Whispering devices: A survey on how side-channels lead to compromised information

Corentin Lavaud, Robin Gerzaguet, Matthieu Gautier, Olivier Berder, Erwan Nogues, Stephane Molton

Whispering devices: A survey on how side-channels lead to compromised information

Corentin Lavaud, Robin Gerzaguet, Matthieu Gautier, Olivier Berder, Erwan Nogues, Stephane Molton

***Abstract*—While operating, information processing devices or communication systems may emit unwanted signals (or alter existing ones) through electromagnetic waves, light, sound or power drain. These side-channels can be intercepted by anyone with scientific or technical knowledge and appropriate equipment, leading to a potentially high risk of security breaches. This survey focuses on these emanation side-channels and provides an extensive literature review. To provide an in-depth analysis despite the variety of attacks, we propose to classify the side-channels based on their criticality, their intentionality, the type of attackers, and the physical medium. Illustrative use-cases are presented and serve as a basis to infer individual threats. Particular attention is paid to electromagnetic side-channels which exhibit the highest criticality and have therefore been used in the most recent attacks. The main characteristics of the side-channels revealed by state-of-the-art papers are summarized and recommendations on countermeasures are provided to protect any sensitive equipment.**

***Index Terms*—Side-channel attacks, electromagnetic emanation, Security and Protection, eavesdropping, TEMPEST, Hardware/Software Protection, Support for security**

I. Introduction

In recent decades, organizations, firms, states and administrations have sought to become more efficient and productive by adopting computer technologies, thus engaging in the process of *digital transformation*. This new era of digital services and globalization has made the movement of goods, services, finance and information easier, and large companies can manage their international operations in a leaner, more efficient way.

However, such large-scale deployment of digital technologies has paved the way to new types of threats. Confidential data may be carried within the same system as ordinary content, blurring the boundary between the sensitive and non-sensitive area and leading to potentially numerous malicious security breaches. With such a wide variety of attacks, many organizations are struggling to identify how to counter the threats they face. Companies tend to focus on protecting data based on their confidentiality (limited access to information), integrity (the equipment used is reliable and accurate) and finally availability (information only accessed by authorized people). To that end, several defense mechanisms have been proposed such as: limited use of control access and systems, security watchdog at every network access point, prevention methods to enhance security and confidentiality through training (awareness campaigns and good practice workshops [1] [2]) and widespread use of cryptography. Although most of these countermeasures relate to software, if the physical layer is not secured, all the upper layers are exposed to major security flaws. Side-channel attacks rely on this hardware vulnerability.

A side-channel denotes the presence of information in an illegitimate channel, whether at hardware or software levels. Side-channel attacks seek these deviations in the implementation of a task (how the task is done) rather than the implemented algorithm weaknesses themselves (what the task does). Several types of side-channels exist and they can be classified into two main categories depending on the nature of the leakage. A *software side-channel* is contained within a device and is based on hardware weaknesses (e.g. RowHammer [3]) or firmware weaknesses (e.g. Meltdown [4], Spectre [5]). On the other hand, as an *emanation side-channel* crosses the device boundary, its exploitation needs specific acquisition equipment according to the nature of the leakage. It is the result of one or more physical phenomena that deviate information from its proper path to reach an unintended one. Recently, some attacks blur the boundaries between software and emanation side-channels such as Plapytus [6] that uses a power line side-channel (i.e. an emanation side-channel) directly at the software level (instead of relaying to external power analysis component).

The present paper focuses on emanation side-channels. Most of existing surveys on information security focus on cryptography [7], or specifically electromagnetic (EM) side-channel [8]. Others are directly focusing on application-use cases covering the scope of covert channels [9] or out-of-band signal injections [10]. This is the core difference with our survey that puts the EM side-channel in perspective with other side-channels. The goal is to address the leak of information from the side-channel outlook to better classify the attacks, the associated risks, and to point out the countermeasures.

This paper addresses information system confidentiality in the event of emanation attacks and presents an in-depth analysis of state-of-the-art emanation side-channels. To that end, emanation side-channels are divided into three distinct classes. These classes, from the attacker profile to the physical side-channel, will serve as a baseline comparison (See Table III on the appendix) and provide an effective means of highlighting the characteristics of side-channel attacks and associated countermeasures. More specifically, EM attacks are

C. Lavaud, R. Gerzaguet, M. Gautier, O. Berder are with Univ Rennes, CNRS, IRISA(email: firstname.name@irisa.fr).

E. Nogues and S. Molton are with DGA-MI (email: firstname.name@intradef.gouv.fr).

0000–0000/00$00.00

the main focus, since this side-channel tends to be more dangerous than the others.

Paper organization: The paper is structured as follows. Sections II exposes the key concepts related to emanation side-channels and data criticality. Section III introduces the proposed classification of emanation side-channels used subsequently in the paper. Section IV deals with non-electromagnetic side-channels (acoustic, light and power consumption) and outlines their threats and limitations. Section V focuses on electromagnetic side-channels and presents state-of-the-art emanation types and their level of risk. Section VI addresses various ways to secure a system against these attacks. Finally, Section VII draws a number of conclusions and presents various challenges.

II. When emanation side channel meets critical data

A. What is an emanation side channel ?

Emanation side-channels include fortuitous emanations caused by the normal functioning of a device as well as the alteration and amplification of an internal signal to produce an emanation. A common feature of these side-channels is their non-intrusive nature, as a direct contact with the target is not needed to get the side-channel. This is in opposition to software side-channel which requires to be inside the target (mostly in the form of a software program). The typical case of a side-channel attack is shown in Fig. 1. In the normal flow, sensitive data is processed and sent to an intended receiver via a legacy channel. However, either the processing system or the legacy channel leaks to another medium i.e. the side-channel. A person gathering this leaked data can recover sensitive information. This person may either be an active attacker if he launches the attack (emits a signal toward the system to generate the side-channel emanation) or an eavesdropper if he only passively intercepts the information. Despite awareness of the potential risks posed by such emanations since the early days of ElectroMagnetic Compatibility (EMC) in the mid-20^{th} century, proof of their actual use has only recently been provided with disclosure of certain tools from the National Security Agency (NSA) [11].

Emanation side-channel attacks may also entail using a leakage as a fully controllable communication medium. Many attacks rely on physical or remote access to a vulnerable target. One straightforward way to counterbalance such attacks is to work within isolated systems (also referred to as air-gapped systems). Isolated systems (or networks) do not allow external access and thus maintain the sensitive data in a closed area. This is true of systems which are not connected to the Internet or those that have no external gateway access. The real threat comes from air-gap bridging which involves creating a communication medium over a protected network [12].

B. On data criticality

Essentially, all data may be considered private or confidential and therefore should not be recovered by an opponent. Some information can nevertheless be defined as less critical than others. Low criticality may be ascribed either due to the nature of the information, or because the information is supposed to be safe (e.g. using encryption). The latter is true of so-called *black data*. In NACSIM report [13], the NSA provided the first definition of TEMPEST (see Section V) and introduced the concept of red and black signals.

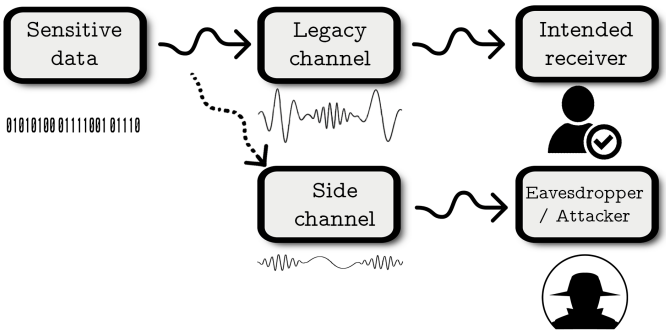


Fig. 1: Overview of emanation side-channel attack.

A *red signal* is an unencrypted signal that must be treated as highly sensitive material. In the NSA specification, this type of signal must be contained within a specific perimeter to ensure security. To that end, security measures [14] have to be taken into account such as shielding the location or ensuring a minimum physical distance between wires (to avoid coupling).

A *black signal* is considered to be a safe signal, i.e. it does not directly carry a compromising signal, using encryption or other methods to render interception impossible. Unlike red signals, black signals are not defined by their secure perimeter.

It should be noted that breaking cryptography does not form part of the work carried out in the present survey. We do acknowledge the importance of this issue and many research activities are currently underway. However, these issues are generally already covered in dedicated surveys (e.g., [15] [16]). Hence in this paper, cryptography systems will be addressed from a side-channel attack perspective (i.e. recovery of a secret key used during ciphering due to side-channel leakage). Generally speaking, all the compromising signals studied in this paper will fall into the red family i.e. unencrypted signals.

C. The emergence of new attacks

The development of new attacks is linked to the development of the targets and occurred in several phases. Analog signals were firstly used to communicate, before the transition to the digital world. This changed the paradigm of the emissions, shifting from low frequency and high amplitude to high frequency and low amplitude (due to the increase in clock frequencies and the overall reduction of operating voltages). Then mobile devices appeared and with them so-called System on Chips (SoC) allowing a size reduction, which obviously brings an additional risk of internal mixing.

Moreover, the worldwide competition led to overall reduction of equipment costs, sacrificing some filtering tasks and shielding that were preventing leaks proliferation. But attacks are also benefiting from the improvement of the hardware devices involved in the interception. These new devices reach

higher bandwidths, are more robust against noise and their increased computation capabilities allow efficient but energy demanding techniques such as emerging machine learning. Finally, privacy is nowadays of prime importance for citizens, and thorough studies and research were conducted on this topic. For all of these reasons, albeit taking root in the very beginning of the electronics area, side-channel attacks have gained an important attractiveness in the past few years.

III. Compromising emanation classification

Compromising emanations can occur from different propagation mediums and may be used by different kinds of attackers. In order to compare the various characteristics of the leakage channels, it is necessary to extract common description keys. To that end, we propose a classification based on three distinct criteria. First, different attacker profiles will be defined based on their resources. Then, classes of attacks will be defined. Finally, classes of side-channel emanations will be introduced. The reader can refer to Table III where all the presented paper are discriminated based on the aforementioned classes.

A. Attacker profiles

All attackers of a system share the common goal of recovering confidential data. However, they may have different profiles and can be distinguished based on their resources (e.g. the hardware they use, the time they spend, etc.), their knowledge (i.e. their scientific and technical background and skills) and their manpower. In this paper, we propose to define three attacker classes to better stress the specificities: researcher, hacker and black hat.

Researcher is defined as someone with a strong scientific background who can use high-end equipment to find novel approaches or improve existing ones. Researchers do not pursue attacks outside their professional area, focusing solely on producing proofs of concept for their work in a controlled environment (i.e. all targets are aware of the attack).

Hacker pursues the same objectives as a researcher, i.e. exposing attacks and making them public knowledge. The differences between a researcher and hacker lie in their resources and technical background. Hackers cannot access high-end equipment and their scientific background is limited to specific topics. However, they are highly motivated and thus spend a lot of time on conducting their attacks. Unlike researchers, hackers demonstrate the effectiveness of their attacks by using them in real-life situations without always asking people consent, although not for malicious purposes (i.e. any confidential data recovered is not be kept or used).

Black hat is a person whose purpose is to use a real attack in a practical way for malicious purposes. To that end, such individuals have access to sufficient hardware and manpower to mount functional attacks (i.e. real attacks and not just proofs of concept). Black hat behavior is a true reflection of genuine security threats due to these individuals malicious intentions. However, since this type of attack is completely illegal, no public publishing activities are possible from them. Nevertheless, some hijacked publications exist, such as the Snowden leaks which disclose the NSA catalog of spying tools [11].

B. Class of attacks

Attacks can be classified based on the activeness of the attackers (active or passive) and based on if the target intentionally or accidentally generates the leak (intentional or non-intentional).

Active vs. passive: An active attack emits a carrier signal from a common active system towards/within the target in order to either tamper with the device proper functioning (e.g. fault-induction attacks aim to induce errors in computation to exploit unconventional target behavior) or cause the target to leak a signal (e.g. emitting a radio wave passing through a target to modulate a red signal). In contrast, passive eavesdropping is simply used to observe the device behavior without disturbing it.

Intentional vs. non-intentional: Non-intentional leakages can be naturally present and therefore carry a red signal resulting from normal functioning. But leakages can be intentionally emitted by a target on a side-channel, which implies that the attacker can access the target to force the leakage. This is the definition of what a covert channel is and such channels are widely used in air-gap bridging scenario as it is the only way to exfiltrate data.

C. Class of side-channel

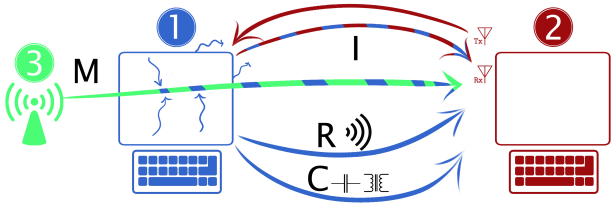
Fig. 2 summarizes the different physical propagation side-channels in which a compromising emanation may occur. These side-channels may either be non-electromagnetic or electromagnetic (using radio-frequency waves).

Electromagnetic side-channel is directly derived from an electronic component. This type of side-channel offers useful propagation characteristics and is currently widely used as a means of communication. Electromagnetic leakages share a common side-channel but are distinguishable by their different origins. As shown in Fig. 2a, these origins can be classified as illumination (I), mixing (M), radiation (R) and coupling (C).
For illumination, the attacker sends a radio beam towards the target. This radio beam enforces a leak of information by acting as the side-channel carrier, therefore the attacker needs to monitor the beam that comes back and contains the information. In the mixing case, the radio beam comes from a legitimate source and not from an attacker.

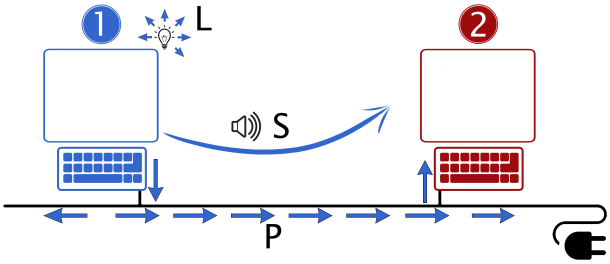
Radiation, probably the most common case of EM side-channel, is due to the generation of a current-induced electromagnetic field. This EM field comes from the different electronic parts, and is directly correlated with the information passing through the device.

Coupling is similar to radiation but propagates in a nearby conductor (metallic housing, power line, water pipe, etc.) and not in the air.

Fig. 2b highlights three main non-electromagnetic side-channels: power line (P), sound (S) and light (L) (light is not referred to as an electromagnetic side-channel in the literature [17]).



(a) Electromagnetic side-channel origins: illumination (I), leak by mixing (M), leak by radiation (R), leak by coupling (C).



(b) Non-electromagnetic side-channels: sound leak (S), leak by the power line (P), light leak (L).

Fig. 2: Typical side-channels for an emanation scenario composed of a sensitive target ❶, an attacker ❷ and a neutral access point ❸.

Power line includes electrical consumption of all the parts of a system. In a processor, the instantaneous energy consumption depends on the data being processed and the operation performed. Clearly, an element with high power consumption will generate a higher trace on the overall consumption. It should be noted that the power line side-channel relates only to electrical consumption and not other leaks such as cross-talk phenomena on power lines (which falls into the electromagnetic class detailed in Section V).

Information processing devices may also emit other types of emanation such as sound, which may be generated by mechanical components (motors, buttons, etc.) or directly by the electronics (capacitor, coil whine, etc.). In precisely the same way as radiation (R), the generated sounds are strongly correlated with the voltage that generates them and therefore with information.

The final reviewed leakage uses light as its side-channel. This leakage has a significant advantage that is also its major drawback: human eyes are sensitive to some of the light spectrum, which increases the risk of detection. On the other hand, many systems include light sources as an interface (screen, state diode, etc.) that can be maliciously used to extract information.

An overview of the proposed classification and the associated paper is shown in Fig 3. A distinction between the targets of each attack is made in the following section and is also visible in the figure. All the cases associated to the EM side-channel have also been depicted in Fig. 5. The next two sections will present each side-channel in greater detail, considering both what information can be reconstructed for each type of emanation and the resources needed for their application.

IV. Analysis of non-electromagnetic side-channels

The previous section highlighted the main characteristics of side-channel emanations. We pointed out that the main disrupting element lies in the medium used. Indeed, the goal is invariably to recover red data: data originating or ending on the user side (screen, speaker, keyboard, etc.), data bus information, or the cryptography key, etc. But even if the methods used to recover data may be independent from the medium, they mostly exploit the medium specificities to improve their performance. Consequently, albeit targeting the same red signal, the medium used will have a significant influence on the ability to retrieve information and therefore on the level of the threat.

This section focuses on the main non-electromagnetic channels: power line, sound, and light. After a brief introduction covering their specific characteristics, countermeasures will be presented and their threat index will be evaluated. This will serve as a baseline for comparison with EM side-channels later on. A brief description of each side-channel can be found in III-C.

A. Non-electromagnetic side-channels

1) Power line: Du et al. [18], have demonstrated that it is possible to recover the keyboard data bus by studying its fingerprint on a power line. The measured consumption is a combination of keyboard consumption and consumption of other components.

Riccardo et al. [19] introduced a way to exfiltrate data via a Universal Serial Bus (USB) cable without the use of the embedded data link. Instead, the power supply provided by the USB cable is used. By creating bursts of current, an On-Off-Keying modulation was achieved, allowing a 2 bit/s link using a smartphone and a tampered phone charger.

Using the same approach, other operations performed on the processor may be retrieved, such as cryptographic operations [49]. By eavesdropping the power consumption of a cryptographic-device, power traces can be analyzed using an algorithm such as Simple Power Analysis (SPA) [22], Differential Power Analysis (DPA) [23], Correlation Power Analysis (CPA) [24] or Differential Fault Analysis (DFA) [25] to derive the system secret key. The remainder of the section will focus on the specificities of these methods and an interested reader can refer to [8] for additional descriptions.

The total power consumption of a CMOS circuit is composed of two terms: the static power and dynamic power. Static power is due to the transistor internal leakage current and is therefore dependent on circuit design. Dynamic power is due to transistor activity (i.e. transistor switching) which depends on the actual operation being performed and the data being processed. Since analysis is aimed at determining a link between power consumption and the data being processed, only dynamic power is relevant. As static power is mostly

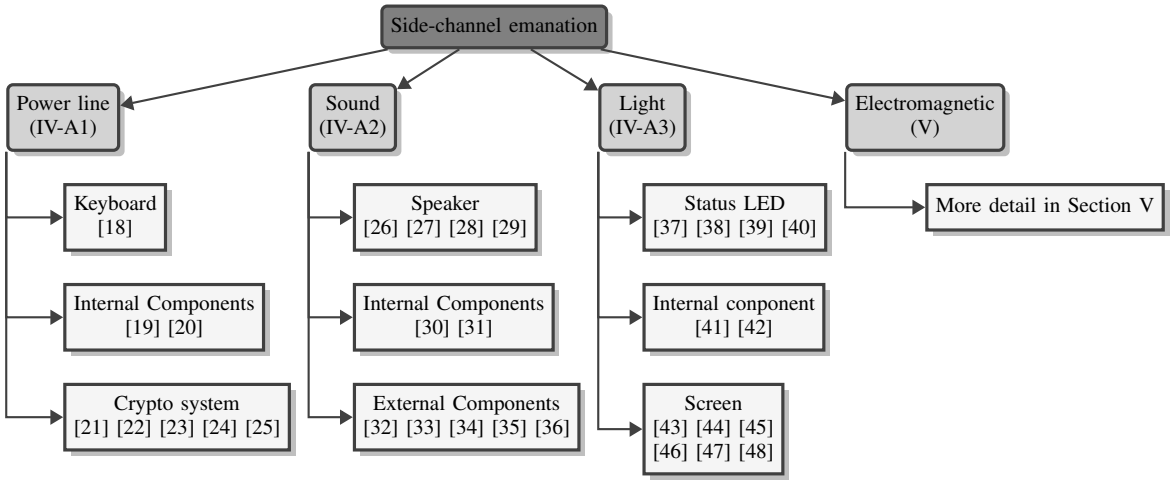


Fig. 3: Classification of the emanation side-channels according to propagation nature.

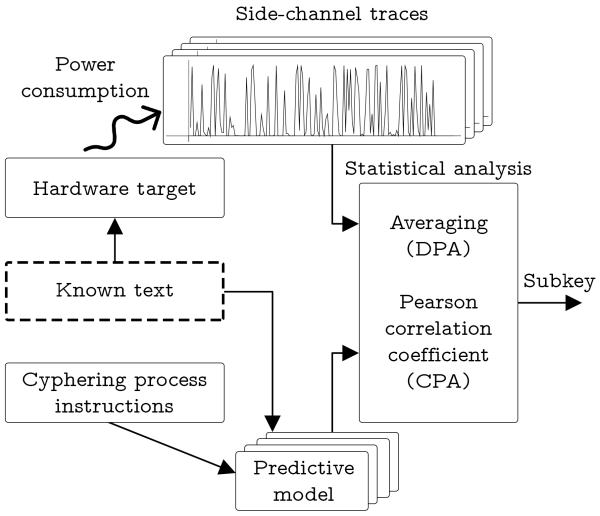


Fig. 4: Outline of the DPA and CPA analysis.

constant, it is straightforward to use total power as a possible side-channel.

SPA is based on the direct interpretation of power consumption measurements since each processor operation has a different trace. In the case of unprotected implementation of cryptographic algorithm, the sequence of operation that is performed is linked to the secret key. Therefore, if one is capable of discriminating operations then he can find out this sequence and finally recovers the secret key [22].

For more powerful attacks, once the observational data have been collected, they must be processed in order to retrieve information. Various methods exist: firstly, DPA combines consumption analysis (SPA) with statistical methods (see Fig. 4). It breaks down the secret key into smaller independent blocks.Hence, DPA attacks have error correction properties which can extract keys from measurements that are too noisy for SPA to work [23].

CPA is a statistical algorithm that uses the Pearson correlation coefficient to correlate data. The subkey is estimated by choosing the one with the highest correlation. This entire process is performed with each subkey, enabling the complete secret key to be collected. Compared to DPA, the CPA method requires fewer power traces. However, it requires an accurate power consumption model in accordance with the targeted hardware.

Finally, the DFA uses injection in order to induce a fault in the device or a deviation from its default behavior. It can be used for example to retrieve an encryption key via side-channel analysis and different fault injections would lead to different propagation errors in the ciphering process. For these different injections, statistical assumptions can be made on secret keys. For example, by injecting eight faults in total into specific rounds of AES execution, the full key can be recovered [25]. In [50] a laser is used in order to recover data stored in memory of a powered-off device. For this purpose, the thermal laser stimulation technique is used, which consists in exciting the silicon transistors with a laser while simultaneously monitoring the device pins to extract the bit state of memory. A more in-depth study on attacks is available in [21], including an explanation of attacks with device awareness (template attack and stochastic model attack).

If power line has been massively used to extract cryptographic secret keys, all CPU activities can be observed and executed instructions (operation code and registry) can be extracted. This approach was applied for instance in [51] which uses Hidden Markov Models on a PIC microcontroller and achieves an instruction recognition rate of up to 70%. In 2018 [52] improves the performance by adding a machine learning algorithm applied to 8-bit microcontroller and was able to correctly recover 99% of the instructions.

2) Sound: The main purpose of sound channel attacks is to recover information passed through acoustic waves due to mechanical or sometimes electronic effects. Different papers focus on this approach and all highlight the need to train the system for identification. This leads to certain drawbacks such as limited recognition capacity (less than 80% without strong a priori hypothesis).

In 2010, Backes et al. proposed acoustic side-channel attacks on printers [32], that were able to recover up to 72% of

printed words. By assuming the language context, the attack achieves recognition rates up to 95% of whole texts. Sound acquisition was performed in the [20;48] kHz band and uses the Hidden Markov Model and the Viterbi algorithm which is regularly used in speech recognition, to determine the most likely sequence of printed words.

Asonov et al. proposed a PC keyboard attack [33] where he eavesdrops on the sound made by each pressed key. This attack is based on the hypothesis that the sound of clicks differs slightly from key to key. A neural network was used to classify clicks. The sound was acquired using a standard microphone and recorded with a standard PC sound card. 79% of the keys pressed were correctly guessed on the keyboard where the neural network was trained. It should also be noted that this ratio falls to 28% on an untrained keyboard. Sound can also be acquired from a legitimate microphone, for instance during a voice over IP call (VoIP). If the attacker can attend the call or access the audio content, he could pick up the keyboard sounds and therefore retrieve the typed message [35] [36]. With a minimum audio rate of 20 kbit/s, 40% of the characters can be recovered, this number increases to 92% with the use of machine learning techniques trained with the writing habits of the person being listened to.

Sound can also be produced by electronic rather than mechanical origins. On modern computers, these acoustic emanations, typically caused by power regulation circuits, are correlated with CPU activity since the power draw is strongly affected by the current executed operation. Shamir et al. [30] and Genkin et al. [31] have shown that when ciphering is performed, the different RSA keys have distinguishable acoustic fingerprints. The full recovery of the key was successful using a cellular phone placed next to the computer or with a directive microphone from a distance of 10 meters. In [30] and [31], this was achieved by repeating the encryption process over many thousands of iterations, which is difficult to assess in an unsupervised attack. Although these methods are promising, due to the low microphone bandwidth (under 20 kHz using common microphones, and a few hundred kHz using ultrasound microphones [30]), it is difficult to distinguish the different instructions.

To prevent keyboard sound eavesdropping, an on-screen keyboard can be used where the key selected is chosen by a mouse or a touch screen. However, another side-channel still exits as Genkin et al. [34] overcame this countermeasure by listening to the power supply noise of a screen in order to recover displayed information (using the same method as a screen power consumption attack). When displaying an on-screen keyboard, word guessing accuracy of 75% was demonstrated using a convolutive neural network-based classifier after a training phase on the same screen.

Many computers have built-in microphones and speakers. Although designed to operate on audible audio, these devices can also emit with reduced performance on the ultrasound band (and thus be undetectable to the human ear). All these elements make the use of ultrasound a useful means of achieving air-gap bridging. Hanspach et al. [26] in addition to simple ultrasound point-to-point communications, they also successfully created a mesh network with an error correction layer and a frequency-hopping spread spectrum transmission (in order to make the system more difficult to intercept). An experiment demonstrated a transmit message rate of approximately 20 bit/s up to a range of 19.7 m between two connected nodes.

Speakers are generally used to generate sound, but can work in reverse. By connecting a speaker to an audio input, it is possible to turn it into a microphone with much lower sensitivity than conventional microphones. Modern audio chips are capable of reversing the direction of connected headphones from output devices into input devices using software functionality. Guri et al. [27] use these special features to create a way of exfiltrating data from a computer which does not contain a microphone (for confidentiality reason) using the near-ultrasonic domain (18 kHz to 24 kHz). A range of about 9 m was achieved with a data rate of 10 bit/s. However, such acoustic communication relies on the availability of speakers on a computer which may not be available on the targeted device. To tackle this challenge, Guri et al. [28] also developed a way of generating an acoustic communication channel using a hard disk drive. By generating a specific pattern of reading operations on the disk, sound can be modulated. A data rate of 3 bit/s was demonstrated up to a range of 2 m. A similar approach can be taken by controlling the computer fan speed [29] for a data rate of 0.25 bit/s up to a range of 8 m.

3) Light: In order to spy on content displayed on a screen, a very basic approach might be to spy on the surface of the screen with a telescope. This method, although very effective, requires a perfect line of sight between the screen and the device. It has been demonstrated that sufficient high-frequency content remains in the emitted light (when the pixel is turned off) to enable reconstruction of the displayed content by deconvolving the signal received with a fast photosensor [43]. Khun was able to reconstruct a displayed image from an out-of-sight cathode-ray tube (CRT) surface (i.e. from a reflection against a wall). The periodic nature of the signal can be used to reduce noise via periodic averaging.

Backes et al. [44] extended this type of attack to a more modern screen using the low reflections of the screen image on eyeglasses, teapots, and even the user eye. Image acquisition was possible at up to 30 m. Later they extended their work to incorporate reflections on walls or clothes [45].

Light-emitting diodes (LEDs) are used in nearly every branch of electronics and in any situation where a fast, bright, highly visible indicator is required. In some networking equipment, a LED is used to show line activity by flashing at the same rate as the information is transmitted. Loughry et al. [37] demonstrated that besides echoing the same flow rate, the LEDs of some equipment are often directly connected to the data line they monitor and may leak into the optical domain. Since these leakages contain all the data transmitted, all parity checking and error correction features embedded in the data stream are available to the eavesdropper too. An error-free reconstruction from emitted light was possible at a distance of 38 m on various equipment such as routers, fax, modems, network cards.

Although humans can see luminous emissions, they are unable to perceive their rapid variations. It was, therefore, logical to use LED variations in order to intentionally exfiltrate information. Guri [38] successfully demonstrated that status LEDs placed on routers can exfiltrate information. He was able to establish a 1000 bit/s per LED communication channel. He shows that this bandwidth can be increased with the use of multiple LEDs. [39] takes a similar approach with a hard disk status LED with a final data rate of 4000 bit/s. [40] uses a monitor status LED with a data rate of 20 bit/s.

Another method of using slow human visual perception was developed, in which data is leaked through hidden images displayed on a computer screen [46]. With this method, a nearly visible QR code (Quick Response code) is embedded on the computer screen. The nearly visible feature is achieved by very low contrast or fast flickering images.

In [33] [35] [36], the authors have shown the retrieval of a keyboard entry with a microphone. But the keyboard sounds can also be recorded with a so-called laser microphone. These microphones pick up the vibrations of a surface by projecting a laser on it and measuring the light time of flight, which depends on the slightest vibration. In [41], these laser microphones were used to listen on a surface close to a keyboard, achieving a 30 m range. Electro-optical sensor through telescope can also be used to monitor the tiny vibrations on a surface allowing to listen to the sounds in a room [53] .

A video recording can be used to identify a password by looking at his arms movements [47]. By knowing the keyboard layout and using the time elapsed between each keystroke, it is possible to estimate the distance between the used keys and a list of potential passwords is then deduced. In [48], the goal is also to retrieve a password but with recording eye movements. As a human eye naturally focuses on the pressed keys, it is possible to translate the eye movements into typed passwords.

It is to note that there is a side-channel due to thermal emissions of a target. However, this threat does not present a significant risk as it has a low bandwidth and a low practical range. Moreover, it is easy to detect due to the changes required at the target: change in the cooling strategy, additional computational load to increase the temperature of a component, etc.

B. Countermeasure applications

In the previous section, several side-channel and multiple data exfiltration scenarios have been described. Although these attacks are very dangerous and potentially critical for information security, several possible countermeasures can be taken against them based on the side-channel they use.

Light side-channels can be mitigated in different ways depending on the target. For screen interception, the low level of the reflected light can be jammed through the use of background illumination with broadband natural light (e.g. halogen or sun) [44]. A lightproof room may be used with all windows covered or special window film installed to prevent optical eavesdropping [38]. The only way of preventing data LED exfiltration is to cover the LEDs with black tape, which will obviously degrade the user experience (since these LEDs are supposed to indicate whether or not the equipment is functioning properly). Banning any equipment capable of detecting light emission (e.g. cameras) will prevent most exploitation of leakage [38]. Finally invoking random LED blinking may jam the recovery process [38].

Sound side-channels suffer from significant damping in the air. All these attacks are short range or require high-end material to improve the distance, such as a directive microphone. Consequently, these attacks are easily noticeable due to the size of the equipment. Regarding soundproofing countermeasures, use of a soundproof room is obviously an effective but costly countermeasure. It should be noted that soundproofing of the compromising equipment comes at the cost of heat issues. Short of adopting such extreme countermeasures, good practice can drastically reduce risk. It has been demonstrated that the attenuation provided by a door may be sufficient [33] due to the low power of the sound signal.

The printer recognition process involves detecting the sound of each character strike based on the assumption of left-to-right writing [32]. If a randomized order is used on the same line (the characters are not written down from left-to-right, but in random order), the reconstruction process is more challenging. Keyboards made of rubber instead of hard plastic or touch-screen keyboards make no keystroke sounds [33]. Moreover, jamming can be used to hide compromising data in noise, with the introduction of a noise source near sensitive equipments, either broadcasting white noise on a voice channel [27] or generating fake keystroke sounds [36]. In any case, denoising of received sounds in order to differentiate them effectively requires complex algorithms as well as expensive equipment that is not available to everyone.

Preventing power analysis is quite simple since all leakages pass through power wires only. Combined with careful design, additional filters may be installed on the power supply stage to reduce the amount of compromising information that can pass through [20]. It is common knowledge that the power supplies follow EMC rules in order to limit the disturbances they generate. However, compromising emissions are so low that they are not considered by the EMC standards. They are not filtered by power supplies since the latter would become too complex and expensive. Specific methods are thus necessary as explained in the Soft TEMPEST countermeasures in Section V.

C. Evaluation of menace index

The previously mentioned side-channels exhibit several weaknesses (summarized in Table I) and are compared to electromagnetic side-channel. The first one is their relatively short range, which is due in particular to their inability to pass through walls. The second drawback relates to signal quality. Combined with the short range, the signal can be distorted on the interception side, making interception difficult and sometimes impossible, even in nominal interception conditions. The third drawback relates to the decoding methods themselves: the equipment required for interception at longer distances is expensive and requires extensive expertise in signal processing in order to be functional.

TABLE I: Comparison of side-channels.

Leakage carrier	Range	Ability to pass wall	Possibility of non-detection	Bandwidth	Cost of material
Light	+	- -	-	- -	+
Sound	-	-	- -	+	++
Power analysis	- -	+	+	-	-
Electromagnetic	++	++	++	++	-

The use of sound to propagate information is a known method and this channel can easily be monitored to detect a possible attack. The usable band is relatively small (0-50 kHz) making it easy to acquire and process the entire band in real time to monitor the potential compromising equipment. Power analysis involves observing only the target consumption. If the observed signal is emitted by several devices, separating the devices is an added difficulty compared to analyzing a single target. For light, as already stated, the necessity of having a line of sight combined with its inability to pass through walls and the necessity of being invisible to the human eye makes this approach difficult to assess in practice.

Electromagnetic waves, on the other hand, do not exhibit the defects mentioned above. They can pass through walls and do not require a line of sight. The modulation techniques and signal processing for these radio waves are very widely spread, making their access easier for everyone and allowing a long range. The usable radio spectrum is quite large, making it easy to hide some radio emissions. Although the cost of equipment can be high, very low-cost alternatives are available as we will discover in the next section. Even if non-EM side-channel threats should not be minimized or ignored (as demonstrated by the numerous presented sources and examples), the aforementioned specificities demonstrate a greater threat of attacks based on electromagnetic side-channels. The next section focuses on this type of side-channel.

V. Electromagnetic side-channel

Sound, light, and power side-channel leakages may have a limited impact as simple but efficient countermeasures can now be easily deployed. On the contrary, electromagnetic emanations are far more difficult to handle than other leakage carriers. The three disruptive differences are: their long range (they still operate even if not in line of sight of the target), ability to pass easily through walls and the large radio spectrum in which the leakage may appear (making these kinds of side-channels hard to detect). This section discusses the various electromagnetic leaks and their possible applications. A synopsis of the studied papers and categorization of the attack targets are provided in Fig. 5. A brief description of each side-channel can be found in III-C.

Electronic equipment unintentionally emits electromagnetic signals while operating (issued by the electromagnetic field, cross-talk, modulation with clock line, etc.). These electromagnetic radiations may contain information on which an adversary may eavesdrop to recover sensitive data (a.k.a. red data) after reconstruction. Unintentional energy emanation from a system is a major threat to privacy and security. Electromagnetic Emission Security (EMSEC) (the term TEMPEST is also frequently used) refers to the various compromising emanations and their uses for eavesdropping as well as information leaked through emanation evaluation.

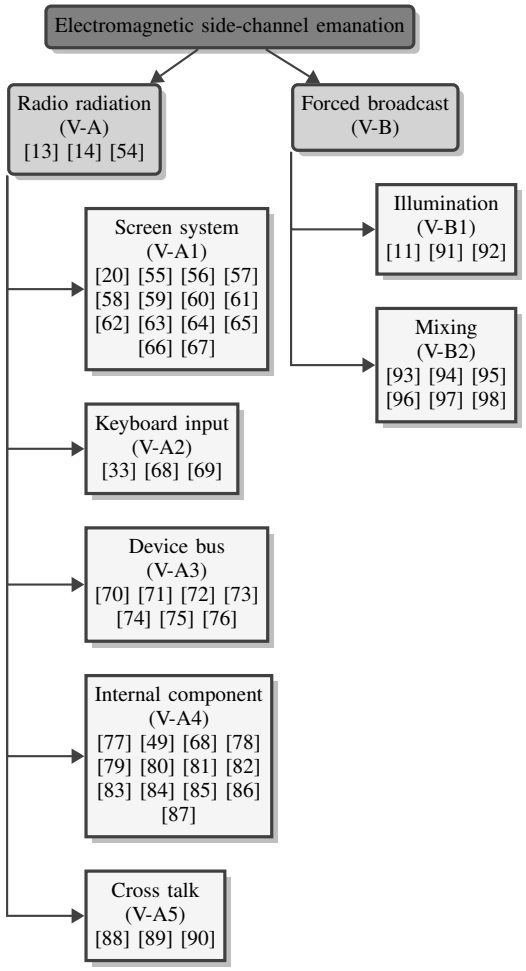


Fig. 5: Overview of the Electromagnetic side-channel categories.

The NSA TEMPEST program is the first known one to address the risk of electromagnetic emanations in terms of security threats. Some of its documents have been declassified, i.e. TEMPEST basics and fundamental principles [13], and the methods and equipment required in order to detect any compromising leaks [54].

EMSEC is linked to EMC [99] insofar as both are based on the study of various electromagnetic emissions of a system. However, while EMC aims to protect equipment and people from electromagnetic radiation, EMSEC transcends EMC as it analyzes these emissions to verify that compromising information is not being emitted, and aims to eliminate them or, at least, make them unusable by an opponent.

A. Radio frequency radiation side-channels

An electromagnetic field may be emitted from a conductor due to transitions in its state (i.e. applied voltage). In this paper, conductors are a generic concept not limited to simple cables or Printed Circuit Board (PCB) track, but also including system components such as inductors and capacitors. These various leaks are directly correlated with the transmitted information on the conductor and therefore anyone recovering these leaks may be able to reconstruct the original information. Fig. 6 illustrates two types of radiation leakages. The source signal (a) generates an electromagnetic field that can be directly picked up by an eavesdropper (b). The resulting side-channel is however in baseband and therefore has a short radio range. Nevertheless, the electromagnetic field of the source also influences the surrounding signals, for example a high frequency clock signal (c) and an Amplitude Modulation (AM) (d) results from mixing these two signals. This AM side-channel can be received at long radio range by an eavesdropper due to the high carrier frequency. Generally, the higher the transition rate (i.e. a data bus or clock signal), the greater the leaks.

1) Leaks induced by screen systems: Screens are key elements of modern computer systems as they provide almost all the information to users. They are therefore ideal targets for an attacker because all the elements displayed are red data. A significant number of publications addresses this target.

Although CRT screens are now considered obsolete, they have laid the foundations for modern screens that still use some standards created for CRT monitors. Since a CRT screen does not store any data, a continuous stream of data is used. However, as screens have different resolutions, control signals must be added for line and image synchronizations, labeled *hsync* and *vsync* in Fig. 7.

A gap interval labeled *vblank* (vertical blanking interval) can be shown in Fig. 7 between the end of the *vsync* pulse and the start of a new image frame. During this interval, no image is displayed but data are still sent to the pixel lines all with the same value. There is also a small horizontal blanking interval after the *hsync* pulse for the same reason. Modern CRT screens do not require such long blanking intervals, and LCD displays require none, but the standards were established when the blanking was needed and thus still remain.

In 1985, Van Eck et al. [55] described a method to infer the output of a CRT monitor at a distance of hundreds of meters using cheap off-the-shelf equipment.

Eavesdropping is achieved by bringing down to baseband a leaking frequency containing video information and sending it to a standard screen. The received signal does not contain the control lines that allow image synchronization. As it stands, the image is received, but moves horizontally and vertically. The quality of reception can be improved by externally generating the necessary synchronization signals and feeding them into the receiving screen.

Kuhn et al. [56] applied similar principles to flat-panel displays in 2005. The nuance is that these screens do not operate with such a high voltage level, making the interception range shorter (around 10 meters). Moreover, the image is rendered row by row and not pixel by pixel like in CRT, so it is not possible to use the same process as Van Eck (because the energy of the pixels on the same row is all mixed at the same time). Kuhn uses another target in which the video data transits: the cable. This cable can leak outside the screen enclosure but also inside in the path which leads to the electronic board. With modern eavesdropping systems, the two synchronization signals do not need to be physically synthesized. However, to produce a stable image, the vertical and horizontal resolutions as well as the refresh rate must be known. Eavesdropping reception is successfully achieved at a 10 m distance through two intermediate offices and without using a directional antenna [57]. With directive log-periodic antenna, the interception range was extended to 46 m [58]. It should be noted that desktop or laptop screens are not the only displays on which it is possible to eavesdrop, as [62] proves that smartphone or tablet screens are also likely to be intercepted.

A leakage channel can be found by checking the presence of periodic signals after an AM demodulation of the received signal [20]. This periodicity is attributable to the redundancy of the information sent to the screen, since an image is generally very close to the one that precedes it. In addition, *vblank* gaps also generate strong redundancy that can be seen when autocorrelation is performed after AM demodulation on the leaked signal. Video signals can be easily separated from background noise because they are highly redundant. Displayed information usually remains unchanged for many seconds and, as a result, periodic averaging at vertical frequency (Screen refresh rate, frequency between the *vblank* gaps) is very effective.

In [59], Zhang et al. have shown that more leaks appear when there are structural asymmetries or impedance discontinuities (e.g. in a poorly designed differential pair or cable connector). [60] introduces a more powerful procedure than autocorrelations to detect a leakage frequency leveraging the frequency estimation of the spectral centroid. This algorithm can detect the horizontal and vertical synchronization frequencies of display video signal in a noisy environment.

Video eavesdropping is not completely blind, and some assumptions can be made to accelerate the estimation of screen parameters. Synchronization frequencies should be limited to certain specific values (as they are closely related to the display resolution) in order to reduce the kernel of frequencies to be checked. This is the method proposed by the open-source software TempestSDR [61], which enables a display to be intercepted in real time. Moreover, some parts of the image may be known in advance, e.g. task bars or application launchers that are always placed at specific locations on the screen. These elements can be used as a reference point to adjust the synchronization frequencies more quickly and accurately [62].

Video leaks usually appear in the VHF band (30-300 MHz) but they can also be found in the UHF band (300-3 GHz). Hence, using an appropriate antenna, data acquisition can be achieved with a commercially available dedicated TEMPEST spectrum analyzer (e.g. R&S FSET, Dynamic Sciences) but their price are very expensive, especially for hackers. A more affordable choice is to use Software-Defined Radio (SDR)

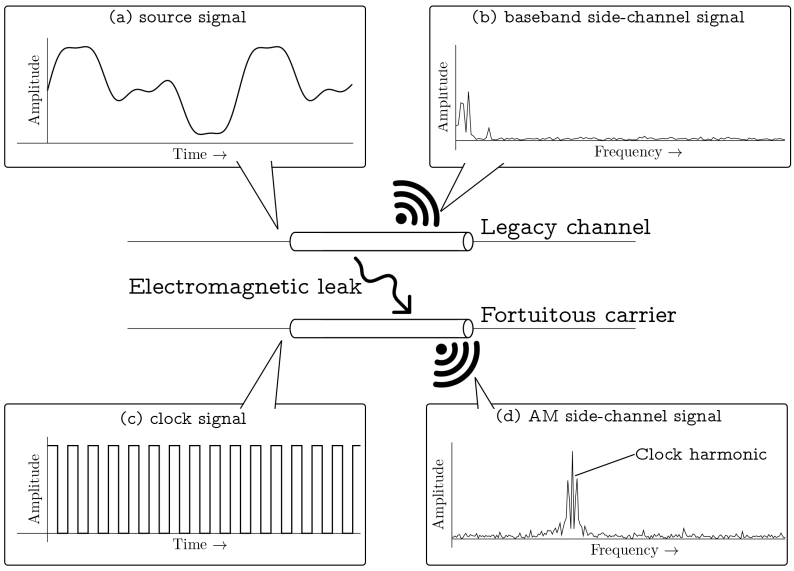


Fig. 6: Examples of electromagnetic radiation side-channel: AM and baseband side-channels.

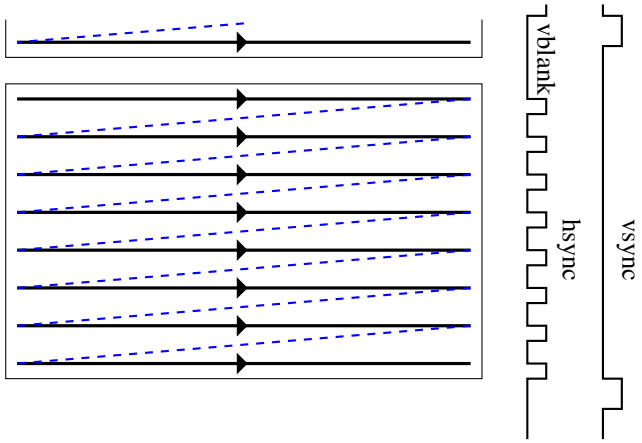


Fig. 7: CRT screen rendering strategies.

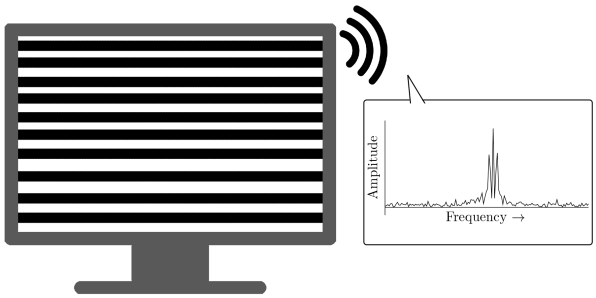


Fig. 8: "TEMPEST for Eliza" operating principle [66].

to intercept the signal [64][62][63]. A bandwidth of 20 to 50 MHz is required to achieve the best video quality [57] but a lower-quality alternative is possible with a tunable TV receiver [65] which is in fact a small SDR with low bandwidth (around 2 MHz).

In 2001, a hacker [66] released software enabling video cable leakage to be used to transmit data, which was audio content in this case. By displaying black and white strip patterns with specific sizing and spacing (see Fig. 8), it is possible to perform AM modulations that a simple AM short wave radio receiver can pick up. This program not only generates a radio broadcast, but the strip pattern causes major fluctuations in the power supply and the audio content can be heard near the screen with a coil whine phenomenon. In 2014, Guri et al. [67] adapted this transmission method to send more traditional data. Data are first encoded using Audio Frequency-Shift Keying (A-FSK) modulation and then, software converts the modulated symbols into pictures for the display. The resulting Frequency Modulation (FM) signal is carried in the 76-87.5 MHz band and the practical range was about 7 m at 480 bit/s.

2) Leaks induced by keyboards: An old example of keyboard eavesdropping occurred during the Second World War when the U.S. military used encrypted teletypewriter communications such as the Bell 131-B2. In a Bell laboratory, a researcher noticed by chance that every time the machine stepped, a peak appeared on an oscilloscope in a remote part of the laboratory. To prove the vulnerability of the device, Bell engineers captured compromising emanations emitted by a Bell 131-B2, located 25 meters away. They were able to recover up to 75% of the plain text [68].

More recently, in addition to sound fingerprint shown by Asonov et al. [33], Vuagnoux et al. demonstrated the possibility of using electromagnetic radiation to recover transcribed information [69]. The first approach involves listening to the wired data communication sent by the keyboard each time a key is pressed. Wired communication is achieved with the PS/2 protocol, in which each key is sent with a 11-bit word at 10-16.7 kHz. This retrieval method raises some difficulties because it targets baseband signals with a low propagation range.

However, this signal can also be unintentionally modulated internally by the keyboard electronics, e.g. by the clock of the internal microcontroller. In this case, AM or FM modulation is generated with the clock (or its harmonics) as carriers. These transmissions are generally less disrupted by noise and obstacles such as walls and floors than baseband signals.

3) Leaks induced by device buses: The higher the throughput of a bus, the more transitions are generated and therefore the more radiation is emitted [100]. However, the higher the throughput, the faster the receiver must be to reconstruct data successfully.

Smulders et al. [71] showed the feasibility of eavesdropping on content passing through an RS-232 bus. The flow rate of this bus is relatively low (less than 200 kbit/s), and therefore its acquisition in baseband is relatively impractical. However, as with a keyboard, the communication bus can be found modulated with a system clock. During experimentation, the bus was found on the FM band at harmonics of the system clock signal (more precisely in 10-130 MHz). The small bandwidth of the RS-232 link reduces the need for very high bandwidth reception materials. In fact, interception is feasible with standard AM/FM radio receivers (intended for broadcasting music) with successful reception at 9 m.

More recent communication buses are also sensitive to eavesdropping. In [76] Schulz et al. have shown the feasibility of listening over an 10 Mbps ethernet cable. They used a near field probe and a 20 MHz SDR to intercept the information passing through the cable. The ethernet forward error correcting code can furthermore be used by the eavesdropper to increase the range of the attack. For higher bandwidths, more probes are needed since Ethernet standards then use multiple twisted pairs at the same time.

USB is one of the most widely used systems present on all computers and several attacks are described in the open literature [72]. The principal difficulty of decoding USB lies in the Non-Return to Zero Inverted (NRZI) coding used. This coding does not code each bit independently, but codes them according to the previous bits. It is therefore necessary to intercept bit-perfect information [73]. Zhang et al. [74] use neural networks (an echo state network) to classify received signals and then select the most likely choice from the coding possibilities, leading to a complex yet functional system.

Apart from eavesdropping, it is also possible to use a USB bus to intentionally leak information. [75] found that transmitting a sequence full of '1' bits to a USB device can generate a detectable emission between 240-480 MHz. This is due to the fact that '1' bits generate a rapid voltage change on each clock cycle. They performed Binary FSK (B-FSK) modulation where the frequency was adjusted with the addition of '0' between '1' (to prevent a voltage shift) in order to lower the carrier leakage frequency and enable modulation of the data stream, a data rate of 640 bit/s was achieved.

4) Leaks induced by system internal components: The main goal of air-gapped computers is to prevent information leaks. These computers are isolated from conventional networks such as the Internet. This, however, does not prevent any potential threats due to breaches in network isolation (for example, the computer may be infected by malware if users plug in their phones to recharge them). In order to prevent any leaks, the number of devices that are connectable to an air-gapped computer must be minimized and limited to a screen and wired mouse keyboard.

However, Guri et al. [79] showed that preventing data exfiltration is insufficient. They demonstrated the potential for using RAM to generate and modulate leaks, by invoking specific memory-related instructions to modulate and transmit electromagnetic signals at cellular frequencies. The leaks occur in the 600-1100 MHz range depending on the generation of Double Data Rate Synchronous Dynamic RAM (DDR-RAM) used. The modulation scheme used was a modified Binary Amplitude-Shift Keying (B-ASK). The '0' is obtained with a near zero amplitude (which is in fact the normal leakage level when nothing special is done). The '1' is obtained by invoking a memory instruction in order to leak a strong signal. This communication channel has a range of about 30 m at a 1 kbit/s data rate with a dedicated SDR receiver.

Funtenna [80] is an open-source software payload that intentionally makes its host hardware act as an improvised RF transmitter (although not initially designed for electromagnetic communication). Mainly intended for embedded systems rather than computers, this software uses a system standard General Purpose Input Output (GPIO) , Pulse Width Modulation (PWM) or Universal Asynchronous Receiver Transmitter (UART) outputs to generate FSK or ASK modulation below 100 MHz.

In 2018, Guri et al. [81] presented a type of malware that can exfiltrate data via low frequency (less than 50 Hz) magnetic signals induced by computer CPU cores. By controlling the workload of the CPU cores with multiple sub-carrier modulations (one carrier per core), a bit rate of 40 bit/s was achieved at 1 m.

Matyunin et al. [82] suggested using a hard disk drive magnetic head to generate magnetic emissions by invoking basic read/write operations on the disk. They used ASK modulations but due to such devices low power consumption, the practical range is lower than with a CPU core at about 15 cm with a data rate of 2 bit/s.

Hardened cryptography systems aim to prevent data retrieval resulting from side-channel attacks by giving the cryptography system a specific architectural design. Although circuits can be protected against intrusive attacks and power analysis, it is more difficult to secure them against radiation attacks since these are capable of targeting very precise points of a chip with near-field probes while remaining perfectly undetectable. These attacks are known as Electro-Magnetic Attacks (EMA) [83] and all the processing and methods applicable to SPA [22] and DPA [23] are possible with EMA [21]. For template attacks [77] the threat mainly lies in the ability to recover a key with few traces. The attacker uses a device identical to the target in order to thoroughly understand its functioning. A great deal of pre-processing can then be performed offline, which fastens the attack.

It should, however, be emphasized that other methods exist, such as using Short Time Fourier Transform (STFT) or AM demodulation to produce a narrower band signal to decrease the effect of noise [85].

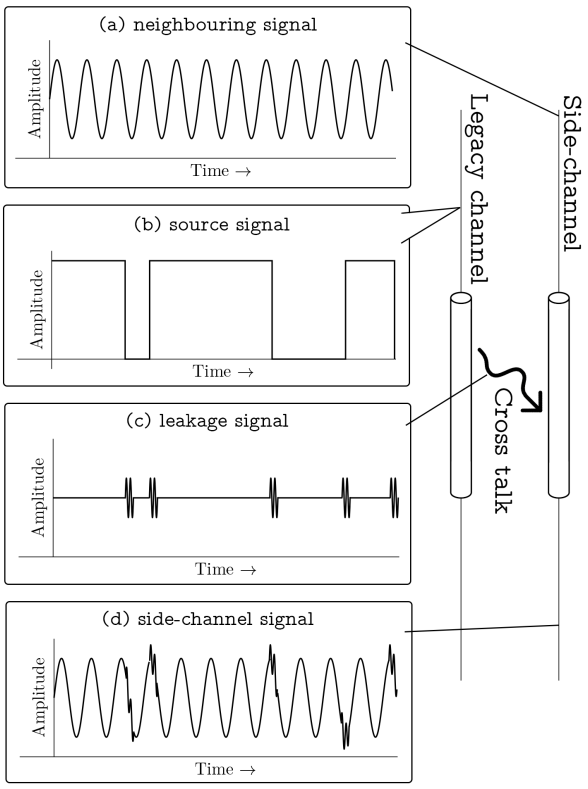


Fig. 9: Cross-talk model.

Aboulkassimi et al. [86] demonstrated the possibility of extracting the key from AES encryption performed on a mobile phone using a near-field electromagnetic probe. [49] found cryptographic related emanations using near-field probes as well as far-field probes (with log-periodic antenna). Goller et al. [84] continued this study of using far-field probes to recover encryption keys. They successfully recovered them at a distance of 80 cm using a commercially available SDR (middle-end type). They also carried out a comparison between the use of a good quality SDR and a low-end SDR (e.g. a DVB-T stick). The difference of signal-to-noise ratio between the middle-end and low-end system was only about 2 dB, but with reduced received power for the low-end system, which, in practice dramatically reduces the recovery range. Consequently, compared to a maximum distance of 80 cm for the middle-end system, the low-cost system is unable to receive a usable signal at a distance greater than 10 cm.

Timing attacks target the execution time of cryptographic instructions. To prevent these attacks, constant-time security is used where every security-critical operation is modified so that it lasts exactly the same time regardless of the input data. Alam et al. [87] utilized security features present in RSA implementation (openSSl) to speed up the extraction of the key. In fact, they only needed one trace to recover the RSA private key using a near-field probe (over 95% successful recovery). They detected the ciphering process through a specific pattern induced by the constant-time countermeasure (protect against timing attack).

5) Leaks induced by cross-talk: Cross-talk is a special case of a radiation side-channel where the radiation originates from a legacy channel, as illustrated by Fig .9. The source signal (b) propagates through an adjacent conductor (a) due to a radiation phenomenon (c), resulting in a leak in the adjacent conductor (d). While this does not change the content carried by the leak, it does change the way it is propagated. Cross-talk phenomena were among the first threats highlighted by TEMPEST [13]. The NSA created a special guide to reduce the incidence of this type of leak [14]. In 1967, Ware [88] suggested that it was conceivable that sensitive information was being eavesdropped by cross-talk but provided no evidence of it.

In a USB, the only security feature lies in the fact that all devices cannot monitor total bus traffic. This security is performed by active components (placed within the bus line) that redirect data flows to the right device. But, in fact, all downstream data (host to devices) are broadcasted to all devices while only the upstream is unicast and redirected by the active component. This implementation has major security problems since all USB devices can listen plainly to all the information sent by the host even if they are not the rightful recipients. Su et al. [89] highlighted a cross-talk phenomenon within USB hubs that provide packet redirection. Most of the time, USB hubs consist of a single-chip solution, and isolation between lines is present. Nevertheless, the small size of the chip and the high data rate can still produce a cross-talk phenomenon between adjacent USB lines. The researchers successfully demonstrated the interception of USB fingerprint scanner data (device to host stream) from an infected USB gadget such as a USB light connected to the same USB hub as the scanner [89].

In [90], an in-depth study of cross-talk phenomena is conducted with particular attention to the reconstruction of digital signals transmitted along differential connections. This paper addresses theoretical aspects and seeks to determine the conditions under which eavesdropping of information is possible. Reconstitution accuracy is dependent on the speed of the signal being listened to (risk of overlapping bits), and the quality of the cable where the red signal is leaking is also of significance. Although several wires can be used to enhance reconstruction quality, algorithmic complexity drastically increases and becomes prohibitive for real-time constraints.

B. Forced broadcast side-channels

Another kind of electromagnetic side-channels is the forced-broadcast, represented in Fig. 10), where the main carrier (a) is issued from outside the target and reflects while being altered by the target (b). This reflection thus leads to a leak of information (c). Forced broadcast is composed of two subcategories, namely illumination and mixing, considered respectively as active and passive attacks.

Radio illumination attacks force a system (screen, keyboard, microphone, etc.) to leak by mixing them with an external carrier and by studying the reflected wave altered by the targeted system. Most of the time, the mixing process results in an AM or FM modulation. These attacks are extremely powerful due to their ability to accurately choose a target

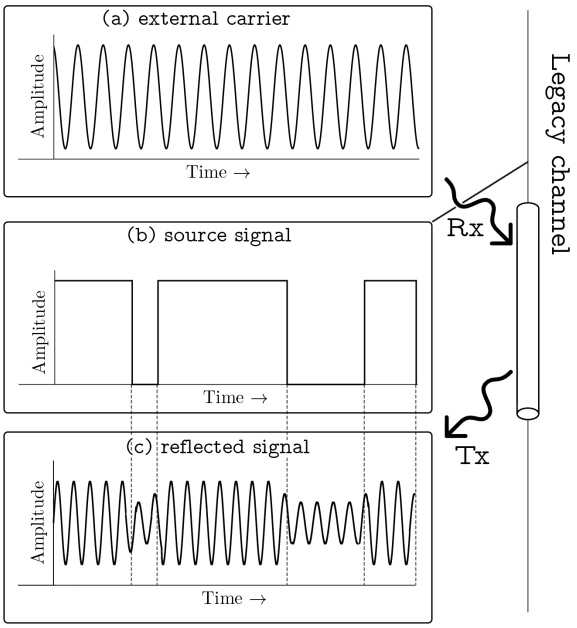


Fig. 10: Example of forced broadcast side-channel.

(directive antenna are generally used) and their long-range (the attacker has plain control on the carrier transmission power and frequency), but they also present a significant disadvantage. The carrier used is generated by the attacker and is not a signal that normally exists in the conventional radio spectrum. As such, the target may notice this abnormal carrier and detect the attack.

A mixing leak is similar to the previous scenario except that the carrier modulated by the system originates from a source other than the attacker (WiFi access point, Digital Enhanced Cordless Telecommunications (DECT) phone, embedded radio transmitters, etc.). The hazards of such attacks are greater because the external signal comes from an authorized source and is therefore not categorized as an abnormal channel source, unlike illumination attacks. In these scenarios, since the attacker becomes totally passive, its detection is impossible [94]. On the downside, weaker signal quality is assumed.

1) Illumination attack: The Thing, also known as The Great Seal Bug [91] (1945), was an unpowered covert listening device developed in the Soviet Union. The device was designed to recover speech. To ensure maximum concealment and eliminate maintenance requirements, the "bug" was totally passive and had to be remotely powered by a radio beam in order to be operated. The device was planted in 1945 but only discovered in 1952.

The NSA used the same principle of a device powered by external sources in their VAGRANT program [11]. Although information regarding this program is supposedly classified, some information has become public knowledge due to the Snowden leaks. The VAGRANT program aims to spy on a user computer interface by installing bugs in the equipment being monitored. Two types of bugs are used. An extremely basic version, which is useful for high-speed side-channels such as video cables, consists of a simple radio reflector placed on the cable. When a continuous carrier radio stream illuminates it, the data is modulated and redirected to the transmitter. A more complex version uses logic components powered by the radio beam to reflect the signal with FSK modulation (between the data lines it taps and an internal clock). The maximal range achieved by such a system was about 12 km in excellent conditions, which is significantly longer than for passive radio eavesdropping.

Due to the nature of the VAGRANT program, no scientific papers have been published on this type of attack, although some explanations may be found in [101] and [102]. In particular, no real expressions of the distances, means of recovering red signals and manufacture of bugs are explained. However, in 2018, Wakabayashi et al. [92] addressed this issue. Rather than recreating the exact same version as the NSA, they used the principle of illumination attacks to create their own version. An interception data rate of approximately 10 Mbit/s was achieved within 10 m using a SDR radio.

Kinugawa et al. [103] extended the scope of the aforementioned attack by targeting PCB in addition to data cables. They were able to record the power supply of a cryptographic circuit, allowing the interception of a secret RSA key up to 5 m. Although some components have been added on the PCB, only a qualified person will be able to differentiate them from the legitimate components. Other interesting targets are smart speakers as they constantly listen to their surroundings in order to detect wake-up words. Kinugawa et al. were able to demonstrate the reception of the inner microphone up to 5 m with a bug placed on an internal wire.

2) Mixing with external carrier attack: With the recent advent of SoC, processors, memories and radio communication circuits can be combined on the same circuit to create smaller and cheaper devices. Although these systems are mainly made up of digital components, an analog part still remains for power supply and communication. While modern radio protocols are digital and most of their layers are implemented in the digital domain, the generation, amplification, and transmission of radio frequency signals are by nature analog operations. The recovery of keys through an analysis of various emanations of a processor or power supply has been widely studied [85] [84]. However, all these methods use probes that must be placed very close to the component being studied, which limits the criticality of the threat. In a system where an SoC is used for encryption, shared power supply between the processor and the radio circuit on the one hand, and physical proximity, on the other hand, may both result in the presence of processor activity on the transmitted radio signals. If, during a radio communication phase, the processor performs encryption (which is very common as secure radio exchange packets are encrypted on the fly), processor activity may then be present in the radio frequency signal. Therefore, it is possible to recover the encryption key remotely by listening to the radio communication. In [93], Camurati et al. presented a successful attack of this kind. The target was an SoC nRF52832 with an internal Bluetooth link from which it was possible to retrieve the RSA encryption key at a distance of 10 m with methods very similar to EMA [83].

The prominence of radio communications and the omnipresence of energy in radio bands make it possible either to conceal a radio illumination attack or use radio waves that are already present. Indeed, one might leverage the presence of electromagnetic waves from legitimate transmissions to search for any relevant side-channel. This has been intensively done using WiFi standard in the so-called WiFi-radar applications. For instance, [95] leverages the fact that WiFi frequencies pass through walls and are reflected on the human body, in order to seek the presence of a person and his movements. Like all radar images, a high signal processing workload is required to obtain usable data. A deep neural network is used to detect joint movement. Moreover, this works even in the presence of a wall and in the absence of light source, unlike the camera-based method. The radio-based system has been proved almost as accurate as the conventional camera-based system up to the maximum range of the router used (which was 12 m).

WiFi may also result in a higher resolution when, instead of targeting a whole body, only a part is monitored. Ali et al. [96] applied gesture recognition to user finger and hand movements above a keyboard in order to recognize keystrokes. They used the fluctuations in the instantaneous channel state information caused by small hand movements. High key accuracy of 89.7% was obtained with k-nearest neighbor classifiers and a multi-antenna setup with off-the-shelf WiFi devices. A similar approach was adopted [97] with the use of an SDR-based system specially designed for this purpose. This increased correct key estimation to 91.8%.

Finally, application can be further extended by targeting a person face. The subtle movements involved require major signal processing as well as beamforming to reduce the noise. However, Wang et al. [98] show the feasibility of such approach. Their system detects nine vowel and consonant patterns and uses context-based error correction techniques to correctly estimate the word pronounced. An efficiency of 91% was observed in a direct line of sight, although this ratio drops to 18% if a wall is interposed. As a conclusion, as they are based on non-intentional passive emissions, WiFi-radar applications exhibit a potential high menace.

Side-channel attacks based on electromagnetic signals are particularly threatening to security and privacy due to the diversity of targets as well as the different possible paths. The low cost of some methods and the low knowledge requirements for carrying them out make them even more cause for concern.

On top of that, several indicators tend to exacerbate this issue. First, the evolution of current technology tends to increase the frequency of system clocks and the number of clock regions. This has two consequences: i) the number of side-channels may increase, and ii) these side-channels may appear on a wide carrier frequency range (and reach values more favorable to their propagation). Secondly, for a defender, potential threats are often identified based initially on channel sounding. Thus, finding a potential compromising signal is more difficult due to the proliferation of classic radio signals. Finally, this section has shown that the cost of interception is decreasing, with smaller yet effective equipment available so that powerful techniques such as machine learning [70] can even be envisioned. Discrete attacks that can be coordinated with very few resources are being leveraged, paving the way to a blurring of the boundaries between the attacker classes set out in Section III. Potential crucial information leaks may appear anywhere and be conducted by anyone with an interest, commitment, and a basic knowledge of electronics.

VI. Countermeasures

Given the wide variety of potential attacks, several protection measures exist. Some of these aim to protect against several attacks, but are generally cumbersome. Most of them therefore target specific attacks, as is the case of screen content interception used hereafter as a typical example of a countermeasure, but can generally be extended to the other data buses.

To choose an appropriate countermeasure, the origin of a leak should first be identified. There are of course specific methods (e.g. defined in TEMPEST) but classic EMC methods (and their related equipment) can also be used. Both side-channel analysis and EMC try to analyze the origin of leaked signal and to mitigate it. But a worthwhile difference lies in the fact that, for side-channel analysis, only red signals are problematic. The analysis methods for side-channel detection can also contribute to EMC studies. By analyzing the red data recovered, it is possible to identify which part of a device is contributing to the leak and then, the designer can redesign this part in order to follow EMC rules. Moreover side-channel analysis can also be used as a non-intrusive debugging and integrity checking [52], as behavioral checking [116] [117] or as neural network reverse engineering [118].

1) Zoning: The countermeasure of zoning is one of the methods suggested by the NSA [13]. It entails keeping an empty space (with no electronic equipment) around the device requiring protection. Its effectiveness is based on the fact that side-channel leaks are very limited in range and therefore a space prevents the installation of interception devices in good reception range. Although this was valid in the 1980s when the recommendations were published, we have seen that some attacks are very long-range, making zoning impractical.

2) Shielding equipment: Shielding is a good way of reducing the electromagnetic emanation exiting a target as well as entering it [104], by using barriers made of conductive or magnetic materials. Shielding is commonly applied to device enclosures to isolate them from the outside. However, in some devices such as screens, a metallic shield covering the full enclosure significantly reduces usability. This difficulty is addressed in [62] by using shielding material made of a conductive mesh. A sufficiently thick polarizing filter is also used as an add-on so that the touch screen can be used consistently. This works by reducing the electrical coupling between the shield and the touch screen.

3) Shielding structure: To be efficient, a shielding must be complete [105], i.e. cover the entire unit without any holes. This can lead to major disadvantages, especially in terms of heat evacuation that can become critical in computers. To overcome this constraint, shielding can be applied to a room or even to a whole building if the information is sufficiently

TABLE II: Comparison of electromagnetic countermeasures.

Countermeasure	Protection performance	Cost	Work on other nature of leaks	Upgrading from non -secured device	Portability of the countermeasure
Zoning [13]	Low	Low	Yes	Yes	No
Shielding equipment [62] [104]	High	High	Yes	Hard	Yes but heavy weight
Shielding structures (room/building) [41] [105]	High	Very high	Yes	Very hard	Mobile but only within the structure
Soft TEMPEST [7] [56] [106] [107] [108] [109] [110]	High (only on specific leaks)	Low	Yes	Yes	Yes
Secured data bus [76]	High (leaks are present but unusable)	Medium	Yes	Hard	Yes
Chip re-design [83] [89] [93] [110] [111] [112]	Medium (prevent only a part of the leaks)	High	Yes	No	Yes
Jamming [113] [114] [115]	High (only on targeted leaks)	Medium	No	Yes	Yes

critical (and the budget allows it). The shielding must also take into account everything that goes in and out of the area, including pipes (heating and water) and the power grid [41].

4) Soft TEMPEST: Another countermeasure that has proved effective for screens requires a software modification to change the pixel data-stream order. Indeed, interception is based on the assumption that pixels are sent from left to right and from the top to the bottom. Sending pixels in random order greatly impedes image reconstruction, but does not prevent emanation interception. The same idea is applicable to other data buses by changing the natural order of transmitted packets. This method requires the modification of the entire image chain for both graphics cards and displays, which are highly standardized, and the cost of these modifications is significant in terms of software development. A more economical method of hampering interception is to use the fact that recovered pixels are not real RGB values, but a mix of three colors with no distinction between one another (grayscale for the analog signal and false color reconstruction for the numeric signal). Interception can be rendered impracticable by adjusting the character colors and background color in order to achieve a constant energy level between all the pixels [106] [56] [107].

5) Secured data bus: A modern video data bus has some internal functionality which can prevent effective interception. The link can operate at a lower refresh rate and be active only when a different image must be rendered. The absence of a periodic signal would make eavesdropping on the interface cable less practical. A second feature, known as High-bandwidth Digital Content Protection (HDCP), is based on encryption and key negotiation between the video content producer (graphics card or stored data) and display. Originally intended to prevent unauthorized copying of video signals by sharing pre-encrypted content for display (through the video cable), with the decryption step occurring in the last device in the chain (the display), it would also render interface cable emanations unreadable by turning video data, considered as red data, into black data. It should be noted that cyphering a transmission is not limited to video information and any data bus can have the same security feature preventing any recovery of confidential data [76].

6) Chip re-design: For leaks resulting from internal mixing of signals, e.g. between several buses [89] or with the radio circuit [93], the close proximity of the various hardware functions on the same silicon die cause leaks. By ensuring that the different mixing parts do not work simultaneously, it is possible to ensure that even if data leaks, it will not be propagated to the outside. In many cases this requires extensive redesign of the firmware and has a major impact on performance.

The various software enhancements seen in Soft TEMPEST can also be integrated into the hardware parts. This is notably the case for cryptosystems, which are generally built as hardware accelerators e.g. Field Programmable Gate Array (FPGA) or Application-Specific Integrated Circuit (ASIC), but use the same principles as software algorithms and are therefore also subject to side-channel threats. One should note that due to the reconfigurable nature of the FPGA, some new attacks need to be taken into account such as clock tampering or internal fault generation [112] [110].

In the same vein of redesigning the whole chip, System in Package (SiP) technologies integrate multiple dies inside one chip [111]. SiP devices have the advantage of being almost as compact as single chip solutions while providing better internal isolation, preventing internal crosstalk and mixing phenomena. The EMA (electromagnetic analysis) targets a specific part of a chip, usually the cryptographic part. Splitting the various functionalities of the cryptographic process on a chip nullifies the precise targeting of EMA, but renders chip design difficult.

Currently most cryptographic circuits are specially optimized IP (Intellectual Property) blocks, which obviously reduces development costs, but entails the drawback of attack portability. If circuit vulnerabilities are present in the IP block, any system that embeds it can be attacked in the same manner. By dispensing entirely with such specialized cryptography circuits, it is possible to hide instructions related to encryption among all the others. However, this has a major impact on performance since dedicated circuits are very fast and low power compared to all-purpose circuits. Another solution is to remove the correlation between the side-channel leaks (i.e. electromagnetic radiation or power consumption) and the processed data/operations. Typically, this is achieved by changing the algorithm and circuit design to produce a constant leak pattern that does not change with the processed

data. Asynchronism [83] can also be added by avoiding a central system clock and instead operating each part of a chip asynchronously. As a result, the clocks radiance, and consequently the emanation range, are reduced. In addition, the use of dual line logic lowers the risk of successful reconstruction by an attacker.

7) Jamming: Finally, if it is not possible to prevent leakage or render it unusable, the remaining method is to hide the leaks by installing jamming systems [113]. This jamming may be wideband, which requires a large amount of power, or target specific frequencies on which leaks or vulnerabilities are known to exist. In the latter case, less power is required. However, it requires an analysis of system leaks to determine where to jam. It should be noted that forced broadcast attacks must also be taken into account, either by detecting then jamming them or by jamming at frequencies where the system is vulnerable to them. A more deceptive approach is to generate traces of false operations in order to lure the attacker, so his reconstruction efforts are parasitized by operations that make no sense or make it appear that another algorithm is being executed [114] [115].

Countermeasures have been developed to protect information from eavesdroppers either by preventing data recovery or making it unusable. However, these countermeasures must not tamper with proper device functioning. Representative measures are listed in Table II. The most reliable and universal scheme is to shield devices, rooms, or occasionally buildings. This prevents radio waves from penetrating or exiting. However, this is usually expensive, especially if shielding rooms or buildings and it is not suitable for mobile equipment. All the other available countermeasures point to either a particular leak or make any leak unreadable.

An important point to remember is that most software developers and hardware architects do not build secure systems, either for performance/cost reasons or more generally because they are not aware of the security vulnerabilities that may exist and therefore cannot limit them.

VII. Conclusion

This paper provides a literature review of side-channel attacks based on emanation. The wide variety of attacks has led to the creation of classifications identifying common points among the various attacks. Illustrative use-cases covering the various side-channels are introduced and used as a basis to derive the individual threat and possible target of such side-channels. Moreover, differences between them are presented. In Appendix, Table III is a summary of the various side-channel emanations discussed in this paper including a classification by target, side-channel, activeness, intentionality and the practical range achieved. Special emphasis has been placed on the electromagnetic side-channel since, although not new, it is the focus of a recent increase in activity through the democratization of software-defined radio, enabling high-performance solutions at low cost. Due to their long range, higher bandwidth, cross-wall ability and concealment capabilities, radio frequency waves are a particular threat when compared to other mediums. Mixing leaks are highlighted due to the increased difficulty involved in detecting them. Their main advantage lies in being present solely when an attacker is attacking and therefore totally vanishing otherwise. In addition, potential countermeasures were discussed with a focus on practical use and the resources involved in such protective action. Depending on the application and operational environment, several countermeasures can be used, but there is no universal solution that is both efficient and low cost.

Technological advances are making hardware more and more effective and smaller, thus this increase of complexity allows the growth of a large number of leaks. In too many cases, the leaks are present because the hardware architect was unaware of the side-channel issue and the associated risks. The purpose of this paper is to identify possible existing leaks so that they can be prevented. There is no silver bullet to solve our security challenge at once. But we have a number of techniques that can make system more secure at the cost of a certain loss of performance or usability.

Under the current guidelines, if a radio transmission combines low probability of interception and detection, the transmission is considered secured. This is true of frequency hopping transmissions thanks to their ability to switch very quickly from one frequency to another, for instance in TRANsmission SECurity (TRANSEC) radio. If, by any side-channel, red information is leaked to the secured transmission, the resulting signal is still considered secured while confidential information is being sent. Not only is this transmission entirely legitimate but is performed over a long range since radio transmission is conducted by conventional means and not the side-channel. It is evident that frequency hopping in Bluetooth [93] has been successfully used to extract red information and it is only a matter of time before more secure transmissions are subject to the same concerns. With the advent of software-defined radio, the resources available to attackers have shifted: solutions that were previously available only to state entities are now available to hackers.

References

[1] D. T. Sullivan, "Survey of Malware Threats and Recommendations to Improve Cybersecurity for Industrial Control Systems," 2015. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a617910.pdf

[2] S. L. Pfleeger and R. Rue, "Cybersecurity Economic Issues: Clearing the Path to Good Practice," *IEEE Software*, vol. 25, no. 1, pp. 35–42, 1 2008.

[3] B. Aichinger, "DDR memory errors caused by Row Hammer," in *Proc. IEEE High Performance Extreme Computing Conference (HPEC)*, 9 2015.

[4] Q. Ge, Y. Yarom, F. Li, and G. Heiser, "Your Processor Leaks Information - and There's Nothing You Can Do About It," 12 2016.

[5] P. Kocher, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom, "Spectre Attacks: Exploiting Speculative Execution," 1 2018.

[6] M. Lipp, A. Kogler, D. Oswald, M. Schwarz, C. Easdon, C. Canella, and D. Gruss, "PLATYPUS: Software-based Power Side-Channel Attacks on x86," in *Proc. IEEE Symposium on Security and Privacy (SP)*, 2021.

[7] J. Fan, X. Guo, E. D. Mulder, P. Schaumont, B. Preneel, and I. Verbauwhede, "State-of-the-art of secure ECC implementations: a survey on known side-channel attacks and countermeasures," in *Proc. IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, jun 2010.

[8] Y.-I. Hayashi and N. Homma, "Introduction to Electromagnetic Information Security," *IEICE Transactions on Communications*, vol. E102.B, no. 1, pp. 40–50, jan 2019. [Online]. Available: https://www.jstage.jst.go.jp/article/transcom/E102.B/1/E102.B_2018EBI0001/_pdf/-char/en

[9] C. Brent and A. Carlisle, "A survey and taxonomy aimed at the detection and measurement of covert channels," in *Proc. 4th ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec)*.

[10] I. Giechaskiel and K. Rasmussen, "Taxonomy and challenges of out-of-band signal injection attacks and defenses."

[11] NSA, "VAGRANT program," Jul. 2008, catalogue extract: http://cryptome.org/2013/12/nsa-catalog-appelbaum.pdf. [Online]. Available: http://cryptome.org/2013/12/nsa-catalog-appelbaum.pdf

[12] M. Guri, "BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets," 4 2018.

[13] NSA, *NACSIM 5000: Tempest Fundamentals. National Security Agency*, Feb. 1982, partially declassified transcript: http://cryptome.org/jya/nacsim-5000/nacsim-5000.htm.

[14] ——, *National Security Telecommunications and Information Systems Security Advisory Memorandum NSTISSAM TEMPEST/2-95: RED/BLACK Installation Guidance*, transcript: http://cryptome.org/tempest-2-95.htm.

[15] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures," *Proceedings of the IEEE*, vol. 100, no. 11, pp. 3056–3076, 2012.

[16] A. Lucas and A. Tisserand, "Microcontroller Implementation of Simultaneous Protections Against Observation and Perturbation Attacks for ECC," in *Proc. International Conference on Security and Cryptography (SECRYPT)*, 6 2018.

[17] M. Guri and Y. Elovici, "Bridgeware," *Communications of the ACM*, vol. 61, no. 4, pp. 74–82, 3 2018.

[18] Y. L. Du, Y.-H. Lu, and J.-L. Zhang, "Novel Method to Detect and Recover the Keystrokes of PS/2 Keyboard," *Progress In Electromagnetics Research C*, vol. 41, pp. 151–161, 6 2013.

[19] R. Spolaor, L. Abudahi, V. Moonsamy, M. Conti, and R. Poovendran, "No free charge theorem: A covert channel via USB charging cable on mobile devices," in *Applied Cryptography and Network Security*, 2017, pp. 83–102.

[20] Y. Hayashi, N. Homma, Y. Toriumi, K. Takaya, and T. Aoki, "Remote Visualization of Screen Images Using a Pseudo-Antenna That Blends Into the Mobile Environment," *IEEE Transactions on Electromagnetic Compatibility*, vol. 59, no. 1, pp. 24–33, 8 2017.

[21] T.-H. Le, C. Canovas, and J. Clédière, "An overview of side channel analysis attacks," in *Proc. ACM symposium on Information, computer and communications security (ASIACCS)*, 2008.

[22] S. Mangard, "A Simple Power-Analysis (SPA) Attack on Implementations of the AES Key Expansion," in *Proc. International Conference on Information Security and Cryptology (ICISC)*, 4 2002, pp. 343–358.

[23] P. Kocher, J. Jaffeand, and B. Jun, "Differential Power Analysis," in *Proc. Advances in Cryptology (CRYPTO)*, 12 1999, pp. 388–397.

[24] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," in *Proc. Cryptographic Hardware and Embedded Systems (CHES)*, 1 2004, pp. 16–29.

[25] E. Biham and A. Shamir, "Differential fault analysis of secret key cryptosystems," in *Proc. Advances in Cryptology (CRYPTO)*, 8 1997, pp. 513–525.

[26] M. Hanspach and M. Goetz, "On Covert Acoustical Mesh Networks in Air," *Journal of Communications*, vol. 8, no. 11, pp. 758–767, 11 2013.

[27] M. Guri, Y. Solewicz, B. Zadov, A. Daidakulov, and Y. Elovici, "MOSQUITO: Covert Ultrasonic Transmissions between Two Air-Gapped Computers using Speaker-to-Speaker Communication," 3 2018.

[28] ——, "Acoustic Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard-Drive Noise ('DiskFiltration')," in *Proc. Computer Security (ESORICS)*, 8 2017, pp. 98–115.

[29] M. Guri, Y. A. Solewicz, A. Daidakulov, and Y. Elovici, "Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers," 6 2016.

[30] E. Tromer, "Acoustic cryptanalysis: on nosy people and noisy machines," *Eurocrypt Rump Session*, 5 2004.

[31] D. Genkin, A. Shamir, and E. Tromer, "RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis," in *Proc. Advances in Cryptology (CRYPTO)*, 10 2014, pp. 444–461.

[32] M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, and C. Sporleder, "Acoustic Side-Channel Attacks on Printers," in *USENIX Security Symposium*, 9 2010, pp. 307–322.

[33] D. Asonov and R. Agrawal, "Keyboard acoustic emanations," in *Proc. IEEE Symposium on Security and Privacy (SP)*, 6 2004.

[34] D. Genkin, M. Pattani, R. Schuster, and E. Tromer, "Synesthesia: Detecting Screen Content via Remote Acoustic Side Channels," 8 2018.

[35] A. Compagno, M. Conti, D. Lain, and G. Tsudik, "Don't Skype & Type!" in *Proc. ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 4 2017. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/3052973.3053005?download=true

[36] S. A. Anand and N. Saxena, "Keyboard emanations in remote voice calls," in *Proc. ACM Conference on Data and Application Security and Privacy (CODASPY)*, 2018.

[37] J. Loughry and D. A. Umphress, "Information leakage from optical emanations," *ACM Transactions on Information and System Security*, vol. 5, no. 3, pp. 262–289, 8 2002.

[38] M. Guri, B. Zadov, A. Daidakulov, and Y. Elovici, "xLED: Covert Data Exfiltration from Air-Gapped Networks via Router LEDs," 6 2017.

[39] M. Guri, B. Zadov, and Y., "LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED," *Detection of Intrusions and Malware, and Vulnerability Assessment*, pp. 161–184, 2 2017.

[40] V. Sepetnitsky, M. Guri, and Y. Elovici, "Exfiltration of Information from Air-Gapped Machines Using Monitor's LED Indicator," in *Proc. IEEE Joint Intelligence and Security Informatics Conference (JISIC)*, 9 2014.

[41] A. Barisani and D. Bianco, "Side channel attacks using optical sampling of mechanical energy and power line leakage," in *defcon 17*, 2009. [Online]. Available: https://www.defcon.org/images/defcon-17/dc-17-presentations/defcon-17-barisani-bianco-sniff_keystrokes.pdf

[42] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, "Light commands: Laser-based audio injection on voice-controllable systems," in *29th USENIX Security Symposium*, 2020. [Online]. Available: https://lightcommands.com/20191104-Light-Commands.pdf

[43] M. G. Kuhn, "Optical Time-Domain Eavesdropping Risks of CRT Displays," in *Proc. IEEE Symposium on Security and Privacy (SP)*, 5 2002.

[44] M. Backes and D. Unruh, "Compromising Reflections-or-How to Read LCD Monitors around the Corner," in *Proc. IEEE Symposium on Security and Privacy (SP)*, may 2008.

[45] M. Backes, T. Chen, M. Duermuth, H. P. Lensch, and M. Welk, "Tempest in a Teapot: Compromising Reflections Revisited," in *Proc. IEEE Symposium on Security and Privacy (SP)*, 5 2009.

[46] M. Guri, O. Hasson, G. Kedma, and Y. Elovici, "An optical covert-channel to leak data through an air-gap," in *Proc. IEEE Annual Conference on Privacy, Security and Trust (PST)*, 12 2016.

[47] K. Balagani, M. Cardaioli, M. Conti, P. Gasti, M. Georgiev, T. Gurtler, D. Lain, C. Miller, K. Molas, N. Samarin, E. Saraci, G. Tsudik, and L. Wu, "Pilot: Password and pin information leakage from obfuscated typing videos," 3 2019.

[48] Y. Chen, T. Li, R. Zhang, Y. Zhang, and T. Hedgpeth, "EyeTell: Video-assisted touchscreen keystroke inference from eye movements," in *IEEE Symposium on Security and Privacy (SP)*, may 2018.

[49] D. Agrawal, B. Archambeault, R. Josyula., and P. Rohatgi, "The EM Side-Channel(s)," in *Proc. Cryptographic Hardware and Embedded Systems (CHES)*, 2 2003, pp. 29–45. [Online]. Available: https://dl.acm.org/citation.cfm?id=752713

[50] H. Lohrke, S. Tajik, T. Krachenfels, C. Boit, and J.-P. Seifert, "Key extraction using thermal laser stimulation," 10 2019.

[51] T. Eisenbarth, C. Paar, and B. Weghenkel, "Building a side channel based disassembler," in *Transactions on Computational Science X*.

[52] J. Park, X. Xu, Y. Jin, D. Forte, and M. Tehranipoor, "Power-based side-channel instruction-level disassembler," in *Proc. ACM/ESDA/IEEE Design Automation Conference (DAC)*.

[53] B. Nassi, Y. Pirutin, A. Shamir, Y. Elovici, and B. Zadov, "Lamphone: Real-time passive sound recovery from light bulb vibrations," in *Blackhat USA*.

[54] NSA, *National Security Telecommunications and Information Systems Security Advi- sory Memorandum NSTISSAM TEMPEST/1-92: Compromising Emanations Lab- oratory Test Requirements*, Dec. 1992, partially declassified transcript: http://cryptome.org/nsa-tempest.htm.

[55] W. V. Eck, "Electromagnetic radiation from video display units: An eavesdropping risk?" *Computers & Security*, vol. 4, no. 4, pp. 269–286, 12 1985.

[56] M. G. Kuhn, "Electromagnetic Eavesdropping Risks of Flat-panel Displays," in *Proc. International Conference on Privacy Enhancing Technologies (PET)*, 5 2004, pp. 88–107.

[57] ——, "Eavesdropping attacks on computer displays," in *Proc. Information Security Summit (ISS)*, 5 2006, pp. 24–25.

[58] F. Elibol, U. Sarac, and I. Erer, "Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system," in *Proc. European Signal Processing Conference (EUSIPCO)*, 8 2012, pp. 1767–1771.

[59] N. Zhang, Y. Lu, Q. Cui, and Y. Wang, "Investigation of Unintentional Video Emanations From a VGA Connector in the Desktop Computers," *IEEE Transactions on Electromagnetic Compatibility*, vol. 59, no. 6, pp. 1826–1834, 12 2017.

[60] J. Shi, W. q. Huang, D. Wei, and D. g. Sun, "A novel method for computer video leaking signal detection," in *Proc. IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, 8 2014.

[61] M. Marinov, "Remote video eavesdropping using a software-defined radio platform," Master's thesis, St Edmund's College, 2014.

[62] Y. Hayashi, N. Homma, M. Miura, T., and H. Sone, "A Threat for Tablet PCs in Public Space," in *Proc. ACM Conference on Computer and Communications Security (SIGSAC)*, 11 2014.

[63] H. S. Lee, D. H. Choi, K. Sim, and J.-G. Yook, "Information Recovery Using Electromagnetic Emanations From Display Devices Under Realistic Environment," *Transactions on Electromagnetic Compatibility*, vol. 61, no. 4, pp. 1098–1106, 8 2019.

[64] W. Yang, Y. Lu, and J. Xu, "Video information recovery from EM leakage of computers based on storage oscilloscope," *Frontiers of Electrical and Electronic Engineering in China*, vol. 5, no. 2, pp. 143–146, 4 2010.

[65] A. Sayakkara, N. Le-Khac, and M. Scanlon, "Accuracy Enhancement of Electromagnetic Side-Channel Attacks on Computer Monitors," in *Proc. International Conference on Availability, Reliability and Security (ARES)*, 8 2018. [Online]. Available: http://doi.acm.org/10.1145/3230833.3234690

[66] E. Thiele, "Tempest for Eliza," 2001. [Online]. Available: http://www.erikyyy.de/tempest/

[67] M. Guri, G. Kedma, A. Kachlon, and Y. Elovici, "AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies," in *Proc. International Conference on Malicious and Unwanted Software (MALWARE)*, 10 2014.

[68] NSA, *TEMPEST: A Signal Problem*, Sep. 2007, transcript: https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-spectrum/tempest.pdf.

[69] M. Vuagnoux and S. Pasini, "Compromising Electromagnetic Emanations of Wired and Wireless Keyboards," in *USENIX Security Symposium*, 8 2009, pp. 1–16.

[70] B. Hettwer, S. Gehrer, and T. Güneysu, "Applications of machine learning techniques in side-channel attacks: a survey," *Journal of Cryptographic Engineering*, apr 2019.

[71] P. Smulders, "The threat of information theft by reception of electromagnetic radiation from RS-232 cables," *Computers & Security*, vol. 9, no. 1, pp. 53–58, 2 1990.

[72] D.-J. Sim, H. S. Lee, J.-G. Yook, and K. Sim, "Measurement and analysis of the compromising electromagnetic emanations from USB keyboard," in *Proc. IEEE Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)*, 5 2016.

[73] H.-J. Choi, H. S. Lee, D. Sim, J.-G. Yook, and K. Sim, "Reconstruction of leaked signal from USB keyboards," in *Proc. IEEE Asia-Pacific Radio Science Conference (RASC)*, 8 2016.

[74] C. Zhang, H. Zhang, J. Luo, and Y. Du, "TEMPEST in USB," in *Proc. IEEE International Symposium on Electromagnetic Compatibility (EMC)*, 10 2017.

[75] M. Guri, M. Monitz, and Y. Elovici, "USBee: Air-gap covert-channel via electromagnetic emission from USB," in *Proc. Annual Conference on Privacy, Security and Trust (PST)*, 12 2016.

[76] M. Schulz, P. Klapper, M. Hollick, E. Tews, and S. Katzenbeisser, "Trust the wire, they always told me!" in *Proc. ACM Conference on Security & Privacy in Wireless and Mobile Networks - (WiSec)*, 2016. [Online]. Available: https://download.hrz.tu-darmstadt.de/media/FB20/Dekanat/Publikationen/SEEMOO/wisec2016-trust-the-wire.pdf

[77] J. Heyszl, S. Mangard, B. Heinz, F. Stumpf, and G. Sigl, "Localized electromagnetic analysis of cryptographic implementations," in *Lecture Notes in Computer Science*, 2012, pp. 231–244.

[78] D. Goodin. (2013) Meet "badBIOS," the mysterious MacPC malware that jumps airgaps. online. [Online]. Available: http://arstechnica.com/security/2013/10/meet-badbios-the-mysterious-mac-and-pc-malware-that-jumps-airgaps/

[79] M. Guri, A. Kachlon, O. Hasson, G. Kedma, Y. Mirsky, and Y. Elovici, "GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies," in *USENIX Security Symposium*, 8 2015.

[80] A. Cui. (2015) Funtenna. [Online]. Available: www.funtenna.org

[81] M. Guri, B. Zadov, A. Daidakulov, and Y. Elovici, "ODINI : Escaping Sensitive Data from Faraday-Caged, Air-Gapped Computers via Magnetic Fields," 2 2018.

[82] N. Matyunin, J. Szefer, S. Biedermann, and S. Katzenbeisser, "Covert channels using mobile device's magnetic field sensors," in *Proc. Asia and South Pacific Design Automation Conference (ASP-DAC)*, 1 2016.

[83] J.-J. Quisquater and D. Samyde, "ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards," in *Proc. International Conference on Research in Smart Cards: Smart Card Programming and Security (E-SMART)*, 9 2001, pp. 200–210.

[84] G. Goller and G. Sigl, "Side Channel Attacks on Smartphones and Embedded Devices Using Standard Radio Equipment," in *Proc. International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE)*, 7 2015, pp. 255–270.

[85] O. Meynard, D. Réal, F. Flament, S. Guilley, N. Homma, and J. Danger, "Enhancement of simple electro-magnetic attacks by pre-characterization in frequency domain and demodulation techniques," in *Proc. Design, Automation Test in Europe (DATE)*, 2011, pp. 1–6.

[86] D. Aboulkassimi, M. Agoyan, L. Freund, J. Fournier, B. Robisson, and A. Tria, "ElectroMagnetic analysis (EMA) of software AES on Java mobile phones," in *Proc. IEEE International Workshop on Information Forensics and Security (WIFS)*, 11 2011.

[87] M. Alam, H. A. Khan, M. Dey, N. Sinha, R. Callan, A. Zajic, and M. Prvulovic, "One&Done: A Single-Decryption EM-Based Attack on OpenSSL's Constant-Time Blinded RSA," in *USENIX Security Symposium*, 8 2018, pp. 585–602. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/alam

[88] W. H. Ware, "Security and privacy in computer systems," in *Proc. Spring joint computer conference (SJCC)*, 4 1967. [Online]. Available: https://pdfs.semanticscholar.org/8bdf/455e0ca083744fc8955276429817178 3703b.pdf

[89] Y. Su, D. Genkin, D. Ranasinghe, and Y. Yarom, "USB Snooping Made Easy: Crosstalk Leakage Attacks on USB Hubs," in *USENIX Security Symposium*, 8 2017, pp. 1145–1161. [Online]. Available: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-su.pdf

[90] K. Yuan, F. Grassi, G. Spadacini, and S. A. Pignari, "Crosstalk-Sensitive Loops and Reconstruction Algorithms to Eavesdrop Digital Signals Transmitted Along Differential Interconnects," *IEEE Transactions on Electromagnetic Compatibility*, vol. 59, no. 1, pp. 256–265, 2 2017.

[91] S. Union. The Thing. [Online]. Available: cryptomuseum.com/covert/bugs/thing/index.htm#ref

[92] S. Wakabayashi, S. Maruyama, T. Mori, S. Goto, M. Kinugawa, Y.-I. Hayashi, and M. Smith, "A Feasibility Study of Radio-frequency Retroreflector Attack," in *USENIX Workshop on Offensive Technologies*, 8 2018. [Online]. Available: https://www.usenix.org/system/files/conference/woot18/woot18-paper-wakabayashi.pdf

[93] G. Camurati, S. Poeplau, M. Muench, T.Hayes, and A. Francillon, "Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers," in *Proc. ACM conference on Computer and communications security (CCS)*, 10 2018.

[94] T. Wei, S. Wang, A. Zhou, and X. Zhang, "Acoustic Eavesdropping through Wireless Vibrometry," in *Proc. International Conference on Mobile Computing and Networking (MobiCom)*, 9 2015.

[95] M. Zhao, T. Li, M. A. Alsheikh, Y. Tian, H. Zhao, A. Torralba, and D. Katabi, "Through-Wall Human Pose Estimation Using Radio Signals," in *Proc. IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 6 2018.

[96] K. Ali, A. X. Liu, W. Wang, and M. Shahzad, "Recognizing Keystrokes Using WiFi Devices," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 5, pp. 1175–1190, 5 2017.

[97] B. Chen, V. Yenamandra, and K. Srinivasan, "Tracking Keystrokes Using Wireless Signals," in *Proc. Annual International Conference on Mobile Systems, Applications, and Services - (MobiSys)*, 9 2015.

[98] G. Wang, Y. Zou, Z. Zhou, K. Wu, and L. M. Ni, "We Can Hear You with Wi-Fi!" *IEEE Transactions on Mobile Computing*, vol. 15, no. 11, pp. 2907–2920, 11 2016.

[99] Z. Jiemin and L. Yongmei, "The study of the standards architecture and the standards attributes based on EMC standards and TEMPEST standards in computer system," in *Proc. International Conference on Computer Science & Education (ICCSE)*, 4 2013.

[100] F. Moll, M. Roca, and E. Isern, "Analysis of dissipation energy of switching digital CMOS gates with coupled outputs," *Microelectronics Journal*, vol. 34, no. 9, pp. 833–842, 9 2003.

[101] GBPPR. (2014) TAWDRYYARD Experiments. [Online]. Available: https://www.qsl.net/n9zia/vision/index.html

[102] M. Ossmann, "The NSA Playset: RF Retroreflectors," in *DEF CON 22*, 8 2014.

[103] M. Kinugawa, D. Fujimoto, and Y. Hayashi, "Electromagnetic Information Extortion from Electronic Devices Using Interceptor and Its Countermeasure," *Proc. IACR Cryptographic Hardware and Embedded Systems (CHES)*, 2019. [Online]. Available: https://tches.iacr.org/index.php/TCHES/article/view/8345/7693

[104] M. Popescu, V. Bindar, R. Craciunescu, and O. Fratu, "Estimate of minimum attenuation level for a TEMPEST shielded enclosure," in *Proc. IEEE International Conference on Communications (COMM)*, 6 2016.

[105] D. Cazanaru, A. Szilagyi, D. Stoica, P. Mazare, A. Stoica, and A. Boteanu, "Shielding screen design optimization," in *Proc. IEEE International Conference on Communications (COMM)*, jun 2010.

[106] R. J. Anderson and M. G. Kuhn, "Soft Tempest – An Opportunity for NATO," in *Information Systems Technology (IST)*, 4 1999.

[107] H. Tanaka, O. Takizawa, and A. Yamamura, "Evaluation and Improvement of the Tempest Fonts," in *Proc. Information Security Applications (WISA)*, 8 2004, pp. 457–469.

[108] L. Tawalbeh, H. Houssain, and T. Al-Somani, "Review of side channel attacks and countermeasures on ecc, rsa, and aes cryptosystems," in *Proc. Journal of Internet Technology and Secured Transaction (JITST)*, vol. 6, 4 2017. [Online]. Available: https://pdfs.semanticscholar.org/fc7c/fca5065504b62a7c279460fb85cc8b1577e7.pdf

[109] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "Stealing keys from PCs using a radio: Cheap electromagnetic attacks on windowed exponentiation," in *Lecture Notes in Computer Science*, 2015, pp. 207–228.

[110] M. Tehranipoor and C. Wang, *Introduction to Hardware Security and Trust*, 2012. [Online]. Available: https://link.springer.com/content/pdf/10.1007%2F978-1-4419-8080-9.pdf

[111] J. Laskar, B. Matinpour, and S. Chakraborty, *Modern Receiver Front-Ends*, feb 2004.

[112] T. Güneysu and A. Moradi, "Generic side-channel countermeasures for reconfigurable devices," in *Cryptographic Hardware and Embedded Systems – CHES*, 2011, pp. 33–48.

[113] Y. Suzuki and Y. Akiyama, "Jamming technique to prevent information leakage caused by unintentional emissions of PC video signals," in *Proc. IEEE International Symposium on Electromagnetic Compatibility (EMC)*, 7 2010.

[114] D. Pamula and A. Tisserand, "Finite-Field Multipliers with Reduced Activity Variations," in *Proc. Arithmetic of Finite Fields (AIFI)*, 7 2012. [Online]. Available: https://www.ebook.de/de/product/25495155/arithmetic_of_finite_fields.html

[115] K. Yao, S. Lan, M. Xia, and L. Chen, "Active countermeasure using EMI honeypot against TEMPEST eavesdropping in high-speed signalling," in *USNC-URSI Radio Science Meeting (Joint with AP-S Symposium)*, jul 2018.

[116] Y. Han, S. Etigowni, H. Liu, S. Zonouz, and A. Petropulu, "Watch me, but don't touch me! contactless control flow monitoring via electromagnetic emanations," in *Proc. ACM SIGSAC Conference on Computer and Communications Security (CCS)*.

[117] N. Sehatbakhsh, A. Nazari, M. Alam, F. Werner, Y. Zhu, A. Zajic, and M. Prvulovic, "REMOTE: Robust external malware detection framework by using electromagnetic signals," 10 2019.

[118] L. Batina, S. Bhasin, D. Jap, and S. Picek, "CSI NN: Reverse engineering of neural network architectures through electromagnetic side channel," in *Proc. 28th USENIX Security Symposium (USENIX Security)*, Aug. 2019. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/batina

APPENDIX

Name	Ref	First Author	Year	Medium	Target	Activeness	Intentionality	Max range
Novel method to detect and recover the keystrokes of PS/2 keyboard	[18]	Du	2013	Power line	External Component	Passive	Non intentional	0 m
A Simple Power-Analysis (SPA) Attack on Implementations of the AES Key Expansion	[22]	Mangard	2002	Power line	Crypto system	Passive	Non intentional	0 m
Differential Power Analysis	[23]	Kocher	1999	Power line	Crypto system	Passive	Non intentional	0 m
Correlation Power Analysis with a Leakage Model	[24]	Brier	2004	Power line	Crypto system	Passive	Non intentional	0 m
Differential fault analysis of secret key cryptosystems	[25]	Biham	1997	Power line	Crypto system	Active	Non intentional	0 m
Localized Electromagnetic Analysis of Cryptographic Implementations	[77]	Heyszl	2012	Power line	Crypto system	Passive	Non intentional	0 m
An overview of side channel analysis attacks	[21]	Le	2008	Power line	Crypto system	Passive	Non intentional	0 m
PLATYPUS: Software-based Power Side-Channel Attacks on x86	[6]	Lipp	2021	Power line	Crypto system	Passive	Non intentional	0 m
Building a Side Channel Based Disassembler	[51]	Eisenbarth	2010	Power line	CPU	Passive	Non intentional	0 m
Power-based side-channel instruction-level disassembler	[52]	Park	2008	Power line	CPU	Passive	Non intentional	0 m
Key extraction using thermal laser stimulation	[50]	Lohrke	2018	Power line	Memory	Active	Non intentional	$\sim$ 1 m
No Free Charge Theorem: A Covert Channel via USB Charging Cable on Mobile Devices	[19]	Spolaor	2017	Power line	Internal Component	Passive	Intentional	0 m
Information leakage from optical emanations	[37]	Loughry	2002	Light	Status LED	Passive	Non intentional	38 m
xLED: Covert Data Exfiltration fromAir-Gapped Networks via Router LEDs	[38]	Guri	2017	Light	Status LED	Active	Intentional	Line of sight
LED-it-GO: Leaking (A Lot of) Datafrom Air-Gapped Computers via the (Small) Hard Drive LED	[39]	Guri	2017	Light	Status LED	Active	Intentional	Line of sight
Exfiltration of Information from Air-Gapped Machines Using Monitor LED Indicator	[40]	Sepetnitsky	2014	Light	Status LED	Active	Intentional	Line of sight
Optical Time-Domain Eavesdropping Risks of CRT Displays	[43]	Kuhn	2002	Light	Screen	Passive	Non intentional	80 m
Compromising Reflections-or-How to Read LCD Monitors around the Corner	[44]	Backes	2008	Light	Screen	Passive	Non intentional	30 m
TEMPEST in a Teapot: Compromising Reflections Revisited	[45]	Backes	2009	Light	Screen	Passive	Non intentional	30 m
An optical covert-channel to leak data through an air-gap	[46]	Guri	2016	Light	Screen	Passive	Intentional	30 m
Side Channel Attacks Using Optical Sampling Of Mechanical Energy And Power Line Leakag	[41]	Barisani	2009	Light	Sound system	Passive	Non intentional	Line of sight
Light Commands: Laser-Based Audio Injection on Voice-Controllable Systems	[42]	Sugawara	2019	Light	Sound system	Active	Intentional	Line of sight
Lamphone: Real-Time Passive Sound Recovery from Light Bulb Vibrations	[53]	Nassi	2020	Light	Sound system	Passive	Non intentional	Line of sight
PILOT: Password and PIN Information Leakage from Obfuscated Typing Videos	[47]	Balagani	2019	Light	External Component	Passive	Non intentional	Line of sight

Table III continued from previous page

Name	Ref	First Author	Year	Medium	Target	Activeness	Intentionality	Max range
EyeTell: Video-Assisted Touchscreen Keystroke Inference from Eye Movements	[48]	Chen	2018	Light	External Component	Passive	Non intentional	Line of sight
On Covert Acoustical Mesh Networks in Air	[26]	Hanspach	2013	Sound	Sound system	Active	Intentional	19.7 m
MOSQUITO: Covert Ultrasonic Transmissions between Two Air-Gapped Computers using Speaker-to-Speaker Communication	[27]	Guri	2018	Sound	Sound system	Active	Intentional	8 m
Acoustic Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard-Drive Noise ('DiskFiltration')	[28]	Guri	2017	Sound	Sound system	Active	Intentional	2 m
Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers	[29]	Guri	2016	Sound	Sound system	Active	Intentional	8 m
Acoustic cryptanalysis: on nosy people and noisy machines	[30]	Tromer	2004	Sound	Internal Component	Passive	Non intentional	2 m
RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis	[31]	Genkin	2014	Sound	Internal Component	Passive	Non intentional	4 m
Acoustic Side-Channel Attacks on Printers	[32]	Backes	2010	Sound	External Component	Passive	Non intentional	4 m
Keyboard acoustic emanations	[33]	Asonov	2004	Sound	External Component	Passive	Non intentional	15 m
Don't Skype & Type!	[35]	Compagno	2017	Sound	External Component	Passive	Non intentional	Internet
Keyboard Emanations in Remote Voice Calls	[36]	Anand	2018	Sound	External Component	Passive	Non intentional	Internet
Synesthesia: Detecting Screen Content via Remote Acoustic Side Channels	[34]	Genkin	2018	Sound	External Component	Passive	Non intentional	10 m
Screaming Channels: When Electromagnetic Side-Channels Meet Radio Transceivers	[93]	Camurati	2018	EM - forced	Internal Component	Active	Non intentional	10 m
Acoustic Eavesdropping through Wireless Vibrometry	[94]	Wei	2015	EM - forced	Sound system	Active	Non intentional	5 m
Through-Wall Human Pose Estimation Using Radio Signals	[95]	Zhao	2018	EM - forced	External Component	Active	Intentional	12 m
Recognizing Keystrokes Using WiFi Devices	[96]	Ali	2017	EM - forced	External Component	Active	Non intentional	4 m
Tracking Keystrokes Using Wireless Signals	[97]	Chen	2015	EM - forced	External Component	Active	Non intentional	5 m
We Can Hear You with Wi-Fi!	[98]	Wang	2016	EM - forced	Sound system	Active	Non intentional	2 m
NSA catalog pages	[11]	NSA	2008	EM - forced	Device cable	Active	Intentional	12 km
A Feasibility Study of Radio-frequency Retroreflector Attack	[92]	Wakabayashi	2018	EM - forced	Device cable	Active	Intentional	10 m
Electromagnetic Information Extortion from Electronic Devices Using Interceptor and Its Countermeasure	[103]	Kinugawa	2019	EM - forced	Internal Component and device cable	Active	Intentional	5 m
The thing	[91]	Soviet Union	1945	EM - forced	Sound system	Active	Intentional	> 30 m
Electromagnetic radiation from video display units: An eavesdropping risk?	[55]	Van Eck	1985	EM - radiation	Screen	Passive	Non intentional	1 km

Table III continued from previous page

Name	Ref	First Author	Year	Medium	Target	Activeness	Intentionality	Max range
Electromagnetic Eavesdropping Risks of Flat-panel Displays	[56]	Kuhn	2004	EM - radiation	Screen	Passive	Non intentional	3 m
Eavesdropping attacks on computer displays	[57]	Kuhn	2006	EM - radiation	Screen	Passive	Non intentional	10 m
Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system	[58]	Elibol	2012	EM - radiation	Screen	Passive	Non intentional	46 m
Investigation of Unintentional Video Emanations From a VGA Connector in the Desktop Computers	[59]	Zhang	2017	EM - radiation	Screen	Passive	Non intentional	~ 10 cm
A novel method for computer video leaking signal detection	[60]	Shi	2014	EM - radiation	Screen	Passive	Non intentional	n.a.
Remote video eavesdropping using a software-defined radio platform	[61]	Marinov	2014	EM - radiation	Screen	Passive	Non intentional	7 m
A Threat for Tablet PCs in Public Space	[62]	Hayashi	2014	EM - radiation	Screen	Passive	Non intentional	10 m
Information Recovery Using Electromagnetic Emanations From Display Devices Under Realistic Environment	[63]	Lee	2019	EM - radiation	Screen	Passive	Non intentional	20 m
Video information recovery from EM leakage of computers based on storage oscilloscope	[64]	Yang	2010	EM - radiation	Screen	Passive	Non intentional	~ 2 m
Accuracy Enhancement of Electromagnetic Side-Channel Attacks on Computer Monitors	[65]	Sayakkara	2018	EM - radiation	Screen	Passive	Non intentional	~ 2 m
TEMPEST for Eliza	[66]	Erikyyy	2001	EM - radiation	Screen	Passive	Intentional	100 m
AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies	[67]	Guri	2014	EM - radiation	Screen	Passive	Non intentional	7 m
TEMPEST: A Signal Problem	[68]	NSA	2007	EM - radiation	External Component	Passive	Non intentional	25 m
Keyboard acoustic emanations	[33]	Asonov	2004	EM - radiation	External Component	Passive	Non intentional	20 m
Compromising Electromagnetic Emanations of Wired and Wireless Keyboards	[69]	Vuagnoux	2009	EM - radiation	External Component	Passive	Non intentional	20 m
The threat of information theft by reception of electromagnetic radiation from RS-232 cables	[71]	Smulders	1990	EM - radiation	Device cable	Passive	Non intentional	9 m
Trust The Wire, They Always Told Me!	[76]	Schulz	2016	EM - radiation	Device cable	Passive	Non intentional	2 cm
Measurement and analysis of the compromising electromagnetic emanations from USB keyboard	[72]	Sim	2016	EM - radiation	Device cable	Passive	Non intentional	~ 20 cm
Reconstruction of leaked signal from USB keyboards	[73]	Choi	2016	EM - radiation	Device cable	Passive	Non intentional	15 cm
TEMPEST in USB	[74]	Zhang	2017	EM - radiation	Device cable	Passive	Non intentional	0 m
USBee: Air-gap covert-channel via electromagnetic emission from USB	[75]	Guri	2016	EM - radiation	Device cable	Passive	Intentional	9 m
TEMPEST: A Signal Problem	[68]	NSA	2007	EM - radiation	Internal Component	Passive	Non intentional	25 m
Meet “badBIOS,” the mysterious MacPC malware that jumps airgaps	[78]	Goodin	2013	EM - radiation	Internal Component	Passive	Intentional	~ 10 m
GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies	[79]	Guri	2015	EM - radiation	Internal Component	Passive	Intentional	30 m

Table III continued from previous page

Name	Ref	First Author	Year	Medium	Target	Activeness	Intentionality	Max range
Funtenna	[80]	Cui	2015	EM - radiation	Internal Component	Passive	Intentional	> 5 m
ODINI : Escaping Sensitive Data from Faraday-Caged, Air-Gapped Computers via Magnetic Fields	[81]	Guri	2018	EM - radiation	Internal Component	Passive	Intentional	1 m
Covert channels using mobile device's magnetic field sensors	[82]	Matyunin	2016	EM - radiation	Internal Component	Passive	Intentional	15 cm
ElectroMagnetic Analysis EMA: Measures and Counter-Measures for Smart Cards	[83]	Quisquater	2001	EM - radiation	Internal Component	Passive	Non intentional	2 cm
Side Channel Attacks on Smartphones and Embedded Devices Using Standard Radio Equipment	[84]	Goller	2015	EM - radiation	Internal Component	Passive	Non intentional	80 cm
One&Done: A Single-Decryption EM-Based Attack on OpenSSL Constant-Time Blinded RSA	[87]	Alam	2018	EM - radiation	Internal Component	Passive	Non intentional	2 cm
Enhancement of simple electromagnetic attacks by pre-characterization in frequency domain and demodulation techniques	[85]	Meynard	2011	EM - radiation	Internal Component	Passive	Non intentional	~ 4 cm
ElectroMagnetic analysis (EMA) of software AES on Java mobile phones	[86]	Aboulkassimi	2011	EM - radiation	Internal Component	Passive	Non intentional	1 cm
The EM Side-Channel(s)	[49]	Agrawal	2003	EM - radiation	Internal Component	Passive	Non intentional	12 m
Security and privacy in computer systems	[88]	Ware	1967	EM - radiation	Device cable	Passive	Non intentional	0 m
USB Snooping Made Easy: Crosstalk Leakage Attacks on USB Hubs	[89]	Su	2017	EM - radiation	Device cable	Passive	Non intentional	0 m
Crosstalk-Sensitive Loops and Reconstruction Algorithms to Eavesdrop Digital Signals Transmitted Along Differential Interconnects	[90]	Yuan	2017	EM - radiation	Device cable	Passive	Non intentional	2 cm

TABLE III: Classification of the papers on side-channel attacks (EM stands for ElectroMagnetic).