzrath, Louis Cesbron Lavau, and Michael Suhrke. Response of the UAV Sensor System to HPEM Attacks. In *2020 International Symposium on Electromagnetic Compatibility - EMC EUROPE*, pages 1–6, 2020. 41

[LRT12] Victor Lomné, Thomas Roche, and Adrian Thillard. On the Need of Randomness in Fault Attack Countermeasures - Application to AES. In *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 85–94, 2012. 68

[MAB+18] M. Madau, M. Agoyan, J. Balasch, M. Grujić, P. Haddad, P. Maurine, V. Rožić, D. Singelée, B. Yang, and I. Verbauwhede. The Impact of Pulsed Electromagnetic Fault Injection on True Random Number Generators. In *2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 43–48, 2018. 57, 64

[Mad19] Maxime Madau. *A Methodology to Localise EMFI Areas on Microcontrollers*. These de doctorat, Montpellier, 2019. 55, 57, 59, 60, 61, 67, 68

[Mar18] Alexandre Martorell. *Détection à Distance d'électroniques Par l'intermodulation*. PhD thesis, Montpellier, 2018. 47

[Mej19] Guillaume Mejecaze. *Analyse des destructions d'alimentations électroniques soumises à un courant impulsionnel fort niveau*. PhD thesis, Université de Bordeaux, 2019. 41, 43, 44, 45, 46

[MNTB07] Daniel Mansson, Tony Nilsson, Rajeev Thottappillil, and Mats Backstrom. Propagation of UWB Transients in Low-Voltage Installation Power Cables. *IEEE Transactions on Electromagnetic Compatibility*, 49(3):585–592, 2007. 42

[MOG+20] Kit Murdock, David Oswald, Flavio D. Garcia, Jo Van Bulck, Daniel Gruss, and Frank Piessens. Plundervolt: Software-based fault injection attacks against intel SGX. In *41st IEEE Symposium on Security and Privacy (S&P'20)*, 2020. 57

[MP16] Nicolas Mora Parra. *Contribution to the Study of the Vulnerability of Critical Systems to Intentional Electromagnetic Interference (IEMI)*. PhD thesis, EPFL, Lausanne, 2016. 36, 39, 40, 45

[MPT+11] Philippe Maurine, François Poucheret, Karim Tobich, Mathieu Lisart, Bruno Robisson, and Laurent Chusseau. Local and direct power injection on CMOS integrated circuits. In *FDTC'2011: Fault Diagnosis and Tolerance in Cryptography*, pages 100–104, Nara, Japan, 2011. 56, 58

[MTOL12] Philippe Maurine, Karim Tobich, Thomas Ordas, and Pierre Yvan Liardet. Yet another fault injection technique : By forward body biasing injection. In *YACC'2012: Yet Another Conference on Cryptography*, Porquerolles Island, France, 2012. 54

[MWM19] Seita Maruyama, Satohiro Wakabayashi, and Tatsuya Mori. Tap 'n Ghost: A Compilation of Novel Attack Techniques against Smartphone Touchscreens. In *2019 IEEE Symposium on Security and Privacy (SP) (SP)*, 2019. 48

[New17] NewAE. Chipwhisperer. https://www.newae.com/chipwhisperer, 2017. 54

[NSFG21] Arash Nateghi, Martin Schaarschmidt, Sven Fisahn, and Heyno Garbe. Susceptibility of Power Line Communication (PLC) Channel to DS, AM and Jamming Intentional Electromagnetic Interferences. In *2021 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)*, pages 1–4, 2021. 47

[O'F17] Colin O'Flynn. *A Framework for Embedded Hardware Security Analysis*. PhD thesis, Dalhousie University, Halifax, Nova Scotia, USA, 2017. 53, 58, 61, 63

[O'F19] Colin O'Flynn. MIN()imum failure: EMFI attacks against USB stacks. In *13th USENIX Workshop on Offensive Technologies (WOOT 19)*, Santa Clara, CA, 2019. USENIX Association. 66

[O'F21a] Colin O'Flynn. ChipJabber-BasicBBI. https://github.com/newaetech/chipjabber-basicbbi, 2021. 54

[O'F21b] Colin O'Flynn. Low-Cost Body Biasing Injection (BBI) Attacks on WLCSP Devices. In Pierre-Yvan Liardet and Nele Mentens, editors, *Smart Card Research and Advanced Applications*, Lecture Notes in Computer Science, pages 166–180. Springer International Publishing, 2021. 54

[OGM17] Sébastien Ordas, Ludovic Guillaume-Sage, and Philippe Maurine. Electromagnetic fault injection: The curse of flip-flops. *Journal of Cryptographic Engineering*, 7(3):183, 2017. 61

[OTL14] Sjoerd Op 'T Land. *La Modélisation de l'immunité Des Circuits Intégrés Au-Delà de 1 GHz*. PhD thesis, 2014. 41

[PCNM15] Sikhar Patranabis, Abhishek Chakraborty, Phuong Ha Nguyen, and Debdeep Mukhopadhyay. A Biased Fault Attack on the Time Redundancy Countermeasure for AES. In Stefan Mangard and Axel Y. Poschmann, editors, *Constructive Side-Channel Analysis and Secure Design*, pages 189–203, Cham, 2015. Springer International Publishing. 61

[pdn17] plutoo, derrek, and naehrwert. Console Security - Switch. In *34th Computer Chaos Club Congress*, Leipzig, Germany, 2017. 65

[Pou15] Clovis Pouant. *Electromagnetic Susceptibility Characterization of the Input Stages of Electronic Devices*. Theses, Université Montpellier, 2015. 40

[PRC17] Pierre Payet, Jérémy Raoult, and Laurent Chusseau. Remote Extinction of a 2.4 GHz RF Front-End Using Millimeter-Wave EMI in the Near-Field. *Progress In Electromagnetics Research Letters*, 68:99–104, 2017. 46

[PS11] L. Palisek and L. Suchy. High Power Microwave effects on computer networks. In *10th International Symposium on Electromagnetic Compatibility*, pages 18–21, 2011. 45

[PZRI04] Y.V. Parfenov, L.N. Zdoukhov, W.A. Radasky, and M. Ianoz. Conducted IEMI threats for commercial buildings. *IEEE Transactions on Electromagnetic Compatibility*, 46(3):404–411, 2004. 42

[QS02] Jean-Jacques Quisquater and David Samyde. Eddy current for magnetic analysis with active sensor. In *Esmart 2002*, Nice, France, 2002. 55

[Res19] Limited Results. Fatal Fury On ESP32 Time To Release HW Exploits. In *Black Hat Europe 2019*, London, UK, 2019. 54, 58, 65

[Res20a] SySS Research. IceStick Glitcher. https://github.com/SySS-Research/icestick-glitcher, 2020. 54

[Res20b] Limited Results. Debug Resurrection On nRF52 Series. In *Black Hat Europe 2020*, 2020. 54, 58, 65

[Res20c] Limited Results. Pocket Glitcher. https://www.tindie.com/products/limited-results/pocketglitcher/, 2020. 54

[Res21] Limited Results. The quest of the geckos. In *NoHat 21*, Bergamo, Italy, 2021. 58, 59

[Riv09] Matthieu Rivain. Differential Fault Analysis on DES Middle Rounds. In *Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems*, CHES '09, pages 457–469, Berlin, Heidelberg, 2009. Springer-Verlag. 64

[RJL+22] Nicolas Ribière-Tharaud, Jean-Christophe Joly, C Laparro, M Schutz, and B Lenoir. IEMI Detection - Setting up relevant threshold. In *GLOBALEM 2022*, page 65, Abu Dhabi, UAE, 2022. 51

[Sab08] F. Sabath. Classification of electromagnetic effects at system level. In *2008 International Symposium on Electromagnetic Compatibility - EMC Europe*, pages 1–5, 2008. 43, 44, 45

[Sco16] Micah Scott. A USB Glitching Attack. In *PoC||GTFO, 2(0x13)*, number 2 in PoC||GTFO,, pages 30–37. 2016. 66

[SD15] Mark Seaborn and Thomas Dullien. Exploiting the DRAM rowhammer bug to gain kernel privileges. In *Black Hat USA 2015*, volume 15, page 71, Las Vegas, USA, 2015. 57

[Sel18] Jayaprakash Selvaraj. *Intentional Electromagnetic Interference Attack on Sensors and Actuators*. PhD thesis, Iowa State University, 2018. 49

[SH07] Jörn-Marc Schmidt and Michael Hutter. Optical and EM fault-attacks on CRT-based RSA: Concrete results. In *Austrochip 2007, 15th Austrian Workhop on Microelectronics, 11 October 2007, Graz, Austria, Proceedings*, pages 61–67. Verlag der Technischen Universität Graz, 2007. 55, 57

[Sko10] Sergei Skorobogatov. Optical Fault Masking Attacks. In *2010 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 23–29, 2010. 52

[SN06] Franck Sabath and D Nietsch. Electromagnetic Effects on Systems and Components. In *American Electromagnetics International Symposium AMEREM 2006*, Santa Barbara, CA, USA, 2006. Summa Foundation. 41, 45

[SZZ+22] H. Shan, B. Zhang, Z. Zhan, D. Sullivan, S. Wang, and Y. Jin. Invisible finger: Practical electromagnetic interference attack on touchscreen-based electronic devices. In *2022 IEEE Symposium on Security and Privacy (SP) (SP)*, pages 1548–1548, Los Alamitos, CA, USA, 2022. IEEE Computer Society. 48

[TM17] N. Timmers and C. Mune. Escalating Privileges in Linux Using Voltage Fault Injection. In *2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 1–8, 2017. 54, 58, 65

[TPR+18] F. Torrés, C. Pouant, A. Reineix, P. Hoffmann, J. Raoult, and L. Chusseau. Time-Domain Analysis and Modeling of Large-Signal RFI Rectification in MOS Transistors. In *2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE)*, pages 433–438, 2018. 40

[Tro21] Thomas Trouchkine. *Evaluation de La Sécurité Physique Des SoC*. These de doctorat, Université Grenoble Alpes, 2021. 52, 57, 58, 60, 61, 62, 63, 67

[TSS17] Adrian Tang, Simha Sethumadhavan, and Salvatore Stolfo. CLKSCREW: Exposing the perils of Security-Oblivious energy management. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 1057–1074, Vancouver, BC, 2017. USENIX Association. 57

[TSW16] Niek Timmers, Albert Spruyt, and Marc Witteman. Controlling PC on ARM using fault injection. In *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2016, Santa Barbara, CA, USA, August 16, 2016*, pages 25–35. IEEE Computer Society, 2016. 65

[TTPH21] Yazhou Tu, Vijay Srinivas Tida, Zhongqi Pan, and Xiali Hei. Transduction Shield: A Low-Complexity Method to Detect and Correct the Effects of EMI Injection Attacks on Sensors. In *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, ASIA CCS '21, pages 901–915, New York, NY, USA, 2021. Association for Computing Machinery. 51

[URS99] URSI. Resolution on Criminal Activities using Electromagnetic Tools. In *General Assembly and Scientific Symposium (URSI GASS), 1999 URSI*, Toronto, Canada, 1999. 35

[Van16] Stefan Van de Beek. *Vulnerability Analysis of the Wireless Infrastructure to Intentional Electromagnetic Interference*. PhD thesis, Universiteit Twente, 2016. 36, 41, 46

[Vit89] Charles Vittitoe, N. Did high altitude EMP cause the hawaian streetlight incident ? *System Design and Assessment Note SDAN*, 31, 1989. 34

[VTM+17] Aurélien Vasselle, Hugues Thiebeauld, Quentin Maouhoub, Adèle Morisset, and Sébastien Ermeneux. Laser-Induced Fault Injection on Smartphone Bypassing the Secure Boot. In *2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 41–48, 2017. 52

[War17] David A Ware. Effects of Intentional Electromagnetic Interference on Analog to Digital Converter Measurements of Sensor Outputs and General Purpose Input Output Pins. Master's thesis, Utah State University, Logan, Utah, 2017. 41

[Wik23] Wikipedia. Starfish Prime. https://en.wikipedia.org/w/index.php?title=Starfish_Prime, 2023. 34

[WMY+22] Kai Wang, Richard Mitev, Chen Yan, Xiaoyu Ji, Ahmad-Reza Sadeghi, and Wenyuan Xu. GhostTouch: Targeted attacks on touchscreens without physical touch. In *31st USENIX Security Symposium (USENIX Security 22)*, Boston, MA, 2022. USENIX Association. 48

[XHJ+21] Zhifei Xu, Runbing Hua, Jack Juang, Shengxuan Xia, Jun Fan, and Chulsoon Hwang. Inaudible Attack on Smart Speakers With Intentional Electromagnetic Interference. *IEEE Transactions on Microwave Theory and Techniques*, 69(5):2642–2650, 2021. 48

[YSW18] Bilgiday Yuce, Patrick Schaumont, and Marc Witteman. Fault Attacks on Secure Embedded Software: Threats, Design, and Evaluation. *Journal of Hardware and Systems Security*, 2(2):111–130, 2018. 61

[ZDC+12] Loïc Zussa, Jean-Max Dutertre, Jessy Clédière, Bruno Robisson, and Assia Tria. Investigation of timing constraints violation as a fault injection means. In *27th Conference on Design of Circuits and Integrated Systems (DCIS)*, page pas encore paru, Avignon, France, 2012. 61

[ZDCT13] L. Zussa, J. M. Dutertre, J. Clédière, and A. Tria. Power supply glitch induced faults on FPGA: An in-depth analysis of the injection mechanism. In *2013 IEEE 19th International On-Line Testing Symposium (IOLTS)*, pages 110–115, 2013. 57, 59

[ZDT+14] Loic Zussa, Amine Dehbaoui, Karim Tobich, Jean-Max Dutertre, Philippe Maurine, Ludovic Guillaume-Sage, Jessy Clediere, and Assia Tria. Efficiency of a glitch detector against electromagnetic fault injection. In *Design, Automation and Test in Europe Conference and Exhibition (DATE), 2014*, pages 1–6. IEEE, 2014. 67

[ZR20] Youqian Zhang and Kasper Rasmussen. Detection of Electromagnetic Interference Attacks on Sensor Systems. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 203–216, 2020. 51

[Zus14] Loic Zussa. *Study of Fault Injections Means Based on Timing Constraints Violation for Physical Cryptanalysis of Secure Circuits*. Theses, Ecole Nationale Supérieure des Mines de Saint-Etienne, 2014. 53, 61

[ZZC+20] Dongxiao Zhang, Xing Zhou, Erwei Cheng, Haojiang Wan, and Yazhou Chen. Investigation on Effects of HPM Pulse on UAV's Datalink. *IEEE Transactions on Electromagnetic Compatibility*, 62(3):829–839, 2020. 41

Contribution

Chapter 3

Effect characterization with a systemic approach

Contents

3.1 Chapter overview

The research featured in this chapter was a collaboration with Dr. Chaouki KASMI, Dr. Valentin HOUCHOUAS and Mathieu RENARD at ANSSI between 2014 and 2015. Several publications have been made in conferences related to EMC and IEMI [HKLEC15, HKLEV16, KLEP+14, KLERD14, KLEA16, KLER14a, KLER14d, KLER14b, KLER14c, KPLE+14, KLE15, KLE16a, KLE16b]. Furthermore, besides having been cited in several conference and journal papers, the approach developed in this chapter was referenced in the IET Code of Practice for Electromagnetic Resilience [IET17] among the electromagnetic resilience techniques and measures for use in system design.

In this chapter, an approach to overcome some limitations of IEMI susceptibility testing regarding the reuse of test results for InfoSec analyses is proposed. This approach is developed around two key ideas. First, fault models provide an abstraction for representing effects of IEMI from a chosen layer viewpoint which is well suited for exploitability analysis, detection and countermeasure design. Second, by choosing fault models at the operating system layer, impacts on the information can be characterized and their propagation to upper layers can be studied. As a result, the targets under test can be instrumented with software specifically designed to detect the occurrence of a set of selected fault models.

This approach might be a promising perspective for effect characterization during susceptibility testing and a basis for an assessment of effects that is no longer dependent on the target function or operational context. Furthermore, the possibility of defining a reference set of failure criteria by target category, i.e., a list of possible fault models to test for, could be envisioned, enabling a better comparability of test results.

A practical application of this approach has been performed on a desktop computer and some example results are given, showing that effect occurrences can be efficiently identified.

Finally, the application of this method in a detection context is proposed. At a single system scale, a self-monitoring for detecting symptoms potentially due to IEMI is possible and such symptoms could be logged to enable forensic analysis. At a network scale, each signal system could measure and report information to a main detection and logging system having an overview of the state of each system on the network. If the physical position of each node of the network is taken into account, it might become possible to detect which physical areas are affected by symptoms potentially due to IEMI and to deduce the potential position of the attacker.

3.2 Towards fault models for IEMI

Fault models are used to analyze, detect, identify and classify effects of EMFI on the target from the viewpoint of a chosen observation layer (e.g., physical layer, logic, micro-architecture). Using fault models also facilitates the investigation of exploitation techniques relying on the observed effects.

IEMI is the only part of EMC considering an intentional generation of target specific EM environment and was integrated to standard since 2005. Before, high-power EM environments were studied, both unintentional (e.g., lightning) and intentional (e.g., nuclear electromagnetic pulse (NEMP)). Inheriting from those approaches, IEMI methods are still focused on high power and impacts on the availability of the main function of the target. However, as IEMI threat models include a variable range attacker, high power sources might no longer be needed for an attacker located close to the target. Therefore, there is room for attackers with moderate or low power sources, which are close enough to achieve a synchronization with the target and aim for impacts on the integrity of the information. To address these new threat models, immunity assessment methods, especially regarding the failure criteria and the detection of effects, need to evolve into new effect observation techniques, which might allow for an easier analysis of the impacts from an InfoSec perspective.

In EMFI studies, fault models are often used to represent the effects occurrence on the target from the viewpoint of a chosen observation layer. Introducing fault models in IEMI methodologies might allow to overcome some of the aforementioned limitations regarding the susceptibility assessment, the exploitability analysis, the detection and the design of countermeasures.

3.2.1 Fault models for susceptibility testing

Following guidance from the standard [ISO20], susceptibility testing against IEMI is very dependent of the target *function* and the *operational* context in which the target is supposed to evolve. More precisely, the tailored test level derivation method shows the following:

- The source categories (hypoband, hyperband, mesoband) are determined by a sort of threat analysis, which is obviously related to both the function of the target and the operational context;
- The EM constraints (fields, voltages, currents) are determined by an analysis of the operational context, such as the expected distance between the attacker and the target, and the propagation channel characteristics;
- The failure criteria are determined in order to estimate the impact on the availability of the main

mission, which is related to the function of the target.

As an outcome, the results of the susceptibility testing campaign of an electronic device cannot be extrapolated to the same electronic device implementing a different function in a different operational context. This lack of genericity is also a problem for generic or multipurpose platforms. How to determine the main mission of a smartphone? How to decide if effects on a sensor in this smartphone are impacting the main function? It obviously depends on how the sensor information is used. Using information oriented fault models as failure criteria might be a way to provide susceptibility testing results that are intrinsic to the target and comparable in terms of exploitability.

3.2.2 Fault models for exploitability analysis

Fault models can be considered as an intermediate representation of the occurrence of an effect at a certain layer, between the physical phenomena and the potential impacts on higher layers (e.g., functional impact, impact on information). As such, it might become easier to investigate potential InfoSec issues related to the occurrence of an effect by representing this effect by a fault model on a layer of interest. Once the fault model of an effect has been observed, it becomes possible to perform an analysis on higher layers inferring the impact of the fault model. For example, if the possibility of affecting sensor readings on a smartphone is observed, it becomes possible to analyze threats on the higher layers (e.g., an application) coming from a loss of integrity of the sensor reading. In [BDH+97], attacks on public key cryptosystems were designed assuming the realization of bit flips at random locations in the information manipulated by the cryptographic processing. Countermeasures were also proposed based on the assumed fault model, without any practical fault injection.

3.2.3 Fault models for countermeasure design

A first consequence of using fault models for the exploitability analysis if that fault models are also a useful tool for designing and implementing countermeasures in higher layers. As it is possible to theoretically assess the impact of the realization of a certain fault model on higher layers, it also becomes possible to study possible high layer countermeasures against a specific fault model. For example, considering a sensor reading corruption fault model, hardware and software countermeasures could be designed, analyzed and implemented, such as sensor redundancy [GR19] or adding dummy sensor readings [TTPH21].

3.2.4 Fault models for detection

Fault models might also be a useful tool for designing detection strategies. Indeed, by choosing fault models at a layer at which the detection might be implemented, it becomes possible to design a specific process to monitor the realization of the fault model, as a way to detect the occurrence of the associated effect. For example, following on the sensor corruption fault model, it might be observed from several layers. An application using sensor readings might be developed to perform some sort of anomaly detection on the values coming from the sensor.

3.3 Systemic approach

Using fault models as a representation of IEMI effects on a chosen layer of observation allows for effect detection, exploitability analysis and countermeasures design. With these objectives in mind, the InfoSec evaluation of a target against IEMI might be decomposed in two steps:

- A classical EMC susceptibility testing using fault models as failure criteria;
- An exploitability analysis based on the observed fault models.

To apply this approach on programmable multipurpose platforms such as computers or smartphones, a *systemic approach* is proposed, consisting in placing the observation layer at the operating system level. To this end, a set of observables that can be measured by the operating system and that are likely to express symptoms of IEMI effects have to be identified. Then, a specific piece of software can be developed and implanted into the target in order to monitor the observables during susceptibility testing.

To choose the set of observables, the approach can be bottom-up, starting with the identification of the physical coupling interfaces of interest. The hardware components likely to be impacted by effects consequently to physical coupling can then be identified. The way these components interact and communicate with the SoC hosting the operating system needs to be understood in order to determine software interfaces which can be queried by a piece of software in order to obtain information about the hardware components status and operation.

Another way to go is top-down, where the goal is to test against specific fault models. In this case, fault models to test have to first be identified. Then, specific code can be written to perform a characterization of the target according to the selected fault models.

Considering a generic electronic device model representative of a computer, a smartphone or an

IoT device, a first coarse grain enumeration of potentially interesting fault models is given in Table 3.1.

Table 3.1 – Systemic approach on a generic device model

Physical interface	**Observable**	**Fault models**
Power cable	Voltages, power consumption	All
Wireless power	Voltages, power consumption	All
Communication cable	Communication rate, errors	Denial of service, signal injection
Wireless communication	Communication rate, errors	Jamming, blocking, signal injection
ICs	Data storage	Data corruption (read, write, at rest)
ICs	Processing	Program data, control flow corruption
Sensors	Sensor readings	Denial of service, signal injection
Actuators	Actuator state	Denial of service, signal injection

3.4 Example results on a COTS computer

To illustrate the use of the systemic approach, a desktop computer enclosing an Intel Pentium IV CPU and running a Debian 7.4 operating system has been instrumented in order to monitor a set of observable during susceptibility testing. Several observables were monitored on this target, they are summarized in Table 3.2.

Table 3.2 – Example application of the systemic approach on a desktop computer

Physical interface	**Observable**	**Software interface**
Internal sensors	Sensor readings	Sensor query interface
RF interfaces	Spectrogram, signal to noise ratio Link rate, modulation, errors Hardware errors	Direct input instrumentation, specific debugging protocols Link status interface System logs, controller status
External wired interfaces	Voltage data Link rates, errors Disconnects, driver errors, hardware errors	Sensor query interface Link status interface System logs, controller status
Internal communication	Link rates, errors	System logs, controller status

As an outcome, several symptoms have been identified by the monitoring software. Two examples are reported in what follows, showing symptoms appearing in the operating system logs and symptoms obtained by monitoring a wired link interface.

3.4.1 Example effects on peripheral interfaces

The tested target was equipped with a USB keyboard, a PS/2 keyboard and a PS/2 mouse. To monitor for effects on those interfaces, the operating system logs were scrutinized and messages coming from the USB and the PS/2 controllers were analyzed.

Parasitic activity on the PS/2 interface generated several log entries, transcribed in Figure 3.1.

```
input: PS/2 Generic Mouse as /devices/platform/i8042/serio1/input/input0
psmouse serio1: bad data from KBC - timeout
atkbd serio0: Unknown key pressed (translated set 2, code 0x9e on isa0060/serio0).
atkbd serio0: Use 'setkeycodes e01e <keycode>' to make it known.
psmouse serio1: alps: Unknown ALPS touchpad: E7=10 00 64, EC=10 00 64
psmouse serio1: bad data from KBC - timeout
```

Figure 3.1 – Log entries generated by effects on the PS/2 interface

The message “bad data from KBC” means that the PS/2 controller received malformed data. So does the line containing “Unknown ALPS touchpad”, showing that the device identifier of the mouse was modified during the transmission. Moreover, the log entries about the “atkbd” are very interesting. Indeed, they show that the EM stimuli induced PS/2 packets which are interpreted as invalid keyboard key codes. All these errors could be explained as a result of EM coupling on the PS/2 cables, on one or both (data or clock) lines [Cha03].

From these observations, a possible explanation of symptoms previously observed in [Hoa07] might be found. Effects of IEMI on a desktop computer were explored by a visual inspection of the activity on the display, showing mouse pointer deflections, moving windows, and random clicks on program icons. The systemic approach provides information on the internal activity and the effects observed on the PS/2 interface might explain the random mouse activity. Such a clue on the underlying phenomena was not possible with only a visual monitoring of the effects on the computer screen, as done in the study.

The same approach has been followed to observe symptoms on the USB peripheral interface. An extract of log entries in the operating system logs concerning this interface is given in Figure 3.2.

The main symptom is a repetition of device disconnections, resets and re-enumerations. It can also be pointed out that several read errors appear during parasitic illumination. These symptoms might be explained as the result of the induction of special USB physical layer symbols (*SE0* and *SE1*) [CHC+00] interrupting the regular communication and inserting *End of Packet* or forbidden symbols in the middle of regular packets. This explains why the USB root hub indicates that there is a possible EMI phenomenon.

```
hub 1-0:1.0: port 1 disabled by hub (EMI?), re-enabling...
usb 1-1: reset full-speed USB device number 2 using uhci_hcd
usb 1-1: USB disconnect, device number 2
usb 1-1: USB disconnect, device number 3
usb 1-1: new low-speed USB device number 4 using uhci_hcd
usb 1-1: device descriptor read/64, error -71
usb 1-1: string descriptor 0 read error: -71
usbhid 1-1:1.0: can't add hid device: -71
usbhid: probe of 1-1:1.0 failed with error -71
usb 1-1: device not accepting address 5, error -71
hub 1-0:1.0: unable to enumerate USB device on port 1
usb 1-1: unable to read config index 0 descriptor/all
usb 1-1: can't read configura
---SYSTEM CRASH
```

Figure 3.2 – Log entries generated by effects on the USB interface

3.4.2 Example effects on a wired network interface

The susceptibility of the Ethernet interface at the physical layer against IEMI has already been demonstrated in several studies [KSG15, PS11]. It was shown that effects decrease the performance of the wired communication interface. In these studies, the measurement of the impact on the network communication was done at the other end of the cable, by the router or a computer. With the systemic approach, the same results were confirmed when observed from within the target.

For testing purposes, common network information tools were used to gather data about errors on the Ethernet interface during illumination. The results are shown in Figure 3.3. The tests show that when the target is illuminated, the errors on the Ethernet link increase drastically.

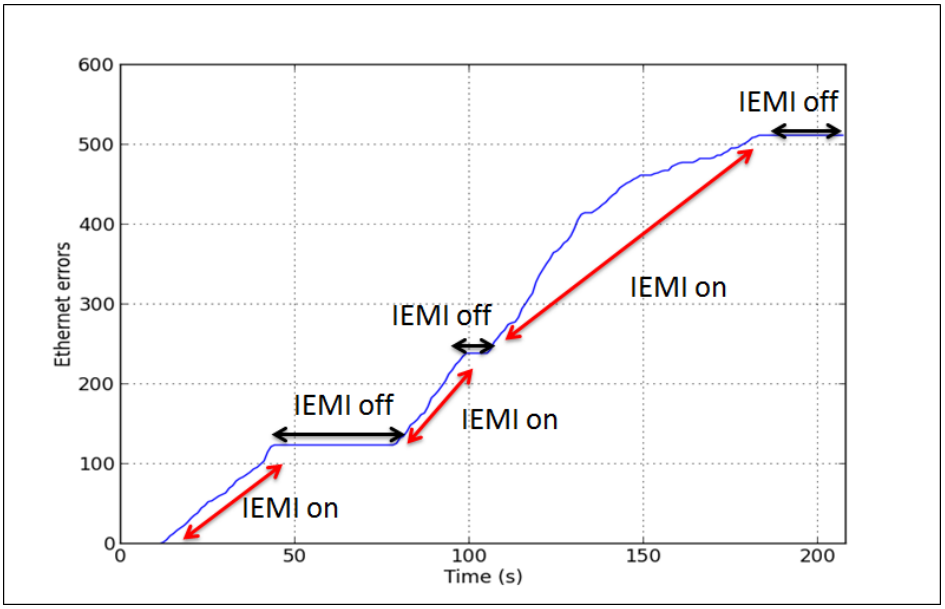


Figure 3.3 – Detected effects on the ethernet interface with a monitoring software

3.5 Contribution to detection and forensics

The systemic approach allows both for testing against specific fault models and for identifying fault models occurring during susceptibility analysis of a target. As aforementioned, fault models can also be used as a basis for the design of detection processes. Detection processes, adopting the systemic approach, monitor a set of observables and/or implement a set of fault model specific test codes in order to witness symptoms of potential IEMI. As it can be expected, the practical operation of such detection processes face many technical challenges or trade-offs related to detection, such as anomaly detection, processing load minimization, sensor fusion and data aggregation, which were left out of the scope of this study.

3.5.1 System scale

Detection using the systemic approach can be implemented on the target, resulting in an internal detection solution. In this case, it consists in a software instrumentation of the target which can be dedicated to susceptibility testing or destined to perform detection aside of the normal operation of the target. This possibility has been explored and resulted in a proof of concept targeting Linux based computers [KLER14a]. This approach has also been referenced as a promising method in guidance related to EMC methods for functional safety [IET17].

Finally, it was observed during tests that some observable were available in the operating system logs, such as errors on peripheral interfaces. These logged observables provide an interesting basis for the detection of IEMI during forensic analysis, which would be an internal detection approach complimentary to existing external detection devices.

3.5.2 Network scale

Detection using the systemic approach could also be extended to a set of computers at the scale of a computer network. Technically, each machine could be considered as a probe gathering information and sending feedback to a central entity in charge of the monitoring of the network state. This approach might be promising as it overcomes some system scale detection limitations and provides additional benefits. First, the extension of the detection capability to the network scale, if coupled to a map of the actual physical position of the monitored computers on site, provides an opportunistic use of those machines as a sensor network which reports localised data about the situation. As the effects of IEMI are range dependent, they might differ according to the relative position of the source and the different targets. As an outcome, such approach might provide information about the state of

each node of the network and help to identify an area in which the source is likely to be located in case of a detection event. Furthermore, in this context, the failure of one or several computers due to an attack still provides valuable and exploitable information to the detection system.

3.6 Discussion and perspectives

To overcome some of the limitations of IEMI effects characterization approaches regarding the exploitation of results for InfoSec, an effects assessment method was proposed. This method relies on the introduction of fault models so as to benefit from easier detection, countermeasure design and exploitability analysis.

On complex targets such as computers or smartphones, placing the fault models at the operating system level seem a promising strategy to assess the impacts of IEMI on the security of the information processed or stored. This strategy was called the systemic approach.

By observing effects as the operating system can perceive them, a focus is made on impacts on the information. Thus, it becomes straightforward to infer the propagation of the impacts to upper layers manipulating this information. The design of countermeasures for protecting those upper layers also becomes possible.

The application of the systemic approach on computers may contribute to detection and forensic analysis. A computer can then be viewed as a probe monitoring a set of observables performing an internal detection of IEMI effects. At a network scale, instrumented computers can be viewed as nodes of a sensor network, gathering information to a central detection system. By coupling information about the physical location of each node, this approach could provide a way to identify the source location.

Such self-monitoring approach has limitations, the main one being the question about the integrity and the availability of the monitoring. Indeed, under attack, the detection software execution might be corrupted or disrupted. At a system scale, this limitation is quite significant, but in a network scale deployment, any perturbation of a subset of machines can still be valuable information for the main detection system.

A software instrumentation of the targets is not always an easy task. It requires to have enough information about the target specifications to choose observables and find a software interface to access them. Furthermore, targets might not be in a state that allows to load and run custom software.

The systemic approach for IEMI susceptibility testing might be a promising perspective for the harmonization and the generalization of failure criteria. For each type of target, a list of commonly

considered fault models could be built, along with a library of the corresponding test software. With such approach, susceptibility test results might become more comparable.

3.7 References

[BDH+97] Feng BAO, Robert H. DENG, Y. HAN, A. JENG, Arcot Desai NARASIMHALU, and T. NGAIR. Breaking public key cryptosystems on tamper resistant devices in the presence of transient faults. In *5th International Workshop on Security Protocols*, volume 1361, pages 115–124, Paris, France, 1997. 86

[Cha03] Adam Chapweske. The PS/2 keyboard and mouse protocol. http://computer-engineering.org/ps2protocol/, 2003. 89

[CHC+00] Compaq Computer Coporation, Hewlett-Packard Company, Intel Corporation, Microsoft Corporation, Lucent Technologies, NEC Corporation, and Koninklijke Philips Electronics. Universal Serial Bus Specification. Standard Revision 2.0, 2000. 89

[GR19] Ilias Giechaskiel and Kasper Bonne Rasmussen. SoK: Taxonomy and Challenges of Out-of-Band Signal Injection Attacks and Defenses. *arXiv:1901.06935 [cs]*, 2019. 86

[HKLEC15] Valentin Houchouas, Chaouki Kasmi, José Lopes Esteves, and Damien Coiffard. Experimental comparison of mode-stirrer geometries for the susceptibility testing of COTS Information Systems in regards of the criticality of effects – Technical report. *System Design and Assessment Note SDAN*, 46, 2015. 84

[HKLEV16] Valentin Houchouas, Chaouki Kasmi, José Lopes Esteves, and Philippe Valembois. Caractérisation logicielle de la susceptibilité d'un capteur de température de PC pour la CEM et la SSI. In *18 Ème Colloque International et Exposition Sur La Compatibilité ÉlectroMagnétique (CEM 2016)*, Rennes, France, 2016. 84

[Hoa07] Richard Hoad. *The Utility of Electromagnetic Attack Detection to Information Security*. PhD thesis, University of Glamorgan, 2007. 89

[IET17] IET. *Code of Practice for Electromagnetic Resilience*. IET Codes and Guidance. The Institution of Engineering and Technology, 2017. 84, 91

[ISO20] ISO/IEC. Electromagnetic compatibility (EMC) - Part 4-36: Testing and measurement techniques – IEMI immunity test methods for equipment and systems. Standard ISO/IEC 61000-4-36:2020, International Organization for Standardization, Geneva, CH, 2020. 85

[KLE15] C. Kasmi and José Lopes Esteves. Automated analysis of the effects induced by radio-frequency pulses on embedded systems for EMC Functional Safety. In *Radio Science Conference (URSI AT-RASC), 2015 1st URSI Atlantic*, pages 1–1, Las Palmas, Spain, 2015. IEEE. 84

[KLE16a] Chaouki Kasmi and José Lopes Esteves. Détection et caractérisation des effets induits par des interférences électromagnétiques sur un ordinateur. In *Journée de l'Aremif*, Paris, France, 2016. 84

[KLE16b] Chaouki Kasmi and José Lopes Esteves. Functional susceptibility of COTS devices to IEMI at local and large-scale levels. In *2016 International Conference on Electromagnetics in Advanced Applications (ICEAA)*, pages 399–402, 2016. 84

[KLEA16] Chaouki Kasmi, José Lopes Esteves, and Keith Armstrong. EMC/EMI and Functional Safety: Methodology to characterize effects of interferences on devices. In *Electromagnetic Compatibility (APEMC), 2016 Asia-Pacific International Symposium On*, volume 1, pages 1178–1180. IEEE, 2016. 84

[KLEP+14] Chaouki Kasmi, José Lopes Esteves, Nicolas Picard, Mathieu Renard, Bruno Beillard, Edson Martinod, Joël Andrieu, and Michèle Lalande. Event logs generated by an operating system running on a COTS computer during IEMI exposure. *IEEE Transactions on Electromagnetic Compatibility*, 56(6):1723–1726, 2014. 84

[KLER14a] C. Kasmi, José Lopes Esteves, and M. Renard. Automation of the Immunity testing of COTS computers by the instrumentation of the internal sensors and involving the operating system logs–Technical report. *System Design and Assessment Note SDAN*, 44, 2014. 84, 91

[KLER14b] Chaouki Kasmi, José Lopes Esteves, and Mathieu Renard. Autonomous electromagnetic attacks detection considering a COTS computer as a multi-sensor system. In *General Assembly and Scientific Symposium (URSI GASS), 2014 XXXIth URSI*, pages 1–4. IEEE, 2014. 84

[KLER14c] Chaouki Kasmi, José Lopes Esteves, and Mathieu Renard. DESIGN OF AN IEMI-ATTACK DETECTOR INVOLVING THE INTERNAL RESOURCES OF A COTS COMPUTER. In *Ninth Future Security*. Fraunhofer Verlag, 2014. 84

[KLER14d] Chaouki Kasmi, José Lopes Esteves, and Mathieu Renard. A Self-monitored Information System for High Power Electromagnetic Attacks Detection. In *AMEREM 2014*, 2014. 84

[KLERD14] Chaouki Kasmi, José Lopes Esteves, Mathieu Renard, and Emmanuel Duponchelle. Méthode pour une analyse autonome des perturbations induites par des interférences électromagnétiques. In *Journées Aremif*, Paris, France, 2014. 84

[KPLE+14] Chaouki Kasmi, Nicolas Picard, José Lopes Esteves, M Renard, Bruno Beillard, Edson Martinod, Joël Andrieu, and Michèle Lalande. Analysis of Hardware and Software Faults induced by IEMI on a COTS Computer. In *ICEEA 2014, 5th International Conference on Environmental Engineering and Applications*, 2014. 84

[KSG15] M. Kreitlow, F. Sabath, and H. Garbe. Analysis of IEMI effects on a computer network in a realistic environment. In *2015 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, pages 1063–1067, 2015. 90

[PS11] L. Palisek and L. Suchy. High Power Microwave effects on computer networks. In *10th International Symposium on Electromagnetic Compatibility*, pages 18–21, 2011. 90

[TTPH21] Yazhou Tu, Vijay Srinivas Tida, Zhongqi Pan, and Xiali Hei. Transduction Shield: A Low-Complexity Method to Detect and Correct the Effects of EMI Injection Attacks on Sensors. In *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, ASIA CCS '21, pages 901–915, New York, NY, USA, 2021. Association for Computing Machinery. 86

Chapter 4

Exploitation of voice assistants

Contents

4.1 Chapter overview

This research was a collaboration with Dr. Chaouki KASMI at ANSSI between 2015 and 2017 and has been disseminated through several publications, both in journals and conference papers focusing on IEMI [KLE15b, KLE15a, LEK18] and InfoSec [KLE16, KLE17a, LEK15b, LEK15a]. Those publications have been cited by more than 80 conference or journal papers and have served as a basis for studies focusing on voice assistant security, conducted IEMI on smartphones, sensors security, speech recognition, IoT security and EMC.

In this chapter, the susceptibility of widespread analog sensors, namely analog microphones, is assessed and the exploitability of the effects is investigated in order to gain remote and silent voice command execution on several smartphone models. Nowadays, voice interfaces are ubiquitous and provide a rich set of features to the users. Operating system editors tend to deploy this technology broadly, especially for smartphones and embedded systems with a high demand of hands-free interactions such as car infotainment systems or smart TVs. The main hardware interface providing the user interaction with the voice assistants consists in a microphone or a microphone array, which are designed to collect acoustic signals. Thus, it is often believed that any unauthorized interaction with these interfaces would be heard by the legitimate user. Besides, several studies focusing on analog sensors have shown that the nonlinear components involved in the amplification, filtering and digitization of the signal may behave as envelope detectors for high frequency out-of-band input signals. This is a perfect scenario for an AM IEMI attack, which provides a silent and remote path to trigger voice commands on a target device.

Both the radiated susceptibility and the conducted susceptibility of the targets is considered, in order to identify the perturbation signal characteristics that maximize coupling. After this characterization, the exploitability of the EM vulnerabilities identified is investigated by targeting several well-known voice assistants in order to trigger commands. To the author's knowledge, this work was the first to propose the use of IEMI with analog microphones for exploiting the voice assistants, which expose critical services. The attack has therefore a high impact on widely deployed devices and might be extended to several other types of targets (e.g., computers, laptops, smart speakers, IoT devices...). Furthermore, very few conducted IEMI studies were performed online, i.e. with power signals coming from the low voltage power network, as it is the case in this work.

This chapter is organized as follows: first, voice command interfaces inner workings are described both from a hardware and software perspective, and the services exposed through these interfaces are briefly reminded. Second, the setup and the methodology used for susceptibility testing are detailed,

both for the radiated coupling threat and for the conducted coupling threat. Third, findings from susceptibility testing are used for introducing an in-band audio signal with an out-of-band IEMI in order to trigger the voice assistants and execute voice commands. Then a security analysis is provided along with a comparison of radiated and conducted interference threats and countermeasures are proposed.

4.2 Voice assistants

4.2.1 Definition

A voice assistant continuously listens to the audio activity awaiting for a voice command to execute. It is a natural way for humans to communicate and it provides the benefit of a hands-free interaction, which can be pretty handy in several situations as driving or cooking. Voice assistants have been deployed in a wide range of devices, such as smartphones, smart speakers or cars and are used for personal, professional and industrial applications. This deployment has been accelerated with the improvements made in speech recognition and the integration of new functionalities such as smart homes and connected cars.

As the available commands give access to more and more features and depending on the context, some of them being critical, there is an increasing need of security for voice assistants, especially against unauthorized use.

In this study, a focus was made on voice assistants in smartphones. However, besides the elements related to the physical introduction of the attacker's signal, some results can be generalized to other platforms.

Hardware interfaces on smartphones

Most modern smartphones provide mainly two voice input interfaces: the built in microphone(s) and the headphone's microphone. Generally, those interfaces are enabled alternatively, depending on the presence of microphone capable headphones. The voice input interfaces are connected to a digital signal processing (DSP) stage which amplifies the electrical signal, low-pass filters remove ambient noise and an ADC digitizes the filtered signal into a digital audio stream and forwards it to the application processor [YJW+22].

Within headphones, the left and right audio outputs can also be used as an input antenna for FM radio signals in FM capable phones. Furthermore, microphone capable headphones provide a

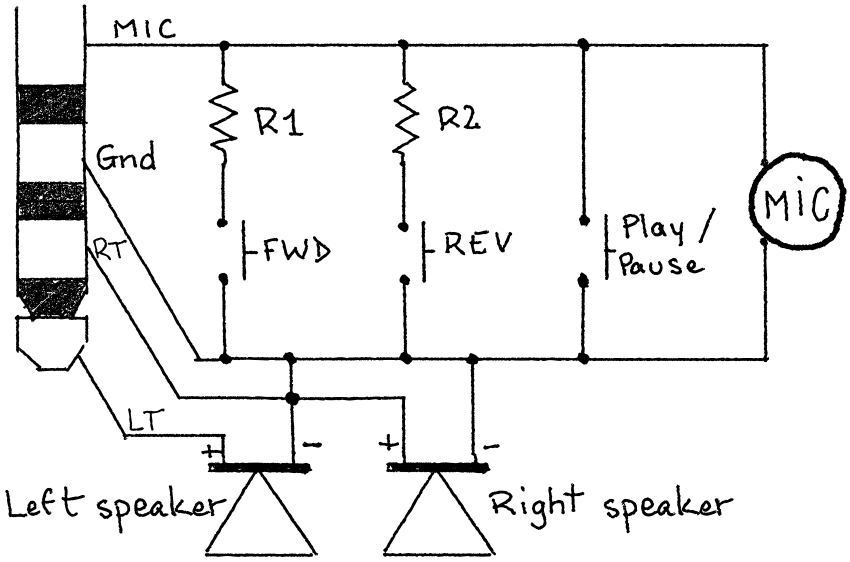


Figure 4.1 – Electrical schematic of headphones

physical button interface (Figure 4.1). A button press changes the impedance of the microphone line, which is detected by the phone.

Software services and features

As voice assistants became more reliable and popular, they have been integrated to most of the recent desktop, mobile and embedded operating systems. Some of the available interpreters at the time of the study are listed hereafter:

- Samsung: Samsung voice control system is called S-Voice [Wik22f]. It is a vendor software layer that is natively included in the Android core;
- Apple: two services provide a voice command interface, namely Voice Control and Siri [Sir, Wik22g]. On the latest versions of iOS, Siri completely replaced Voice Control;
- Google: Google Voice Search is the original voice command interface and was merged to Google Now [Wik21] since Android Jelly Bean;
- Microsoft: Cortana [Wik22c] is the voice assistant which superseded Speech.

Since, Google Now evolved into Google Assistant [Ass, Wik22e], Samsung S-Voice became Samsung Bixby in 2017 [Wik22b] and Amazon Alexa [Wik22a] was widely adopted.

Editors and manufacturers tend to expose more and more features through the voice interface. These features can be classified in four main categories:

- Internet services: web search, web browsing, sending emails, posting to social media, ordering stuff on the editor's marketplace;
- Telephony services: placing phone calls, sending text messages, resolving contact numbers from names;
- Local services: setting alarms up, creating calendar events and reminders, changing the device's settings;
- Third-party services: launching applications.

Activation

It is important to understand the way voice assistants can be activated because they can expose several features to a pre-authentication use. Indeed, the voice interface remains hands-free as long as the user is not required to enter his PIN code to unlock the phone.

When the voice assitant is not enabled permanently, it is generally activated by manually launching the software application or by a hardware button press. The hardware button can generally be a button on the handset or a button from the remote command of the headset (e.g. button referenced as the Play/Pause one in Figure 4.1).

To simplify the user experience and to encourage the use of this voice interface, the voice assistant tends to be always activated and running in the background, waiting for the user to pronounce a keyword (e.g. "OK Google", "Hey Siri"). This naturally raises question about the risk introduced by such service for the privacy of users. In some cases, the activation of the voice assistant is conditioned by specific behaviour. For example, Google now and Siri documentation stated that they were automatically enabled when the smarphone was charging.It is also still the case when the smartphones are connected to a vehicle's infotainment system (e.g., with Android Auto).

Voice command processing

The processing of the voice command is based on a two-step procedure.

The voice assistant, when enabled, keeps listening to the audio input waiting for the user to pronounce a keyword (e.g., "OK Google" for Google products, "Hey Siri" for Apple Siri).

The keyword recognition is performed locally on the smartphone and in the most recent versions, it is often coupled to a biometric identification of the user's voice saying the keyword [KLE17b].

When the keyword is recognized and, optionally, when the user is identified, the user can throw a voice command.

The audio stream is recorded and sent to a remote server of the service provider. The stream is processed by a speech recognition engine. The recognized text is analyzed and can be sent to third party service providers and/or back to the mobile.

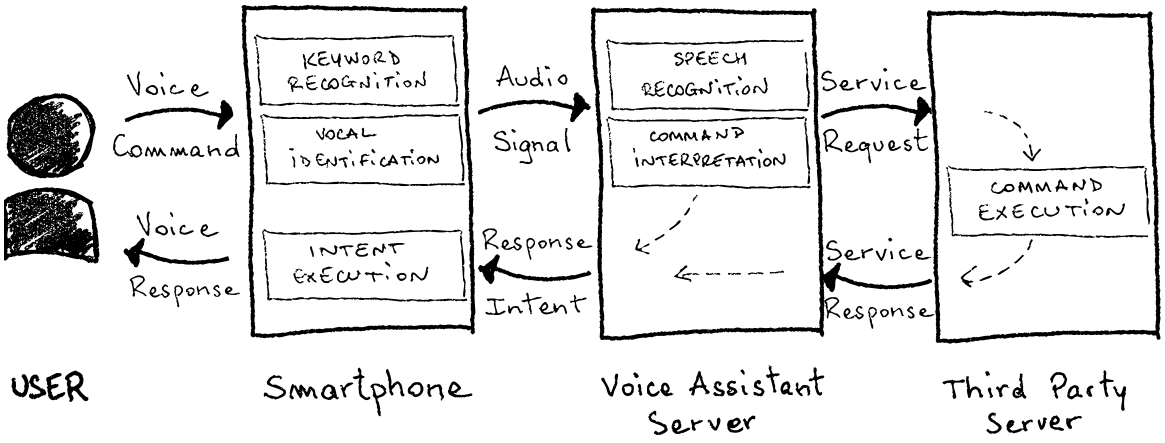


Figure 4.2 – Voice command execution process (derived from [YJW+22])

4.2.2 Related work

At the time of this study, the voice command interface has been subject to very few security analyses. Mostly, some proofs of concept have been published about using Siri to bypass the lock screen PIN code authentication in order to gain access, most of the times restricted, to other functionalities on the device [Gon14]. Focusing on the network service, security researchers performed a complete reverse engineering of the early versions of Siri's protocol and provided a framework to include Siri voice interpretation capabilities inside any web application [App21]. However, they did not further investigate the possibility to exploit this vector to compromise the device. The privacy aspects of Siri have also been discussed after Apple announced they share the voice samples collected by the remote interpreter service to third parties [Wei15]. Concerning Google Voice Search, an application with no specific permission on an Android device has been shown to be able to activate the voice interpreter and send commands through the phone's speaker, as stated in [DLZZ14]. However, the

main limitation of this work is the use of the speaker to send the commands, which is not silent and can be easily detected by the victim. An interesting local attack vector to overcome this limitation could be the exploitation of the software sound mixer to provide the malicious command to the software audio input pipe without playing it out loud. This same idea has been further investigated in [VZSS15]. After a detailed analysis of the speech analysis process, the voice signal characteristics necessary for a correct interpretation have been identified. A voice mangling algorithm has been designed in order to modify legitimate voice commands so that they become unintelligible for a human while still containing enough spectral content to be correctly interpreted by speech recognition engines. This approach has then been improved resulting in an unnoticeable inclusion of mangled voice commands into video files [CMV+16].

Since, voice assistants have evolved and have been integrated into a wide variety of devices, such as smart speakers or cars. The services they give access to have also evolved and voice assistants became scrutinized from different perspectives. A comprehensive survey on voice assistant security is provided in [YJW+22]. Attacks are categorized in four groups:

- Inaudible signal attacks: the attacker targets the audio front-end to introduce signals inaudible to humans but still interpreted by voice assistants. Several examples of such attacks are given using ultrasound (e.g., [YLZ+20]), light (e.g., [SCR+20]), conducted or radiated IEMI (featuring the research described in this chapter);

- Attacks on the speech recognition engine: the attacker exposes the target to sounds which are not recognized by humans as a voice command, but are still interpreted that way by voice assistants (e.g., [CMV+16]);

- Attacks on the voice recognition engine: recent voice assistants perform a biometric identification of the legitimate enrolled user's voice on the keyword, such identification might be vulnerable to presentation attacks (e.g., [MKMF19]). As a follow-up of the research presented in this chapter, a study on the voice recognition has also been done [KLE17b];

- Attacks on the intent: the attacker tricks the user into launching the wrong application or action by registering command names in the voice assistant which are phonetically very close to other applications or actions (e.g., [ZMF+19]).

4.3 Susceptibility testing

In this section, the method that was followed for susceptibility testing is explained. Two coupling paths have been considered:

- A radiated interaction with the wires of a wired headphone plugged into the target;
- A conducted interaction through the USB charging port of the target.

For each case, the experimental setup is described and the characterization process for assessing the susceptibility of the audio input interface is detailed.

4.3.1 Target description

Several targets have been considered during the tests in order to have a representative set of devices in terms of brands and models, operating system (OS) types and versions, hardware capabilities. However, in what follows, a focus is made on a single specific target which has been easy to prepare and has shown to be very responsive to both radiated and conducted pertubations.

Target specifications

The target is a Samsung Galaxy Nexus smartphone, the Google phone from late 2011. It has the hardware and software specifications [IFi] summarized in Table 4.1 and is depicted in Figure 4.3:

Table 4.1 – Specifications of the Samsung Galaxy Nexus

Feature	Description
Storage	16 GB
Memory	1 GB RAM
Chipset	Ti OMAP 4460
CPU	Dual-core 1.2 GHz Cortex-A9
OS	Android 4.3 Jelly Bean
Voice assistant (voice command interface (VCI))	Google Now v.1.3.large
Sensors	accelerometer, gyroscope, compass, barometer, magnetometer
Front-door interfaces	Wi-Fi 2.4 GHz and 5 GHz (802.11a/b/g/n), NFC 13.56 MHz, Bluetooth 2.4 GHz, GSM/GPRS/EDGE/HSDPA/HSUPA

Target software instrumentation

The targeted functional interface is the analog audio input interface. For applying the approach from chapter 3, it was decided to install an audio recording application on the target. During the tests, two

Figure 4.3 – The target: a Samsung Galaxy Nexus smartphone

applications have been used:

- Sony Audio Recorder [Son]: for high quality recordings and on target storage;
- Wireless MIC [Wir]: for streaming the recorded audio over Wi-Fi, allowing near real-time effect monitoring.

For real-time effect detection, the target was associated to a Wi-Fi access point inside the test facility, which acts also as an ethernet switch. The other front-door coupling interfaces have been left initialized in their default state (e.g., no airplane mode).

4.3.2 Radiated characterization

Radiated coupling has been the first case study. In this case, the characterization was directly focused on exploitation and was made in two steps. First, the feasibility of introducing an audio signal into the audio front-end has been empirically determined. Then, a focus was made on the introduction of voice commands, without optimizing the coupling efficiency.

Tested interaction

In the radiated coupling scenario, the audio input interface was targeted with a radiated IEMI through the headphone cable. The headphone cables enclose an analog microphone, a remote control and are commonly used as an antenna for FM radio broadcast reception on FM capable smartphones. Indeed, their dimensions are comprised between half-wavelength and quarter-wavelength for signals around 100 MHz (FM radio broadcast is located between 65 MHz and 108 MHz, aggregating spectrum regulation from international radio and television organisation (OIRT), Japan and international

telecommunication union (ITU) [Wik22d]). This allows considering the headphones cable as a front-door interface for radiated signals which main spectral components are within this frequency range.

As discussed in chapter 2, analog sensors are known to be vulnerable to AM IEMI and the digitization front-end components non linearities can produce an envelope detection phenomenon. This approach, nicely described in [KBC+13] while targeting a webcam microphone and a wireless headset microphone, results in a digitization of the low frequency modulating component of the coupled signal. As the headphones are targeted as a front-door interface, the carrier frequency of the attack signal can trivially be chosen in the 65–108 MHz range.

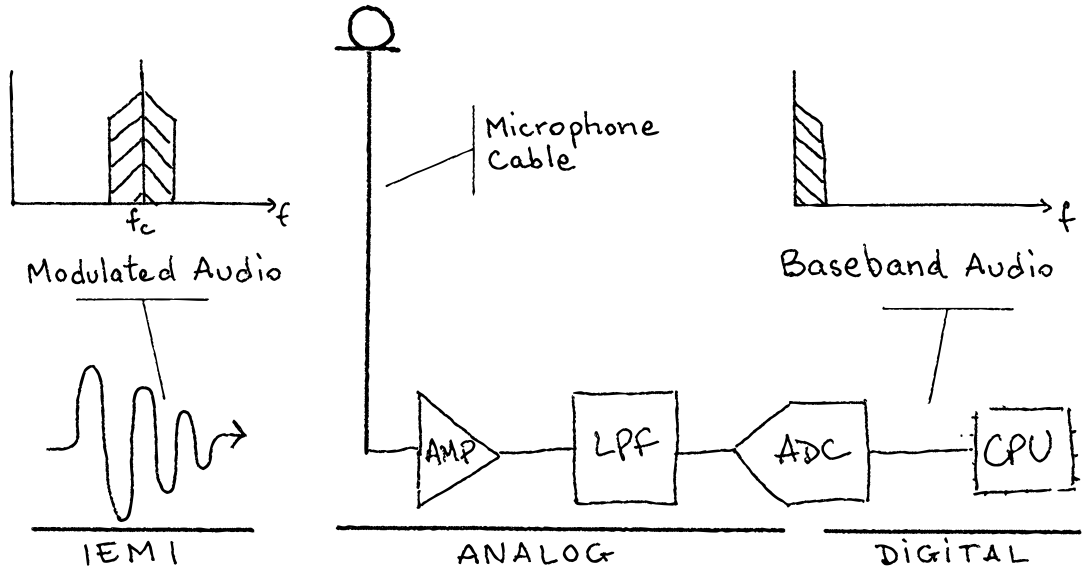


Figure 4.4 – Radiated interaction: the IEMI signal is an audio signal modulating a carrier in amplitude; it gets collected by the headphones cable and the audio front-end components demodulate the parasitic signal and feed the baseband audio to the digital processing parts of the target.

Figure 4.4 shows the whole approach. The transmitted signal consists in an AM audio signal, as the target is the audio input front-end, which has a carrier frequency in [65 MHz, 108 MHz] allowing efficient coupling with the headphone cable. With the non-linearities, the signal should be demodulated, creating a baseband electrical signal in the audio frequency range interpreted as if it was originated from the microphone.

Experimental setup

The target was equipped with its standard out-of-the-box wired stereo headphones which also enclose a microphone and a remote. It was held in a near-vertical position with a custom made foam piece.

The headphones were plugged into the bottom audio female plug connector and the wire was kept in a vertical position by attaching its upper extremity to a desk lamp. The target was battery powered during the tests as no charging cable was plugged into the charging port, in order to limit the connected cables to the headphones cable only. There was no specific effort made to have a precise reproducibility regarding the target positioning as the study was focused on demonstrating the feasibility of the attack. Furthermore, it can also be considered as a more realistic approach, despite of being less prone to a precise comparison of the results.

The tests were run inside a FARADAY cage with the following equipment:

- A Wi-Fi access point ("WiFi" in Figure 4.5) and ethernet switch to bring connectivity (to the internet and/or to a monitoring computer) to the target;
- An ethernet to optical transducer ("E/O" in Figure 4.5) to route signals outside the FARADAY cage;
- A log-periodic antenna (EMCO 3146).

The antenna was placed at the same high as the target and approximately at a one meter distance.

Outside the facility, the setup is completed with devices dedicated to signal generation and effect analysis:

- A computer running a custom piece of software for real-time effects analysis and target monitoring;
- An optical to ethernet transducer ("O/E" in Figure 4.5) for communication with devices inside the cage;
- An IFR 2023A 9 kHz to 1.2 GHz signal generator, configured with an external AM source;
- A 50W1000B Amplifier Research 1–1000 MHz 50 W CW solid state amplifier;
- An audio source, smartphone or computer, playing a song or a voice command in a loop and connected to the signal generator external modulation port.

The full experimental setup is depicted in Figure 4.5.

4.3.3 Conducted characterization

The conducted coupling path was explored after the success of the radiated case study. Due to the complexity of the electrical topology of the target coupling interface, reasoning was less straightforward. Again, the whole system between the physical point of injection and the logical signal obtained

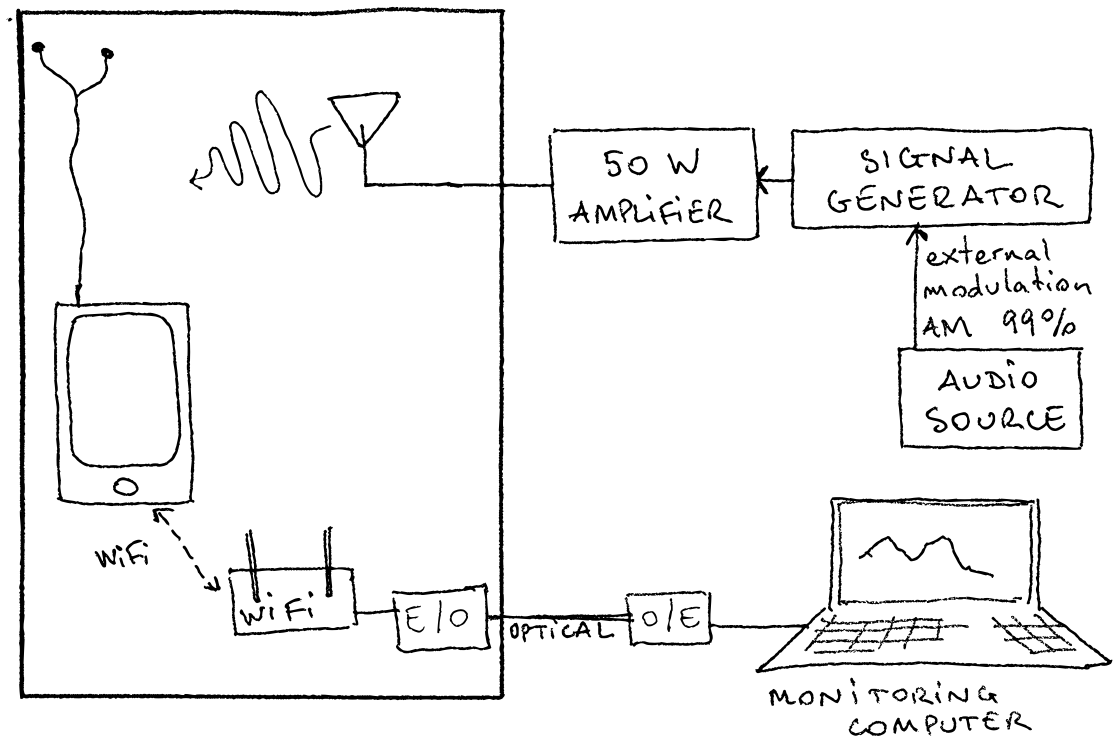


Figure 4.5 – Experimental setup for radiated coupling characterization

has been considered as a black box. However, an effort was made to decompose the approach in order to gain some insight on the underlying phenomena.

Tested interaction

In the conducted coupling scenario, the audio input interface was targeted with a conducted IEMI through the smartphone charging port. The target smartphone charges through a micro-USB to USB cable which is intended to be plugged into a USB charger. In this case, in contrary to the radiated case, there is no first order front-door coupling interface for which a set of efficient carrier frequencies is known. Besides these considerations about the physical coupling path, the same phenomena were expected to occur: the non-linearities of the audio front-end components would perform an envelope detection resulting in a digitization of the low-frequency modulating component of the coupled signal.

Fig. 4.6 shows the whole approach. The transmitted signal consists in an AM audio signal, as the target is the audio input front-end. The carrier frequency has to be first determined in order to maximize the coupling into the audio front-end while avoiding saturation or distortion. Therefore, the characterization was led with a methodology similar to the approach followed in [KBC+13].

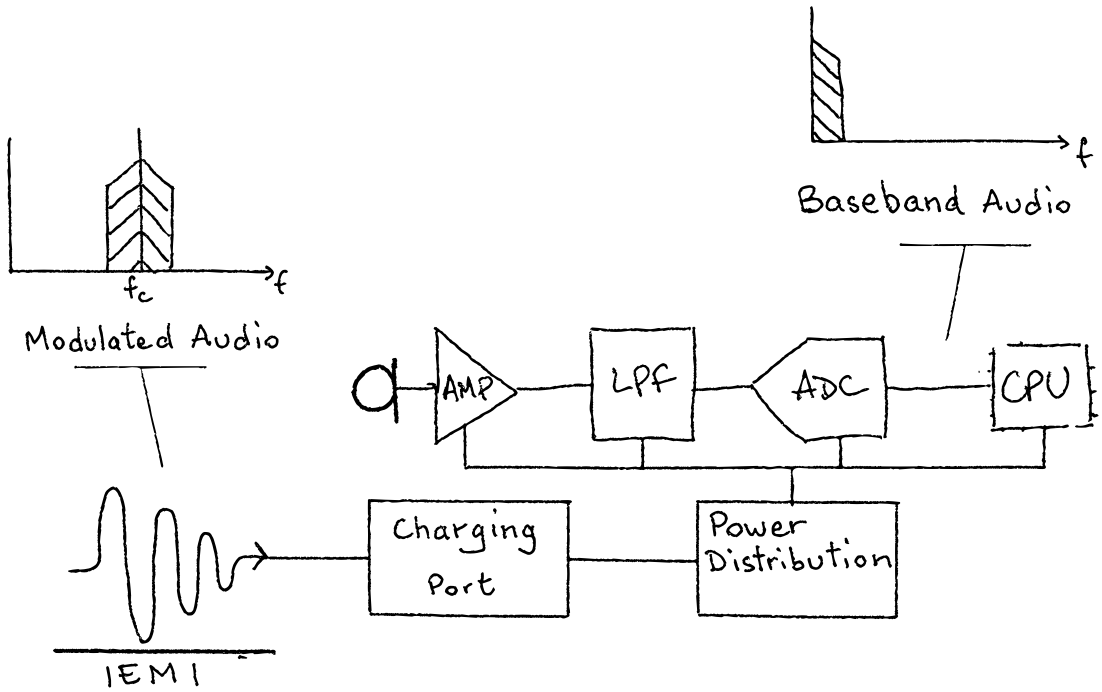


Figure 4.6 – Conducted interaction: the IEMI signal is and audio signal modulating a carrier in amplitude; it is injected in the power network and penetrates the target through its charging port, a parasitic signal reaches the audio front-end and gets demodulated, bringing the baseband audio to the digital processing parts of the target.

Experimental setup

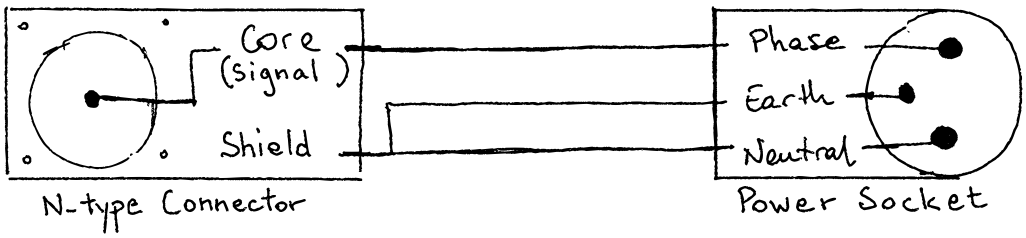
The characterization was done considering two signal injection modes:

- An *offline mode*, where the target charger was not connected to the power network, but to a modified power socket into which the interference was injected;
- An *online mode*, where the target charger was connected to the power network through a power socket.

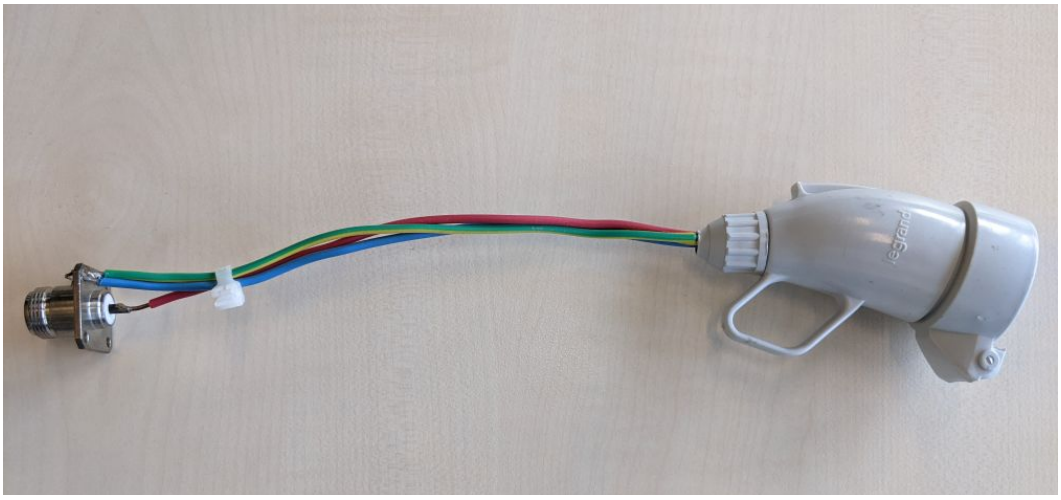
In offline mode, the target smartphone was not connected to the power network and from a hardware and software perspective, it did not consider itself as charging. For introducing the interference signal into the charging port, a custom made power socket adapter has been created in order to route the RF signal coming from the signal source to the two ports of the charger. The schematics of this adapter are shown in Figure 4.7a and the adapter is depicted in Figure 4.7b.

The interference was therefore brought into the charger in differential mode, as the signal was fed into the phase line only.

In online mode, the target smartphone was connected to the power network through a multiple outlet power strip. The interference was injected using a F-140 bulk current injection probe (Figure 4.8a) from Fischer Custom Communications Inc [FCC] clamped around the genuine power strip cable as



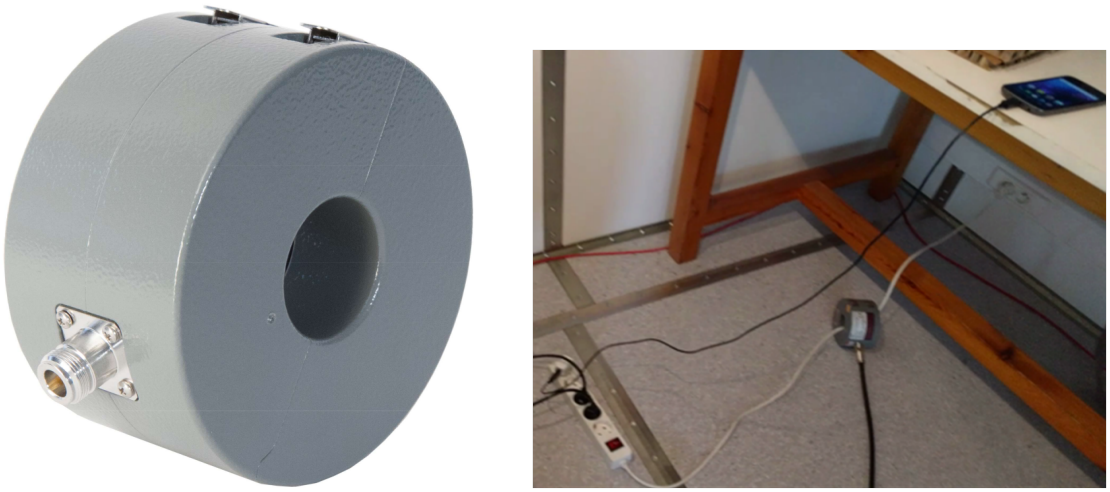
(a) Schematic



(b) Picture

Figure 4.7 – Custom made N-type to power socket adapter used for offline injection

shown in Figure 4.8b. Therefore, in this case, the interference was brought in common mode as we did not instrument the phase line only. A common-mode to differential mode conversion of a parasitic signal injected in the internal power network of a microcontroller has been documented in [JJW+22] and studied in [Bac17] is likely to happen and bring back the interference into a differential mode current.



(a) FCC F-140 bulk current injection probe

(b) Online injection probe clamped on the power cable

Figure 4.8 – The bulk current injection probe used for online testing

In both injection modes, the target smartphone has been disposed on a table inside a FARADAY cage equipped with the following:

- A Wi-Fi access point and ethernet switch to bring connectivity (to the internet and/or to a monitoring computer) to the target;
- An ethernet to optical transducer to route signals outside the FARADAY cage.

The setup is completed with devices dedicated to signal generation and effect analysis:

- A computer running VLC media player for real-time effects analysis;
- An optical to ethernet transducer for communication with devices inside the cage;
- An IFR 2023A 9 kHz to 1.2 GHz signal generator, configured in AM mode with a sweep from 1 Hz to 23 kHz;
- A 50W1000B Amplifier Research 1–1000 MHz 50 W CW solid state amplifier.

A picture showing an experiment during offline testing is given in Figure 4.9.

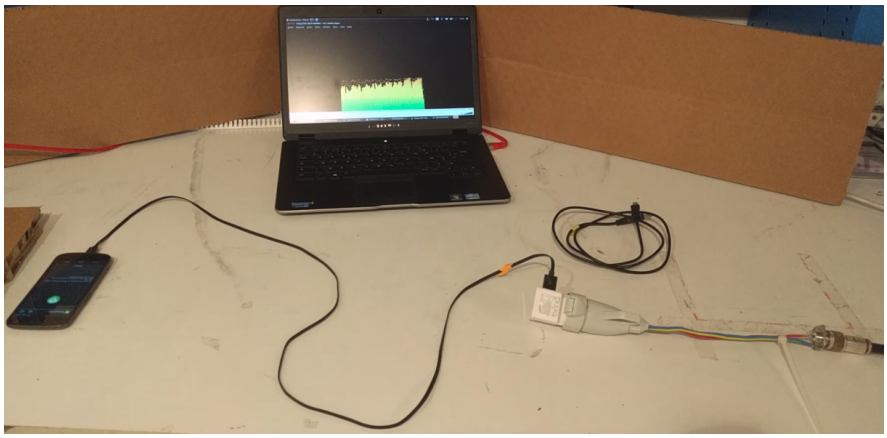


Figure 4.9 – An example of test setup for offline characterization: the target (left) was connected to a USB charger (white), which in turn was plugged to the custom adapter. An application streaming the audio input via Wi-Fi is running on the target. The stream is analyzed on a computer (the spectrogram view of VLC media player).

4.3.4 Results

Radiated IEMI

The characterization in the radiated case was focused on the exploitation of the voice assistants. The carrier frequencies of the AM IEMI were known in advance due to the first order front door coupling mode interface characteristics. Therefore, the experiments were focused on coarsely determining the characteristics of the source, in terms of emitted power, required to obtain a successful interpretation of the injected commands by the voice assistant.

To this end, the carrier frequency has been arbitrarily set to 103 MHz. The modulating audio signal involved in this characterization phase was a recording of a voice saying the keyword and a command for opening the Gmail application, which comes bundled in every Android release. The payload was saying "OK Google, démarrer Gmail", as the system was configured in French.

Voice command injection was successful for output power values close to 0 dBm fed from the signal generator into the 50 W amplifier. Electric field values at the target position were measured with a Dare Development RadiSense CTR1001B laser powered electric field sensor. The order of magnitude was approximately in the range $25\,\mathrm{V}\cdot\mathrm{m}^{-1}$-$30\,\mathrm{V}\cdot\mathrm{m}^{-1}$.

This showed the feasibility of this interaction mode to remotely introduce voice commands interpreted by voice assistants. Other audio payloads have been considered in order to test several exploitation scenarios.

Conducted IEMI

Off-line testing allowed for characterizing the impact of the elements of the propagation path on the injected signal.

With this configuration, the elements on the signal propagation path are limited to the charger and the USB charging cable. Furthermore, as these are not connected to the power network, only the injected signal propagates towards the target, with no additional noise due to the power network or the loads connected to it.

The determination of the target resonant frequencies was done following the methodology described in [KBC+13]. The emitted signal parameters were fixed to arbitrary values except for the carrier frequency. The modulating signal frequency was fixed to a 1 s sweep from 1–23 000 Hz and the emitted signal was set with a constant output power.. On the target, the audio input was recorded and the peak amplitude was calculated over the 1 s windows containing the sweeps while exploring several carrier frequencies.

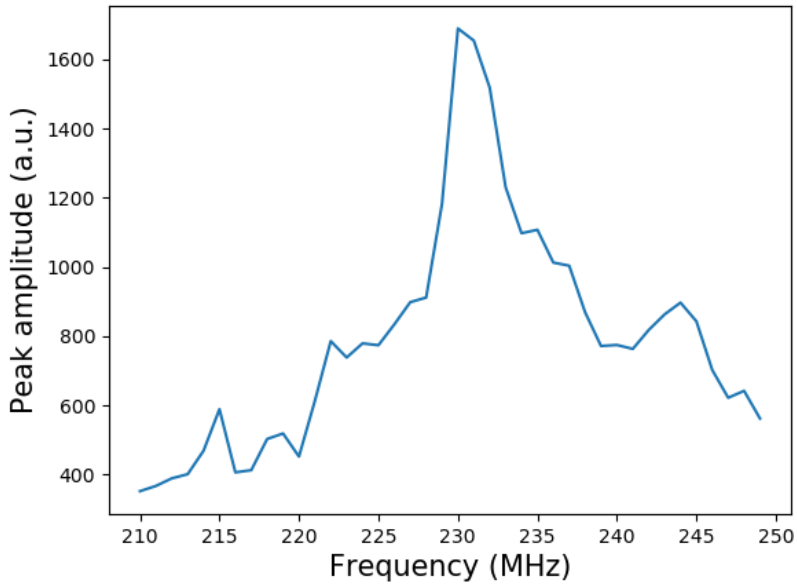


Figure 4.10 – Resonant frequencies between 210 MHz and 250 MHz

An example result of this resonant frequency search phase is provided in Figure 4.10, which shows the recovered peak amplitude relatively to the carrier frequency between 210 MHz and 250 MHz.

It appears that in this frequency band, the strongest induced signal corresponds to carrier frequencies around 231 MHz. To analyze the quality of the recorded audio signal, two complementary approaches have been considered. The first simply consisted in submitting voice commands at the detected resonating frequency and use the voice assistant as an oracle for sound quality. A similar

approach has been followed in [KBC+13] using the Shazam music recognition service as an oracle. The second consisted in analyzing the spectral content of the recorded audio signal resulting from the injection of a 1–23 000 Hz sweep modulating a 231 MHz carrier. This approach was used to identify potential filtering elements on the propagation path. It was also useful to compare the contribution of several components of the propagation path. More precisely, two USB chargers and several USB cables have been tested.

The offline characterization has led to the determination of resonant frequencies of the target allowing to maximize the induced signal amplitude. The potential filtering elements on the propagation path have also been assessed and it has been observed that under 17 kHz the response was flat, which gave a good confidence in the preservation of the spectral characteristics of the audio signal. Figure 4.11 shows the spectral content of the recorded audio signal resulting from the injection of a 1–23 000 Hz sweep modulating a 231 MHz carrier.

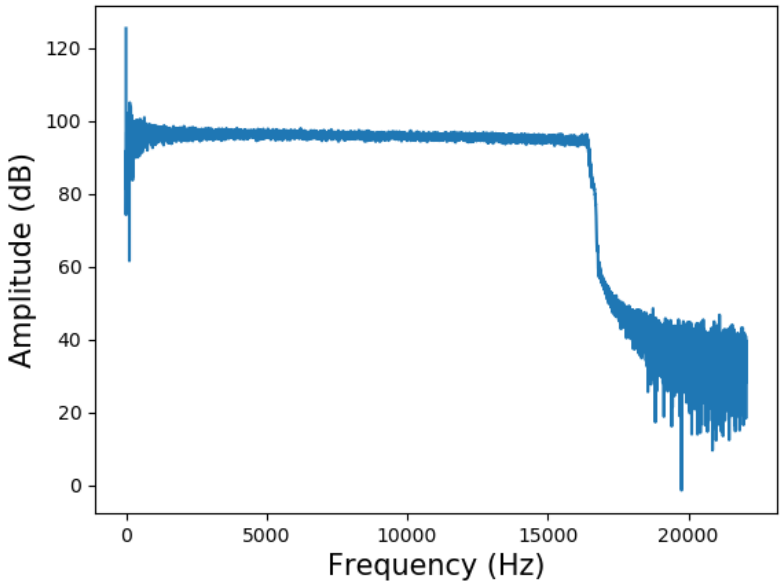


Figure 4.11 – Spectrogram of the injected audio signal

Figure 4.11 shows the spectral content of the recorded audio signal resulting from the injection of a 1–23 000 Hz sweep modulating a 231 MHz carrier.

4.4 Security discussion

4.4.1 Exploitation scenarios

The feasibility of using a narrow band AM IEMI for remotely injecting voice commands into smartphone audio front-ends such that they get interpreted correctly by voice assistants has been characterized. In this section, several exploitation scenarios are provided considering both the operational conditions enabling one of the studied EM interactions and the outcome for the attacker.

Radiated voice command injection

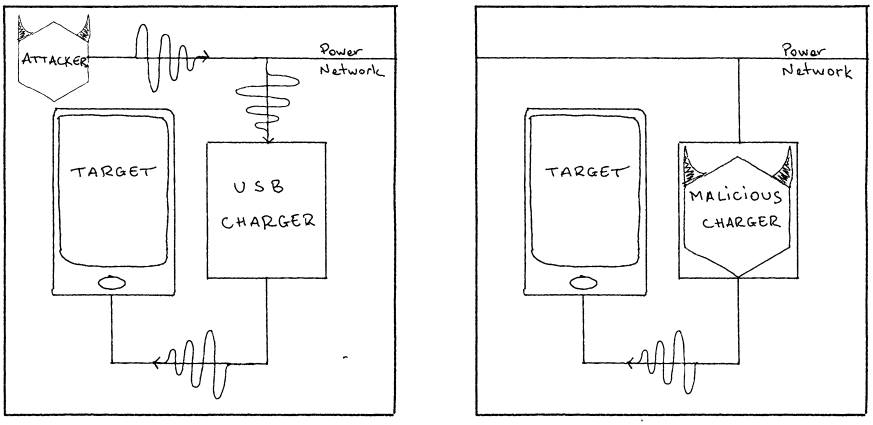
Due to the electric field levels needed to introduce a parasitic audio signal processed correctly by voice assistants, the most plausible scenario would be of an attacker located only a few meters away from the target. In this scenario, wired headphones with a microphone have to be plugged in and the voice assistant has to be awaiting for the keyword. If the user is using the headphones, he should hear audio feedback from the voice assistant when it is triggered. He might also hear some noise during the emission of the attacker signal.

Conducted voice command injection

Two injection scenarios were envisioned for the conducted case, where the injection point is at different locations in the low voltage power network. Again, the voice assistant has to be awaiting for the keyword (which is supposed to be the case when the target smartphone is charging). In this case, the activity of the voice assistant (feedback sounds, confirmation phrases) might be heard if the target is not mute. Furthermore, the user could also notice visually that there is an activity on the target.

Scenario 1: Smartphones are charging through an USB charger connected to the power network: in this context, the devices are connected to the power network through a genuine power charger provided by the manufacturer. The point of injection of the parasitic signal is located somewhere in the power network behind the power socket. The electromagnetic waves have to by-pass the transformers and the EMC high-pass filters encountered in the propagation path. The signal attenuation might be highly dependent on the power network topology and the connected electrical equipment.

Scenario 2: Smartphones are connected to a malicious USB power charger dock: this scenario is likely to be the most efficient as there are less filtering elements on the propagation path of the parasitic signal. Indeed, the point of injection is located within the charger directly on the output power signal of the USB charging cable. A modified USB charging device (or a portable power bank) is considered here, which is able to properly provide the power required by the target device (5 V,



(a) Scenario 1 (b) Scenario 2

Figure 4.12 – Charging scenarios considered for the exploitation tests

150 mA for USB 1.0, until 240 W in USB type C 2.1) and also to superimpose a malicious parasitic signal intended to exploit the voice interface. The target device is thus directly exposed to the parasitic signal.

Voice assistant unauthorized use

If an attacker is successful in introducing arbitrary audio signals into a target smartphone, he will be able to emit voice commands towards the voice assistants. As a result, the attacker could virtually perform any action exposed on the vocal interface. Some scenarios where an attacker could be interested in taking advantage of this possibility are given below.

Audio spying: The attacker sends a voice command to place a phone call to his own eavesdropping phone, doing so he is able to listen to the targets surrounding acoustic environment.

Paid services: The attacker sends a command to subscribe to paid services via text messages or to place a call to a premium-rate number in order to earn money.

Reputation or phishing: The attacker exploits the communication features accessible by voice, text messages, emails or social networks to publish information that can be compromising for the user, or containing links to malicious content.

Advanced compromising: The IEMI could be used as a primary interaction leading to a second attack step. The voice interface could be used to visit a malicious website for example, which would then try to exploit a software vulnerability on the target smartphone. The activation of wireless interfaces would expose the target smartphone to threats related to active wireless interfaces, such as detection and tracking [Wil14], or even zero-click exploitation of software vulnerabilities as

in [Bee20, Ben17b, Ben17a].

4.4.2 Countermeasures

This study illustrates a two-stage exploitation resulting in a stealth, remote and unauthorized abuse of voice assistants. The first stage takes advantage of the electrical and microelectronic design of the targets and their robustness against IEMI and results in an injection of malicious signals into their audio front-end input stage. This possibility emphasizes the fact that from an information security point of view, standard EMC practices provide limited protection. Indeed, their scope is limited to unintentional parasitic signals and do not take a malicious behavior of an attacker into account. For software security engineers, input interface filtering against malicious inputs is a common practice. Electronic devices destined to critical applications should enforce the same principles on their interfaces (analog, digital and power inputs) by properly filtering signals the closest to their operational frequency band, integrating filters or designing low-level sub-domains mutually isolated on the PCB.

The second stage takes advantage of the access control for the voice interface. Since the deployment of voice assistants, editors seem to have been focusing on its ease of use in order to identify potential usages and encourage its adoption by end-users and service providers. As a consequence, it can be foreseen that the number of critical actions achievable via voice assistants will keep increasing. As voice commands could be submitted and executed without the user noticing, editors could consider several layers of countermeasures. Voice recognition for authenticating (or at least identifying) the user would force the attacker to forge or to acquire voice samples of the target user. Challenge-response confirmation protocols, such as audio captchas, would make it necessary for an attacker to intercept the challenge in order to forge a response signal. Allowing for personalizing the keyword would also impose an information gathering step for an attacker and restrict the exploitation to a targeted attack. In order to both make the user more conscious of the risks and allow for tuning the impact of this vulnerability, editors should provide finer grain settings for choosing which actions and which applications should be available through voice assistants, and which should require an authentication. Finally, to further mitigate the risk for security unaware users, editors should set up secure default settings and inform the user of the risks when he opts for less secure settings.

4.5 Conclusion

This chapter was focused on exploiting the effects of IEMI on analog microphones enclosed in smartphones in order to obtain a remote, stealthy and unauthorized access to voice assistants. Two ways

for the IEMI to reach the target have been explored. First, a radiated first-order front-door coupling on the headphones wire was considered. Then, a conducted interaction through the charging port has been demonstrated. To the author's knowledge, this was the first proof of concept of a conducted IEMI on smartphones.

In both cases, the attacker's goal was a signal injection into the audio input front-end. The IEMI signal was composed of a signal in the target interface frequency band (audio) modulating the amplitude of a carrier with a frequency determined empirically to provide an injected signal with enough quality.

Logical effects have been studied with a software instrumentation of the target. Then, exploitation scenarios have been determined and the possibility to introduce voice commands correctly interpreted by voice assistants has been demonstrated. Again, the possibility of using IEMI to exploit voice assistants had not been explored before.

However, the characterization of EM interactions could be further investigated. The whole propagation chain has been considered as a black box and studies dedicated to getting insight on the underlying phenomena would be relevant. Regarding the radiated approach, it would be interesting to analyze the impact of different headphone cable positions on the attack success. A (conducted) direct injection test campaign into the audio front-end (via the jack plug) would also help understanding the parasitic signal parameters that lead to the envelope detection. Regarding the conducted experiments, a rigorous analysis of the injection modes would provide valuable information both from an EMC and anInfoSec perspectives. More precisely, comparisons of online injection and offline injection, common mode and differential mode (on phase and on neutral) would allow reasoning on the best attack scenario and would probably provide base information to understand how the IEMI signal reaches the audio front-end from the charging port and on common mode to differential mode conversion mechanisms.

From an information security perspective, the most practical scenario is probably the conducted injection from a malicious custom charging station. However, the EM interactions involved are target specific and the attack parameters (frequencies, required power) are very likely to change with the target brand, model, operating system version, voice assistant version, biometric voice model state (if vocal identification is enabled). This means that an attacker would have to perform a characterization of each potential target before practical exploitation.

As a possible further work, it would be interesting to develop a source prototype for the online conducted injection. It could be a device with the circuitry dedicated to generate and amplify the IEMI signal and superimpose it to the power signal. It could perform the injection into the low

voltage network through the power socket or directly to a target device (through a USB cable or a USB charger). An advanced version with a microphone could be able to synchronize and react to audio feedback from the voice assistant.

Regarding voice assistant security, several challenges still remain, the first being the usability / security trade-off . The threat of an unauthorized use of this interface is still only mitigated by a voice biometrics identification. In biometrics community, voice is considered among the less reliable characteristics [BBB+03]. Furthermore, the identification is performed only on the keyword, which gives very few information to build models as it is intended to be very short. For these reasons, attack surface and impact reduction strategies seem the most relevant. Attack surface reduction would imply to allow the user to easily enable and disable the voice assistant or even to provide a way to define when to do so. Impact reduction would consist in giving the possibility to define several profiles for which the available voice commands are listed along with a confirmation level required to launch them (e.g., voice confirmation, voice challenge-response, PIN authentication). This would place the user at the center of the security strategy and compensate the limitations related to the mitigation of unauthorized use by both audible acoustic interaction and by inaudible signal injection attacks.

4.6 References

[App21] Applidium/Cracking-Siri. Applidium, 2021. 100

[Ass] Assistant Google – Toujours là pour vous. https://assistant.google.com/intl/fr_fr/. 98

[Bac17] Yann Bacher. *Study and Modelling of the Disturbances Produced within the STM32 Microcontrollers under Pulsed Stresses*. Theses, Université Côte d'Azur, 2017. 109

[BBB+03] Jean-Francois Bonastre, Frédéric Bimbot, Louis-Jean Boe, Joseph P. Campbell, Douglas A. Reynolds, and Ivan Magrin-Chagnolleau. Person authentication by voice: A need for caution. In *Proc. 8th European Conference on Speech Communication and Technology (Eurospeech 2003)*, pages 33–36, 2003. 117

[Bee20] Ian Beer. Project Zero: An iOS zero-click radio proximity exploit odyssey, 2020. 115

[Ben17a] Gal Beniamini. Project Zero: Over The Air - Vol. 2, Pt. 1: Exploiting The Wi-Fi Stack on Apple Devices, 2017. 115

[Ben17b] Gal Beniamini. Project Zero: Over The Air: Exploiting Broadcom's Wi-Fi Stack (Part 1), 2017. 115

[CMV+16] Nicholas Carlini, Pratyush Mishra, Tavish Vaidya, Yuankai Zhang, Micah Sherr, Clay Shields, David Wagner, and Wenchao Zhou. Hidden voice commands. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 513–530, Austin, TX, 2016. USENIX Association. 101

[DLZZ14] Wenrui Diao, Xiangyu Liu, Zhe Zhou, and Kehuan Zhang. Your Voice Assistant is Mine: How to Abuse Speakers to Steal Information and Control Your Phone. In *Proceedings*

of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices, SPSM '14, pages 63–74, New York, NY, USA, 2014. Association for Computing Machinery. 100

[FCC] FCC F-140 BCI Probe - Fischer CC. 107

[Gon14] Niel Gonzalez. Siri Exploited—Again: How to Bypass the Lock Screen in iOS 8 (& How to Protect Yourself). https://ios.gadgethacks.com/how-to/siri-exploited-again-bypass-lock-screen-ios-8-protect-yourself-0157749/, 2014. 100

[IFi] iFixit - Samsung Galaxy Nexus Repair. https://fr.ifixit.com/Device/Samsung_Galaxy_-Nexus. 102

[JJW+22] Y. Jiang, X. Ji, K. Wang, C. Yan, R. Mitev, A. Sadeghi, and W. Xu. WIGHT: Wired ghost touch attack on capacitive touchscreens. In *2022 2022 IEEE Symposium on Security and Privacy (SP) (SP)*, pages 1537–1537, Los Alamitos, CA, USA, 2022. IEEE Computer Society. 109

[KBC+13] Denis Foo Kune, John Backes, Shane S. Clark, Daniel Kramer, Matthew Reynolds, Kevin Fu, Yongdae Kim, and Wenyuan Xu. Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors. In *2013 IEEE Symposium on Security and Privacy*, pages 145–159, 2013. 104, 106, 111, 112

[KLE15a] Chaouki Kasmi and José Lopes Esteves. IEMI and Smartphone Security: A smart use of front door coupling for remote command execution. In *Asia Electromagnetics Symposium (ASIAEM 2015)*, Jeju-si, Jeju Province, South Korea, 2015. 96

[KLE15b] Chaouki Kasmi and José Lopes Esteves. IEMI threats for information security: Remote command injection on modern smartphones. *IEEE Transactions on Electromagnetic Compatibility*, 57(6):1752–1755, 2015. 96

[KLE16] Chaouki Kasmi and José Lopes Esteves. Whisper in the Wire: Voice Command Injection Reloaded. In *Hack In Paris*, Paris, France, 2016. 96

[KLE17a] Chaouki Kasmi and José Lopes Esteves. Electromagnetic Threats for Information Security: Ways to Chaos in Digital and Analogue Electronics. In *34th Chaos Computer Club Congress*, Leipzig, Germany, 2017. 96

[KLE17b] Chaouki Kasmi and José Lopes Esteves. Ventrilock: Exploring Voice-based Authentication Systems. In *Hack In Paris 2017*, Paris, France, 2017. 100, 101

[LEK15a] José Lopes Esteves and Chaouki Kasmi. Injection de commandes vocales sur ordiphone. In *Symposium Sur La Sécurité Des Technologies de l'Information et Des Communications (SSTIC)*, Rennes, France, 2015. 96

[LEK15b] José Lopes Esteves and Chaouki Kasmi. You don't hear me but your phone's voice interface does. In *Hack In Paris 2015*, Paris, France, 2015. 96

[LEK18] José Lopes Esteves and Chaouki Kasmi. Remote and Silent Voice Command Injection on a Smartphone through Conducted IEMI: Threats of Smart IEMI for Information Security. *System Design and Assessment Note SDAN*, 48, 2018. 96

[MKMF19] Mirko Marras, Pawel Korus, Nasir D. Memon, and Gianni Fenu. Adversarial Optimization for Dictionary Attacks on Speaker Verification. In *Interspeech 2019*, 2019. 101

[SCR+20] Takeshi Sugawara, Benjamin Cyr, Sara Rampazzi, Daniel Genkin, and Kevin Fu. Light commands: Laser-Based audio injection attacks on Voice-Controllable systems. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 2631–2648. USENIX Association, 2020. 101

[Sir] Siri. https://www.apple.com/fr/siri/. 98

[Son] Sony Audio Recorder 1.00.35 APK Download by Sony Mobile Communications. 103

[VZSS15] Tavish Vaidya, Yuankai Zhang, Micah Sherr, and Clay Shields. Cocaine noodles: Exploiting the gap between human and machine speech recognition. In *9th USENIX Workshop on Offensive Technologies (WOOT 15)*, Washington, D.C., 2015. USENIX Association. 101

[Wei15] Wang Wei. Apple Admits Siri Voice Data is Being shared with Third Parties. https://thehackernews.com/2015/03/apple-siri-voice-data-sharing.html, 2015. 100

[Wik21] Wikipedia. Google Now. https://en.wikipedia.org/w/index.php?title=Google_Now&oldid=1057019621, 2021. 98

[Wik22a] Wikipedia. Amazon Alexa. https://en.wikipedia.org/w/index.php?title=Amazon_Alexa&oldid=1115506606, 2022. 98

[Wik22b] Wikipedia. Bixby (software). https://en.wikipedia.org/w/index.php?title=Bixby_(software)&oldid=1106343600, 2022. 98

[Wik22c] Wikipedia. Cortana (virtual assistant). https://en.wikipedia.org/w/index.php?title=Cortana_(virtual_assistant)&oldid=1116467521, 2022. 98

[Wik22d] Wikipedia. FM broadcast band. https://en.wikipedia.org/w/index.php?title=FM_broadcast_band&oldid=1104228366, 2022. 104

[Wik22e] Wikipedia. Google Assistant. https://en.wikipedia.org/w/index.php?title=Google_Assistant&oldid=1109330344, 2022. 98

[Wik22f] Wikipedia. S Voice. https://en.wikipedia.org/w/index.php?title=S_Voice&oldid=1092994255, 2022. 98

[Wik22g] Wikipedia. Siri. https://en.wikipedia.org/w/index.php?title=Siri&oldid=1116468224, 2022. 98

[Wil14] Glenn Wilkinson. The machines that betrayed their masters. In *Black Hat Asia 2014*, 2014. 114

[Wir] Wireless MIC APK pour Android Télécharger. https://apkpure.com/fr/wireless-mic/com.shenyaocn.android.WirelessMIC. 103

[YJW+22] Chen Yan, Xiaoyu Ji, Kai Wang, Qinhong Jiang, Zizhi Jin, and Wenyuan Xu. A Survey on Voice Assistant Security: Attacks and Countermeasures. *ACM Computing Surveys*, 2022. 97, 100, 101

[YLZ+20] Qiben Yan, Kehai Liu, Qin Zhou, Hanqing Guo, and Ning Zhang. SurfingAttack: Interactive hidden attack on voice assistants using ultrasonic guided wave. In *Network and Distributed Systems Security (NDSS) Symposium*, 2020. 101

[ZMF+19] Nan Zhang, Xianghang Mi, Xuan Feng, XiaoFeng Wang, Yuan Tian, and Feng Qian. Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1381–1396, 2019. 101

Chapter 5

Bridging air gaps with IEMI

Contents

5.1 Chapter overview

The research featured in this chapter is the result of a collaboration with Dr. Chaouki KASMI, Dr. Valentin HOUCHOUAS and Philippe VALEMBOIS at ANSSI between 2015 and 2016. Several publications have been made in conferences focusing on IEMI [HKLEV16, KLEV16b, KLE16a, KLE16b] and InfoSec forensics [KLEV15, KLEV16a, LEK16]. Overall, this work has been cited in more than 20 papers from the fields of EMC, cyber-physical systems security, physical covert channels.

In this chapter, the EM susceptibility of an analog temperature sensor in a desktop computer is assessed and exploited so as to set a covert communication channel up with a malicious software implant. This exploitation scenario is particularly relevant when considering an air-gapped target computer, i.e. belonging to an information system which is isolated from unsecure information systems (e.g., connected to the internet) in order to mitigate the risks coming from a communication with remote entities.

Information systems protected by an air gap are pretty common when it comes to manipulating highly sensitive or classified information. Therefore, this security measure is widespread in critical infrastructures and governmental institutions. When applied correctly, an air gap consists in a complete physical removal of any communication interfaces between information systems of different security contexts. As a consequence, it becomes very hard for an attacker to interact with air-gapped computers remotely. One of the residual vulnerabilities which would enable this interaction is the possibility for an attacker to set a physical covert communication channel up. This requires the presence of a software implant on the target and a shared physical interface with the attacker which can convey information.

The shared physical interface can be the EM environment, and as explained in chapter 1, several studies focused on exploiting software controllable EM spurious emissions in order to create an outbound covert channel, a class of attacks called soft-tempest. However, the work presented in this chapter is the first to propose the exploitation of EM susceptibility of a target in order to create an inbound covert communication channel, allowing for an attacker to send information to a software implant on the target.

As a result, a software implant has been developed which behaves as a receiver, listening to a logical interface impacted by the EM susceptibility of the CPU temperature diode electronic circuit of the target computer and awaiting for known frames. The susceptibility of the temperature diode has been assessed along with the resulting covert channel capacity, which has shown to be bound by the sampling rate of the logical interface.

This chapter is organized as follows: the main principles of air gaps are presented and a review of air gap bypass techniques, which involve physical covert channels, is proposed in section 5.2. Section 5.3 details the characterization of the EM susceptibility of the target interface. Then in section 5.3.4, the method for setting the covert communication channel up and determining the channel capacity is explained. Finally, a security discussion is proposed in section 5.4.

5.2 Air gap: principle and limitations

5.2.1 Principle

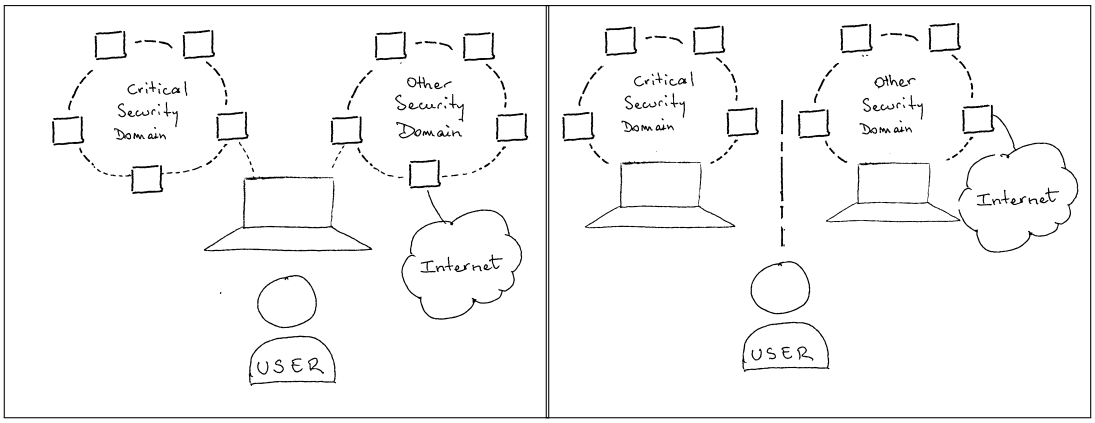
Most critical infrastructures, organizations and companies have to compose with several information systems with different levels of trust. In order to communicate with external entities and access public information, there is a need for internet connectivity. Besides, internal information systems are in place, both for internal organizational processes and operational processes, some of them being more sensitive or critical.

Good information system security practices [ANS20, RWM22] involve a partitioning of the information system into security domains and the enforcement of security policies between security domains based on how data and information must be protected. This partitioning of security domains can include considerations of classification of the information and is the root of multi-level security [And20]. Security policies in this context concern the control of information flows between security domains.

The permeability between security domains introduces security risks and several practices can be applied in order to mitigate this attack vector, such as firewalls, diodes, virtualisation or air gaps.

The air gap is a security measure which consists in isolating physically a sensitive security domain from the other ones. The physical isolation usually involves a complete dedication of all information technology resources in order to avoid sharing hardware or software with other security domains and a suppression of communication interfaces with other security domains. Figure 5.1 illustrates the partitioning of an information system into two security domains of different sensitivity. An air gap is set up in order to minimize the existing interfaces between the critical security domain and other security domains (e.g., the security domain connected to the Internet), thus reducing the attack surface of the critical security domain.

However, the air gap is a security measure which comes with several drawbacks and limitations. Information technology costs are substantially higher due to the hardware and software duplication. Air gaps are very constraining for users which have to constantly switch between several machines,



(a) Before the air gap, several security domains coexist on the same computer

(b) With the air gap, the critical security domain is physically isolated

Figure 5.1 – Air gap between a critical security domain computer and an internet connected computer

manage accounts and passwords, and as information flows between isolated domains are usually still required, technical and organizational security procedures might be really annoying. If air gap benefits are misunderstood by users, the acceptability of the constraints is likely to be low and as a consequence, the security provided by this measure can be weakened due to wrong user behavior. As the next section will show, the exploitation residual vulnerabilities of air-gapped systems may be facilitated in this case.

5.2.2 Review of air gap bypass techniques

The air gap consists in a physical and logical segregation of security domains. Therefore, circumventing an air gap implies the introduction of a communication channel between computers belonging to two security domains. This is why it is also called "air gap bridging". As the communication channel used for bridging an air gap is neither intentional nor legitimate, it is called a covert channel.

Covert channels

A covert channel consists in unidirectional or bidirectional communication between entities which are not allowed to communicate using a channel not intended for communication [Lam73]. Three classes of covert channels are identified in [Car16]: host-based, network-based or air gap-based covert channels and are defined as follows:

- Host-based covert channels create a communication between processes on a host [MWZ+16], such as shared file system or shared hardware [PGM+16]. They can be based either on storage or on timing.

- Network-based covert channels create a communication between remote processes on connected hosts. The information can be hidden in protocol data unit (PDU) or through the timing of PDUs or protocol commands [MWZ+16, PGM+16, TA05].

- Air gap-based covert channels create a communication between remote processes on disconnected hosts by the exploitation of shared physical medium such as light, pressure, vibration, sound, temperature, electromagnetic environment or noise [SB09]. They are also called physical covert channels.

Following the covert channel taxonomy, a general threat model for air gap bridging can be defined as follows (Figure 5.2):

- Machine A belongs to a security domain H
- Machine B belongs to a security domain L
- A and B are air-gapped
- The attacker has introduced a software implant S_A in A and S_B in B
- The attacker's goal is to establish a communication from S_A to S_B or from S_B to S_A

Software implants S_A and S_B interact with a covert exploit [Car16] (which can be different on A and B), which provides access to the covert communication channel, and implement a method for establishing a communication over this channel, which actually reduces to a traditional communication problem (performing the appropriate modulation, channel and source coding schemes). Covert exploits are called invasive if they imply a hardware modification of the target, semi-invasive if they require a software modification of the target (e.g., a privilege escalation) and non-invasive if no modification of the target is necessary to access to the communication channel.

Wireless communication interfaces abuse

While machines A and B are intended to be isolated from each other with an air gap, they may enclose and operate wireless communication interfaces. Obviously, isolating A from B does not exclude the possibility of A communicating with other entities from security domain H through wireless protocols (same stands for B in security domain L). In this case, a covert exploit could benefit from this link in order to provide access to a covert channel.

In [BGAS16], direct interaction with a RF front-end is used to introduce polyglot modulations: an over-modulation of an already modulated signal by modifying complementary parameters (between

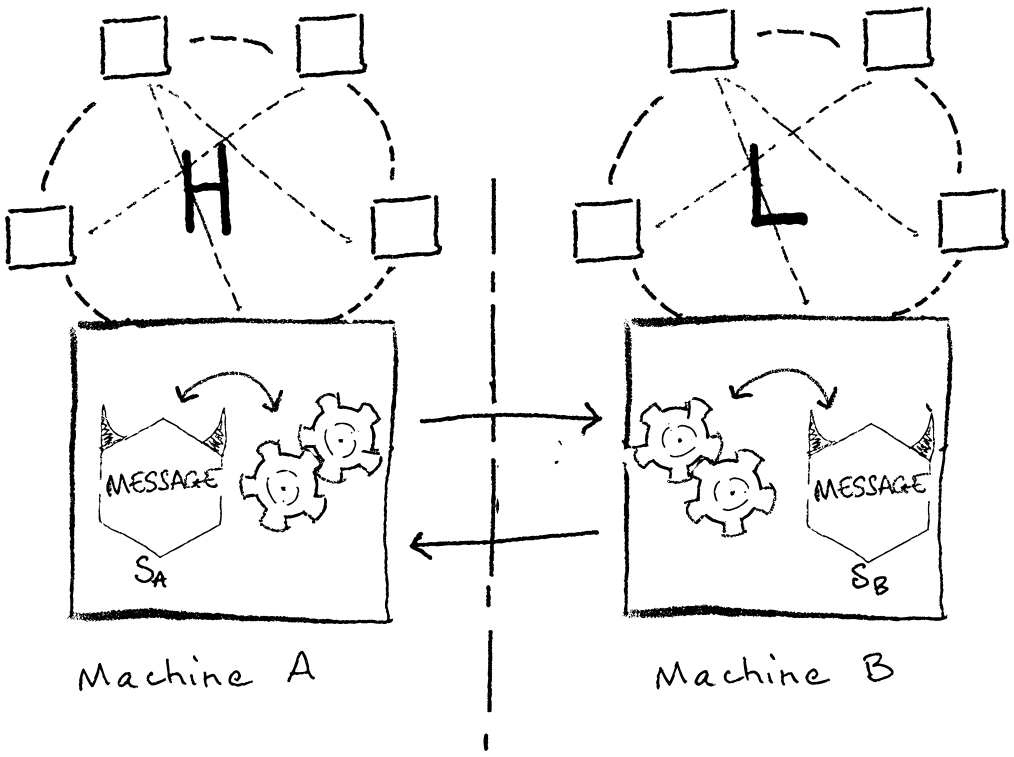


Figure 5.2 – Air gap bridging with a covert channel: a threat model

phase, amplitude and frequency). As a result, signals carrying a legitimate information flow can be modulated to introduce a covert communication flow, such as a signal carrying simultaneously a phase shift keying (PSK) and a on-off keying (OOK) modulations. Extending this concept, in [LECK17, LECK18] the possibility of an EM interaction between a low power soft-tempest leakage source and a RF front-end leading to polyglot modulations is demonstrated.

The possibility of establishing a covert communication by jamming a (802.11) RF receiver is explored in [SB09]. Cross-technology communication can allow for using a RF front-end dedicated to a certain legitimate protocol (e.g., Zigbee) in order to send packets compatible with another protocol (e.g., Bluetooth low energy), as demonstrated in [CGA+21]. The same idea had been investigated by [GBM+11] but with an interaction in the upper layers of the wireless communication. More precisely, it has been shown that a 802.15.4 payload containing application layer data encoded as a whole MAC layer 802.15.4 frame could be, on the receiver side, interpreted as a legitimate frame.

In cases where wireless communication interfaces have no legitimate reason to be used, they might have been logically disabled. However, trusting such logical removal of interfaces is questionable as it can surely be reversible by a privileged piece of software (i.e., part of a semi-invasive covert exploit). Furthermore, disabling logically a wireless communication interface does not necessarily

imply the interruption of the hardware RF front-end activity. For example, in Android smartphones, disabling Wi-Fi or enabling airplane mode does no shut down the Wi-Fi chipset, which stays active for precise geolocation. The wireless chipset could also run malicious code [SM15] and keep providing a software implant with a wireless communication interface despite a logical deactivation by the operating system.

Shared peripherals

It can also happen that machines A and B share simultaneously or alternatively peripherals. For example, there might be a need for exchanging data between A and B and a USB mass storage peripheral could be used. Another common example is the temptation to share human interface devices, such as displays, keyboards, mice...

Although it is quite obvious that a USB mass storage used alternatively on A and B can be abused as a storage covert channel, it is not the case for other types of shared peripherals which are not explicitly dedicated to data storage. However, peripherals are embedded systems which enclose persistent storage capabilities in order to store firmware or configuration data. When these storage capabilities can be read or written by the host, these can provide a covert storage channel.

Furthermore, peripherals implement host-peripheral communication protocols which can sometimes also provide covert timing channels, especially when peripherals are shared through peripheral sharing devices such as a KVM switch. Such threats are considered by secure switching device manufacturers as mandated by the Peripheral Sharing Device CC Protection Profile [NIA19]. In [LER21], a filtering device is installed on a HDMI link in order to suppress unwanted channels involving displays.

Hardware implants

To establish a communication channel between two isolated machines with no common communication interface, a pretty straightforward possibility is to equip both machines with a hardware implant enclosing a communication interface. In 2013, a NSA offensive tooling catalog was published [EFF14], which contains a toolset dedicated to bridging air gaps with hardware implants hidden into USB connectors. They were given the codename COTTONMOUTH and the technical description indicates that they are covert exploits enclosing a short-range wireless interface.

This strategy is not restricted to state-sponsored anymore as several products exist for InfoSec audit professionals. For example, the USB Ninja [USB] is a crowdfunded Bluetooth capable embedded system which is to be connected to a target computer's USB port in order to provide a wireless remote

access to the target via human interface device (HID) USB (e.g., keyboard and mouse). The OMG cable [MG] is a Wi-Fi capable embedded system which can be enclosed (hidden) into a USB cable or an Apple Lightning cable. Again, it aims at providing security auditors with a way to remotely send payloads to an air-gapped target machine.

Out-of-band covert channels

Out-of-band covert channels are air gap covert channels that are enabled by semi-invasive and non-invasive covert exploits and have been extensively studied in [Car16]. In this category, the covert exploits provide an interface to a shared physical characteristic that can be modulated by the sender and measured by the receiver. In other words, the practicality of attacks based on out-of-band covert channels is conditioned by the presence of resources on the sender side enabling the modulation (called the modulator) and by the presence of sensing resources on the receiver side enabling reception and demodulation (called the demodulator). Therefore, when it comes to risk analysis, it is relevant to consider two cases for the sender and receiver: if resources are already present in the targets or if custom hardware is needed for these modulating or demodulating capacities.

A survey of out-of-band covert channels has been proposed in [CA16] and five physical channels have been referenced.

Acoustic Proposals of using sound waves as a carrier for a covert communication have mostly focused on ultrasonic (over 20 kHz) or near-ultrasonic (in 17–20 kHz) frequencies. Widespread modulators (audio speakers) and demodulators (microphones) are present in commodity hardware which is the main benefit of this physical channel. For this reason, acoustic covert channel studies considered covert signals below 24 kHz as most COTS audio devices support a 48 kHz sampling rate. For example, in [HG13], an acoustic covert network between several laptops in the 17–20 kHz range at a speed of 20 bits per second is evaluated up to a distance of 19.7 m. Exotic demodulators have been investigated: the possibility of configuring sound cards to use loudspeakers as audio input has been explored in [LKY16] demonstrating a speaker to speaker communication reaching 8 bits per second up to 7 m in the 3–6 kHz frequency range and up to 10 cm in the ultrasonic range. The possibility of exploiting unintended modulators, which can be considered a form of acoustic soft-tempest, has also been demonstrated. For example, modulating the rotation speed of fans [GSE20] or exploiting the piezoelectric effect of electronic components of computer power supplies [Gur21b] have been proposed recently.

Light Visual indicators, screens or light emitting diode (LED) being pretty common, using light as a cover channel has been considered in several studies. The most common demodulators for this

kind of channel would be ambient light sensors and video cameras. Modulating LEDs of electronic equipment has been proposed in [LU02]. In [HSH+13], modulating intensity of light bulbs in order to communicate with a demodulator accessing to an ambient light sensor on a smartphone has been demonstrated. Exotic demodulators were considered in [NSE17], where a software implant in a scanner was receiving information sent by a smart light bulb and a laser source.

Thermal A thermal covert channel requires a modulator being able to change the temperature in the environment of a demodulator temperature sensor. It is proposed in [Bit] to use the room's temperature to communicate. In the proposed scenario, the attacker can control the air conditioning and heating system of the room the target is in. Exploiting that, it has been demonstrated that the target computer can then monitor the temperature reported by its internal sensors and retrieve the data, resulting in a very low bandwidth covert channel. The main drawback of thermal channels is the very low bandwidth due to the thermal inertia.

Magnetic Malware command and control using magnetic signals has been explored in [HSH+13] where the modulator is a programmatically-controlled electromagnet and the demodulator is a smartphone's magnetometer. In [Gur21a], the modulator controls the CPU workload in order to send data collected by a smartphone's magnetometer a few centimeters away.

Radio-frequency Out of band covert channels using RF signals to carry information were extensively studied in the context of data exfiltration, i.e. an outgoing communication channel. In this case, the threat is called soft-tempest, where a software implant controls an EM emission source it modulates to send information. A detailed review of soft-tempest is provided in chapter 1 (section 1.4.1). Commonly considered demodulators are embedded (COTS) radio receivers or specialized electromagnetic signal analysis equipment.

A summary of out of band covert channel performance is proposed in [Car16] and synthesized in Table 5.1.

Table 5.1 – Summary of out of band covert channels performance, inspired from [Car16](only maximum values were kept);

Covert channel	Acoustic	Light	Thermal	Magnetic	RF
Order of data rate (bps: bits per second)	10^3 bps	10^2 bps	10^{-3} bps	1 bps	10^2 bps
Order of distance	10^1 m	meters	meters	10^{-1} m	10^1 m

In the next sections, an out of band RF unidirectional incoming air gap bridging covert channel is proposed, exploiting the susceptibility of the CPU diode of a desktop computer.

5.3 Design and exploitation of a EM-based physical covert channel

5.3.1 Target specification

The target was a desktop computer running a Debian 7.4 operating system and equipped with the following hardware components:

- QDI Platinix 2-A motherboard;
- Intel Pentium-IV CPU;
- Winbond W83627HF-AW SuperIO controller;
- PS/2 IBM 89P8310 keyboard and DELL LZC3425959 mouse;
- HEDEN XP-V7.5C-350W ppower supply;
- TP-LINK TL-WN751ND 802.11n PCI Wi-Fi card;
- Intel PRO 100 PCI Ethernet controller;
- DELL monitor.

According to the CPU datasheet [Cor04], the CPU package contains an on-die thermal diode to provide a thermal sensor chip located on the main board with a way to monitor the die temperature for thermal management. The thermal diode's anode and cathode are exposed through two pins which are routed to the SuperIO chip. The documentation of the SuperIO [Win02] indicates that an 8-bit ADC is specifically dedicated to temperature measurement from Intel CPU thermal diodes. The recommended electrical schematics of the thermal diode interface with the SuperIO chip are given in Figure 5.3.

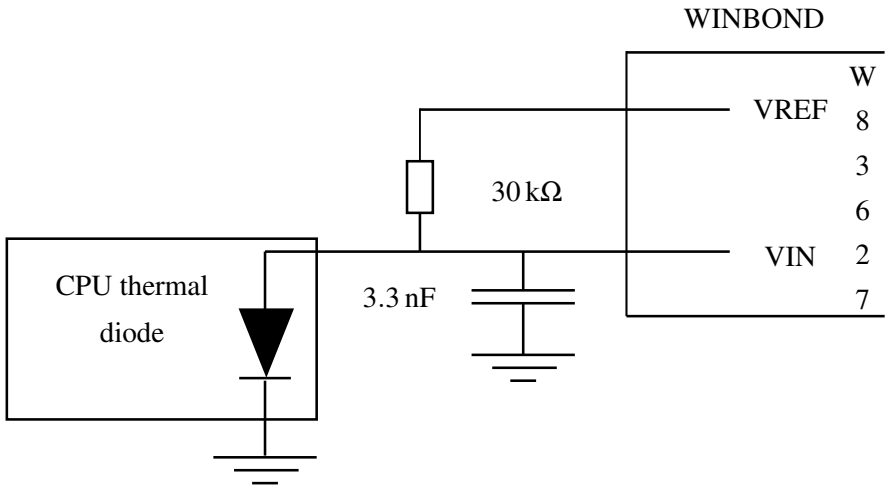


Figure 5.3 – Recommended electrical schematics of the thermal diode - SuperIO interface routing (from [Win02])

In order to communicate with the CPU, the SuperIO chip exposes a low pin count (LPC) interface which can be configured with a 24 MHz or a 48 MHz clock speed.

5.3.2 Target software instrumentation

The targeted functional interface is the analog CPU temperature diode. Applying the approach proposed in chapter 3, a software dedicated to interactions with a set of sensors present on the host. The Debian package called *lm-sensors* [Deb] has been installed and the host has been scanned for available sensors. The CPU temperature was accessible as the *temp1* value from the *acpitz-acpi-0* sensor in *lm-sensors* output.

A *bash* script (Listing 5.1) reading the temperature in a loop and logging it into the system logs every second was used to perform a first characterization of the EM susceptibility of the target.

Listing 5.1 – bash one-liner for continuous monitoring of the temperature

```
while true; do sensors acpitz-acpi-0 | sed -n 3p | logger ; sleep 1; done
```

System logs are natively stored by the operating system, providing a way to access to measurements after test campaigns. The operating system was configured to forward the system logs to a remote computer over the ethernet interface in order to allow a real-time monitoring of the effects on the CPU temperature interface.

5.3.3 Radiated characterization

An analysis of the susceptibility of the target interface against a radiated IEMI has been performed. Effects on the CPU temperature reported by the target were used as a susceptibility criterion.

Tested interaction

The thermal diode is an analog sensor and its output is processed by an ADC. The physical target is the electrical interface between the CPU thermal diode and the SuperIO chip ADC input. Therefore, an AM IEMI has been considered because of the potential rectification effect due to the non-linearities of the digitization stage, as explained in chapter 2. Figure 5.4 shows the approach. The transmitted signal consists in an AM signal which will be used as a baseband covert communication and which has a carrier frequency that provides an efficient coupling with the target physical interface. The carrier frequency has been determined in order to maximize the coupling while avoiding saturation or unwanted side-effects (e.g., target rebooting).

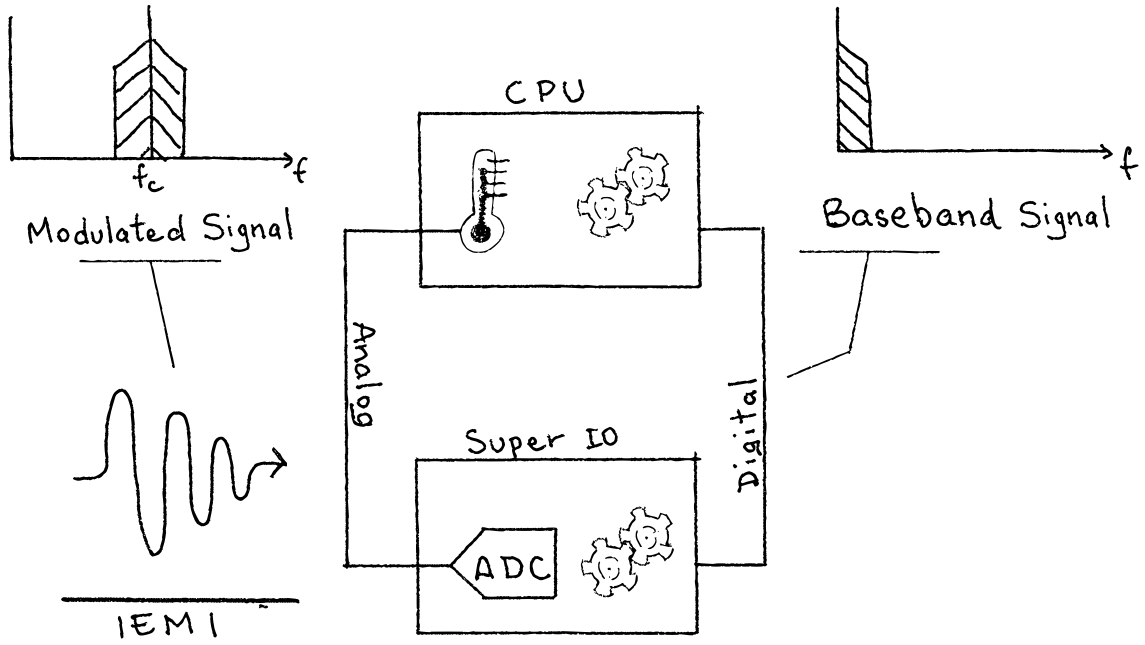


Figure 5.4 – Radiated interaction with the thermal diode measurement circuit

Experimental setup

The target desktop computer was positioned on a table inside a FARADAY cage, initialized in a nominal configuration with its keyboard, mouse and VGA display. It has been connected to a monitoring computer located outside of the FARADAY cage with an ethernet link transiting through ethernet-optical transducers, in order to forward the temperature readings in real time during susceptibility testing. The IEMI signal was radiated by a log-periodic antenna (EMCO 3146). The left side panel of the computer chassis has been removed during the tests and a electric field probe has been placed inside the computer chassis.

Outside the facility, the setup was completed with devices dedicated to signal generation and effect analysis:

- A computer running a custom piece of software for real-time effects analysis and target monitoring;
- An optical to ethernet transducer ("O/E" in Figure 5.5) for communication with devices inside the cage;
- An USRP B200 software defined radio from Ettus Research controlled by a laptop running

GNURadio [GNUa, GNUb] signal processing software to generate the signal;

- A 50W1000B Amplifier Research 1–1000 MHz 50 W CW solid state power amplifier.

The full experimental setup is depicted in Figure 5.5.

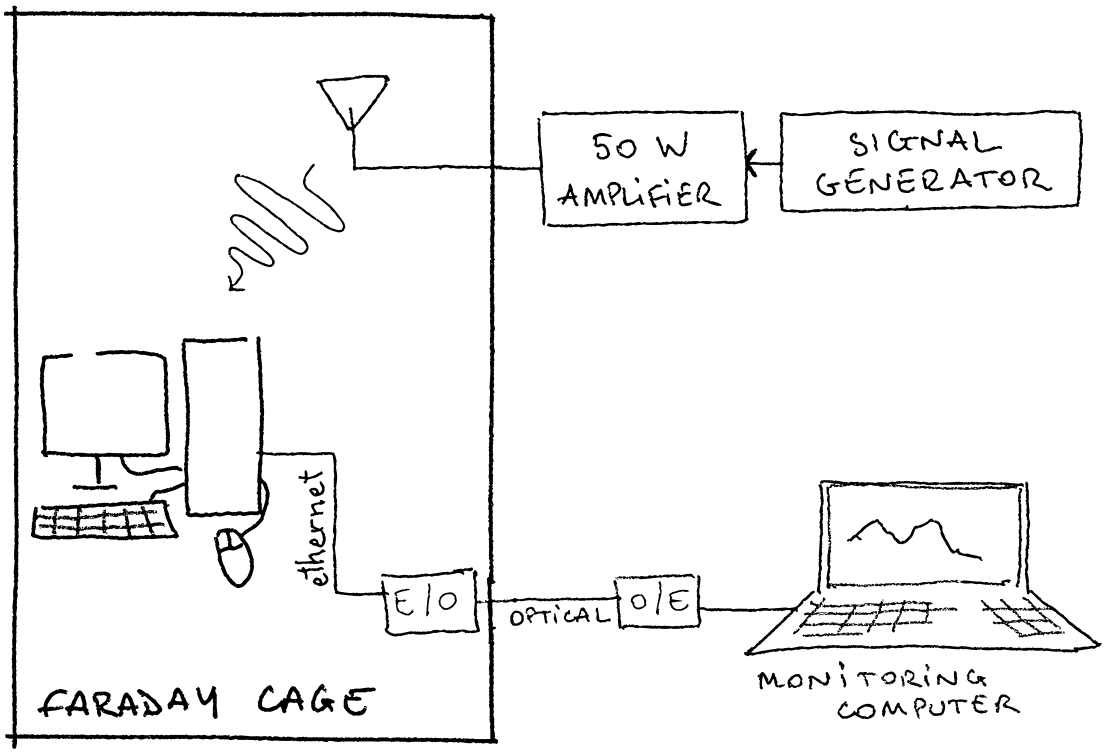


Figure 5.5 – Experimental setup for radiated coupling characterization

First results

Several IEMI carrier frequencies have shown to provide effects on the temperature readings. In some cases collateral effects were also happening simultaneously: computer fan speed increased, system rebooted.

A precise characterization of efficient carrier frequencies has been left as future work. For an arbitrarily fixed carrier frequency of 2 GHz which has shown to produce effects on the temperature reading without side-effects, an analysis of the impact electric field magnitude on the effect intensity has been done. The electric field probe, placed inside the target computer chassis, was used to measure the electric field magnitude. Figure 5.6 shows that the temperature offset is monotonically increasing with the electric field magnitude. This observation confirms the possibility of performing an amplitude modulation of the temperature reading values by modulating the electric field magnitude.

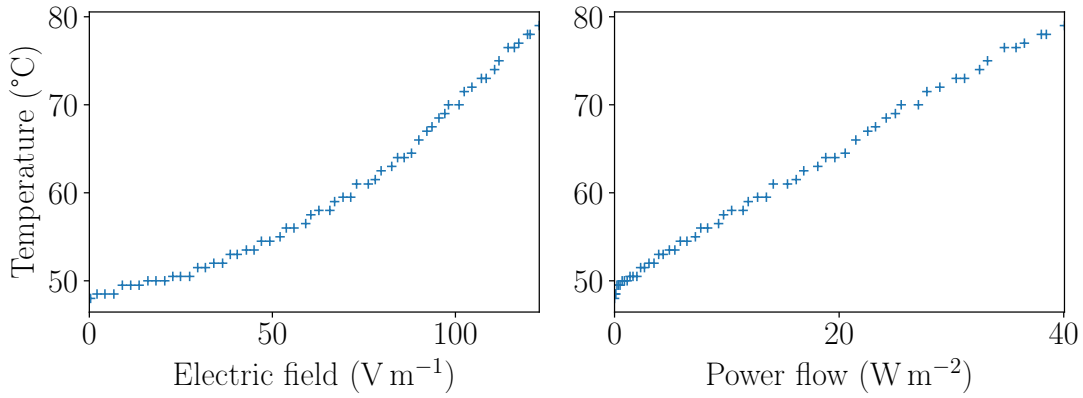


Figure 5.6 – Relationship between electric field magnitude and temperature reading offset

5.3.4 Covert exploit design

Based on the possibility of inducing reading errors on the temperature sensor we created a proof of concept receiver. In order to set-up a mono-directional communication link between the computer under test and the control and command source, a software implant was implemented which monitors the temperature level and seeks for a known pattern.

Considering that a high level of emitted signals introduced temperature reading errors and that the temperature was decreasing instantaneously when the source was stopped, the carrier CW signal was first modulated using a OOK scheme. A 0-symbol meant that no RF field was emitted and a 1-symbol meant that a RF field was radiated.

As the time needed to query sensors was not constant, the sampling of temperature had some jitter. To immunize the decoder against de-synchronization, a Manchester coding was chosen. Manchester coding makes clock recovery easier because there is a transition for each bit transmitted. The clock must have a frequency twice higher than the bit-rate and the bit sequence is XORed with the clock sequence. As a consequence, the clock is included in the signal with the data.

In order to start the recording and the decoding of the sent commands, a frame format has been chosen, starting with a preamble. The chosen preamble was a Barker sequence of 7 bits, prepended by a 0 bit which gave the bit sequence “01110010”. The Barker sequence facilitates the detection of starting packets by autocorrelation. The preamble was followed by a size field indicating the size of the data payload to let the decoder determine when to end the sampling.

The frame composition is shown in Table 5.2.

Table 5.2 – Frame format for the covert communication

Bit offset	0 - 7	8 - 15	16 - $15 + Size \times 8$
Field	Preamble	Size (bytes)	Payload

The demodulator consisted in monitoring continuously the temperature reported by the sensor. The results were then continuously averaged. When the measured temperature was higher than 1.05 times the average, a logical high was read. Otherwise, a logical low was read.

An example frame received by the covert exploit is shown in Figure 5.7.

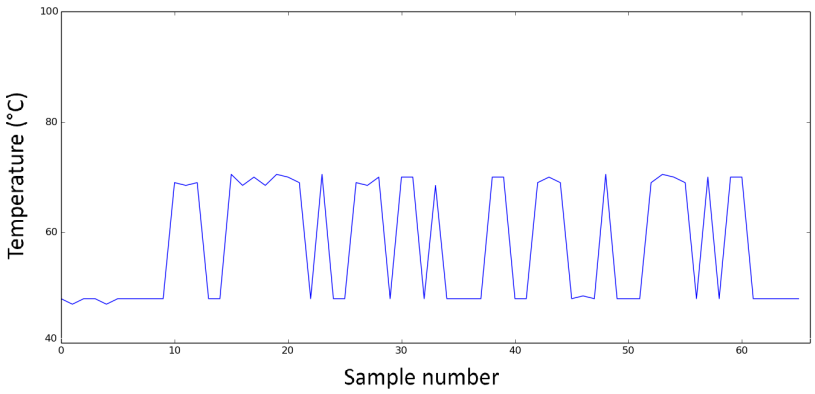


Figure 5.7 – Example OOK frame sampled by the covert exploit

Each level was then mapped to a symbol 0 (low) or 1 (high). Then, based on the observation of symbol changes, it was possible to correct the timing and recover the bits transmitted. The sampling rate needed to correctly decode the bits was then four times the bit-rate: twice to isolate each symbol (according to the Nyquist-Shannon sampling theorem) and twice to decode the Manchester coding and get the bit sequence.

The bit-rate is therefore related to the hardware and software time constraint for accessing the temperature sensor measurement. After the first proof of concept covert exploit, ways to increase the transmission rate were explored. The first potential bottleneck was the analog signal acquisition chain. In order to accelerate the software access to the temperature reading, it was decided to stop using the *lm-sensor* tool suite, as the thermal diode temperature value was only updated every second. A custom driver was developed in order to query directly the SuperIO chip for updated temperature values. However, the maximum temporal sensitivity that was obtained was way slower than the code querying the SuperIO chip.

It was empirically determined by increasing the modulation frequency (i.e., reducing the symbol time) until the covert exploit was not able to sample symbol changes anymore. In Figure 5.8, an upper bound for the sampling rate can be determined, as no variations shorter than 100 ms are captured by the covert exploit.

Knowing this maximum sampling rate, a second proof of concept was prototyped including changes in the transmission choices. A 4-amplitude shift keying (ASK) modulation has been chosen and a new source coding has been proposed, with a preamble containing a sequence of the four

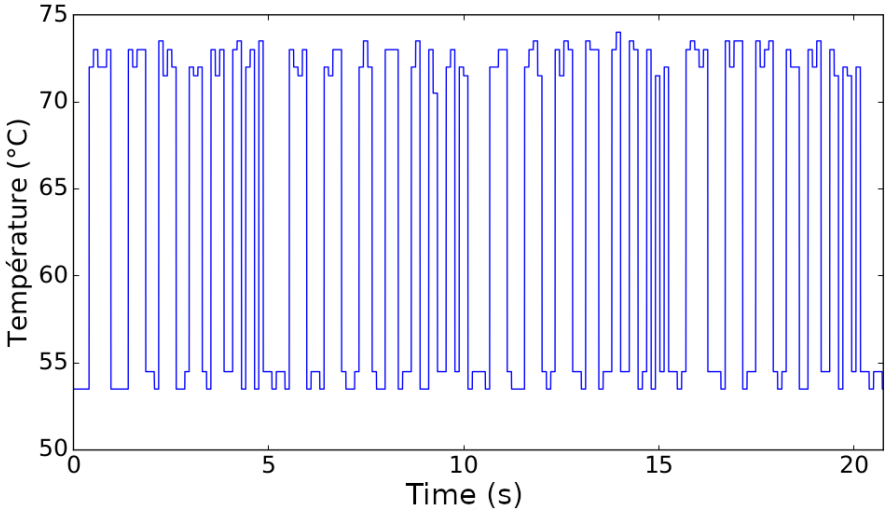


Figure 5.8 – Empirical determination of the maximum sampling rate of the covert exploit: the minimum temporal sensitivity is 100 ms

symbols. In Figure 5.9, a source baseband frame encoding "hello scientists!" and the frame sampled by the covert exploit are shown. During the experiments, a bit rate of 10 bits per second was obtained.

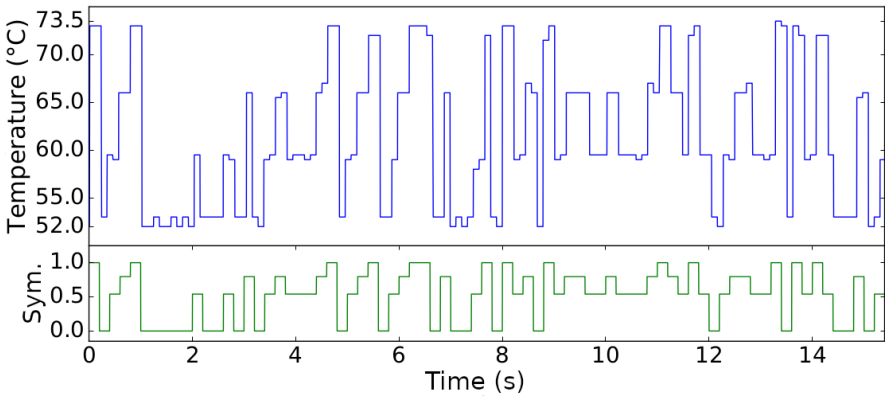


Figure 5.9 – An example 4-ASK frame as received by the covert exploit and corresponding symbols coded before modulation by the sender

5.3.5 Channel capacity

Two proof of concept covert exploits were designed providing different communication channel characteristics. From an InfoSec viewpoint, the maximum transmission rate is an interesting characteristic as it would allow to determine the criticality of the presence of the covert channel. This theoretical upper bound for the transmission rate is called the channel capacity. Several approaches were proposed to estimate the channel capacity for covert channels [Car16], including the well-known Shannon capacity [Sha48]. In order to simplify the determination of the channel capacity, several approximations are made. These approximations provide an overestimation of the channel capacity which can be enough for InfoSec risk analysis.

- The channel is considered a noiseless discrete channel;
- The symbol rate that was measured on the demodulator side is considered;
- The maximum number of symbols is directly derived from the ADC specification.

The channel is considered a noiseless discrete channel, which implies that considerations related to the IEMI source, the signal propagation, coupling and the quantization noise are discarded. Under this assumption, the channel capacity C is defined as follows:

$$C = \lim_{t \to \infty} \frac{\log_2 N(t)}{t} \tag{5.1}$$

where $N(t)$ is the number of allowed signals of duration t.

The maximum number of symbols can also be bound by the maximum number of values sampled by the ADC, which is an 8-bit ADC according to the specification of the SuperIO chip [Win02]. Therefore, the maximum number of representable symbols is $N = 2^8$. Assuming the N symbols are equiprobable, the number of possible signals of duration t can be written:

$$N(t) = N^{R_{sym} \cdot t} \tag{5.2}$$

which gives

$$\frac{\log_2 N^{R_{sym} \cdot t}}{t} = \frac{R_{sym} \cdot t \cdot \log_2 N}{t} = R_{sym} \cdot \log_2 N$$

which simplifies equation 5.1:

$$C = R_{sym} \cdot \log_2 N \tag{5.3}$$

To determine the maximum symbol rate, the Nyquist rate was considered, i.e., that at least two samples per symbol were required to avoid distortion due to sampling. Considering the maximum sample rate of the covert exploit that was experimentally determined $R_{samp} = 10\,\mathrm{S} \cdot \mathrm{s}^{-1}$, the symbol rate is derived as $R_{sym} = 0.5 \cdot R_{samp} = 5\,\mathrm{Sym} \cdot \mathrm{s}^{-1}$.

These considerations yield a worst case channel capacity $C = R_{sym} \cdot \log_2 N = 40\,\mathrm{bps}$.

5.4 Security discussion and countermeasures

Most studies on covert channels focus on outbound communication channels with the objective of data exfiltration from an isolated computer. This threat model is certainly inherited from the field of multi-level security and the Bell-Lapadula model, which focuses on controlling information flows

from a high classification level to a low classification level. In the Bell-Lapadula model, an entity from the low classification level writing information into a high classification entity is not considered as a problematic flow [And20]. However, if a primary infection is considered, i.e., a software implant may be running on the high classification entity, new threats arise and the Bell-Lapadula properties are not sufficient anymore.

A software implant on an air-gapped system can benefit from an inbound (covert or overt) channel. First, the software implant could be waiting for commands or triggers in order to execute the right payloads synchronously with other attacker actions. In this case, low bandwidth channels may still be interesting for the attacker.

Due to size constraints, the software implant code might have been reduced to a minimal set of functions for the primary infection. An inbound communication channel would give the possibility to update the executable code of the software implant and to expand its offensive functionalities. This possibility has also been investigated with the idea of providing executable code to a software implant running on a platform implementing code attestation or block program code from being written at runtime [PPB16].

Most studies related to out of band covert channels exhibit interfaces reachable by covert exploits in order to send or receive information over the considered communication channel. Feasibility is usually demonstrated empirically with proofs of concept tested in a laboratory environment. The metrics provided to evaluate the performance of the covert channels, to compare to related work are very often limited to the maximum communication rate and the maximum distance that were achieved experimentally. Unfortunately, communication rate and distance depend on transmission choices (e.g., modulation, source and channel coding...) and on the physical channel characteristics. A good example is given in this chapter, as two transmission choices are tested and provide different communication rates. Therefore, the provided figures can neither be compared to nor be generalized.

An estimation of the channel capacity seems to be a much more relevant metric to evaluate the performance of the covert channel and the impacts in terms of InfoSec risk analysis. This can be really challenging, especially when the threat model involves a specific modulator or demodulator, which characteristics are not specified. The covert channel presented in this chapter involves a specific modulator, the IEMI source, which is unspecified (e.g., in terms of maximum power). To cope with this difficulty, a worst case channel capacity has been determined using Shannon's discrete noiseless channel capacity formula and by making assumptions which result in an overestimation of the actual channel capacity. The calculated worst case channel capacity informs about the maximum achievable transmission rate with a semi-invasive covert exploit independently of the IEMI source and the prop-

agation and coupling conditions. In the framework of an InfoSec risk analysis, this information might be sufficient to decide if the risk is acceptable.

5.4.1 Countermeasures

The air gap is a very constraining security measure which provides a better control over information flows between machines from different security domains. As it has been shown in this chapter, residual vulnerabilities exist which might still result in uncontrolled communication between security domains. Exploiting these vulnerabilities to this end implies setting covert channels up.

Setting a covert channel up first requires a preliminary infection which lets the attacker benefit from a software implant on both ends of the channel. This is a fundamental prerequisite and this primary infection is to be avoided. Thus, technical and organizational good practices to prevent and detect malware infection shall be applied on both security domains. Remaining necessary cross-domain data flows should be supervised, controlled and filtered. Benefits of the air gap should be explained to users so that to increase the acceptability of the constraints and reduce the temptation of deceptive behaviour and misconceptions about the risks.

Of course, it is important that users follow the security policy, especially the restrictions related to the usage of peripherals. The introduction of uncontrolled peripherals (such as personal peripherals) and the use of peripherals on machines from different security domains increase the probability of primary infection and might provide storage covert channel media. Potential covert channels through hardware implants are also more likely to happen.

If possible, wireless communication interfaces should be physically removed from critical security domains. If not, a supervision of the RF activity could allow to detect anomalies and abuses. In [Cay22], a RF intrusion detection system is proposed based on a monitoring of the physical layer activity in a chosen part of the RF spectrum. In [LECK17, LECK18], an approach was proposed to detect physical layer covert channels carried by legitimate RF channels by inspecting the receiver's correction factors (e.g., equalization, carrier recovery...) looking for periodicity (e.g., cyclostationary analysis).

For out of band covert channels, a combination of technical and organizational countermeasures can be applied. The main principles will rely on a limitation of modulation and demodulation interfaces and with a limitation of the propagation of the carrier signals. The limitation of the propagation of the signals involve the equivalent of filtering, shielding and zoning for each physical medium. The limitation of intentional modulation and demodulation interfaces implies removing unnecessary input-output interfaces (e.g., microphones and speakers). For unintentional interfaces, their detection

and characterization should ideally be done but might be quite challenging in practice.

Lastly, it might be relevant, if out of band covert channel attacks are considered, to introduce specific detection procedures focusing on covert exploits in malware analysis solutions. To do so, it is worth noticing that a covert exploit needs to implement a transmission stack, i.e., source and channel (de)coding, (de)modulation... Furthermore, the covert exploit might also try to find an available channel by enumerating resources. These might be the most characteristic behaviours to focus on.

5.5 Conclusion

A novel method for setting a RF out of band covert channel has been proposed and several proofs of concept have been developed. This RF covert channel is the first inbound covert channel exploiting the EM susceptibility of a target. An analog sensor, the CPU thermal diode, and the electronic circuit dedicated to digitizing the sensor values have been shown to be vulnerable to an AM IEMI. This vulnerability has been exploited to design an AM communication channel between an IEMI source and a software implant executed on the target. First, a non-invasive covert exploit has been implemented, providing a very low bandwidth covert channel. Then, a semi-invasive approach has been followed in order to accelerate the covert exploit sampling rate, resulting in a 10 bps communication rate.

The covert channel capacity has been given an upper bound of 40 bps, which has been estimated using information gathered from a hardware analysis of the components and measurements. This estimation of a worst case channel capacity is a significant contribution as this information is much more relevant for risk analysis than empirical maximum rate and maximum distance which is usually given in other studies on out of band covert channels. Indeed, this worst case channel capacity informs about the attacker's maximum achievable gain with a semi-invasive covert exploit whatever the IEMI source and the propagation and coupling conditions may be.

This approach overestimates the channel capacity and it might be relevant in some cases to determine more precisely what the channel capacity might be relatively to a certain distance, to deploy countermeasures such as zoning. To do so, a better characterization of the target's EM susceptibility would be necessary in order to identify, for each tested frequency, the required EM environment to increase the reported temperature. Furthermore, the proposed estimation does not take noise into account. The actual temperature of the target at the time of the attack can reduce significantly the number of usable symbols for the covert channel. Thus, a precise estimation of the channel capacity would depend on the IEMI signal frequency and the target's temperature. This might be an interesting research perspective.

From an EMC viewpoint, this study could also provide promising perspectives. On complex systems such as our target (a desktop computer motherboard), it might be difficult to determine the value of the parasitic currents or voltages introduced in the circuit during susceptibility testing. Simulation would require precise information about the physical characteristics of the target and measurement approaches could be hard to apply without modifying the target. With the proposed software instrumentation approach, the effect on the logical value, digitized by an ADC and converted and rescaled by a software driver is obtained. When the ADC specifications are known, it might be possible to get insight on the parasitic currents or voltages. For example, the ADC of the target studied in this chapter is documented as having an 8 bits resolution, a maximum input voltage of 4096 mV and a 16 mV least significant bit (LSB). Therefore, if the effects are completely due to the parasitic signals introduced on the analog sensor interface, every 1 °C increase might reveal a 16 mV parasitic offset on the input line of the ADC.

Finally, this study shows the main limitations of the air gap for information security. Covert channels are generally hard to detect and their prevention involves heavy physical and organizational measures. Additionally, the security brought up by air gaps can be circumvented if the technical and organizational best practices are not correctly applied. The huge constraints air gaps imply for the users in their day to day work can lead to small deceptive behaviors from legitimate users, who often assume that the isolation will be enough to support their deception. This shows that besides the technical and organizational measures that should be enforced for an air gap to be efficient, the education of the users is also mandatory to fully benefit from the security brought by this security measure.

5.6 References

[And20] Ross J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley Publishing, 2 edition, 2020. 123, 138

[ANS20] ANSSI. Recommandations relatives à l'interconnexion d'un système d'information à internet. Guide ANSSI ANSSI-PA-066, ANSSI, 2020. 123

[BGAS16] Sergey Bratus, Travis Goodspeed, Ange Albertini, and Debanjum S. Solanky. Fillory of PHY: Toward a periodic table of signal corruption exploits and polyglots in digital radio. In *10th USENIX Workshop on Offensive Technologies (WOOT 16)*, Austin, TX, 2016. USENIX Association. 125

[Bit] BitWhisper: Covert Signaling Channel between Air-Gapped Computers Using Thermal Manipulations | IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/7243739. 129

[CA16] Brent Carrara and Carlisle Adams. Out-of-Band Covert Channels—A Survey. *ACM Computing Surveys*, 49(2):23:1–23:36, 2016. 128

[Car16] Brent Carrara. *Air-Gap Covert Channels*. PhD thesis, Faculty of Engineering, University of Ottawa, Ottawa, Canada, 2016. 124, 125, 128, 129, 136

[Cay22] Romain Cayre. *Offensive and Defensive Approaches for Wireless Communication Protocols Security in IoT*. PhD thesis, INSA de Toulouse, 2022. 139

[CGA+21] Romain Cayre, Florent Galtier, Guillaume Auriol, Vincent Nicomette, Mohamed Kaâniche, and Géraldine Marconato. WazaBee: Attacking zigbee networks by diverting bluetooth low energy chips. In *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2021)*, Taipei (virtual), Taiwan, 2021. 126

[Cor04] Intel Corporation. Intel Pentium 4 Processor with 512-KB L2 cache on 0.13 Micron Process Datasheet. Datasheet 298643-012, 2004. 130

[Deb] Debian – Détails du paquet lm-sensors dans sid. https://packages.debian.org/sid/utils/lm-sensors. 131

[EFF14] EFF. NSA ANT Catalog. https://www.eff.org/document/20131230-appelbaum-nsa-ant-catalog, 2014. 127

[GBM+11] Travis Goodspeed, Sergey Bratus, Ricky Melgares, Rebecca Shapiro, and Ryan Speers. Packets in packets: Orson welles' In-Band signaling attacks for modern radios. In *5th USENIX Workshop on Offensive Technologies (WOOT 11)*, San Francisco, CA, 2011. USENIX Association. 126

[GNUa] GNU Radio. https://github.com/gnuradio. 133

[GNUb] GNU Radio - The Free & Open Source Radio Ecosystem · GNU Radio. https://www.gnuradio.org/. 133

[GSE20] Mordechai Guri, Yosef Solewicz, and Yuval Elovici. Fansmitter: Acoustic data exfiltration from air-Gapped computers via fans noise. *Computers & Security*, 91:101721, 2020. 128

[Gur21a] Mordechai Guri. MAGNETO: Covert channel between air-gapped systems and nearby smartphones via CPU-generated magnetic fields. *Future Generation Computer Systems*, 115:115–125, 2021. 129

[Gur21b] Mordechai Guri. POWER-SUPPLaY: Leaking Sensitive Data from Air-Gapped, Audio-Gapped Systems by Turning the Power Supplies into Speakers. *IEEE Transactions on Dependable and Secure Computing*, pages 1–1, 2021. 128

[HG13] Michael Hanspach and Michael Goetz. On Covert Acoustical Mesh Networks in Air. *Journal of Communications*, 8(11):758–767, 2013. 128

[HKLEV16] Valentin Houchouas, Chaouki Kasmi, José Lopes Esteves, and Philippe Valembois. Caractérisation logicielle de la susceptibilité d'un capteur de température de PC pour la CEM et la SSI. In *18 Ème Colloque International et Exposition Sur La Compatibilité ÉlectroMagnétique (CEM 2016)*, Rennes, France, 2016. 122

[HSH+13] Ragib Hasan, Nitesh Saxena, Tzipora Haleviz, Shams Zawoad, and Dustin Rinehart. Sensing-enabled channels for hard-to-detect command and control of mobile devices. In *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, ASIA CCS '13, pages 469–480, New York, NY, USA, 2013. Association for Computing Machinery. 129

[KLE16a] Chaouki Kasmi and José Lopes Esteves. Détection et caractérisation des effets induits par des interférences électromagnétiques sur un ordinateur. In *Journée de l'Aremif*, Paris, France, 2016. 122

[KLE16b] Chaouki Kasmi and José Lopes Esteves. Exploitation des effets induits par des interférences électromagnétiques pour la commande et le contrôle d'un code malveillant présent sur une machine isolée. In *Journée de l'Aremif*, Paris, France, 2016. 122

[KLEV15] Chaouki Kasmi, José Lopes Esteves, and Philippe Valembois. Air-gap Limitations and Bypass Techniques:"Command and Control" using Smart Electromagnetic Interferences. In *Bot Conf.*, 2015. 122

[KLEV16a] Chaouki Kasmi, José Lopes Esteves, and Philippe Valembois. Air-gap Limitations and Bypass Techniques:"Command and Control" using Smart Electromagnetic Interferences. *The Journal on Cybercrime & Digital Investigations*, 1(1):13–19, 2016. 122

[KLEV16b] Chaouki Kasmi, José Lopes Esteves, and Philippe Valembois. Susceptibility testing for detecting IEMI-based covert channels. In *European Electromagnetics International Symposium EUROEM 2016*, London, UK, 2016. 122

[Lam73] Butler W. Lampson. A note on the confinement problem. *Communications of the ACM*, 16(10):613–615, 1973. 124

[LECK17] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. A Ghost in your Transmitter : Analyzing polyglot signals for physical layer covert channels detection. In *Hardwear.Io*, The Hague, Netherlands, 2017. 126, 139

[LECK18] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. Second Order SoftTempest in RF Front-Ends: Design and Detection of Polyglot Modulations. In *Electromagnetic Compatibility-EMC EUROPE, 2018 International Symposium On*, Amsterdam, Netherland, 2018. IEEE. 126, 139

[LEK16] José Lopes Esteves and Chaouki Kasmi. Contournement d'air gaps par canaux cachés électromagnétiques. In *DNAC*, Paris, France, 2016. 122

[LER21] José Lopes Esteves and Pierre-Michel Ricordel. Un Pare-Feu pour le HDMI. In *Symposium Sur La Sécurité Des Technologies de l'Information et Des Communications (SSTIC)*, Rennes, France, 2021. 127

[LKY16] Eunchong Lee, Hyunsoo Kim, and Ji Won Yoon. Various Threat Models to Circumvent Air-Gapped Systems for Preventing Network Attack. In Ho-won Kim and Dooho Choi, editors, *Information Security Applications*, Lecture Notes in Computer Science, pages 187–199, Cham, 2016. Springer International Publishing. 128

[LU02] Joe Loughry and David A. Umphress. Information Leakage from Optical Emanations. *ACM Trans. Inf. Syst. Secur.*, 5(3):262–289, 2002. 129

[MG] O.MG. https://o.mg.lol/. 128

[MWZ+16] Wojciech Mazurczyk, Steffen Wendzel, Sebastian Zander, Amir Houmansadr, and Krzysztof Szczypiorski. *Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures*. John Wiley & Sons, 2016. 124, 125

[NIA19] NIAP. Protection Profile for Peripheral Switching Device. Common Criteria Protection Profile pp_psd_v4.0, National Information Assurance Partnership (NIAP), 2019. 127

[NSE17] Ben Nassi, Adi Shamir, and Yuval Elovici. Oops!...I think I scanned a malware, 2017. 129

[PGM+16] Peter Pessl, Daniel Gruss, Clémentine Maurice, Michael Schwarz, and Stefan Mangard. DRAMA: Exploiting dram addressing for cross-cpu attacks. In *Proceedings of the 25th USENIX Conference on Security Symposium*, SEC'16, pages 565–581, USA, 2016. USENIX Association. 124, 125

[PPB16] Nilesh Patel, Patrick Plenefisch, and Nicholas Brown. SCREAM: Sensory Channel Remote Execution Attack Methods. Master thesis, Worcester Polytechnic Institute, 2016. 138

[RWM22] Ron Ross, Mark Winstead, and Michael McEvilley. Engineering Trustworthy Secure Systems. NIST Special Publication SP 800-160v1, National Institute of Standards and Technology, 2022. 123

[SB09] Gaurav Shah and Matt Blaze. Covert channels through external interference. In *Proceedings of the 3rd USENIX Conference on Offensive Technologies*, WOOT'09, page 3, USA, 2009. USENIX Association. 125, 126

[Sha48] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423, 1948. 136

[SM15] Mickey Shkatov and Jesse Michael. The Hidden Dangers Inside The Platform. In *Hackito Ergo Sum*, Paris, 2015. 127

[TA05] E. Tumoian and M. Anikeev. Network Based Detection of Passive Covert Channels in TCP/IP. In *The IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05)l*, pages 802–809, 2005. 125

[USB] USBNinja - Fast, Stealth and Ninja-Like ! https://usbninja.com/. 127

[Win02] Winbond. W83627HF/F Winbond I/O. Datasheet 2.0, 2002. 130, 137

Chapter 6

Electromagnetic watermarking

Contents

6.1 Chapter overview

The research summarized in this chapter was a collaboration with Dr. Chaouki KASMI and Dr. Emmanuel COTTAIS between 2017 and 2018 at ANSSI. Findings were published in several conferences focusing on InfoSec and forensics [LE19a, LE19c, LECK18b], electronic warfare [LE21], EMC [LECK18c, LE19b], high power electromagnetics [LE20b, LE20a, LEC19, LECK18a]. Those publications have been cited by more than 30 research articles investigating unmanned aerial vehicle (UAV) security, sensor security, UAV forensics and UAV EMC.

This chapter explores the idea of using some specific effects of IEMI on electronic systems in order to store information remotely and covertly into a non cooperating target, a new approach that we called electromagnetic watermarking (EMW). Some effects of IEMI have an impact which spreads to the software (logical) layer. Such impact can be further cascading towards a modification of a logical state of the target, resulting in a storage channel. This EM storage channel can be exploited to introduce information into the target, which can be detected or extracted later when needed.

The concept of EMW is defined and formalized. The methodology for identifying and characterizing EMW channels is decribed. It involves the EM susceptibility testing of the target and the estimation of the EMW channel capacity.

An example of application of such technique has been implemented on a civilian UAV, which has shown to fit particularly well for such so-called electromagnetic watermarking. EMW has been applied to perform forensics tracking, which consists in providing information about a target activity in space and time. In the case of UAVs, it is proposed as an interesting alternative to complete neutralization against intruders, by inserting a watermark that ties the target to the intrusion event and place. This watermark can be detected and extracted afterwards, during the forensic analysis of a suspicious UAV.

This chapter is organized as follows: in section 6.2, an introduction to digital watermarking is proposed to briefly define the main principles relating to covert information embedding. As an example application of digital watermarking, forensics tracking is also presented.

Section 6.3 introduces this new concept of EMW along with necessary definitions. A methodology to identify and characterize EMW channels on a target is also detailed.

A practical application of EMW is presented in section 6.4 in the framework of C-UAS. The methodology is applied to a civilian COTS UAV with the perspective of providing forensic tracking as a complimentary option to neutralization. As an outcome, several EMW channels are identified and characterized, illustrating the methodology and the practicality of the approach.

A concluding discussion is provided in section 6.5.

6.2 Digital watermarking and forensic tracking

6.2.1 Digital watermarking

Digital watermarking relates to the art of covertly embedding a piece of information into a host digital signal in a way that it can be detected or extracted afterwards while guaranteeing several properties chosen regarding the application, such as allowing to verify the integrity or the authenticity of the signal or surviving to modifications of the host signal like compression [CMB+07].

Such techniques are used for a wide range of applications including owner identification, content authentication, copy control, traitor tracing or forensic tracking and in most cases, the host signal is an audio-visual signal [CMB+07].

The generic model describing the digital watermarking process is communication oriented and involves the following three steps:

- Embedding: the information to embed is encoded and inserted into the host signal, producing the marked signal;
- Processing: the marked signal is processed through a channel, which can be untrusted and expose the signal to attackers;
- Detection: the presence of the watermark is verified and the embedded information is retrieved.

In this model it is usually assumed that the embedding process is performed by a trusted entity which has a privileged access to the host signal by producing it, distributing it or broadcasting it. The embedding process can therefore be chosen and configured by taking into account the characteristics of the host signal for providing specific features (e.g., related to the perceptibility of the watermark).

Several properties characterize digital watermarking techniques, among which the embedding capacity (number of bits which can be embedded into the host signal), the detector performance and the watermark security (authentication, resistance to forgery).

6.2.2 Forensic tracking

While traditional digital forensics aims at extracting evidence of criminal activities from electronic devices, forensic tracking consists in investigating the activity of a target in order to prove, or at least indicate, that the target was at a specific location at a specific time [AW11].

Forensic tracking can either be performed by extracting location traces inside the target such as a list of GPS coordinates [SKC13] or by identifying traces of the target left on other devices (e.g., a network of CCTV cameras [AW11]). In [ZZLT17], a method of forensic tracking of audio recordings is proposed relying on the analysis of the variations of the electrical network frequency, which are consistent at different places of the same electrical power grid.

Forensic tracking using digital watermarking is widespread in digital cinema [LKL09, vLCK07] determining the location in time and space of the recording of pirate copies of movies captured with a digital camera during the in-theater projection of the movie. In this case, the host signal is the motion picture and the information to embed contains an identifier of the theater room and a timestamp. The embedding is performed in real-time by the play back device. The processing channel would include the capture by the digital camera, the compression and format conversions that may have occurred between the capture and the share of a copy. The detection step will consist in searching for the watermark presence in a version of the motion picture and extracting the theater identifier and the timestamp, which will allow for further investigating on the piracy act.

6.3 Electromagnetic Watermarking

6.3.1 Effects and logical storage

A classification of the IEMI effects on electronic devices based on their duration has been proposed [Sab08, SN06] as summarized in Table 6.1. Moreover, as outlined in chapter3, some effects have an impact at the software level which can be detected by software.

When effects from categories (E) and (T) lead to logical impacts that can be observed by a piece of software, it becomes possible to take advantage of IEMI effects to create a unidirectional inbound physical covert communication channel, as demonstrated in chapter 5.

Effects from category (H) allow sending one piece of information per human intervention and effects from category (P) allow sending one piece of information only once. Thus, communication channels exploiting effects from those categories are likely to have a very restrained channel capacity.

If the logical repercussion of an effect directly or indirectly alters the state of the target, then it might be exploited as a storage channel. Effects from category (P) can lead to a permanent write once storage channel. As for effects from the other categories, sometimes the effect occurrence is logically stored in the target electronic systems (e.g., in the operating system logs).

Table 6.1 – Classification of IEMI effects by duration [Sab08]

Category	Duration	Description
U	Unknown	No effect occurs or the duration has not been observed (e.g., observer was unable to determine duration due to effects on another component)
E	During exposure only	Observed effect is present only during exposure to the EM environment, system functionality is completely available when environment has vanished
T	Some time after exposure	Effect is present some time after the EM environment has vanished
H	Resistant until human intervention	Effect is persistent until human intervention, the system is not able to recover to normal operation
P	Permanent until replacement of hardware or software	Effect has damaged hardware to the point that it must be replaced or software to the point that it must be reloaded

6.3.2 Definitions

Electromagnetic watermarking (EMW) can be defined as the process of exploiting effects of IEMI that have persistent impacts on the target in order to remotely introduce (to store) a piece of information (the *watermark*) into a non cooperating electronic target. Conceptually, this can be modeled as the combination of an IEMI based covert communication channel and a storage channel (see Figure 6.1). In this framework, in can be viewed as a covert communication channel for which the covert exploit is not a software implant but, instead, a persistence mechanism intrinsic to the target. The *watermark* can then be detected and extracted later during a second phase in order to at least determine that the target has been in contact with an EMW environment.

The *watermark* is the information embedded into the target.

The *EMW channel* is the remote storage channel resulting from chaining the covert communication channel and the storage channel. The *EMW channel capacity* is a metric that relates to the amount of information that can be stored through an EMW channel. It is limited by the covert communication channel capacity and the data storage process characteristics (rate and maximum storage capacity). The estimation of the EMW channel capacity is discussed in section 6.3.5.

6.3.3 Target characterization

The first step of the target characterization requires an electromagnetic susceptibility analysis in order to identify effects of IEMI along with the electromagnetic environments which lead to the appearance of these effects. Among the effects that were identified during this experimental step, a focus has

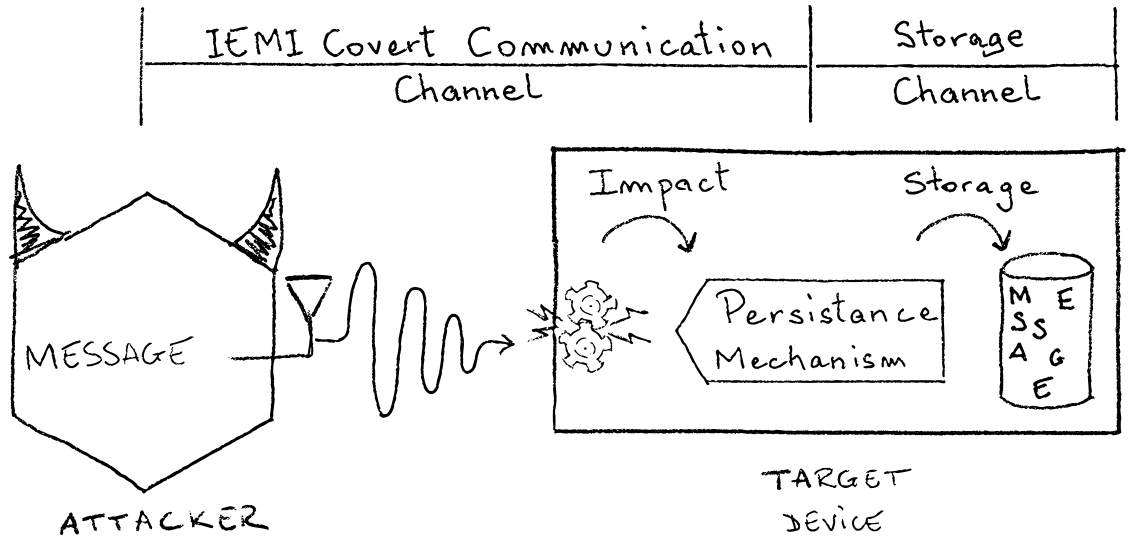


Figure 6.1 – Modeling of EMW as the combination of an IEMI covert channel and a storage channel

to be made on those which are well suited for establishing a covert communication channel. As a consequence, effects from categories (E) and (T) will be preferred as they might allow modulating information more easily.

6.3.4 Identification of persistent impacts

A second non negligible prerequisite for the application of EMW is the presence of a mechanism bringing a form of persistence for each effect. More precisely, effects which have a persisting impact on the state of the target will be eligible for EMW. The persistence mechanism might be permanent, providing a sort of *write-once* possibility. In contrary, the persistence mechanism can also keep track of changes in time, providing a sort of *serial write* possibility.

Understanding the persistence mechanism is important for determining the extraction conditions. Indeed, it can be relevant to identify if this storage mechanism will survive to reboots of the target. If not, the watermark detection and/or extraction steps will have to be performed before the target is shut down or rebooted. This is also particularly relevant as the target could be affected by the EM perturbations in such a way that it shuts down or freezes during the watermark embedding process. The best case is of course to find a persistence mechanism which allows for a *serial write* possibility and survives reboots.

6.3.5 Channel capacity estimation

Once the effects are characterized and the persistence mechanism identified, it may be useful to estimate the EMW channel capacity. This allows knowing how much data can be written into the target during its passage within the required electromagnetic environment. This depends both on the target (effects, persistence mechanism) and on the context (target orientation, electromagnetic environment, exposure duration). Therefore, a fine study of each target is necessary to know how much data can be embedded during a realistic exposure duration under a given context.

The EMW channel can be decomposed in an EM inbound covert channel and an effect storage channel. With this model, the EMW channel can be viewed as an EM inbound covert channel for which the receiver is not a covert exploit, but rather a persistence mechanism which reads the effect occurrence and stores information in a medium. If C_{covert} is the covert communication channel capacity and $C_{storage}$ is the storage rate of the persistence mechanism, the EMW channel capacity C_{EMW} is:

$$C_{EMW} = min\left(C_{covert}, C_{storage}\right)$$

The maximum amount of information S_{EMW} that can be stored through the EMW channel within a exposure time t, assuming the maximum storage capacity of the persistence mechanism is $S_{storage}$, becomes:

$$S_{EMW}(t) = min\left(C_{EMW} \cdot t, S_{storage}\right)$$

6.3.6 Watermark detection and extraction

Embedding information into the target can provide means of modifying its behavior by exploiting components that consume this information. The purpose of EMW is different as it provides a way to insert information so that it can be read back afterwards. At this step two different strategies can be considered: simply detecting the watermark (identifying the presence of information) or extracting the watermark (accessing to the contents). For each strategy, specific processes have to be designed, which are deeply depending on the exploited effect, the persistence mechanism and the operational context.

As some effects might, in some cases, trigger several storage channels simultaneously, their combination could improve the reliability of the detection or extraction of the watermark.

6.4 EMW for forensics tracking of a UAV

In this section, a practical realization of EMW is proposed on a civilian UAV. All the steps required for designing an EMW system are detailed and the efficiency of the proof of concept is evaluated. An operational scenario for performing EMW on a UAV is considered in the framework of C-UAS and it is shown that EMW can provide a way to perform forensics tracking.

6.4.1 Context

During the last decade, UAVs have been spreading in both civilian and military contexts. Their use is expanding rapidly and some models can be bought and flown very easily. Furthermore, the open source and do-it-yourself communities are extremely active on that topic, contributing to a true democratization of this technology. Along with this rapid adoption, malicious uses of UAVs have increased, such as critical infrastructure flyovers [DC18] or forbidden goods drops in prisons [Guy23]. The problem of their neutralization (C-UAS) has become of high interest for security aware organizations. Among the proposed solutions, RF directed energy weapon (DEW) are also considered and commercial products already exist (e.g., Diehl HPEM Counter UAS System [HPE19]). In such cases, it could be interesting to be able to mark the target with specific information which would facilitate the investigation in case it is retrieved after an incident, as it is already done with biological markers in some commercial facilities during robberies.

In such context, EMW can be a relevant solution for forensic tracking of UAVs involved in unauthorized flights nearby critical infrastructures. The main principle would be to perform EMW in complement or as an alternative to a neutralization process. When an incident occurs, a detection phase is triggered. In this phase, depending on the C-UAS solution, the presence of the intruder, its position and its trajectory are determined. Second, an identification phase follows, aiming at the determination of the characteristics of the intruder, ideally the brand and model of the UAV. Only after those steps, the response can take place.

After the identification phase, it is possible to know if the target model is supported by an EMW system and to select the appropriate payloads for the watermark, accordingly to the EMW channel capacity. It could be, for example, a random number generated by the C-UAS system and stored in the incident database or a digital fingerprint derived from the identification phase concatenated with a timestamp and encrypted with a secret key unique to the critical infrastructure. In the case the target is not neutralized, the watermark presence will allow law enforcement units to determine that it was involved in the incident if they encounter the target afterwards. In the case neutralization is decided,

the watermark can still be performed simultaneously in order to tie the target to the incident. If the neutralization fails, the watermark might still remain.

6.4.2 Susceptibility of UAVs

The EMC of UAVs has also been evaluated in different contexts. In order to study the efficiency and the reliability of using UAVs for emergency operations, the EM immunity of UAVs has been investigated [ACJ+15]. A focus was made on perturbations in close proximity of several RF communication infrastructures and radars [TYE13, TMMP13]. The effects observation was focused on the behavior of the RF links of the UAVs during parasitic illumination. IEMI effects on UAVs have also been recently investigated. The reported effects affected mostly the motors and the RF links [ZXY+17, SSUG18]. After the publication of the results presented in this chapter, the susceptibility of civilian UAVs was assessed in several studies.

In [LLLS20], the reaction on motors and sensors of an UAV to narrowband radar pulses in 100–3400 MHz frequency range was observed, both using video cameras and inspecting the flight logs after the tests. This approach is inspired by the target instrumentation presented in the next section, but preserves the software integrity of the target at the cost of disabling the real-time monitoring during tests. Effects on the motors were reported ranging from jamming to flight termination due to engine stop.

Later in [YMW22], a 500 MW source emittng a damped sine with a main frequency around 350 MHz was shown to cause several malfunctions on civilian UAVs, on communication links and the flight attitude, when the electric field around the target was above $10\,\mathrm{kV}\cdot\mathrm{m}^{-1}$.

Again, the method for observing the effects is a limiting factor for the understanding of the underlying mechanisms. All studies rely on a visual inspection of the target attitude and/or the ground station screen, which might be insufficient for the identification of the affected elements (sensors, motors, controllers, etc.).

6.4.3 Target characterization

Target topology

The targeted UAV is a COTS quadcopter which is marketed as a photo and video acquisition device. The topology of the whole system is depicted in Figure 6.2. The air segment is composed of the quadcopter aircraft equipped with a digital camera payload. The ground segment is composed of a remote controller and a proprietary mobile application.

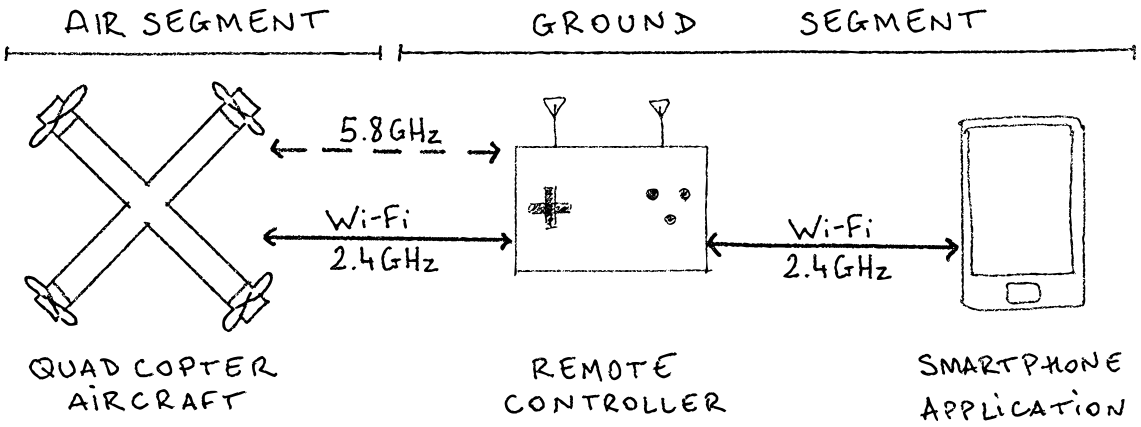


Figure 6.2 – The target system topology: the aircraft, the remote controller and the mobile application

The communication scheme is organized around the remote controller. It hosts a 2.4 GHz Wi-Fi access point. It is also in charge of relaying packets between all the components. A proprietary RF protocol in the 5.8 GHz band is used for sending line of sight flight control commands from the remote controller to the aircraft.

The aircraft encloses a main microcontroller running a *Unix* distribution commonly found in wireless routers and called *OpenWRT* [Bro16]. Besides, a couple of other microcontrollers are in charge of the avionics functions and real-time interactions with the sensors and the motors. Those microcontrollers communicate with the main microcontroller over an asynchronous serial link with a proprietary protocol, in order to both send telemetry data from the sensors and receive commands. The main microcontroller then forwards some of those packets through the Wi-Fi link to the remote controller and the mobile application.

Following the methodology described in chapter 3, the target is first decomposed by coupling interfaces, as summarized in Table 6.2.

Table 6.2 – Summary of coupling interfaces and the corresponding observable

Coupling mode	Hardware interface	Software observable
Front door	Wi-Fi	Signal quality (RSSI)
	5.8 GHz radio	Communication rate
	GPS	Link errors
Back door	Sensors	Raw sensor readings
	Motors	Motor state
	SoCs	System state

The front-door coupling interfaces are the Wi-Fi front-end, the proprietary 5.8 GHz interface and

a global positioning system (GPS) receiver interface. The interesting back-door coupling interfaces can be summarized as follows: the motor driving cables, the several ribbon cables for internal PCB to PCB communication, the embedded sensors and their analog or digital communication links, the power supply network, the analog and digital ICs and components. As the target is an UAV, it encloses several components which are related to the autopilot and other avionics functions. A lot of sensor information is displayed on the mobile application main view, such as GPS latitude, longitude and altitude, gyroscope measurements, accelerometer measurements, gimbals movements, battery charge, voltage, temperature, motors states, etc.

Target instrumentation

One of the main challenges with the proposed approach for analyzing final products (instead of development boards or open prototypes) is to find ways to get access to the observable data gathered by the target. In this case, several options were possible, starting with relying solely on the mobile application. Unfortunately, one would have to interact physically with the smartphone during the tests or to observe the smartphone screen showing a view of the application exposing some of the observables. Furthermore, the mobile application does not gather all the information that are available.

Another possibility would be to rely on local logs available on the aircraft. Indeed, very huge log files are present on a dedicated SD card inside the aircraft. However, this SD card is not easily accessible (several parts need to be removed, and the SD card is glued on its slot). Furthermore, the content of the log files is not clear text, although a partial decoding was proposed in [CMBB17]. Flight log extraction interfaces could also be used, however on some products the data extracted is only a subset of the data stored in the aircraft, as it is the case on an equivalent UAV [Par21]. Finally, this strategy is not suitable for a real-time analysis of the observable.

The strategy that was chosen consisted in gaining a privileged access on the aircraft's main microcontroller and to run a specific piece of software to gather information, store it locally and send it to a remote monitoring computer. Indeed, this main microcontroller is in charge of forwarding the telemetry messages coming from the sensors and actuators enclosed in the air segment to the remote controller or the mobile application. As such, it seems to be a relevant observation spot. In order to achieve this, the hardware architecture has been analyzed in detail. Each part of the aircraft has been reverse-engineered and a serial console port has been found, providing a privileged administrative (*root*) access to the *OpenWRT*.

This privileged access has allowed performing an in-depth analysis of the operating system configuration to determine the most efficient ways to gather the information about the observable. In

particular, a proprietary piece of software is manipulating serial packets coming from the different parts of the UAV (sensors, etc.), probably containing interesting data. Also, it supported a special configuration flag enabling a debugging mode, resulting in writing all those packets in hexadecimal format in the system log files. After enabling remote system logging in the operating system configuration, all those packets were streamed in real time towards the monitoring computer thanks to a Raspberry Pi computer used as a data packets router.

A parser for the acquired packets has been developed in order to interpret the gathered data. The protocol structure has been inferred from a software reverse engineering of the mobile application for Android which had very little code protection and which is not detailed here. This target preparation allowed to perform a first susceptibility analysis and a fast identification of IEMI effects.

6.4.4 Experimental setup

A susceptibility testing campaign was performed on the target in order to identify logical effects that were suitable for EMW. The target was placed on a table in a FARADAYcage together with the remote controller and a smartphone running the mobile application. The aircraft had its propellers removed in order to avoid difficulties due to flying or falling. The remote controller was started and the aircraft and the smartphone attached on the Wi-Fi network. A Raspberry Pi was also added and attached to the remote controller Wi-Fi network and configured to act as a Wi-Fi to ethernet bridge. All incoming packets on the Wi-Fi interface were forwarded to a monitoring computer outside the cage through a pair of ethernet to optical transducers (named "O/E" and "E/O" in Figure 6.3).

The IEMI emission chain was composed of the following:

- An IFR 2023A 9 kHz to 1.2 GHz signal generator, configured with an internal AM source;
- An Amplifier Research 50W1000B 1 MHz to 1 GHz 50 W CW solid state amplifier;
- An EMCO 3146 200 MHz to 1 GHz log-periodic antenna.

The software instrumentation described in the previous sections was configured to forward the system logs to the Raspberry Pi, thus providing a real-time monitoring capacity on the monitoring computer. During the tests, once interesting effects were identified, a Dare Development RadiSense CTR1001B laser powered electric field sensor was positioned as the target in order to provide the electric field magnitude.

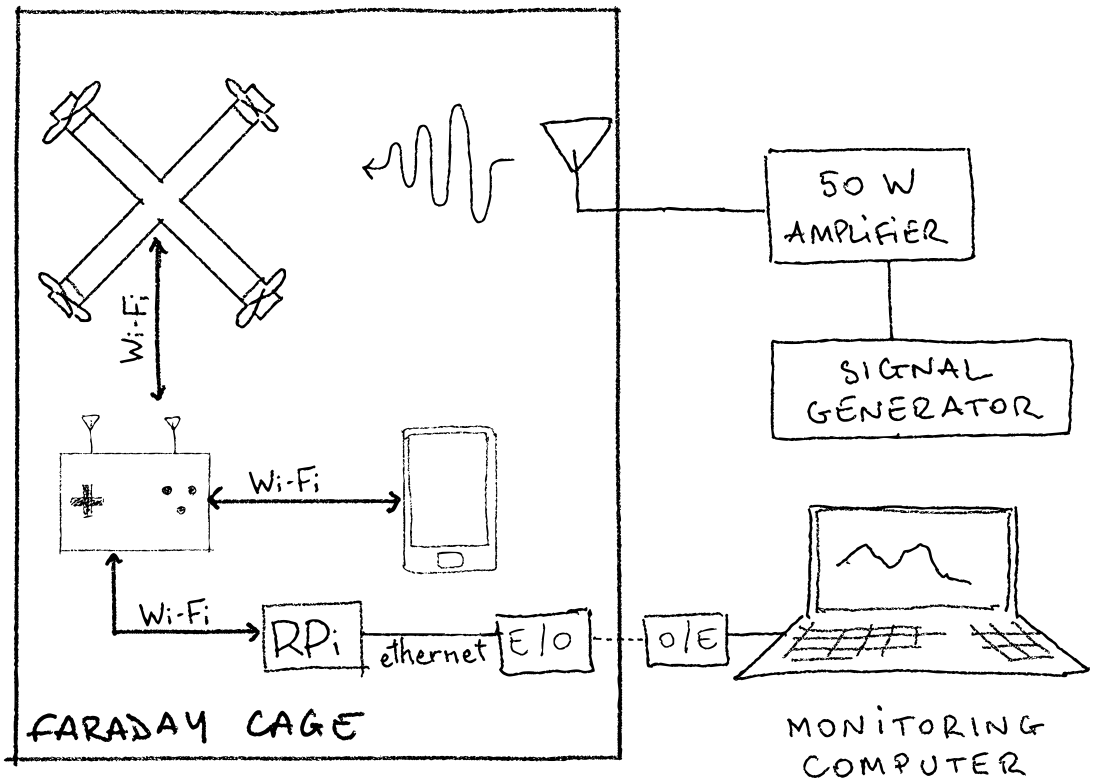


Figure 6.3 – Experimental setup for radiated EMW characterization (E/O and O/E are ethernet-optical converters and RPi is a Raspberry Pi).

6.4.5 Storage channel and watermark extraction

After identifying effects from the right categories along with the IEMI waveforms that cause them, the determination of storage mechanisms for the selected effects had to be performed. For this, UAVs provide a genuine built-in feature which makes this kind of target suitable for EMW: the flight logs.

Civilian UAVs provide flight logs for allowing manufacturers to gather data for enhancing product performance and for doing accident forensic analysis, and for allowing users to share flight experience. To this aim, data from internal sensors are sampled and stored locally. Besides, a software interface gives the possibility to extract the flight logs (e.g., activating a log download mode via USB) and sometimes to share them on the internet (e.g., on the manufacturer community forum).

The data is sampled and logged at different frequencies, depending on the sensor capabilities, the nature of the information and the extraction mode. For example, the maximum sampling rate onboard is 200 Hz and only 5 Hz for the online sharing mode in the Parrot Anafi [Par19]. Referring to [Ano19], the sampling rate for flight logs can reach tens of MHz depending on the UAV model.

On the target, the maximum logging frequency is 250 Hz, which means there is a new log entry every 4 ms. Each log entry contains a set of raw sensor values which have their own update rate. However, 250 Hz is the fastest sampling rate we can expect when reading the values from the flight logs. After each test, the flight logs were extracted from the internal storage of the target and analyzed.

6.4.6 Results

In this section, information gathered during susceptibility testing and EMW characterization is provided. Several effects were identified during susceptibility testing and a subset of these is exposed hereafter. However, all these effects are not equally suitable for designing EMW channels.

Then, a focus is made on the exploitation of some chosen effects in order to set EMW channels up and their characterization. More specifically, the chosen effects have to benefit from the identified storage channel (i.e., to be written in the flight logs). After each test, the flight logs were extracted from the internal storage of the target and analyzed.

Susceptibility testing

Susceptibility testing has been performed with a specific software instrumentation of the target. This gave access to several observable values which allow for identifying which parts of the target show symptoms due to parasitic exposure.

A front-door coupling on the Wi-Fi interface could be observed during the tests. The software

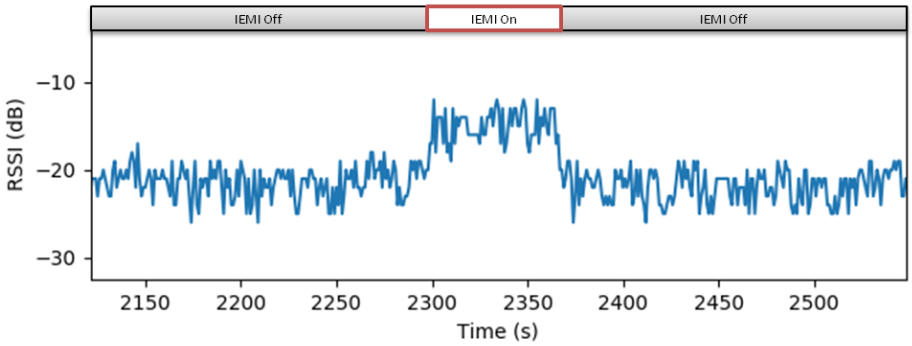


Figure 6.4 – Effect of front-door out-of-band coupling of a 300 MHz CW signal on the 2.4 GHz Wi-Fi front-end

interface providing this information was the *iw* utility, which gives the received signal strength indicator (RSSI) of the wireless interface, which was collected every second. Figure 6.4 shows the impact of a 300 MHz CW on the RSSI of the Wi-Fi front-end.

It was observed that reading errors can be induced on the battery temperature sensor. A variation of 10 degrees has been obtained for an electric field magnitude varying between 75 $\mathrm{V \cdot m^{-1}}$ and 95 $\mathrm{V \cdot m^{-1}}$ around the target. A parametric analysis has been applied to have a clue on the reproducibility of the reading errors. As depicted in Figure 6.5, it can be observed that the reading error is directly related to the electric field magnitude.

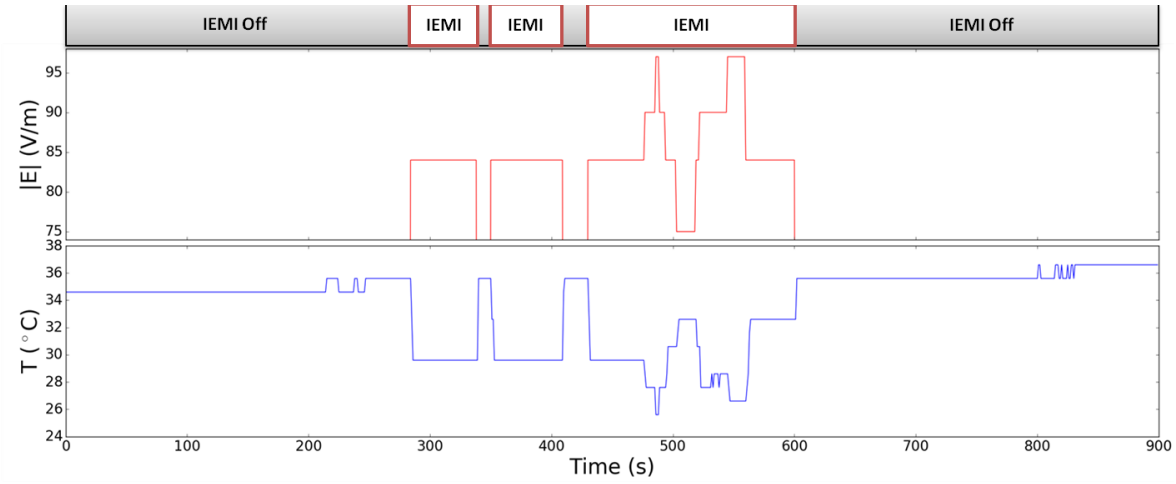


Figure 6.5 – Effect of back-door coupling on the battery temperature sensor interface of the UAV

EMW on the battery temperature sensor

During the experiments, the variations of a value labelled "Battery Temperature" in the flight logs have been analyzed. This observable has been identified for producing an immediate effect of category (E) (see Table 6.1). This value is sampled in the logs at a rate of 1 $\mathrm{S \cdot s^{-1}}$. Thus, considering the Nyquist rate as a maximum for the symbol rate, it can be concluded that the EMW channel symbol rate in this

case will be $R_{sym} = 0.5\,\text{Sym} \cdot \text{s}^{-1}$.

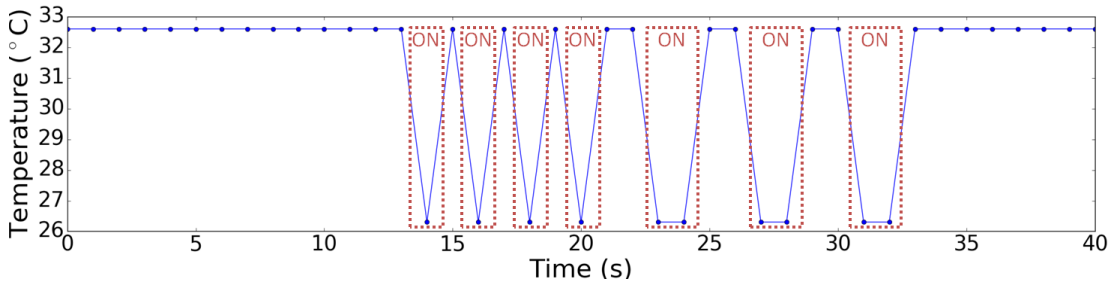


Figure 6.6 – EMW channel on the battery temperature sensor, with a symbol rate of $0.5\,\text{Sym} \cdot \text{s}^{-1}$

An example of non return to zero coding into the flight logs with IEMI is proposed in Figure 6.6. It can be verified that this effect is both reproducible and faster than the log sampling rate. Information can then be coded by just turning the IEMI source on and off.

According to the specification of the battery microcontroller (which is a MSP430G2755 from Texas instruments), the built-in ADC has a 10-bits resolution. The maximum number of different symbols which can be sampled is therefore $N = 2^{10}$. This yields a channel capacity estimation using equation 5.3:

$$C_{EMW} = R_{sym} \cdot \log_2 N = 5\,\text{bps}$$

As this channel capacity estimation is based on the assumption of a noiseless discrete channel (cf. section 5.3.5 in chapter 5), it gives a theoretical upper bound which does not really take into account factors which could impact the signal to noise ratio on the EMW channel, as the EM environment required to trigger the effect and the actual fluctuation of the impacted signal (battery temperature). The formulation of a parametric channel capacity depending on parameters such as source capability, distance, target battery temperature would be an interesting further work.

EMW on the gimbal

Another effect of category (E) has been observed and exploited to perform EMW. It had an impact on a value called "accel:z" in the flight logs, which is interpreted as the vertical acceleration in g. This value seems to be sampled in the logs at a frequency of nearly 250 Hz (according to the timestamps in the log file). In this case, the channel capacity has not been estimated. However, it is a relevant example to document as the effect impacts several sensor values simultaneously, which might be a way to improve the watermark detection and extraction reliability.

This effect results in the appearance of a 15 Hz sinusoidal offset on the actual vertical acceleration value, as shown in Figure 6.7.

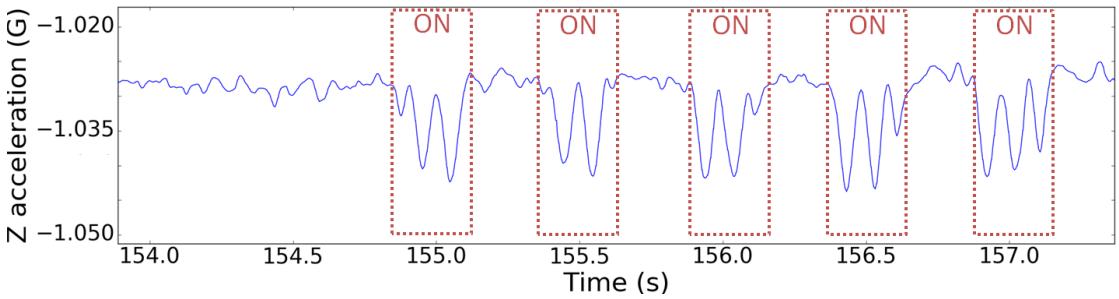


Figure 6.7 – EMW channel on the vertical acceleration

A proof of concept transmission based on an OOK modulation and a non return to zero (NRZ) coding has been realized. Considering one period of the 15 Hz signal is necessary to encode a symbol, a bit rate of 15 bps can be reached. Thus, considering a target flying at $60\,\mathrm{km}\cdot\mathrm{h}^{-1}$, during the writing of a byte, the target will have moved of approximately 8 m. Therefore, depending on the source power, it will be possible to write one or several bytes on the target logs during illumination.

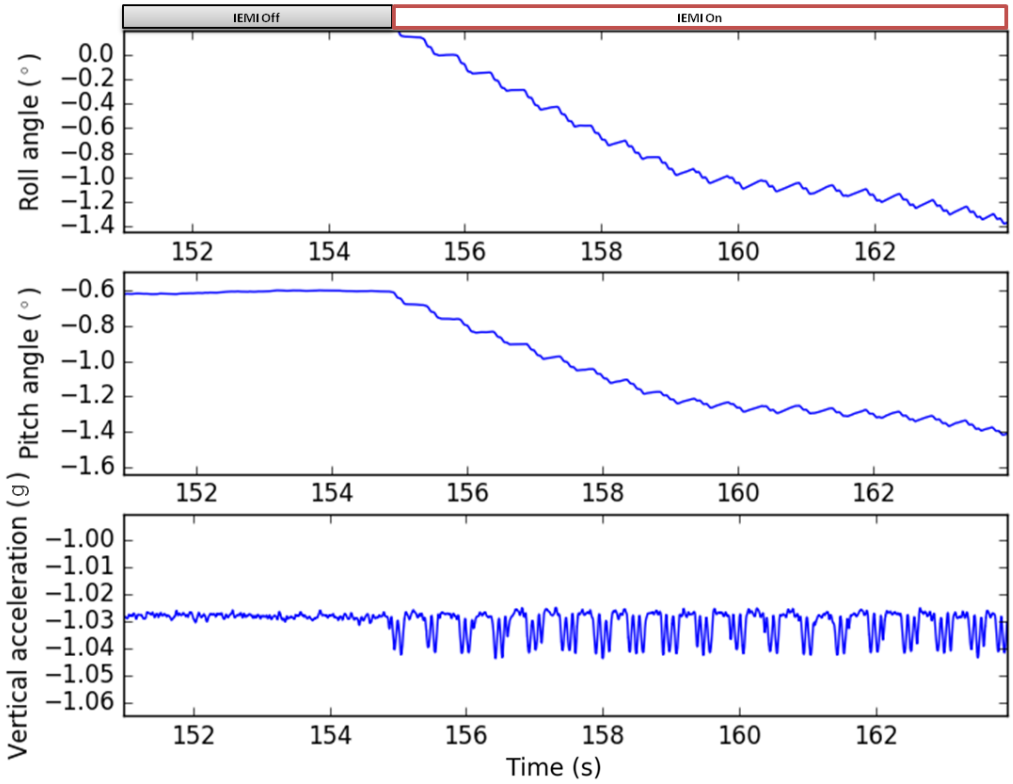


Figure 6.8 – Simultaneous effect on vertical acceleration, roll and pitch (x axis is time in seconds).

Simultaneously, the roll and pitch angle values are also affected and the 15 Hz component is also present as shown in Figure 6.8. Those category (E) effects appear as soon as the signal source is switched on.

The presence of the carrier signal in several observable values may allow for a robust detection and

extraction of the embedded information. For example, when the effect was detected on the vertical acceleration curve, it could be confirmed by the switch of the slope sign of the pitch and roll curves to increase the probability of detection and reduce the false positive probability.

6.4.7 Limitations and perspectives

While EMW opens interesting perspectives in terms of application contexts as a technical process to embed information into remote and non cooperative targets, its practical application involves several challenging steps. Furthermore, overcoming these challenges provides an electromagnetic watermarking solution which is intrinsically context-dependent and target-specific. The design of an EMW framework which is efficient for several different targets and contexts would require reproducing the characterization steps for each target. After the characterization step, considerations regarding the design of the EM source and target selection strategies would still have to be solved.

Regarding the application to UAVs, the raw sensor reading high-frequency logging system is a very suitable persistence mechanism and EMW provides an interesting response to unlicensed fly-overs which is complimentary to neutralization. However, UAVs are moving targets and this raises difficulties to maintain them in the required electromagnetic environment. Several challenges are hidden behind this remark, such as the number of sources to deploy, their physical repartition, the reactivity of the signal relatively to the target's position, the possibly changing incidence angle, etc. Furthermore, the tested target was static during tests and therefore the host signals carrying the watermark did not have the same dynamics as in real flight conditions, under which a different signal to noise ratio can be expected.

Some UAVs log the received signal strength indicator of several wireless communication interfaces, such as GPS, WiFi or custom remote control protocols. Front-door coupling interfaces might be quite relevant to target for EMW in this case as their exploitation might require less power and be depend less on the incidence angle of the watermarking signal.

Interesting perspectives can however be envisioned. For a single target, increasing the EMW capacity could result from a simultaneous exploitation of several different effects, which could be seen as a parallelization of EMW channels. In this case, a formalization of the overall channel capacity estimation from the single channel capacities could be of particular interest. As shown in this chapter, effects which have the same impact on several independent observables offer the possibility to increase the SNR of the watermarking channel and to facilitate the detection and extraction phases. Again, these options shall be both formalized and characterized in order to better understand the performances that can be expected from electromagnetic watermarking.

6.5 Conclusion

In this study, the possibility of embedding information remotely and covertly into non cooperative electronic devices by using IEMI was explored. It was shown that specific effects impacting the logical layer in such a way that a non volatile logical state change occurs can be exploited as a covert remote storage channel. This novel technique was formalized and called the electromagnetic watermarking. It can be conceptually viewed as the combination of an EM covert channel and a local storage channel. In this framework, the efficiency and the practicality of such approach can be studied by characterizing the EM covert channel, the storage channel and their interaction. The efficiency can be quantified with the calculation of the EMW channel capacity, which is target dependent. The practicality is related to the conditions needed to maintain the target into the required EM environment which depends on the target and the operational scenario.

The methodology one needs to follow in order to identify and characterize EMW channels on a target has been detailed. A first susceptibility testing campaign has to be performed in order to identify effects suitable for an EM covert channel along with the EM environments that trigger them. Then, the effects benefiting from a storage channel on the target have to be determined. The EMW channel capacity can then be calculated.

The formulation of the EMW channel capacity might be improved in several ways. The proposed approach tends to provide an upper bound for the remote storage rate and the maximum amount of information implantable. However, in order to make decisions about the operational deployment of EMW, it would be very useful to determine the minimum amount of information which can be implanted given operational conditions, such as the EM environment and the exposure duration. Such a metrics could also be derived for taking the characteristics of a specific source and the propagation of the IEMI signal into account.

This information is also capital when it comes to determining the content of the watermark. Depending on the expected minimal watermark size, the relevance of using EMW in a specific scenario can be discussed. Furthermore, technical decisions could be made about the robustness of the watermarking and about security assurance. Indeed, introducing redundancy to compensate the communication channel effects and using cryptography to provide watermark authentication or confidentiality might require more storage space.

The applicability of such technique has been demonstrated on a civilian UAV. It is a promising application context as UAVs enclose a lot of sensors and log a lot of information at high frequency. An electromagnetic watermarking system could then be an interesting alternative or complement to

existing electromagnetic based UAV neutralization techniques, allowing for the insertion of a watermark proving the exposure of the target to the specific electromagnetic environment generated during the incident response.

However, the operational deployment of EMW in this scope raises technical challenges which can limit the practicality of the technique. It would be interesting to find contexts in which EMW might be a relevant technical solution and practical constraints are more relaxed. Furthermore, the flight logs do not provide systematic guarantees in terms of security or integrity, meaning they can be altered, deleted or replaced, raising questions about the confidence one can have in case of the presence or the absence of a watermark. On this aspect, regulatory evolutions might help, as the need of providing security in the UAVs for legal issues might introduce a kind of *black box* protecting the flight logs.

6.6 References

[ACJ+15] C. Adami, S. Chmel, M. Jöster, T. Pusch, and M. Suhrke. Definition and test of the electromagnetic immunity of UAS for first responders. *Advances in Radio Science*, 13:141–147, 2015. 153

[Ano19] Anonymous. DatCon, 2019. 158

[AW11] S. Al-Kuwari and S. D. Wolthusen. Fuzzy Trace Validation: Toward an Offline Forensic Tracking Framework. In *2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, pages 1–4, 2011. 147, 148

[Bro16] Rich Brown. Welcome to the OpenWrt Project. https://openwrt.org/start, 2016. 154

[CMB+07] Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, and Ton Kalker. *Digital Watermarking and Steganography*. Morgan kaufmann, 2007. 147

[CMBB17] Devon R. Clark, Christopher Meffert, Ibrahim Baggili, and Frank Breitinger. DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III. *Digital Investigation*, 22:S3 – S14, 2017. 155

[DC18] Geert De Clercq. Greenpeace crashes Superman-shaped drone into French nuclear plant. *Reuters*, 2018. 152

[Guy23] Guyenne. Drogue, téléphones et console de jeux : les livraisons par drone en prison, phénomène "récent" à Varennes-le-Grand. https://france3-regions.francetvinfo.fr/bourgogne-franche-comte/saone-et-loire/chalon-sur-saone/drogue-telephones-et-console-de-jeux-les-livraisons-par-drone-en-prison-phenomene-recent-a-varennes-le-grand-2732970.html, 2023. 152

[HPE19] HPEM system from Diehl Defence protects against mini-drones - Diehl Defence. https://www.diehl.com//defence/en/press-and-media/news/hpem-system-from-diehl-defence-protects-against-mini-drones/, 2019. 152

[LE19a] José Lopes Esteves. Agressions Electromagnétiques et Forensics. In *Conférence Sur La Réponse Aux Incidents et l'investigation Numérique (CoRI&IN) 2019*, Lille, France, 2019. Cecyf. 146

[LE19b] José Lopes Esteves. Electromagnetic Watermarking: Exploiting IEMI effects for forensic tracking of UAVs. In *Electromagnetic Compatibility-EMC EUROPE, 2019 International Symposium On*, Barcelona, Spain, 2019. IEEE. 146

[LE19c] José Lopes Esteves. Watermarking Electromagnétique de Drones. In *Symposium Sur La Sécurité Des Technologies de l'Information et Des Communications (SSTIC)*, Rennes, France, 2019. 146

[LE20a] José Lopes Esteves. Active Forensics Tracking Exploiting Logical Effects of HPEM. In *General Assembly and Scientific Symposium (URSI GASS), 2020 XXXIIIrd URSI*, Rome, Italy, 2020. 146

[LE20b] José Lopes Esteves. Electromagnetic security exploitation of the susceptibility of a UAV. In *Directed Energy Research Symposium (DERC 2020)*, 2020. 146

[LE21] José Lopes Esteves. Implantation d'information dans des cibles non coopératives par perturbations EM : Application à la lutte anti-drones. In *Journées d'études Electromagnetisme et Guerre Electronique (EM+GE 21)*, Toulouse, 2021. 146

[LEC19] José Lopes Esteves and Emmanuel Cottais. Covert Information Embedding in Remote Targets with HPEM. In *Asia Electromagnetics Symposium (ASIAEM 2019)*, Xian, China, 2019. Summa Foundation. 146

[LECK18a] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. Software Instrumentation of an Unmanned Aerial Vehicle for HPEM Effects Detection. In *Radio Science Conference (URSI AT-RASC), 2018 2nd URSI Atlantic*, Las Palmas, Spain, 2018. IEEE. 146

[LECK18b] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. Strategies to harden and neutralize UAV using RF DEW. In *Hardwear.Io*, The Hague, Netherlands, 2018. 146

[LECK18c] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. Unlocking the Access to the Effects induced by IEMI on a Civilian UAV. In *Electromagnetic Compatibility-EMC EUROPE, 2018 International Symposium On*, Amsterdam, Netherland, 2018. IEEE. 146

[LKL09] Min-Jeong Lee, Kyung-Su Kim, and Heung-Kyu Lee. Forensic Tracking Watermarking against In-theater Piracy. In Stefan Katzenbeisser and Ahmad-Reza Sadeghi, editors, *Information Hiding*, Lecture Notes in Computer Science, pages 117–131. Springer Berlin Heidelberg, 2009. 148

[LLLS20] Grzegorz Lubkowski, Marian Lanzrath, Louis Cesbron Lavau, and Michael Suhrke. Response of the UAV Sensor System to HPEM Attacks. In *2020 International Symposium on Electromagnetic Compatibility - EMC EUROPE*, pages 1–6, 2020. 153

[Par19] Parrot. Parrot ANAFI Specifications, 2019. 158

[Par21] Parrot. Anafi Ai - The 4G robotic UAV. https://www.parrot.com/assets/s3fs-public/2021-10/white-paper-anafi-ai-v1.5.pdf, 2021. 155

[Sab08] F. Sabath. Classification of electromagnetic effects at system level. In *2008 International Symposium on Electromagnetic Compatibility - EMC Europe*, pages 1–5, 2008. 148, 149

[SKC13] S. Sack, K. Kröger, and R. Creutzburg. Location tracking forensics on mobile devices. In *Multimedia Content and Mobile Devices*, volume 8667 of *procspie*, page 866712, 2013. 148

[SN06] Franck Sabath and D Nietsch. Electromagnetic Effects on Systems and Components. In *American Electromagnetics International Symposium AMEREM 2006*, Santa Barbara, CA, USA, 2006. Summa Foundation. 148

[SSUG18] Konstantin Sakharov, Alexander Sukhov, Vladimir Ugolev, and Yuri Gurevich. Study of UWB Electromagnetic Pulse Impact on Commercial Unmanned Aerial Vehicle. In *2018 International Symposium on Electromagnetic Compatibility (EMC Europe 2018)*, Amsterdam, Netherland, 2018. IEEE. 153

[TMMP13] Livio Torrero, Paolo Mollo, Andrea Molino, and Alberto Perotti. RF immunity testing of an Unmanned Aerial Vehicle platform under strong EM field conditions. In *Antennas and Propagation (EuCAP), 2013 7th European Conference On*, pages 263–267. IEEE, 2013. 153

[TYE13] Zhang Tao, Chen Yazhou, and Cheng Erwei. Continuous wave radiation effects on UAV data link system. In *2013 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference*, pages 321–324, 2013. 153

[vLCK07] Michiel van der Veen, Aweke Lemma, Mehmet Celik, and Stefan Katzenbeisser. Forensic Watermarking in Digital Rights Management. In Milan Petković and Willem Jonker, editors, *Security, Privacy, and Trust in Modern Data Management*, Data-Centric Systems and Applications, pages 287–302. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007. 148

[YMW22] Chaochao Yang, Jin Meng, and Haitao Wang. Susceptibility Of Civilian UAV To Wideband High Power Electromagnetic Pulses. *Progress In Electromagnetics Research Letters*, 104:15–25, 2022. 153

[ZXY+17] Qiao Zhijun, Pan Xuchao, He Yong, Chen Hong, Shen Jie, and Ye Cheng. Damage of high power electromagnetic pulse to unmanned aerial vehicles. *High Power Laser and Particle Beams*, 29(11), 2017. 153

[ZZLT17] Lilei Zheng, Ying Zhang, Chien Eao Lee, and Vrizlynn L. L. Thing. Time-of-recording estimation for audio recordings. *Digital Investigation*, 22:S115–S126, 2017. 148

Conclusion and perspectives

Conclusion

Contribution summary

The work in this thesis was focused on the effects of intentional electromagnetic interference (IEMI) on electronic devices and their impact on information security. More precisely, the transposition of approaches coming from electromagnetic fault injection (EMFI) to intentional electromagnetic interference (IEMI) resulted in a methodology for a characterization of effects on information through the prism of cybersecurity, allowing for easier exploitability analysis, detection and countermeasure design. This methodology was applied on different targets and allowed to design original attacks and uncover new threat models.

On a smartphone, a new attack was designed involving IEMI to obtain a remote, stealthy, unauthorized use of voice assistants by exploiting the susceptibility of the audio front-end.

On a computer, a new threat model was discovered and demonstrated, consisting in an exploitation of IEMI for the establishment of covert communication channels with software implants, allowing a remote attacker to send commands, updates or payloads.

On a drone, a new threat model was explored, *electromagnetic watermarking*, which exploits specific IEMI effects to introduce information into a remote non-cooperating target. A practical application was proposed to provide a forensics tracking capability in a framework of counter unmanned aerial systems (C-UAS).

Overall, the contributions on threat models exploiting IEMI can be placed in the panorama of electromagnetic security threats as depicted in Figure C.1.

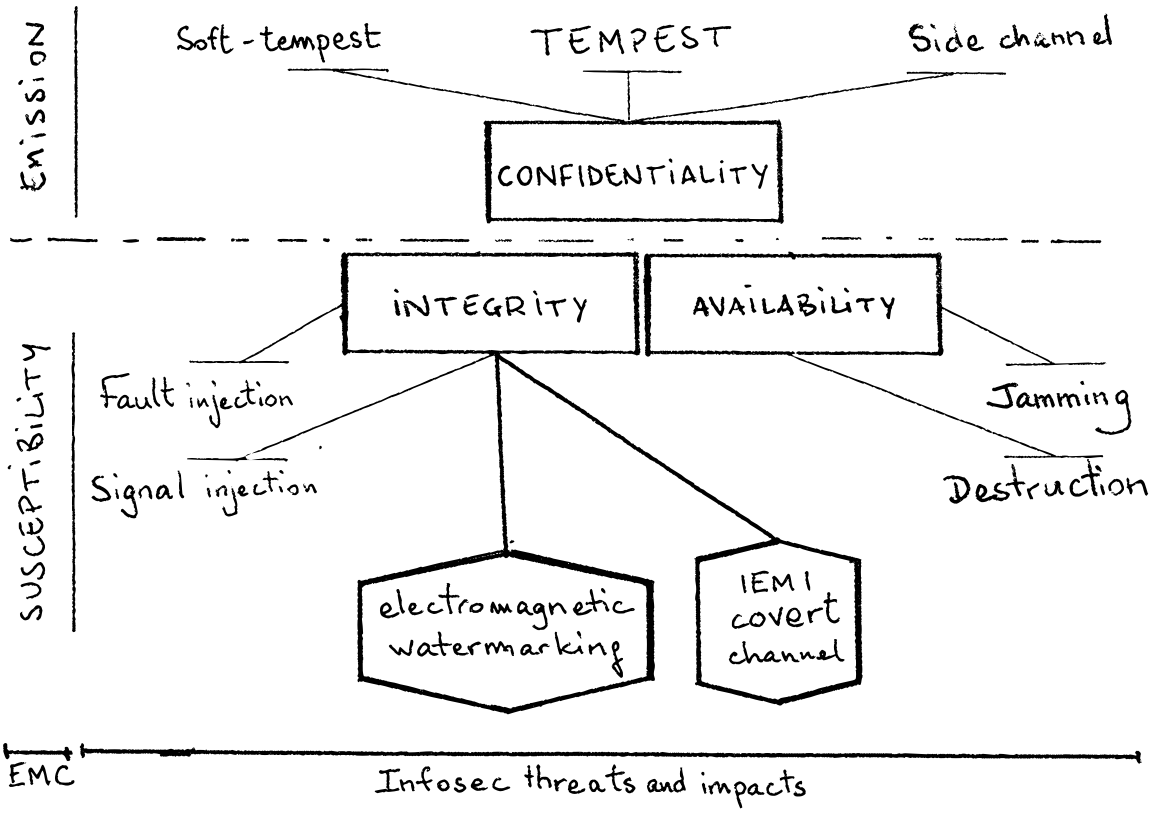


Figure C.1 – Summary of electromagnetic security threats including contributions from this thesis

General conclusion

Electronic devices have become ubiquitous in all sectors of our lives, from military to civilian, from critical infrastructures to our homes, our pockets, our pacemakers. This widespread comes with increasing needs for the security of the information manipulated by electronic devices.

Electromagnetic security is the art of managing information security risks which arise from interaction between electronic devices and their electromagnetic (EM) environment. It is at the intersection of electromagnetic compatibility (EMC) and information security (InfoSec). Chapter 1 provided an overview of both fields. Their intersection was formalized, arguing that EMC emission problems could lead to a compromise of the confidentiality and susceptibility problems to a compromise of the availability and the integrity of information. While EMC focuses on measuring and limiting emission and susceptibility of devices and on the understanding of the underlying physical phenomena, cybersecurity focuses on managing the risks related to the intentional exploitation of a vulnerability by an attacker to compromise the security of the information. In electromagnetic security, the exploited vulnerabilities are directly related to the EM emission and susceptibility.

Chapter 2 provided an in depth description of two approaches dedicated to the study of the exploitation of the EM susceptibility: electromagnetic fault injection (EMFI) and IEMI. EMFI is a

cybersecurity discipline and as such, it involves testing and modeling methodologies which are intended to provide information enabling a security analysis. Fault models describe of the impact of a fault at a chosen observation layer and can be viewed as a link between the actual underlying phenomena and the ways the impact could propagate to upper layers. They provide an interesting ground for exploitability analysis. However, EMFI focuses on intergated circuit (IC), and methodologies are not directly transposable to the analysis of more complex systems. IEMI is the only threat considered in EMC which involves the intentionality of an attacker. The targets and the threat models are very diverse and of different scales. Test methods are not well tailored for cybersecurity analysis because they deeply depend on the operational context of the target and the failure criteria are focused on coarse grain functional performance. For those reasons, test results do not provide a way to analyze the potential impacts on the security of the information manipulated by the target. Meanwhile, in sensor security, new threat scenarios are considered, where the IEMI can occur in close proximity of the target, with a synchronization with the target activity.

In chapter 3, the opportunity of using fault models more systematically for analyzing IEMI effects was evoked. It becomes possible to benefit from the advantages given by fault models for the identification and the detection of the effects. InfoSec analyzes are facilitated as fault models ease exploitability analysis and countermeasure design. On complex multipurpose targets such as computers or internet of things (IoT) devices, it is proposed to consider fault models at the operating system layer, a layer which is close to the information to protect. The application of this approach was illustrated in practice on a desktop computer, and it was shown valuable for the detection of effects and their explanation. Using this approach, several contributions related to the exploitability of the effects of IEMI were made and described in the following chapters.

An original exploitation of signal injection with IEMI against a smartphone has been proposed in chapter 4. An analog microphone interface has been targeted and the possibility to introduce an arbitrary parasitic signal interpreted as an audio input was demonstrated. A radiated propagation scenario was explored, where the attacker signal couples into wired headphones. A conducted propagation scenario was also considered, where the attacker signal penetrates the target through the low voltage power charging cable. An exploitation scenario targeting voice assistants was investigated. The outcome of the attack was a remote unauthorized use of the voice assistant via IEMI.

The exploration of a new threat model for IEMI has been detailed in chapter 5. This threat model considers an attacker exploiting the EM susceptibility of a target in order to communicate with a software implant through a covert channel. This new covert channel has been positioned relatively to existing air-gap covert channel techniques and guidelines for the characterization of impacting

parameters, such as the channel capacity, were given. A practical proof of concept exploiting the susceptibility of a temperature sensor interface in a desktop computer has been produced. The experimental methodology has been documented and a security analysis of the resulting attack has been done. The attack resulted in a 40 bits per second covert channel capacity.

Chapter 6 introduced a new threat model for IEMI called *electromagnetic watermarking*. In this threat model, the attacker exploits specific effects of IEMI in order to introduce information into remote non cooperative targets. Electromagnetic watermarking (EMW) was modeled as the combination of an IEMI covert channel and a local storage channel. With this model, relevant characteristics, such as the EMW channel capacity, were defined. A practical application was proposed in the context of C-UAS, allowing to perform forensic tracking of intruder unmanned aerial vehicle (UAV). The experimental design and the characterization of EMW channels on a commercial off the shelf (COTS) UAV were detailed. As an outcome, several EMW channels were found, with capacities up to 15 bits per second.

Perspectives

The multidisciplinary contribution of this thesis opens interesting perspectives on methodological, conceptual and practical aspects, for EMC and electromagnetic security.

Towards remote EMFI

The comparison of IEMI and EMFI threat models in chapter 2 has shown several gaps that remain little explored. As IEMI inherits from high altitude electromagnetic pulse (HEMP) and research about directed energy weapons, attackers were mostly considered at a significant distance from the target and aiming impacts on availability. Sources and environments were defined in this perspective, explaining the high magnitude of considered power, fields, currents and voltages. EMFI focuses on IC security and therefore considers attackers with a physical access to the target, the ability to prepare its environment and to synchronize finely with its activity.

Investigation of the use of IEMI to obtain EMFI impacts without opening the target enclosure to access the ICs might be worthy. This is an important question for InfoSec risk analysis and assumptions about the prerequisites for EMFI may need to be reevaluated.

Towards test software for susceptibility evaluation

The software instrumentation approach for IEMI effects identification might provide several benefits in an EMC context. First, unseen effects from categories "unknown" and "no effect" which were simply not observed with the right measurement method might be identified. As shown in chapter 3, observing effects from within the target and focusing on information might also allow to find explanations for already known effects and the underlying phenomena.

Secondly, equipment profiles could be defined, such as computers, smartphones, cyberphysical systems, and a generic set of fault models could be identified for each profile. Test software libraries could be developed and adapted to specific equipment before susceptibility tests. This would bring a

common basis for failure criteria and may provide comparability of test results for equipment of the same profile.

Finally, a fault model oriented software instrumentation could improve the research on equipment susceptibility with test conditions that are more representative of the reality, by adding an intermediary layer of abstraction between the hardware and the software. Indeed, it may happen that, for intellectual property reasons, constitutive components of tested equipment are replaced by digital twins, mimicking part of the functional behaviour of the genuine components. As a result, the hardware topology of the tested equipment differs from the real one, which might change the EM interactions. With a software instrumentation using fault models replacing the confidential production software of the components for the tests, the actual hardware could be included in the tests and the results would be usable by the software developers for risk assessment and countermeasure design.

Towards software IEMI detection

The strategy proposed in chapter 3 in the scope of a detection system has not been investigated in depth. Further work on this subject would be necessary to consider technical challenges of designing monitoring and detection systems, such as anomaly detection and classification, networking performance considerations, observable confidence and ponderation, load balancing on the hosts...

A coupling with external hardware IEMI detectors could also be considered.

Towards a parametric covert channel capacity

Most air-gap covert channel studies provide an experimental estimation of the channel capacity along with the attack distance. This information is insufficient because it does not state about the covert channel performance with different transmission choices (e.g., coding, modulation) or capacity (e.g., amplification). However, in chapter 5, the channel capacity was theoretically formulated as an upper bound, which is more relevant for risk analysis. To do so, the IEMI propagation and coupling have been idealized. The formulation of the channel capacity could be improved to take these parameters into account, and provide a way to determine an upper bound depending on the propagation and/or the source characteristics.

Extending the work on EMW

Chapter 6 introduced the concept of EMW and a proof of concept was proposed on an UAV and was placed in a context of C-UAS. This example target was interesting because of the many sensors and actuators it encloses. But it also brought practical limitations because it is a target moving fast. Therefore, using EMW for forensic tracking of UAVs is very challenging. It might be interesting to find other targets and other use cases for which EMW would be relevant and less constraining.

Besides, the concept of EMW might be generalized to the combination of any perturbation technique with a local storage channel. For example, like with IEMI, interaction with a laser could produce effects on sensors. Modulating the ambient light to store information in videos could be another example. Extending the principles of EMW to other forms of interaction would be an interesting topic to investigate.

Towards a parametric EMW channel capacity

The same direction might also stand in the case of the estimation of EMW channel capacity which could be parametric to take the propagation or the source characteristics into account. Furthermore, in the case of EMW, it might also be relevant to question the interest of determining a lower bound together with an upper bound for the channel capacity. Indeed, for a practical deployment of EMW, it might be worth determining the minimum watermark size which could be embedded in a target given operational conditions, such as exposure duration. This information could help determining the contents of the watermark.

Appendix

Appendix A

Author's publication list

A.1 Author identifiers

- Full name: José LOPES ESTEVES
- IdHAL: jose-lopes-esteves
- ORCID: 0000-0002-9340-2599
- IdRef: 118599100

A.2 Publications in EMC, IEMI, HPEM

A.2.1 Journals

[1] C. Kasmi, José Lopes Esteves, and M. Renard. Automation of the Immunity testing of COTS computers by the instrumentation of the internal sensors and involving the operating system logs–Technical report. *System Design and Assessment Note SDAN*, 44, 2014.

[2] Chaouki Kasmi, José Lopes Esteves, Nicolas Picard, Mathieu Renard, Bruno Beillard, Edson Martinod, Joël Andrieu, and Michèle Lalande. Event logs generated by an operating system running on a COTS computer during IEMI exposure. *IEEE Transactions on Electromagnetic Compatibility*, 56(6):1723–1726, 2014.

[3] Chaouki Kasmi and José Lopes Esteves. IEMI threats for information security: Remote command injection on modern smartphones. *IEEE Transactions on Electromagnetic Compatibility*, 57(6):1752–1755, 2015.

[4] Valentin Houchouas, Chaouki Kasmi, José Lopes Esteves, and Damien Coiffard. Experimental comparison of mode-stirrer geometries for the susceptibility testing of COTS Information Systems in regards of the criticality of effects – Technical report. *System Design and Assessment Note SDAN*, 46, 2015.

[5] Chaouki Kasmi, Sébastien Lalléchère, José Lopes Esteves, Sébastien Girard, Pierre Bonnet, Françoise Paladian, and Emmanuel Prouff. Stochastic EMC/EMI experiments optimization using resampling techniques. *IEEE Transactions on Electromagnetic Compatibility*, 58(4):1143–1150, 2016. ISSN 0018-9375. doi: 10.1109/TEMC.2016.2557847.

[6] José Lopes Esteves and Chaouki Kasmi. Remote and Silent Voice Command Injection on a Smartphone through Conducted IEMI: Threats of Smart IEMI for Information Security. *System Design and Assessment Note SDAN*, 48, 2018.

[7] Valentin Houchouas, Muriel Darces, Marc Hélier, Emmanuel Cottais, and José Lopes Esteves. Applications of the Random Coupling Model to Assess Induced Currents or Voltages in Reverberant Environment. In *Progress In Electromagnetic Research (PIERC)*, volume 102, pages 109–125, 2020. doi: doi:10.2528/PIERC20022707.

A.2.2 International conferences

[1] Chaouki Kasmi, José Lopes Esteves, and Mathieu Renard. A Self-monitored Information System for High Power Electromagnetic Attacks Detection. In *AMEREM 2014*, 2014.

[2] Chaouki Kasmi, José Lopes Esteves, and Mathieu Renard. Autonomous electromagnetic attacks detection considering a COTS computer as a multi-sensor system. In *General Assembly and Scientific Symposium (URSI GASS), 2014 XXXIth URSI*, pages 1–4. IEEE, 2014.

[3] Chaouki Kasmi, Nicolas Picard, José Lopes Esteves, M Renard, Bruno Beillard, Edson Martinod, Joël Andrieu, and Michèle Lalande. Analysis of Hardware and Software Faults induced by IEMI on a COTS Computer. In *ICEEA 2014, 5th International Conference on Environmental Engineering and Applications*, 2014.

[4] Valentin Houchouas, Chaouki Kasmi, José Lopes Esteves, and Damien Coiffard. Experimental comparison of mode-stirrer geometries for EMC. In *Asia Electromagnetics Symposium (ASIAEM 2015)*, Jeju-si, Jeju Province, South Korea, 2015.

[5] C. Kasmi and José Lopes Esteves. Automated analysis of the effects induced by radio-frequency pulses on embedded systems for EMC Functional Safety. In *Radio Science Conference (URSI AT-RASC), 2015 1st URSI Atlantic*, pages 1–1, Las Palmas, Spain, 2015. IEEE. doi: 10.1109/URSI-AT-RASC.2015.7303039.

[6] Chaouki Kasmi and José Lopes Esteves. IEMI and Smartphone Security: A smart use of front door coupling for remote command execution. In *Asia Electromagnetics Symposium (ASIAEM 2015)*, Jeju-si, Jeju Province, South Korea, 2015.

[7] Chaouki Kasmi and José Lopes Esteves. Functional susceptibility of COTS devices to IEMI at local and large-scale levels. In *2016 International Conference on Electromagnetics in Advanced Applications (ICEAA)*, pages 399–402, 2016. doi: 10.1109/ICEAA.2016.7731410.

[8] Chaouki Kasmi, José Lopes Esteves, and Keith Armstrong. EMC/EMI and Functional Safety: Methodology to characterize effects of interferences on devices. In *Electromagnetic Compatibility (APEMC), 2016 Asia-Pacific International Symposium On*, volume 1, pages 1178–1180. IEEE, 2016. doi: 10.1109/APEMC.2016.7522979.

[9] Chaouki Kasmi, José Lopes Esteves, and Philippe Valembois. Susceptibility testing for detecting IEMI-based covert channels. In *European Electromagnetics International Symposium EUROEM 2016*, London, UK, 2016.

[10] Sébastien Lalléchère, Sébastien Girard, Pierre Bonnet, Françoise Paladian, Chaouki Kasmi, José Lopes Esteves, and Laurent Patier. Optimization of EMC aerospace margins using resampling techniques with Monte Carlo simulations. In *2016 IEEE Metrology for Aerospace (MetroAeroSpace)*, pages 161–165, Florence, Italy, 2016. doi: 10.1109/MetroAeroSpace.2016.7573205.

[11] Emmanuel Cottais, José Lopes Esteves, Valentin Houchouas, and Chaouki Kasmi. Effects of intentional electromagnetic interference on an adaptive predistortion algorithm. In *Electromagnetic Compatibility-EMC EUROPE, 2017 International Symposium On*, pages 1–6, Angers, France, 2017. IEEE. doi: 10.1109/EMCEurope.2017.8094783.

[12] Valentin Houchouas, José Lopes Esteves, Emmanuel Cottais, Chaouki Kasmi, and Keith Armstrong. Immunity assessment of a servomotor exposed to an intentional train of RF pulses. In *Electromagnetic Compatibility-EMC EUROPE, 2017 International Symposium On*, pages 1–5. IEEE, 2017. doi: 10.1109/EMCEurope.2017.8094785.

[13] Chaouki Kasmi and José Lopes Esteves. Emerging Threats of IEMI for Information Security: Recent advances. In *Asia Electromagnetics Symposium (ASIAEM 2017)*, 2017.

[14] José Lopes Esteves, Chaouki Kasmi, Andy Degraeve, Davy Pissoort, and Keith Armstrong. Analysis of Effects induced by EM disturbances on COTS Devices, from an EM Security and Functional Safety perspective. In *Developments in System Safety Engineering - Proceedings of the Twenty-fifth Safety-Critical Systems Symposium*, pages 313–324, Bristol, UK, 2017. SCSC on Amazon / CreateSpace.

[15] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. Analysis of HPEM perturbations induced on the navigation system of a UAV. In *American Electromagnetics International Symposium AMEREM 2018*, Santa Barbara, CA, USA, 2018. Summa Foundation.

[16] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. Remote Detection of HPEM attacks on Wireless Front-Ends. In *American Electromagnetics International Symposium AMEREM 2018*, Santa Barbara, CA, USA, 2018. Summa Foundation.

[17] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. Second Order Soft-Tempest in RF Front-Ends: Design and Detection of Polyglot Modulations. In *Electromagnetic Compatibility-EMC EUROPE, 2018 International Symposium On*, Amsterdam, Netherland, 2018. IEEE. doi: 10.1109/EMCEurope.2018.8485134.

[18] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. Software Instrumentation of an Unmanned Aerial Vehicle for HPEM Effects Detection. In *Radio Science Conference (URSI AT-RASC), 2018 2nd URSI Atlantic*, Las Palmas, Spain, 2018. IEEE.

[19] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. Unlocking the Access to the Effects induced by IEMI on a Civilian UAV. In *Electromagnetic Compatibility-EMC EUROPE, 2018 International Symposium On*, Amsterdam, Netherland, 2018. IEEE. doi: 10.1109/EMCEurope.2018.8484990.

[20] José Lopes Esteves. Electromagnetic Watermarking: Exploiting IEMI effects for forensic tracking of UAVs. In *Electromagnetic Compatibility-EMC EUROPE, 2019 International Symposium On*, Barcelona, Spain, 2019. IEEE. doi: 10.1109/EMCEurope.2019.8872027.

[21] José Lopes Esteves and Emmanuel Cottais. Covert Information Embedding in Remote Targets with HPEM. In *Asia Electromagnetics Symposium (ASIAEM 2019)*, Xian, China, 2019. Summa Foundation.

[22] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. Analysis of Soft Faults induced by IEMI for Elementary Functions and Complex Electronics. In *Radio Science Conference (URSI AP-RASC), 2019 URSI Asia Pacific*, New Dehli, India, 2019. IEEE. doi: 10.23919/URSIAP-RASC.2019.8738740.

[23] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. Second Order Soft Tempest: From Internal Cascaded Electromagnetic Interactions to Long Haul Covert Channels. In *Radio Science Conference (URSI AP-RASC), 2019 URSI Asia Pacific*, New Dehli, India, 2019. IEEE. doi: 10.23919/URSIAP-RASC.2019.8738370.

[24] V. Houchouas, M. Darces, Marc Hélier, Emmanuel Cottais, and José Lopes Esteves. Applications of the Random Coupling Model for stacked printed circuit boards. In *2020 International Symposium on Electromagnetic Compatibility - EMC EUROPE*, pages 1–6, 2020. doi: 10.1109/EMCEUROPE48519.2020.9245733.

[25] Valentin Houchouas, Muriel Darces, Marc Hélier, Emmanuel Cottais, and José Lopes Esteves. Applications of the Random Coupling Model for stacked printed circuit boards. In *General Assembly and Scientific Symposium (URSI GASS), 2020 XXXIIIrd URSI*, Rome, Italy, 2020. IEEE.

[26] José Lopes Esteves. Active Forensics Tracking Exploiting Logical Effects of HPEM. In *General Assembly and Scientific Symposium (URSI GASS), 2020 XXXIIIrd URSI*, Rome, Italy, 2020.

[27] José Lopes Esteves. Electromagnetic security exploitation of the susceptibility of a UAV. In *Directed Energy Research Symposium (DERC 2020)*, 2020.

[28] Guillaume Bouffard, Valentin Houchouas, José Lopes Esteves, and Thomas Trouchkine. Fault injection effectiveness compared to reflection coefficient of antenna/target couple. In *Radio Science Conference (URSI AP-AT-RASC), 2022 URSI Joint Atlantic and Asia-Pacific*, Las Palmas, Spain, 2022.

[29] José Lopes Esteves. Comparing Intentional Electromagnetic Interference and Electromagnetic Fault Injection for electromagnetic security applications. In *Radio Science Conference (URSI AP-AT-RASC), 2022 URSI Joint Atlantic and Asia-Pacific*, Las Palmas, Spain, 2022.

A.2.3 Local conferences, workshops, invited talks

[1] Chaouki Kasmi, José Lopes Esteves, Mathieu Renard, and Emmanuel Duponchelle. Méthode pour une analyse autonome des perturbations induites par des interférences électromagnétiques. In *Journées Aremif*, Paris, France, 2014.

[2] Valentin Houchouas, Chaouki Kasmi, José Lopes Esteves, and Philippe Valembois. Caractérisation logicielle de la susceptibilité d'un capteur de température de PC pour la CEM et la SSI. In *18 Ème Colloque International et Exposition Sur La Compatibilité ÉlectroMagnétique (CEM 2016)*, Rennes, France, 2016.

[3] Chaouki Kasmi and José Lopes Esteves. Détection et caractérisation des effets induits par des interférences électromagnétiques sur un ordinateur. In *Journée de l'Aremif*, Paris, France, 2016.

[4] Chaouki Kasmi and José Lopes Esteves. Exploitation des effets induits par des interférences électromagnétiques pour la commande et le contrôle d'un code malveillant présent sur une machine isolée. In *Journée de l'Aremif*, Paris, France, 2016.

[5] Sébastien Lalléchère, Chaouki Kasmi, José Lopes Esteves, Sébastien Girard, Pierre Bonnet, and Françoise Paladian. Apport de l'analyse statistique de ré-échantillonnage pour l'optimisation CEM. In *18 Ème Colloque International et Exposition Sur La Compatibilité ÉlectroMagnétique (CEM 2016)*, Rennes, France, 2016.

[6] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. Détection de Diaphonie et AGREMI par une approche SSI. In *19 Ème Colloque International et Exposition Sur La Compatibilité ÉlectroMagnétique (CEM 2018)*, Paris, France, 2018.

[7] José Lopes Esteves. Exemples d'interactions entre CEM et Sécurité de l'Information. In *Conférence Plénière Du GDR Ondes*, Gif sur Yvette, France, 2019.

[8] Valentin Houchouas, Muriel Darces, Marc Hélier, Emmanuel Cottais, and José Lopes Esteves. Application du modèle de couplages aléatoires pour l'évaluation de probabilités d'occurrence de courants induits. In *20ème Colloque International et Exposition Sur La Compatibilité ÉlectroMagnétique*, Lyon, France, 2020.

[9] José Lopes Esteves, Valentin Houchouas, Guillaume Bouffard, and Thomas Trouchkine. Caractérisation d'antennes pour l'injection de fautes sur composants électroniques. In *Conférence Plénière Du GDR Ondes*, Lille, France, 2021.

A.3 Publications information security

A.3.1 Journals

[1] Chaouki Kasmi, José Lopes Esteves, and Philippe Valembois. Air-gap Limitations and Bypass Techniques:"Command and Control" using Smart Electromagnetic Interferences. *The Journal on Cybercrime & Digital Investigations*, 1(1):13–19, 2016. ISSN 2494-2715. doi: 10.18464/cybin.v1i1.4.

A.3.2 International conferences

[1] Chaouki Kasmi, José Lopes Esteves, and Mathieu Renard. DESIGN OF AN IEMI-ATTACK DETECTOR INVOLVING THE INTERNAL RESOURCES OF A COTS COMPUTER. In *Ninth Future Security*. Fraunhofer Verlag, 2014. ISBN 978-3-8396-0778-7.

[2] Chaouki Kasmi, José Lopes Esteves, and Philippe Valembois. Air-gap Limitations and Bypass Techniques:"Command and Control" using Smart Electromagnetic Interferences. In *Bot Conf.*, 2015.

[3] José Lopes Esteves and Chaouki Kasmi. Injection de commandes vocales sur ordiphone. In *Symposium Sur La Sécurité Des Technologies de l'Information et Des Communications (SSTIC)*, Rennes, France, 2015.

[4] José Lopes Esteves and Chaouki Kasmi. You don't hear me but your phone's voice interface does. In *Hack In Paris 2015*, Paris, France, 2015.

[5] Chaouki Kasmi and José Lopes Esteves. Whisper in the Wire: Voice Command Injection Reloaded. In *Hack In Paris*, Paris, France, 2016.

[6] Patrick Haddad, Chaouki Kasmi, José Lopes Esteves, and Valentin Houchouas. Electromagnetic Harmonic Attack on Transient Effect Ring Oscillator based True Random Generator. In *Hardwear.Io*, The Hague, Netherlands, 2016.

[7] José Lopes Esteves and Chaouki Kasmi. Contournement d'air gaps par canaux cachés électromagnétiques. In *DNAC*, Paris, France, 2016.

[8] Ryad Benadjila, Mathieu Renard, José Lopes Esteves, and Chaouki Kasmi. From Academia to Real World: A Practical Guide to Hitag-2 RKE System Analysis. In *Symposium Sur La Sécurité Des Technologies de l'Information et Des Communications (SSTIC)*, Rennes, France, 2017.

[9] Ryad Benadjila, Mathieu Renard, José Lopes Esteves, and Chaouki Kasmi. One Car, Two Frames: Attacks on Hitag-2 Remote Keyless Entry Systems Revisited. In *11th USENIX Workshop on Offensive Technologies (WOOT 17)*, Vancouver, BC, 2017. USENIX Association.

[10] Chaouki Kasmi and José Lopes Esteves. Electromagnetic Threats for Information Security: Ways to Chaos in Digital and Analogue Electronics. In *34th Chaos Computer Club Congress*, Leipzig, Germany, 2017.

[11] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. A Ghost in your Transmitter : Analyzing polyglot signals for physical layer covert channels detection. In *Hardwear.Io*, The Hague, Netherlands, 2017.

[12] Chaouki Kasmi and José Lopes Esteves. Ventrilock: Exploring Voice-based Authentication Systems. In *Hack In Paris 2017*, Paris, France, 2017.

[13] Tristan Claverie, José Lopes Esteves, and Chaouki Kasmi. Smart TVs: Security of DVB-T. In *Symposium Sur La Sécurité Des Technologies de l'Information et Des Communications (SSTIC)*, Rennes, France, 2018.

[14] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. Strategies to harden and neutralize UAV using RF DEW. In *Hardwear.Io*, The Hague, Netherlands, 2018.

[15] Tristan Claverie and José Lopes Esteves. A LoRaWAN security assessment test bench. In *European GNU Radio Days 2019*, Besançon, France, 2019.

[16] José Lopes Esteves. Agressions Electromagnétiques et Forensics. In *Conférence Sur La Réponse Aux Incidents et l'investigation Numérique (CoRI&IN) 2019*, Lille, France, 2019. Cecyf.

[17] José Lopes Esteves. Watermarking Electromagnétique de Drones. In *Symposium Sur La Sécurité Des Technologies de l'Information et Des Communications (SSTIC)*, Rennes, France, 2019.

[18] José Lopes Esteves and Tristan Claverie. Testing for Weak Key Management in Bluetooth Low Energy Implementations. In *Symposium Sur La Sécurité Des Technologies de l'Information et Des Communications (SSTIC)*, Rennes, France, 2020.

[19] Tristan Claverie and José Lopes Esteves. BlueMirror: Defeating Bluetooth authentication protocols. In *Hardwear.Io*, The Hague, Netherlands, 2021.

[20] José Lopes Esteves and Tristan Claverie. BlueMirror: Reflections on Bluetooth Pairing and Provisioning Protocols. In *15th USENIX Workshop on Offensive Technologies (WOOT 21)*. IEEE Computer Society, 2021.

[21] José Lopes Esteves, Tristan Claverie, and Nicolas Docq. Analyse des propriétés de sécurité dans les implémentations du Bluetooth Low Energy. In *Symposium Sur La Sécurité Des Technologies de l'Information et Des Communications (SSTIC)*, Rennes, France, 2021.

[22] José Lopes Esteves and Pierre-Michel Ricordel. Un Pare-Feu pour le HDMI. In *Symposium Sur La Sécurité Des Technologies de l'Information et Des Communications (SSTIC)*, Rennes, France, 2021.

[23] Nicolas Mora, Chaouki Kasmi, David Martinez, Felix Vega, and José Lopes Esteves. Electromagnetic Security: A Deep dive into Electromagnetic Compatibility through the Information Security Lens, 2021.

A.3.3 Local conferences, workshops and invited talks

[1] José Lopes Esteves. Sécurité et objets connectés: Regard sur l'évolution de la menace. In *ESIEA Secure Edition*, Paris, France, 2015.

[2] José Lopes Esteves. Implantation d'information dans des cibles non coopératives par perturbations EM : Application à la lutte anti-drones. In *Journées d'études Electromagnetisme et Guerre Electronique (EM+GE 21)*, Toulouse, 2021.

[3] José Lopes Esteves. Interférences intentionnelles et attaques en faute : Différentes similarités. In *Journée Thématique Sur Les Attaques Par Injection de Fautes (JAIF 21)*, Paris, France, 2021.

A.3.4 Scientific magazines

[1] Chaouki Kasmi and José Lopes Esteves. Agressions électromagnétiques et risques SSI. *MISC*, HS n°16(16):54–61, 2017. ISSN 1631-9036.

Appendix B

Résumé étendu en français

Contents

B.1 Introduction

Les équipements électroniques sont devenus omniprésents dans tous les secteurs de nos vies, du militaire au civil, des infrastructures critiques à nos maisons, nos pacemakers. Par ailleurs, des équipements "sur étagère", sont de plus en plus considérés y compris dans des contextes sensibles. Cette prolifération introduit de nouveaux besoins de sécurité pour l'information manipulée par ces équipements. En particulier, des scénarios de menace impliquant un attaquant ayant un accès physique aux équipements, à proximité ou au contact, voient leur vraisemblance augmenter. Cela expose les équipements à des attaques physiques, où l'attaquant exploite les propriétés physiques de la cible ou de son environnement.

Dans le cas de perturbations électromagnétiques (EM), comme les attaques par interférences électromagnétiques intentionnelles (IEMI), la propriété physique est l'environnement EM et l'attaquant est considéré actif, i.e. ayant la possibilité d'imposer de l'énergie EM à la cible. Cela a pour effet l'apparition de courants et tensions parasites dans les éléments conducteurs constitutifs de la cible. Les effets électriques peuvent se propager aux couches logiques pour impacter une fonction de la cible ou l'information traitée.

Dans le domaine scientifique de la compatibilité électromagnétique (CEM), l'étude de ces effets est un sujet exploré depuis plusieurs décennies dans le but d'en comprendre les mécanismes physiques et d'en limiter les impacts fonctionnels. Cependant, les méthodes de CEM sont peu adaptées pour répondre à des problèmes liés à la sécurité de l'information.

Un champ de recherche en sécurité de l'information s'intéresse à l'injection de fautes EM sur des composants électroniques. Une caractérisation des effets logiques est effectuée pour déterminer des modèles de fautes, qui permettent de faciliter l'analyse d'exploitabilité et la conception de contre-mesures. Cependant, les approches développées et les modèles de menaces considérés sont peu adaptés à l'étude de systèmes complexes.

Cette thèse de doctorat est dédiée à l'étude des effets des IEMI sur des équipements électroniques et l'analyse de leurs impacts pour la sécurité de l'information traitée. Les contributions principales sont les suivantes:

- Une méthode de caractérisation reposant sur une instrumentation logicielle de la cible, spécifiquement conçue pour tester des modèles de faute et faciliter l'analyse d'exploitabilité, la détection et l'investigation numérique;
- Une attaque originale exploitant les effets des IEMI sur des ordiphones et permettant une interaction silencieuse en non autorisée avec un assistant vocal;

- L'exploration d'un nouveau modèle de menace exploitant les IEMI et permettant l'établissement d'un canal de communication caché avec un implant logiciel dans un ordinateur de bureau isolé;

- La proposition d'un nouveau modèle de menace appelé *watermarking électromagnétique*, permettant l'implantation d'information dans des cibles distantes non-coopératives via IEMI.

Dans ce résumé, la section B.2 rappelle les grands principes régissant la CEM et la cybersécurité. Ces deux thématiques se rejoignent pour former la sécurité électromagnétique, dont les principaux modèles de menace sont décrits.

La section B.3 présente les deux approches existantes étudiant les effets des perturbations EM causées par un attaquant: les IEMI, discipline issue de la CEM, et l'injection de fautes EM qui est une discipline de cybersécurité.

Dans la section B.4, une méthode de caractérisation des effets des IEMI sur un équipement électronique utilisant des modèles de faute au niveau du système d'exploitation est proposée. Cette approche, dite *systémique*, requiert une instrumentation logicielle de la cible pendant les tests et facilite l'analyse d'exploitabilité des effets et le détection. La mise en œuvre de cette approche est proposée sur un ordinateur de bureau et illustrée par quelques exemples d'effets identifiés.

Une attaque originale exploitant les effets des IEMI sur un ordiphone est proposée dans la section B.5. L'attaquant introduit des signaux parasites dans le système de numérisation de l'entrée audio et obtient ainsi un moyen d'interaction avec l'assistant vocal de la cible. Il s'agit de la première attaque par IEMI sur un ordiphone ainsi que la première attaque visant un assistant vocal par perturbation du capteur audio.

La section B.6 explore un nouveau modèle de menace exploitant les IEMI afin de mettre en place un canal de communication caché avec un implant logiciel. Ce modèle de menace est formalisé, puis mis en pratique dans un scénario ciblant un ordinateur de bureau isolé par un *air gap*.

Un nouveau modèle de menace, le *watermarking électromagnétique*, est également proposé en section B.7. Il s'agit là de l'exploitation de certains effets des IEMI ayant un impact persistant afin d'implanter de l'information à distance dans des cibles non coopératives. Cette information peut alors être extraite ou identifiée *a posteriori*, constituant ainsi une forme de tatouage numérique. Une application pratique dans un contexte d'investigation numérique et de lutte anti-drone (LAD) est proposée pour permettre du *forensic tracking* sur un drone.

Enfin, la section B.8 propose des perspectives de recherche découlant de l'ensemble des travaux présentés dans ce mémoire.

B.2 Sécurité électromagnétique

B.2.1 Sécurité de l'information

La sécurité de l'information regroupe plusieurs disciplines visant à protéger l'information durant son cycle de vie au sein d'un système d'information et à gérer les risques liés à une éventuelle compromission. Les méthodes de protection de l'information et de gestion des risques sont spécifiées dans la famille de normes ISO/IEC 27000 [ISO18]. La sécurité y est définie ainsi: "la sécurité de l'information assure la confidentialité, la disponibilité et l'intégrité de l'information. Cela est obtenu par l'implémentation d'un ensemble de contrôles incluant des politiques, processus, procédure, structures organisationnelles, logicielles ou matérielles pour protéger les biens sensibles." Les étapes principales pour un système de gestion de risques en sécurité de l'information sont les suivantes [ISO18]:

- Identifier les biens à protéger et leurs besoins en sécurité;
- Analyser et traiter les risques pour la sécurité de l'information;
- Sélectionner et implémenter des contrôles pour gérer les risques inacceptables;
- Superviser, maintenir et améliorer l'efficacité des contrôles.

Les besoins en sécurité sont définis dans plusieurs ouvrages de référence [And20, ANS10, Cri17b, ISO18]:

- La confidentialité de l'information est la propriété assurant que l'information n'est révélée qu'aux entités autorisées par la politique de sécurité;
- La disponibilité de l'information est la propriété assurant que l'information est accessible et utilisable à la demande par toute entité autorisée par la politique de sécurité;
- L'intégrité est la propriété assurant que l'information est complète, précise et n'a pu être modifiée que par des entités autorisée par la politique de sécurité.

La gestion des risques et le dimensionnement des contremesures nécessitent la mise en œuvre d'analyses de sécurité ayant pour but d'identifier le niveau de robustesse des fonctions de sécurité présentes pour protéger l'information sensible. Pour chaque fonction de sécurité, il est nécessaire de déterminer ce qu'elle protège, de quels types d'attaque et dans quelles conditions opérationnelles. Il est également nécessaire d'identifier si des vulnérabilités permettent de la contourner et de quantifier le profil d'attaquant requis pour exploiter ces vulnérabilités. Différentes approches pour l'évaluation

de sécurité sont documentées [ANS20, Cri17a, Cri17b]. En particulier, le concept de modèle de menace est introduit comme décrivant les capacités maximales allouées à un attaquant ainsi que l'ensemble ses actions et ses objectifs potentiels.

La supervision, la maintenance, et l'amélioration de l'efficacité des contrôles fait intervenir le domaine de l'investigation numérique et de la réponse à incident [Joh20]. Aucune sécurité absolue n'est possible et il est admis, dans une démarche de gestion des risques, que le système d'information pourra être compromis. Il devient alors indispensable de détecter la compromission, de la contenir et la circonscrire, de reprendre une fonctionnement sain et d'analyser les actions de l'attaquant ayant permis la compromission.

B.2.2 Compatibilité électromagnétique

La CEM est définie comme la capacité d'un équipement ou un système à fonctionner de manière satisfaisante dans son environnement EM sans introduire de perturbations EM intolérables à toute autre entité dans cet environnement [ISO92]. L'environnement EM désigne l'ensemble des phénomènes EM existant à un endroit donné. Une perturbation EM peut être tout phénomène EM qui pourrait dégrader la performance d'un équipement ou d'un système, ou affecter de la matière vivante ou inerte. En d'autres termes, un système est électromagnétiquement compatible si il satisfait trois critères [Pau06]:

- Il n'interfère pas avec d'autres systèmes;
- Il n'est pas susceptible aux émissions des autres systèmes;
- Il n'interfère pas avec lui-même.

Un problème de CEM s'intéresse à la génération (par une source), la transmission (par un chemin de couplage) et la réception (par un récepteur) d'énergie EM. Suivant ce modèle, trois approches générales sont envisageables pour éviter un problème de CEM:

- Supprimer l'émission à sa source;
- Rendre le chemin de couplage inefficace;
- Rendre le récepteur moins susceptible à l'émission.

Lorsque l'on se focalise sur un système électronique ou électrique, résoudre un problème de CEM revient à en maîtriser les émissions et la susceptibilité. En pratique, on s'assure que les émissions et la susceptibilité restent inférieures à des seuils, standards, correspondant à des environnements

EM cibles. Le transfert d'énergie EM entre une source et un récepteur est généralement envisagé sous deux formes. Lorsque l'énergie est complètement guidée par conduction galvanique, on parle d'émissions conduites de la source ou de susceptibilité conduite pour le récepteur. Dans le cas contraire, l'énergie électromagnétique est dite rayonnée et peut être collectée par les éléments conducteurs du récepteur. On parlera alors d'émissions ou de susceptibilité rayonnées.

B.2.3 Sécurité électromagnétique

Bien que la CEM et la sécurité de l'information aient des objectifs bien distincts, les phénomènes étudiés en CEM peuvent être exploités intentionnellement par un attaquant pour porter atteinte à la sécurité de l'information. La sécurité EM peut être définie comme un sous domaine de la sécurité de l'information focalisé sur les menaces pour la sécurité de l'information traitée par un équipement électronique et qui ont pour origine des interactions avec son environnement EM. Dans ce cadre, on peut considérer que les émissions EM d'un équipement électronique peuvent constituer des menaces pour la confidentialité de l'information traitée. Réciproquement, les problèmes de susceptibilité d'un équipement peuvent constituer des menaces pour l'intégrité ou la disponibilité de l'information traitée.

La menace TEMPEST concerne l'exploitation des émissions EM pour obtenir de l'information sur les informations traitées par un équipement électronique cible. L'activité électrique ou électronique légitime de la cible, lorsqu'elle traite des informations sensibles, s'accompagne d'émissions EM qui peuvent être collectées par un attaquant. L'attaquant peut alors, dans certaines conditions, aller jusqu'à reconstruire l'information traitée. Lorsque ces émissions parasites sont liées aux informations sensibles, on parle de signaux parasites compromettants.

Un modèle de menace appelé Soft-Tempest repose sur l'exploitation intentionnelle des émissions EM par un implant logiciel présent dans le système cible. Cet implant cherche à contrôler les émissions parasites de manière à moduler de l'information en vue de l'établissement d'un canal de communication caché avec l'attaquant. L'attaquant, en collectant les émissions parasites, peut alors se comporter comme un récepteur et les démoduler, décoder pour accéder à l'information émise par l'implant logiciel.

Les attaques dites par canaux auxiliaires EM exploitent les émissions EM des composants électroniques pour attaquer des implémentations de mécanismes cryptographiques. Dans ce modèle de menace, l'attaquant a généralement accès physiquement au composant électronique cible, peut déclencher des opérations cryptographiques, effectuer des mesures des émissions EM et avoir accès au résultat des opérations. Sur la base de ces éléments, les secrets cryptographiques (clés) peuvent

parfois être déterminés.

Une des premières exploitations de la susceptibilité EM a été de profiter des effets destructifs des signaux agresseurs dans les systèmes cibles. Des effets thermiques ou électriques peuvent porter atteinte aux composants électroniques, aux circuits intégrés, aux circuits imprimés, impactant ainsi la disponibilité de la cible. Lorsque les signaux agresseurs atteignent des circuits de réception radiofréquence, l'impact sur la disponibilité de la communication pourra être assimilé à du brouillage.

D'autres attaques peuvent impacter l'intégrité de l'information traitée par la cible, comme les attaques par injection de signal. Dans ce modèle de menace, l'attaquant exploite la susceptibilité EM de la cible pour introduire des courants ou tensions parasites qui seront interprétés comme des signaux légitimes. Lorsque le signal parasite n'a pas les mêmes caractéristiques que le signal légitime cible, il est dit hors bande et devra être transformé ou converti par la cible pour être ramené dans la bande du signal cible.

Enfin, les attaques par injection de faute EM exploitent la susceptibilité EM de composants électroniques. D'abord focalisées sur la cryptanalyse, les techniques d'attaques par injection de faute ont ensuite été mises en œuvre pour biaiser des générateurs d'aléa, porter atteinte à l'intégrité des données, des instructions ou du flot d'exécution de programmes, ou encore à l'intégrité de données stockées.

B.3 Attaques par perturbation EM

Deux domaines de recherche sont concernés par l'étude des effets des perturbations EM intentionnelles sur des équipements ou des systèmes électroniques. Dans le cadre de la CEM, l'étude des effets collatéraux lors d'essais nucléaires a donné lieu à des recherches sur les impulsions EM d'origine nucléaire, les micro-ondes de forte puissance, les IEMI. Dans le cadre de la cryptanalyse, l'étude de l'impact de défaillances matérielles sur des implémentations de mécanismes cryptographiques a ouvert la voie à des recherches sur les attaques par injection de faute EM sur des composants électroniques.

B.3.1 Les interférences électromagnétiques intentionnelles

Les IEMI peuvent être modélisées comme suit: un attaquant dispose d'une source capable de générer de l'énergie EM destinée à un système électronique cible. Cette énergie, pour atteindre la cible, subit une propagation par rayonnement ou conduction. Lorsqu'elle atteint la cible, des courants et tensions parasites apparaissent dans les parties conductrices par un phénomène de couplage. Ces courants

et tensions parasites, en touchant l'électronique de la cible, peuvent produire des impacts physiques et/ou logiques.

Lorsque l'IEMI se couple à une interface conçue pour collecter des signaux EM comme les front-ends radio, on parle de couplage direct. Le couplage direct est dit du premier ordre lorsque les signaux agresseurs ont les caractéristiques spectrales dans la bande de l'interface cible. On parle de couplage direct du second ordre, ou hors bande, lorsque les signaux agresseurs ne se situent pas dans la bande de l'interface cible. Le couplage indirect désigne une interaction de l'IEMI à travers des câbles, ouvertures, imperfections du boîtier de la cible.

Contrairement aux autres environnements EM standardisés en CEM, ceux de l'IEMI ne peuvent pas être déterminés par une approche empirique ou stochastique. La prise en compte d'un attaquant rend la menace IEMI protéiforme et par conséquent imprévisible. Pour faire face à cette problématique, les environnements EM de l'IEMI sont classifiés par rapport aux caractéristiques du signal source. En particulier, afin de pouvoir comparer des signaux maintenus et des signaux transitoires, le *band ratio (br)* est utilisé. Il s'agit du rapport entre les fréquences haute et basse entre lesquelles 90% de l'énergie est contenue [GHS20]. Les sources sont regroupées en quatre catégories:

- Hypoband: $br \leq 1.01$
- Mesoband: $1.01 < br \leq 3$
- Sub-hyperband: $3 < br \leq 10$
- Hyperband: $10 < br$

Les capacités des sources sont des éléments dimensionnants du profil d'attaquant et des contraintes opérationnelles. Différentes classifications des sources selon différents critères reflétant les enjeux à la fois technologiques et en termes d'analyse de risques sont proposées dans [MP16], qui fait référence dans l'étude des sources pour des IEMI. A partir des caractéristiques de la source, différents groupes de capacité technique sont définis dans [ISO20]:

- Novice: individus ou petits groupes avec un soutien financier ou technique minimal;
- Compétent: adversaires modérément financés ayant une formation et une expertise dans les technologies concernées;
- Spécialiste: adversaires financés à la hauteur de leur besoin, ayant une formation de troisième cycle et un accès à des capacités conséquentes de recherche.

Les caractéristiques du signal produit (fréquence, puissance, fréquence de répétition, longueur d'impulsion...) ou encore le niveau de portabilité de la source sont également des éléments qui peuvent être pris en compte dans une démarche de gestion des risques liés aux IEMI. Une tendance a été observée concernant l'évolution de la production de sources [MP16]: l'intérêt initial s'est porté sur des sources de très forte puissance, large bande, génériques, pour progressivement se diriger vers de sources à bande plus étroite, plus intelligentes.

Une spécificité des standards de CEM traitant des IEMI est la grande diversité des cibles envisagées, en particulier en termes d'échelles. Ainsi, les cibles des études de susceptibilité peuvent aller de composants électroniques (diodes, transistors, circuits intégrés...) à des infrastructures bâtimentaires ou des véhicules.

Face à cette multiplicité de menaces, de cibles, le dimensionnement des tests de susceptibilité est très complexe. Dans [ISO20], la spécification des tests se fait en plusieurs étapes:

- Comprendre la menace par IEMI pour la cible;
- Mesurer le niveau de protection de la cible;
- Prédire les signaux induits au niveau de la cible;
- Créer des prédictions des enveloppes de signaux touchant la cible;
- Analyser la susceptibilité en injectant les formes d'onde prédites.

Par conséquent, le dimensionnement des tests de susceptibilité nécessite à la fois une prédiction du type de menace (donc du profil d'attaquant), une prise en compte du contexte opérationnel (pour la mesure du niveau de protection) et la définition de critères de défaillance liés aux fonctions principales de la cible.

Par ailleurs, différentes approches pour la classification des effets observés ont été proposées. Cependant, elles sont majoritairement dépendantes du contexte opérationnel où la cible est vouée à évoluer. De plus, les critères de défaillance sont essentiellement focalisés sur la disponibilité de la fonction principale de la cible.

Dans les études de susceptibilité face à des menaces de type IEMI, les effets obtenus ont été exploités à différentes finalités. Tout d'abord, la destruction d'éléments conducteurs ou de composants électroniques a été largement documentée [GHS20, Int78, Mej19, SN06]. La dégradation des performances d'équipements réseau [PS11] ou de lecteurs de passeports [ASP+14] a été également documentée.

Des dégradations sur des composants de systèmes de transmission radiofréquences ont également été obtenues, en particulier sur des boucles à verrouillage de phase [Dub11], des amplificateurs faible bruit ou des amplificateurs de puissance [PRC17].

Des attaques en injection de signal sur des interfaces de communication conduite ont également été réalisées, comme l'universal asynchronous receiver transmitter (UART) ou l'I2C [DMGM22] ou encore le courant porteur en ligne (CPL) [GP22, NSFG21].

Des capteurs et des actionneurs ont également été impactés par les effets des IEMI. De l'injection de signal est démontrée sur différents capteurs analogiques, microphones [KBC+13], capteurs optiques [KBM22] ou encore des écrans tactiles [JJW+22, MWM19, SZZ+22, WMY+22]. Des servomoteurs pilotés en pulse width modulation (PWM) ont également été perturbés [DSM+22].

Pour se protéger de telles attaques, plusieurs contre-mesures sont complémentaires. Le filtrage et le blindage de la cible et de ses interfaces peuvent entraver le couplage et la propagation des signaux agresseurs. Le zonage permet d'éloigner les équipements sensibles de l'attaquant. Les techniques logicielles et matérielles de tolérance aux fautes peuvent être envisagées. La redondance permet de réduire les impacts de l'attaque en assurant une continuité des fonctions principales et oblige l'attaquant à multiplier les attaques. La supervision externe permet de faire de la détection. Plusieurs détecteurs externes d'IEMI rayonnée ont été proposés [DFK+14, EWHR22, HRP+22, RJL+22]. La détection se fait sur des niveaux de puissance dépassant des seuils sur différentes bandes. Des caractéristiques des signaux détectés sont journalisées. La détection peut également être envisagée au niveau de la cible, au sein des capteurs [TTPH21, ZR20].

B.3.2 Injection de faute électromagnétique

Le domaine de recherche en injections de faute EM et l'exploitation de ces techniques dans un contexte de sécurité de l'information semble hériter des travaux sur la tolérance aux fautes des composants et de la cryptanalyse. Dans ce domaine, l'attaquant interagit avec un circuit intégré implémentant une fonction cible en imposant un environnement électromagnétique agresseur, par conduction directement via ses broches d'entrée-sortie ou par un couplage capacitif ou inductif en champ proche. Dans le modèle de menace générique de cette approche, l'attaquant peut également préparer la cible pour faciliter son attaque, dispose d'un contrôle de ses entrées-sorties et de moyens de se synchroniser à son activité [Tro21]. Récemment, l'obtention de fautes via une interaction logicielle a également été démontrée ([SD15] par exemple).

Les attaques par injection de faute ciblent exclusivement des composants électroniques plus ou moins complexes, cartes à puce [SH07], micro-contrôleurs [DDR+12], field programmable gate array

(FPGA) [MAB+18], systèmes sur puce [Tro21], mémoires flash [Ame15].

Les signaux agresseurs considérés peuvent être classés en deux catégories:

- Les signaux impulsionnels sont considérés comme impactant plutôt les circuits numériques
- Les signaux bande étroite sont considérés comme ayant un impact sur les fonctions analogiques

D'autres paramètres expérimentaux peuvent avoir une influence sur l'efficacité d'une campagne d'injection de faute, comme la position du point d'injection sur le composant ou le moment de l'injection par rapport à l'activité de la cible.

Pour l'observation des effets, des modèles de faute sont souvent utilisés. Un modèle de faute correspond à la manifestation d'un effet depuis un niveau d'observation donné. Par exemple, un modèle de faute au niveau physique peut être l'apparition d'une tension parasite dépassant un certain seuil. Le même phénomène, observé au niveau de la micro-architecture, peut être modélisé par une corruption de registre par exemple.

Les méthodes d'attaques par injection de faute sont conçues dans une perspective de sécurité de l'information. Certaines études visent explicitement une fonction de sécurité et réduisent l'effort à l'exploration d'un scénario unique. Des approches plus génériques procèdent d'abord à une caractérisation de la cible pour identifier des modèles de faute et des positions d'injection efficaces, pour explorer ensuite l'exploitation des modèles de faute les plus intéressants.

La première application de l'injection de faute envisagée concerne la cryptanalyse. Plusieurs attaques visant des implémentations de mécanismes cryptographiques, symétriques ou asymétriques, de chiffrement ou de signature ont été proposées, fournissant à l'attaquant les secrets cryptographiques comme les clés secrètes ou privées. Pour une mise en œuvre correcte de protocoles cryptographiques, la bonne génération d'aléa est d'une importance capitale. Des implémentations matérielles de génération d'aléa ont été attaquées avec pour impact l'introduction de biais dans les séquences de nombres aléatoires générées. Les impacts sur l'intégrité du flot d'exécution de programmes, des données ou des instructions, ont été exploités sur plusieurs types de plateformes matérielles pour contourner des fonctions de sécurité. Des élévations de privilèges dans de systèmes d'exploitation [TM17], des contournements de chaînes de démarrage sécurisées [Res19] ou la réactivation d'interfaces de programmation ou de déverminage [Res20] ont été obtenus. Enfin, des lectures de zones mémoire non autorisées ont également été observées, fournissant à l'attaquant des informations non prévues, comme des secrets cryptographiques [O'F19] ou des *firmwares*.

Des contre-mesures sont proposées, à commencer par le blindage des composants cibles. L'ajout de capteurs au sein des circuits intégrés a également été exploré, en utilisant des fils de *bonding* ou des

éléments sensibles (comme des fonctions analogiques) [ERM16, Mad19, ZDT+14]. La redondance logicielle ou matérielle est également envisagée, de manière à obliger l'attaquant à réussir plusieurs fautes pour attaquer. Les mécanismes de vérification de flot de contrôle lors de l'exécution permettent de s'assurer de l'absence de faute lors d'opérations sensibles. Une revue exhaustive des contre-mesures logicielles est proposée dans [Mad19, Tro21].

B.4 Approche systémique

Les méthodes héritées de la CEM pour les tests de susceptibilité à l'IEMI considèrent des sources de forte puissance et des impacts sur la disponibilité des fonctions principales de la cible. Le dimensionnement des tests est dépendant du contexte opérationnel. Les méthodes mise en œuvre en injection de faute EM sont focalisées sur l'étude de composants électroniques et non des systèmes plus complexes. L'utilisation de modèles de fautes lors de l'étape de caractérisation a cependant montré son intérêt pour des analyses en sécurité de l'information.

Les modèles de faute au niveau informationnel pourraient apporter une forme de généricité des résultats observés en décorrélant les effets observés du contexte opérationnel et des fonctions principales. Par ailleurs, en ayant recours à des modèles de faute fournissant un moyen d'observer des symptômes sur l'information, il devient envisageable de raisonner sur la propagation de ces symptômes sur la sécurité d'applications qui utilisent l'information impactée. Enfin, les modèles de faute représentent l'occurrence d'un effet. Des applications en détection basées sur l'observation de la réalisation de modèles de faute peuvent ainsi être pertinentes pour ouvrir des perspectives en investigation numérique.

Ainsi, nous proposons d'utiliser des modèles de faute pour la caractérisation de systèmes électroniques lors de tests de susceptibilité à l'IEMI. En choisissant des modèles de faute de niveau informationnel, il devient possible d'observer l'occurrence d'effets tels que le système d'exploitation pourrait les percevoir. C'est l'idée structurante de *l'approche systémique*.

L'idée sous-jacente à l'approche systémique repose sur une instrumentation logicielle de la cible pour les tests de susceptibilité. Un ensemble d'observables logicielles doit d'abord être identifié pour détecter l'occurrence d'un modèle de faute. Le choix de ces observables peut être réalisé dans un mode *bottom-up* sur la base des interactions physiques envisagées. Il s'agit alors d'identifier les interfaces de couplage à surveiller, des modèles de faute pouvant toucher ces interfaces, puis des interfaces logicielles permettant d'en observer l'occurrence. Une approche *top-down* peut également être envisagée: à partir d'un ensemble d'informations à protéger (manipulées par une application

par exemple), on identifie des modèles de faute pouvant les affecter. Il s'agira alors de focaliser les critères de défaillance des tests sur la réalisation de ces modèles de faute. Un ou plusieurs codes de test peuvent ensuite être développés puis implantés dans la cible.

Cette approche systémique présente plusieurs avantages. Tout d'abord, l'implantation de codes de test permet l'observation des effets "depuis l'intérieur" de la cible, comme les verront des applications qui utilisent les informations impactées. Cette observation peut se faire en temps réel (ou en léger différé) pendant les tests. Ensuite, les analyses d'exploitabilité des effets sont facilitées. Le fait d'identifier des impacts sur l'information permet non seulement d'identifier les conséquences pour la sécurité des applications qui les manipulent, mais aussi de se projeter sur des scénarios d'exploitation reposant sur les impacts identifiés.

L'approche systémique ouvre des perspectives dans le domaine de la détection. Des codes de supervision peuvent être développés en implantés dans la cible de manière à transformer la cible en un ensemble de capteurs à la recherche de l'occurrence d'effets des IEMI. Avec cette auto-supervision, il peut être envisagé que la cible adapte son comportement aux informations remontées par ses capteurs selon l'activité EM environnante.

A l'échelle d'un parc informatique, si l'on considère que chaque machine possède cette capacité d'autosupervision, un système de supervision et de détection global pourrait être envisagé. Chaque machine pourrait ainsi faire des remontées à un système central de manière à fournir une vision de son état et de son environnement EM. De cette manière, en présence de signaux agresseurs, il est probable que seules certaines machines colocalisées feront état de symptômes de forte intensité, fournissant au système central une manière de localiser physiquement la provenance des signaux agresseurs.

En contrepartie, l'approche systémique présente des limites importantes. Tout d'abord, cette approche repose sur une autosupervision de la cible qui est agressée. Les système d'autosupervision peut tout à fait être impacté par les effets des IEMI et l'intégrité des observations doit être par conséquent questionnée. Par ailleurs, l'identification d'interfaces logicielles instrumentables peut être une étape complexe sur des systèmes fermés. Enfin, pour les mêmes raisons, l'implantation des codes test peut également nécessiter de gros efforts lors de tests sur des systèmes sur lesquels on n'a pas un contrôle total.

B.5 Attaque d'assistant vocal par IEMI

Dans cette section, la susceptibilité d'un microphone analogique à des IEMI est étudiée. L'exploitabilité des effets obtenus est démontrée par la mise en œuvre d'une attaque par injection de signal hors bande

qui permet à un attaquant distant d'introduire des signaux parasites qui seront transformés par les étages de numérisation de l'entrée audio en un signal audio. Ce signal audio sera consommé par une application, l'assistant vocal, en écoute permanente sur l'entrée audio et en attente de commandes vocales. L'attaquant obtient ainsi un accès distant, silencieux, non autorisé à l'assistant vocal de la cible, par IEMI.

Les assistants vocaux sont de plus en plus déployés sur différents systèmes électroniques comme les ordiphones, les ordinateurs de bord de voiture, les montres connectées, les enceintes connectées... Leur fonctionnement est réparti entre la détection d'un mot clé d'activation qui est faite localement sur le système, puis l'interprétation d'une commande vocale, généralement effectuée sur un serveur distant. Enfin, une fois interprétée, la commande peut être exécutée localement ou par un service distant. L'interaction homme-machine se fait par l'interface audio, ce qui permet une utilisation du système les mains libres.

Des analyses de la sécurité de ces assistants vocaux ont été réalisées, et plusieurs catégories d'attaque ont été identifiées [YJW+22], dont des attaques dites par signaux inaudibles. En effet, l'interaction légitime étant vocale, elle peut être considérée comme audible et facilement détectable. Une injection de signal inaudible permet alors à l'attaquant de profiter d'un cas non prévu et d'échapper à certaines mesures de sécurité qui reposeraient sur l'hypothèse d'une interaction audible.

Dans notre étude, deux modes de couplage on été explorés:

- Une IEMI conduite, via le port de charge de la cible;
- Une IEMI rayonnée, via le câble des écouteurs de la cible.

La cible est un ordiphone Samsung Galaxy Nexus, donc les principales caractéristiques sont rappelés dans la Table 4.1, équipé de l'assistant vocal Google Now [Wik21].

Suivant l'approche systémique, une instrumentation logicielle a permis la détection des effets lors de la phase de caractérisation, puis la détermination des paramètres d'injection propices à l'exploitation de l'assistant vocal. Cette instrumentation a consisté en l'installation de deux applications provenant du magasin d'applications officiel et permettant l'enregistrement et la diffusion en Wi-Fi de l'activité en entrée de la carte son.

Dans les deux modes de couplage explorés, l'attaquant émet un signal agresseur hors bande, qui sera transformé par les non linéarités des composants électroniques en charge de la numérisation du signal électrique en entrée du front-end audio, comme documenté dans [KBC+13]. Le signal agresseur est constitué d'un signal audio (ayant des caractéristiques spectrales dans la bande

0–22 kHz) modulant une porteuse dont la fréquence doit être déterminée de manière à optimiser le couplage sur la cible.

Dans le cas rayonné, la fréquence porteuse a été choisie dans la bande allouée à la diffusion de la radio FM (80–120 MHz), puisque les caractéristiques électriques des câbles des écouteurs en font de bonnes antennes de réception dans cette bande.

Dans le cas conduit, la fréquence porteuse a été déterminée empiriquement par un balayage de la fréquence porteuse modulée par un *sweep* dans la bande audio, en observant les fréquences porteuses permettant d'injecter le signal ayant la plus grande amplitude mesurée par l'instrumentation logicielle. Une illustration de cette étape est fournie en Figure 4.10.

Suite à l'étape de caractérisation, un signal audio modulant contenant le mot clé "OK Google" et différentes commandes vocales a été utilisé pour étudier l'exploitabilité de l'assistant vocal. L'interaction avec l'assistant vocal a été réalisée sans difficulté lorsque les paramètres d'injection optimaux issus de la phase de caractérisation on été utilisés.

Une analyse de sécurité a été menée et différents scénarios ont été envisagés. L'attaquant, en interagissant librement avec l'assistant vocal, obtient un accès à l'ensemble des fonctionnalités exposées. Dans le cas d'un ordiphone, une captation de l'environnement sonore de la cible peut être envisagée, par l'envoi d'une commande vocale déclenchant un appel sur le téléphone de l'attaquant. L'utilisation de services de communication expose les contacts de la victime à des messages de hameçonnage. L'utilisation de services de téléphonie peut permettre à l'attaquant de causer un préjudice financier en souscrivant à des services payants, par SMS par exemple. Enfin, l'exploitation de l'IEMI peut être envisagée comme un point d'entrée d'une attaque avancée, en réactivant les interfaces radiofréquence comme le Wi-Fi par exemple, ce qui expose les piles protocolaires derrière ces interfaces. En déclenchant la visite d'une page web malveillante, une vulnérabilité logicielle dans le navigateur web pourrait être exploitée.

Des contre-mesures peuvent être mises en place contre cette attaque. Tout d'abord, des mesures visant à réduire les couplages ou à filtrer les signaux pourraient être envisagées, ce qui aurait pour effet d'augmenter le niveau de l'attaquant nécessaire à la réalisation de l'attaque, en termes de capacités de la source notamment. Des mesures relatives au contrôle d'accès de l'assistant vocal ont déjà été déployées, comme la biométrie vocale ou l'interactivité. La biométrie vocale fournit l'identification de l'utilisateur légitime à partir des caractéristiques de sa voix. Elle n'est réalisée que sur le mot clé, ce qui oblige l'attaquant à se procurer des échantillons de voix de la victime pour attaquer. De l'interactivité pourrait être introduite, demandant à l'utilisateur de répéter une séquence de chiffres aléatoire pour réaliser certaines actions sensibles. Il pourrait également être pertinent de fournir à

l'utilisateur des moyens de configurer plus finement ses besoins en sécurité, les fonctionnalités qu'il souhaite exposer à l'interface vocale.

B.6 Contournement d'air gap par IEMI

Dans cette section, la susceptibilité EM d'un capteur de température dans un ordinateur de bureau est exploitée afin de permettre l'établissement d'un canal de communication caché avec un implant logiciel. Ce scénario d'exploitation est particulièrement pertinent lorsque l'on considère que l'ordinateur cible est isolé par un *air gap*.

Les systèmes d'information (SI) protégés par un *air gap* sont assez communément répandus dans des contextes ou de l'information sensible est manipulée. Cette mesure de protection consiste en une isolation complète d'un SI sensible en allouant des ressources matérielles et logicielles dédiées exclusivement à ce SI et en supprimant toute interface de communication avec d'autres SI. La mise en place de cette mesure de sécurité est illustrée Figure 5.1, l'utilisateur ne peut plus avoir accès à la fois au SI sensible et à un SI connecté à internet à partir de ressources matérielles et logicielles partagées. Cela supprime le risque de compromission du SIsystème d'information sensible depuis internet.

L'*air gap* est une mesure très coûteuse et extrêmement contraignante pour l'utilisateur qui doit interagir avec plusieurs SI et parfois effectuer des échanges de données entre ces SI. Cependant, cette mesure de sécurité peut être contournée, par exemple par la mise en place d'un canal de communication caché.

Un canal de communication caché est un moyen permettant à deux entités qui ne sont pas supposées communiquer via une interface qui n'est pas supposée servir à l'établissement d'une communication [Lam73]. Un canal de communication caché échappe ainsi par construction à toute supervision.

Un prérequis important pour la mise en place d'un canal de communication caché entre deux entités est la nécessité pour chaque entité de connaître le canal et les modalités de transmission. Cela implique donc que l'émetteur et le récepteur doivent être compromis ou sous le contrôle de l'attaquant.

Dans notre étude, le scénario opérationnel implique un ordinateur de bureau isolé par un *air gap* sur lequel un implant logiciel malveillant a été introduit. L'attaquant va exploiter les effets des IEMI sur le capteur de température du microprocesseur pour envoyer de l'information à l'implant logiciel.

L'approche systémique a été utilisée afin d'identifier les effets d'une IEMI sur le capteur de température du microprocesseur de la cible. Pour cela, un code de test relevant les valeurs de la température du microprocesseur le plus fréquemment possible a été implanté dans la cible pour la phase de

caractérisation.

Ce capteur de température analogique module une tension sur une piste qui est numérisée par un composant électronique. Ce composant communique la valeur de la température au microprocesseur par un protocole de communication numérique.

Comme précédemment, l'attaquant va tirer profit de comportements non linéaires des étages de numérisation pour faire une attaque par injection de signal hors bande sur la température. Le signal agresseur est composé d'une porteuse, dont la fréquence sera déterminée empiriquement pendant la phase de caractérisation, modulée par le signal à injecter. Il a été noté, lors de la caractérisation, que l'attaquant parvient à introduire un écart entre la température réelle et la température "fautée" qui évolue linéairement par rapport à la densité de puissance du signal agresseur (Figure 5.6). Un canal de communication caché par modulation d'amplitude est donc possible.

Plusieurs stratégies de transmission ont été explorées, menant à des canaux de communication ayant un taux de transmission de 10 bits par seconde. Afin d'établir une borne supérieure théorique du taux de transmission, une approche pour calculer la capacité du canal de communication a été proposée, basée sur la formule de Shannon [Sha48]:

- Le canal a été considéré sans bruit et discret
- La fréquence d'échantillonnage maximale par l'implant logicielle a été déterminée de manière empirique
- Le nombre de symboles maximal a été déduit des capacités du convertisseur analogique-numérique

Avec cette approche, une capacité de canal de 40 bits par seconde a été déterminée, ce qui signifie qu'un attaquant, quels que soient ses moyens, ne pourra pas dépasser ce taux de transmission. Cette information est déterminante pour des analyses de risques.

Plusieurs contre-mesures peuvent être envisagées. Tout d'abord, toute mesure visant à prévenir la diffusion d'un implant logiciel sur une machine isolée contribuera à réduire dramatiquement la surface d'attaque. En effet, pour la mise en place d'un canal caché, la présence d'un implant est indispensable.

La suppression physique des interfaces de communication radio des machines du SI déconnecté est également indispensable pour éviter une réactivation opportuniste ou un détournement d'usage de ces interfaces par l'implant logiciel.

Pour limiter la capacité du canal de communication, il peut être judicieux de limiter la fréquence d'échantillonnage et la dynamique du convertisseur analogique-numérique au strict minimum requis.

Ajouter des procédures recherchant des routines de transmission dans les sondes inspectant les programmes installés ou les binaires transitant sur des réseaux supervisés pourrait également permettre de détecter des implants logiciels cherchant à mettre en place des canaux de communication cachés.

B.7 Watermarking électromagnétique

Dans cette section, un nouveau modèle de menace est exploré: le *watermarking électromagnétique*.

Le watermarking électromagnétique (WEM) peut être défini comme l'exploitation d'effets des IEMI ayant un impact persistant sur la cible pour introduire (stocker) un élément d'information (le *watermark*) dans un système électronique non coopératif. Ce *watermark* peut alors être identifié ou extrait *a posteriori* pour répondre à un besoin opérationnel. L'enjeu ici est donc d'identifier des impacts d'effets des IEMI bénéficiant d'un mécanisme de persistance intrinsèque à la cible qui permette de laisser une trace de l'effet sur la cible. Ce mécanisme de persistance, qui n'est pas sous le contrôle de l'attaquant, va naturellement dimensionner la performance du WEM ainsi que les mécanismes d'identification et d'extraction du *watermark*.

Le WEM peut être modélisé comme étant la conjugaison d'un canal de communication caché par IEMI et d'un canal de stockage. Le canal de WEM est le canal de stockage distant par IEMI résultant de la conjugaison des canaux de communication et de stockage. La capacité de canal de WEM est une métrique mesurant la performance du canal de WEM par la quantification du volume maximal de données pouvant être stockées par WEM. En reprenant le modèle proposé, cette capacité de canal WEM peut être formalisée comme suit: Si C_{covert} est la capacité du canal de communication caché et $C_{storage}$ est le taux de stockage du mécanisme de persistance, la capacité du canal de WEM C_{WEM} est:

$$C_{WEM} = min\left(C_{covert}, C_{storage}\right)$$

La quantité maximale d'information S_{WEM} pouvant être stockée par WEM pendant une durée d'exposition t, en considérant un volume de stockage maximal par le mécanisme de persistance $S_{storage}$, s'écrit alors:

$$S_{WEM}(t) = min\left(C_{WEM} \cdot t, S_{storage}\right)$$

La procédure pour l'identification et l'exploitation de canaux de WEM est la suivante:

1. Caractérisation de la cible pour énumérer les effets des IEMI

2. Sélection d'effets reproductibles et transitoires, bénéficiant d'un mécanisme de persistance

3. Estimation de la capacité du canal de WEM pour chacun des effets retenus

4. Conception d'une méthode d'identification et/ou d'extraction du *watermark*

5. Définition des éléments liés au contexte opérationnel: taille et contenu du *watermark*

Afin d'illustrer cette démarche, le WEM a été mis en œuvre sur un drone civil pour fournir une capacité de *forensics tracking* dans un cadre de LAD. La prolifération des drones, leur facilité d'accès par le grand public et l'augmentation de leurs capacités entraine de nouveaux risques relatifs à la sécurité physique des infrastructures critiques et des personnes. Dans une démarche de protection, différentes solutions sont proposées pour la détection, l'identification, la neutralisation de drones. Cependant, ces solutions ont des limites conséquentes, en particulier les risques de chute lors de la neutralisation. Des effecteurs à énergie dirigée EM font partie de l'arsenal technique pouvant contribuer à la neutralisation. L'utilisation du WEM pour fournir une capacité de *forensics tracking* permettrait d'envisager l'insertion d'un marqueur dans un drone agresseur durant un incident par IEMI. De cette manière, en cas d'investigation numérique sur ce drone, la présence du marqueur pourrait attester de sa présence sur les lieux au moment de l'incident, à portée de l'effecteur EM.

Pour l'étape de caractérisation, l'approche systémique a été mise œuvre. Une instrumentation logicielle de la cible, et plus précisément la prise de contrôle privilégiée du système d'exploitation tournant sur un des composants présents dans le drone, a permis d'accéder en temps réel à des données de télémétrie issues des nombreux capteurs servant à la fonction d'autopilote.

Les drones présentent une particularité qui en fait des cibles particulièrement adaptées au WEM. En effet, des journaux de vol sont alimentés dès la mise sous tension du drone, jusqu'à sa mise hors tension. Dans ces journaux de vol, des données issues ou dérivées des informations en provenance des capteurs sont échantillonnées à des fréquences plus ou moins élevées. Sur la cible de notre étude, la fréquence maximale de journalisation est de 250 Hz, ce qui correspond à une entrée toutes les 4 ms. Les journaux de vol peuvent être extraits du drone *a posteriori* par une connexion universal serial bus (USB) ou en accédant à une carte mémoire interne.

A l'issue de la caractérisation, plusieurs effets ont été identifiés, dont certains présentant des caractéristiques reproductibles et transitoires. Après extraction et inspection des journaux de vol, les effets bénéficiant de ce mécanisme de persistance ont été identifiés. Pour montrer la faisabilité de la démarche expérimentale, deux canaux de WEM ont été mis en œuvre.

Un premier canal de WEM exploitant des effets sur la température de la batterie a été caractérisé.

La capacité du canal de communication WEM a été estimée à 5 bits par seconde. Un second canal de WEM a été démontré, exploitant des effets simultanés sur les capteurs fournissant l'accélération verticale, le roulis et le tangage, pour une capacité de canal estimée à 15 bits par seconde.

B.8 Conclusion et perspectives

Le travail défendu dans cette thèse de doctorat s'est focalisé sur les effets des IEMI sur des équipements électroniques et leur impact sur la sécurité de l'information traitée. Plus précisément, la transposition d'approches utilisées en injection de faute EM pour la caractérisation de la susceptibilité face à des IEMI a permis d'élaborer une méthodologie d'analyse des effets sur l'information, sous l'angle de la cybersécurité, facilitant les analyses d'exploitabilité et la conception de méthodes de détection et de mesures de protection. Cette méthodologies a été appliquée à différentes cibles et a permis la réalisation d'attaques originales et la découverte de nouveaux modèles de menace.

Sur un ordiphone, une attaque originale par IEMI permet d'obtenir un accès distant, discret et non autorisé à des assistants vocaux en exploitant la susceptibilité des étages d'entrée audio. Sur un ordinateur de bureau, un nouveau modèle de menace a été exploré, permettant l'établissement d'un canal de communication caché avec des implants logiciels par IEMI. Sur un drone, un nouveau modèle de menace a été proposé, le *watermarking électromagnétique*, qui exploite certains effets spécifiques des IEMI pour introduire de l'information dans des cibles distantes et non coopératives. Une application pratique de *watermarking électromagnétique* a été démontrée pour fournir une capacité de *forensic tracking* de drones dans un contexte de lutte anti-drones.

La Figure C.1 met en perspective les contributions de la thèse dans le panorama des menaces en sécurité électromagnétique.

Ce travail de thèse a ouvert plusieurs perspectives intéressantes en CEM et en sécurité électromagnétique. Tout d'abord, la comparaison des domaines de l'injection de faute EM et des IEMI met en évidence un champ de scénarios expérimentaux et de modèles de menace peux explorés. Entre l'injection de faute EM, où l'attaquant émet en champ proche des signaux impulsionnels et profite de sa proximité avec le composant cible pour se synchroniser finement, et l'IEMI qui est envisagée à forte puissance et à plus distance avec une grande variété de signaux agresseurs, il peut être pertinent d'envisager des scénarios de menace impliquant un attaquant proche du système cible ayant recours à des IEMI de puissance modérée pour obtenir de l'injection de faute EM.

La méthode systémique peut évoluer vers une approche plus générique et systématique des tests de susceptibilité CEM. Des codes de test, ou un ensemble de codes de test évaluant des modèles de

faute correspondant à un profil ou une famille de systèmes cibles pourraient être envisagés. Ainsi, les évaluations de systèmes complexes génériques, comme des ordinateurs ou des systèmes embarqués, pourraient être comparables.

Cette méthode systémique ouvre également des perspectives en cybersécurité et investigation numérique. La mise en œuvre d'agents logiciels de supervision pour réaliser de la détection, à l'échelle d'une machine ou d'un parc informatique pourrait être explorée. Ces systèmes de détection pourraient être couplés à des systèmes de détection d'IEMI externes.

L'estimation des capacités de canal, que ce soit dans le cas de canaux cachés par IEMI ou de canaux de WEM, pourrait être formalisée de manière à intégrer les capacités de l'attaquant et la configuration opérationnelle (distance, effets de la propagation, des couplages...). Cela permettrait une estimation plus précise dans les cas où la détermination d'un majorant ne serait pas suffisante.

B.9 Références

[Ame15] Mohamed Amellal. *Electromagnetic Immunity Modeling of Components for the Obsolescence Management of Systems and Electronic Modules*. PhD thesis, INSA de Rennes, 2015. XVII

[And20] Ross J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley Publishing, 2 edition, 2020. X

[ANS10] ANSSI. EBIOS: Expression des Besoins et Identification des Objectifs de Sécurité - méthode de gestion des risques. Standard, Agence Nationale de la Sécurité des Systèmes d'Information, Paris, France, 2010. X

[ANS20] ANSSI. Criteria for evaluation in view of a first level security certification. Standard ANSSI-CSPN-CER-P-02_v4.0, ANSSI, 2020. XI

[ASP+14] Christian Adami, Michael Suhrke, Thorsten Pusch, Michael Joester, Nikita Kolosnev, Georg Neubauer, and Alexander Preinerstorfer. Investigation of the impact of various IEMI sources to electronic passport readers. In *Future Security 2014*, pages 430–436, Berlin, Germany, 2014. XV

[Cri17a] Common Criteria. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model. Standard Version 3.1 Revision 5, 2017. XI

[Cri17b] Common Criteria. Common Methodology for Information Technology Security Evaluation - Evaluation methodology. Standard Version 3.1 Revision 5, 2017. X, XI

[DDR+12] A. Dehbaoui, J. M. Dutertre, B. Robisson, P. Orsatelli, P. Maurine, and A. Tria. Injection of transient faults using electromagnetic pulses -Practical results on a cryptographic system-. Technical Report 123, 2012. XVI

[DFK+14] J F Dawson, I D Flintoft, P Kortoci, L Dawson, A C Marvin, M P Robinson, Mirjana Stojilovic, Marcos Rubinstein, Benjamin Menssen, Heyno Garbe, Werner Hirschi, and Loubna Rouiller. A Cost-Efficient System for Detecting an Intentional Electromagnetic Interference (IEMI) attack. In *2014 International Symposium on Electromagnetic Compatibility*, pages 1252–1256, 2014. XVI

[DMGM22] Gökçen Yılmaz Dayanıklı, Abdullah Zubair Mohammed, Ryan Gerdes, and Mani Mina. Wireless Manipulation of Serial Communication. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '22, pages 222–236, New York, NY, USA, 2022. Association for Computing Machinery. XVI

[DSM+22] Gökçen Yılmaz Dayanıklı, Sourav Sinha, Devaprakash Muniraj, Ryan M. Gerdes, Mazen Farhood, and Mani Mina. Physical-Layer attacks against pulse width Modulation-Controlled actuators. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 953–970, Boston, MA, 2022. USENIX Association. XVI

[Dub11] Tristan Dubois. Etude de formes d'onde d'agressions électromagnétiques hyperfréquences sur la vulnérabilité de circuits électroniques. Post Doctoral, 2011. XVI

[ERM16] David El-Baze, Jean-Baptiste Rigaud, and Philippe Maurine. An Embedded Digital Sensor against EM and BB Fault Injection. In *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 78–86, 2016. XVIII

[EWHR22] Eric Easton, Cyril Wafo, Richard Hoad, and Tim Rees. Real-time Substation Shielding Compromise and HPEM Event detection. In *GLOBALEM 2022*, page 3, Abu Dhabi, UAE, 2022. XVI

[GHS20] Dave Giri, Richard Hoad, and Franck Sabath. *High-Power Electromagnetic Effects on Electronic Systems*. Artech House, 2020. XIV, XV

[GP22] Ben Gardiner and Chris Poore. Talking PLC4TRUCKS Remotely with an SDR. In *DefCon 30*, Las Vegas, USA, 2022. XVI

[HRP+22] Richard Hoad, Tim Rees, Barney Petit, Anatoly Krasavin, Grant Hainsworth, and Sam Hole. Real-time Substation Shielding Compromise and HPEM Event detection. In *GLOBALEM 2022*, page 19, Abu Dhabi, UAE, 2022. XVI

[Int78] Integrated Circuit Electromagnetic Susceptibility Handbook. Technical Report MDC-E1929, McDonnell Douglas Astronautics Company, 1978. XV

[ISO92] ISO/IEC. Electromagnetic compatibility (EMC) - Part 1-1: General - Application and interpretation of fundamental definitions and terms. Standard ISO/IEC 61000-1-1:1992, International Organization for Standardization, Geneva, CH, 1992. XI

[ISO18] ISO/IEC. Information technology — Security techniques — Information security management systems. Standard ISO/IEC 27000:2018, International Organization for Standardization, 2018. X

[ISO20] ISO/IEC. Electromagnetic compatibility (EMC) - Part 4-36: Testing and measurement techniques – IEMI immunity test methods for equipment and systems. Standard ISO/IEC 61000-4-36:2020, International Organization for Standardization, Geneva, CH, 2020. XIV, XV

[JJW+22] Y. Jiang, X. Ji, K. Wang, C. Yan, R. Mitev, A. Sadeghi, and W. Xu. WIGHT: Wired ghost touch attack on capacitive touchscreens. In *2022 IEEE Symposium on Security and Privacy (SP) (SP)*, pages 1537–1537, Los Alamitos, CA, USA, 2022. IEEE Computer Society. XVI

[Joh20] G. Johansen. *Digital Forensics and Incident Response: Incident Response Techniques and Procedures to Respond to Modern Cyber Threats, 2nd Edition*. Packt Publishing, 2020. XI

[KBC+13] Denis Foo Kune, John Backes, Shane S. Clark, Daniel Kramer, Matthew Reynolds, Kevin Fu, Yongdae Kim, and Wenyuan Xu. Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors. In *2013 IEEE Symposium on Security and Privacy*, pages 145–159, 2013. XVI, XX

[KBM22] Sebastian Köhler, Richard Baker, and Ivan Martinovic. Signal Injection Attacks against CCD Image Sensors. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '22, pages 294–308, New York, NY, USA, 2022. Association for Computing Machinery. XVI

[Lam73] Butler W. Lampson. A note on the confinement problem. *Communications of the ACM*, 16(10):613–615, 1973. XXII

[MAB+18] M. Madau, M. Agoyan, J. Balasch, M. Grujić, P. Haddad, P. Maurine, V. Rožić, D. Singelée, B. Yang, and I. Verbauwhede. The Impact of Pulsed Electromagnetic Fault Injection on True Random Number Generators. In *2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 43–48, 2018. XVII

[Mad19] Maxime Madau. *A Methodology to Localise EMFI Areas on Microcontrollers*. These de doctorat, Montpellier, 2019. XVIII

[Mej19] Guillaume Mejecaze. *Analyse des destructions d'alimentations électroniques soumises à un courant impulsionnel fort niveau*. PhD thesis, Université de Bordeaux, 2019. XV

[MP16] Nicolas Mora Parra. *Contribution to the Study of the Vulnerability of Critical Systems to Intentional Electromagnetic Interference (IEMI)*. PhD thesis, EPFL, Lausanne, 2016. XIV, XV

[MWM19] Seita Maruyama, Satohiro Wakabayashi, and Tatsuya Mori. Tap 'n Ghost: A Compilation of Novel Attack Techniques against Smartphone Touchscreens. In *2019 IEEE Symposium on Security and Privacy (SP) (SP)*, 2019. XVI

[NSFG21] Arash Nateghi, Martin Schaarschmidt, Sven Fisahn, and Heyno Garbe. Susceptibility of Power Line Communication (PLC) Channel to DS, AM and Jamming Intentional Electromagnetic Interferences. In *2021 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)*, pages 1–4, 2021. XVI

[O'F19] Colin O'Flynn. MIN()imum failure: EMFI attacks against USB stacks. In *13th USENIX Workshop on Offensive Technologies (WOOT 19)*, Santa Clara, CA, 2019. USENIX Association. XVII

[Pau06] Clayton R Paul. *Introduction to Electromagnetic Compatibility*, volume 184. John Wiley & Sons, 2006. XI

[PRC17] Pierre Payet, Jérémy Raoult, and Laurent Chusseau. Remote Extinction of a 2.4 GHz RF Front-End Using Millimeter-Wave EMI in the Near-Field. *Progress In Electromagnetics Research Letters*, 68:99–104, 2017. XVI

[PS11] L. Palisek and L. Suchy. High Power Microwave effects on computer networks. In *10th International Symposium on Electromagnetic Compatibility*, pages 18–21, 2011. XV

[Res19] Limited Results. Fatal Fury On ESP32 Time To Release HW Exploits. In *Black Hat Europe 2019*, London, UK, 2019. XVII

[Res20] Limited Results. Debug Resurrection On nRF52 Series. In *Black Hat Europe 2020*, 2020. XVII

[RJL+22] Nicolas Ribière-Tharaud, Jean-Christophe Joly, C Laparro, M Schutz, and B Lenoir. IEMI Detection - Setting up relevant threshold. In *GLOBALEM 2022*, page 65, Abu Dhabi, UAE, 2022. XVI

[SD15] Mark Seaborn and Thomas Dullien. Exploiting the DRAM rowhammer bug to gain kernel privileges. In *Black Hat USA 2015*, volume 15, page 71, Las Vegas, USA, 2015. XVI

[SH07] Jörn-Marc Schmidt and Michael Hutter. Optical and EM fault-attacks on CRT-based RSA: Concrete results. In *Austrochip 2007, 15th Austrian Workhop on Microelectronics, 11 October 2007, Graz, Austria, Proceedings*, pages 61–67. Verlag der Technischen Universität Graz, 2007. XVI

[Sha48] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423, 1948. XXIII

[SN06] Franck Sabath and D Nietsch. Electromagnetic Effects on Systems and Components. In *American Electromagnetics International Symposium AMEREM 2006*, Santa Barbara, CA, USA, 2006. Summa Foundation. XV

[SZZ+22] H. Shan, B. Zhang, Z. Zhan, D. Sullivan, S. Wang, and Y. Jin. Invisible finger: Practical electromagnetic interference attack on touchscreen-based electronic devices. In *2022 IEEE Symposium on Security and Privacy (SP) (SP)*, pages 1548–1548, Los Alamitos, CA, USA, 2022. IEEE Computer Society. XVI

[TM17] N. Timmers and C. Mune. Escalating Privileges in Linux Using Voltage Fault Injection. In *2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 1–8, 2017. XVII

[Tro21] Thomas Trouchkine. *Evaluation de La Sécurité Physique Des SoC*. These de doctorat, Université Grenoble Alpes, 2021. XVI, XVII, XVIII

[TTPH21] Yazhou Tu, Vijay Srinivas Tida, Zhongqi Pan, and Xiali Hei. Transduction Shield: A Low-Complexity Method to Detect and Correct the Effects of EMI Injection Attacks on Sensors. In *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, ASIA CCS '21, pages 901–915, New York, NY, USA, 2021. Association for Computing Machinery. XVI

[Wik21] Wikipedia. Google Now. https://en.wikipedia.org/w/index.php?title=Google_Now&oldid=1057019621, 2021. XX

[WMY+22] Kai Wang, Richard Mitev, Chen Yan, Xiaoyu Ji, Ahmad-Reza Sadeghi, and Wenyuan Xu. GhostTouch: Targeted attacks on touchscreens without physical touch. In *31st USENIX Security Symposium (USENIX Security 22)*, Boston, MA, 2022. USENIX Association. XVI

[YJW+22] Chen Yan, Xiaoyu Ji, Kai Wang, Qinhong Jiang, Zizhi Jin, and Wenyuan Xu. A Survey on Voice Assistant Security: Attacks and Countermeasures. *ACM Computing Surveys*, 2022. XX

[ZDT+14] Loic Zussa, Amine Dehbaoui, Karim Tobich, Jean-Max Dutertre, Philippe Maurine, Ludovic Guillaume-Sage, Jessy Clediere, and Assia Tria. Efficiency of a glitch detector against electromagnetic fault injection. In *Design, Automation and Test in Europe Conference and Exhibition (DATE), 2014*, pages 1–6. IEEE, 2014. XVIII

[ZR20] Youqian Zhang and Kasper Rasmussen. Detection of Electromagnetic Interference Attacks on Sensor Systems. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 203–216, 2020. XVI

Appendix C

List of acronyms

ABS Anti-lock Braking System. 23

ADC analog to digital converter. 35, 41, 47, 79, 110, 111, 117, 121, 138

AES the AES symmetric cryptography primitive. 20, 24, 51, 57, XXXIII

AM amplitude modulation. 18–20, 23, 35, 40–43, 78, 85–88, 91, 94, 111, 120, 134

ANSSI agence nationale de la sécurité des systèmes d'information. 9, 68, 78, 102, 124

ASIC application specific integrated circuit. 52

ASK amplitude shift keying. 115, 116

CC Common Criteria. 9, 10, 107

CEA commissariat à l'énergie atomique et aux énergies alternatives. 45

CEM compatibilité électromagnétique. vi, VIII, IX, XI–XV, XVIII, XXVI

COMP-128 the COMP-128 symmetric cryptography primitive. 20

COTS commercial off the shelf. 1, 33, 108, 109, 124, 131, 148

CPL courant porteur en ligne. XVI

CPU central processing unit. 58, 72, 84, 102, 109–111, 120

CRP Code Readout Protection. 59

CSS chirp spread spectrum modulation. 20

C-UAS counter unmanned aerial systems. v, 2, 4, 124, 130, 145, 148, 151

CW continuous wave. 23, 33, 35, 40–42, 47, 49, 50, 53, 61, 62, 87, 91, 112, 114, 134, 137

DAC digital to analog converter. 48

DC direct current. 47, 48

DES the DES symmetric cryptography primitive. 20, 24, 57

DEW directed energy weapon. 130

DFA differential fault analysis. 57

DFIR digital forensics and incident response. 11, 24, 26

DRAM dynamic random access memory. 50

DSP digital signal processing. 79

DSSS direct sequence spread spectrum modulation. 20

DVI digital visual interface. 16, 17

ECDSA elliptic curve digital signature algorithm. 20

EM electromagnetic. 1–3, 8, 23, 27–31, 33, 34, 36–38, 41–45, 49, 54, 56, 61–63, 69, 73, 78, 94, 98, 102, 103, 106, 109, 111, 120, 121, 124, 126, 129, 131, 138, 140, 141, 146, 147, 150, VII–IX, XI–XIV, XVI, XVIII, XIX, XXII, XXV, XXVI

EMC electromagnetic compatibility. v, 2, 3, 8, 11–15, 18, 24, 25, 28, 29, 31, 36, 62, 68, 69, 71, 75, 78, 95, 96, 98, 102, 121, 124, 131, 146, 147, 149

EMFI electromagnetic fault injection. 2, 3, 23, 24, 28, 46, 49–52, 56–63, 69, 145–147, 149

EMI electromagnetic interference. 28, 29, 33, 42, 62, 74

EMP electromagnetic pulse. 29

EMSEC electromagnetic security. 15

EMW electromagnetic watermarking. 3, 4, 124, 127–130, 134–142, 148, 151

ESD electro-static discharge. 13, 28, 33, 37

FBBI forward body biasing injection. 48

FM frequency modulation. 19, 20, 79, 85

FPGA field programmable gate array. 47, 48, 50, 51, 56, 57, XVI

GPIO general purpose input/output. 23

GPS global positioning system. 132, 133, 140

HDMI high-definition multimedia interface. 17, 107

HEMP high altitude electromagnetic pulse. 14, 28, 33, 149

HF high frequency. 52

HID human interface device. 107

HIRF high intensity radiated field. 33

HPEM high power electromagnetic. 14, 45

I2C inter-integrated circuit communication protocol. 17, 41, XVI

IC intergated circuit. 2, 3, 17, 20–24, 28, 34, 35, 37, 45–54, 56, 60–63, 72, 133, 147, 149

IEC international electrotechnical commission. 29

IEEE Institute of Electrical and Electronics Engineers. XXXIII

IEMI intentional electromagnetic interference. v, vi, 1–4, 14, 25, 27–43, 45, 61–63, 67–69, 71, 73–76, 78, 79, 83, 85, 86, 88, 89, 91, 92, 94, 96–98, 101–122, 124, 126–128, 131, 134, 136, 138, 141, 145–151, VIII, IX, XIII–XVI, XVIII–XXII, XXIV–XXVII

InfoSec information security. 2, 3, 8, 11, 14, 15, 24, 25, 31, 43, 45, 48, 49, 63, 68–71, 75, 78, 98, 102, 107, 117, 119, 124, 146, 147, 149

IO input/output. 46, 47, 51, 52, 58, 61

IoT internet of things. 1, 71, 78, 147

ISP In-System Programming. 59

IT information technology. 10, 35, 39

ITU international telecommunication union. 85

LAD lutte anti-drone. IX, XXV

LED light emitting diode. 108

LNA low noise amplifier. 22, 35, 40

LoRa LoRa modulation. 20

LPC low pin count. 110

LSB least significant bit. 121

MCU microcontroller unit. 51

MOS Metal Oxide Semiconductor. 34

MOSFET Metal Oxide Semiconductor Field Effect Transistor. 39, 47

NASA national aeronautics and space administration. 28

NEMP nuclear electromagnetic pulse. 69

NRZ non return to zero. 139

NSA National Security Agency. 18, 107

OCD On-Chip Debugging. 59

OFDM orthogonal frequency division multiplexing modulation. 20

OIRT international radio and television organisation. 85

OOB out-of-band. 23

OOK on-off keying. 106, 114, 115, 139

OS operating system. 84

PA power amplifier. 40

PCB printed circuit board. 21–23, 35, 38, 44, 47, 48, 52, 61, 97, 133

PDU protocol data unit. 104

PLC power line communication. 41

PLL phase locked loop. 35, 40

PM phase modulation. 20

PSK phase shift keying. 106

PWM pulse width modulation. 23, 39, 43, XVI

QPSK quadrature phase shift keying. 40

RF radio frequency. 14, 20, 22, 23, 30, 40, 41, 45, 47, 48, 52, 63, 72, 89, 106, 109, 119, 120, 130–132

RFID radio frequency identification. 40

RSA the RSA asymmetric cryptography primitive. 20, 24, 57

RSSI received signal strength indicator. 132, 137

SCA side channel attack. 20

SDR software defined radio. 17

SI système d'information. XXII, XXIII

SNR signal to noise ratio. 40, 140

SoC System on chip. 24, 41, 43, 48, 50, 51, 58, 59, 71, 132

SPI Serial Peripheral Interface. 41, 48

TRNG True Random Number Generator. 24, 48, 57, 58

UART universal asynchronous receiver transmitter. 41, 52, XVI

UAV unmanned aerial vehicle. 35, 43, 123, 124, 130, 131, 133, 134, 136, 137, 140–142, 148, 151

UHF ultra high frequency band: radio signals between 300 MHz and 3 GHz. 16

URSI international union of radio science. 29

USB universal serial bus. 24, 40, 42, 50, 72–74, 83, 88, 92, 93, 95, 96, 98, 107, 136, XXV

VCI voice command interface. 84

VGA video graphics array. 16, 111

WEM watermarking électromagnétique. XXIV, XXV, XXVII

WLCSP wafer level chip-scale packaging. 48

Appendix D

Glossary

firmware firmware is a specific class of computer software that provides the low-level control for a device's specific hardware. 19

KVM switch a device allowing to share a Keyboard, a Video display and a Mouse between several host computers. 107

MILENAGE a cryptosystem based en AES and used for authentication of user equipment in 3G mobile networks. 20

PS/2 The PS/2 protocol is a bidirectional synchronous serial channel dedicated to keyboards and mice.. 72, 73

TETRA a wireless communication protocol family used for mission-critical communications such as in public safety, military, law enforcement and operating between 100 MHz and 900 MHz. 40

Wi-Fi Wireless Fidelity, a wireless communication protocol family standardized as Institute of Electrical and Electronics Engineers (IEEE) 802.11 for wireless local area networks. 39, 131, 132, 134, 136, 137, XX