Compromising Electromagnetic Emanations of Wired and Wireless Keyboards

Martin Vuagnoux
LASEC/EPFL
martin.vuagnoux@epfl.ch

Sylvain Pasini
LASEC/EPFL
sylvain.pasini@epfl.ch

Abstract

Computer keyboards are often used to transmit confidential data such as passwords. Since they contain electronic components, keyboards eventually emit electromagnetic waves. These emanations could reveal sensitive information such as keystrokes. The technique generally used to detect compromising emanations is based on a wide-band receiver, tuned on a specific frequency. However, this method may not be optimal since a significant amount of information is lost during the signal acquisition. Our approach is to acquire the raw signal directly from the antenna and to process the entire captured electromagnetic spectrum. Thanks to this method, we detected four different kinds of compromising electromagnetic emanations generated by wired and wireless keyboards. These emissions lead to a full or a partial recovery of the keystrokes. We implemented these side-channel attacks and our best practical attack fully recovered 95% of the keystrokes of a PS/2 keyboard at a distance up to 20 meters, even through walls. We tested 12 different keyboard models bought between 2001 and 2008 (PS/2, USB, wireless and laptop). They are all vulnerable to at least one of the four attacks. We conclude that most of modern computer keyboards generate compromising emanations (mainly because of the manufacturer cost pressures in the design). Hence, they are not safe to transmit confidential information.

1 Introduction

Today, most of the practical attacks on computers exploit software vulnerabilities. New security weaknesses are disclosed every day, but patches are commonly delivered within a few days. When a vulnerability is based on hardware, there is generally no software update to avoid the exposure: the device must be changed.

Computer keyboards are often used to transmit sensitive information such as passwords, e.g. to log into computers, to do e-banking money transfer, etc. A weakness in these hardware devices will jeopardize the security of any password-based authentication system.

Compromising electromagnetic emanation problems appeared already at the end of the 19^{th} century. Because of the extensive use of telephones, wire networks became extremely dense. People could sometimes hear other conversations on their phone line due to undesired coupling between parallel wires. This unattended phenomenon, called *crosstalk*, may be easily canceled by twisting the cables.

A description of some early exploitations of compromising emanations has been recently declassified by the National Security Agency [26]. During World War II, the American Army used teletypewriter communications encrypted with Bell 131-B2 mixing devices. In a Bell laboratory, a researcher noticed, quite by accident, that each time the machine stepped, a spike appeared on an oscilloscope in a distant part of the lab. To prove the vulnerability of the device, Bell engineers captured the compromising emanations emitted by a Bell 131-B2, placed in a building across the street and about 25 meters away. They were able to recover 75% of the plaintext.

During the Vietnam war, a sensor called *Black Crow* carried aboard C-130 gunships was able to detect the electromagnetic emanations produced by the ignition system of trucks on the Ho Chi Minh trail, from a distance up to 10 miles [25, 11].

1.1 Related Work

Academic research on compromising electromagnetic emanations started in the mid 1980's and there has been significant recent progresses [28, 1]. The threat related to compromising emanations has been constantly confirmed by practical attacks such as Cathode Ray Tubes (CRT) displays image recovery [34], Liquid Crystal Display (LCD) image recovery [20], secret key disclosure [16], video displays risks [18, 33] or radiations from

FPGAs [24].

Compromising electromagnetic emanations of serial-port cables have been already discussed by Smulders [30] in 1990. PS/2 keyboards still use bi-directional serial communication to transmit the pressed key code to the computer. Hence, some direct compromising electromagnetic emanations might appear. However, the characteristics of the serial line changed since the 90's. The voltage is not 15 volts anymore and the transition times of the signals are much longer (from picoseconds to microseconds).

Since keyboards are often the first input device of a computer system, they have been intensively studied. For instance, the exploitation of visual compromising information leaks such as optical reflections [5] which could be applied to keyboards, the analysis of surveillance video sequences [6] which can be used by an attacker to recover the keystrokes (even with a simple webcam) or the use of the blinking LEDs of the keyboard as a covert channel [21]. Acoustic compromising emanations from keyboards have been studied as well. Asonov and Agrawal [4] discovered that each keystroke produces a unique sound when it is pressed or released and they presented a method to recover typed keystrokes with a microphone. This attack was later improved, see [38, 7]. Even passive timing analysis may be used to recover keystrokes. Song et al. highlighted that the keystroke timing data measured in older SSH implementations [32] may be used to recover encrypted passwords. A risk of compromising emission from keyboards has been postulated by Kuhn and Anderson [20, 17, 2]. They also proposed countermeasures (see US patent [3]). Some unofficial documents on *TEMPEST* [37] often designate keyboards as potential information leaking devices. However, we did not find any experiment or evidence proving or refuting the practical feasibility to remotely eavesdrop keystrokes, especially on modern keyboards.

1.2 Our Contribution

This paper makes the following main contributions:

A Full Spectrum Acquisition Method. To detect compromising electromagnetic emanations a receiver tuned on a specific frequency is generally used. It brings the signal in base band with a limited bandwidth. Therefore, the signal can be demodulated in amplitude (AM) or frequency (FM). This method might not be optimal. Indeed, the signal does not contain the maximal entropy since a significant amount of information is lost. We propose another approach. We acquire the raw signal directly from the antenna and analyze the entire captured electromagnetic spectrum with Short Time Fourier Transform (also known as *Waterfall*) to distill potential compromising emanations.

The Study of Four Different Sources of Information Leakage from Keyboards. To determine if keyboards generate compromising emanations, we measured the electromagnetic radiations emitted when a key is pressed. Due to our improved acquisition method, we discovered several direct and indirect compromising emanations which leak information on the keystrokes. The first technique looks at the emanations of the falling edges (i.e. the transition from a high logic state to a low logic state) from the bi-directional serial cable used in the PS/2 protocol. It can be used to reveal keystrokes with about 1 bit of uncertainty. The second approach uses the same source, but consider the rising and the falling edges of the signal to recover the keystrokes with 0 bits of uncertainty. The third approach is focused on the harmonics emitted by the keyboard to recover the keystrokes with 0 bits of uncertainty. The last approach considers the emanations emitted from the matrix scan routine (used by PS/2, USB and Wireless keyboards) and yields about 2.5 bits of uncertainty per keystroke. This compromising emanation has been previously posited by Kuhn and Anderson [3], although that work provided no detailed analysis.

The Implementation and the Analysis of Four Keystroke Recovery Techniques in Four Different Scenarios. We tested 12 different keyboard models, with PS/2, USB connectors and wireless communication in different setups: a semi-anechoic chamber, a small office, an adjacent office and a flat in a building. We demonstrate that these keyboards are all vulnerable to at least one of the four keystroke recovery techniques in all scenarios. The best attack successfully recovers 95% of the keystrokes at a distance up to 20 meters, even through walls. Because each keyboard has a specific *fingerprint* based on the clock frequency inconsistencies, we can determine the source keyboard of a compromising emanation, even if multiple keyboards from the same model are used at the same time. First, we did the measurements in a semi-anechoic electromagnetic chamber to isolate the device from external noise. Then we confirmed that these compromising emanations are exploitable in real situations.

We conclude that most of modern computer keyboards generate compromising emanations (mainly because of the manufacturer cost pressures in the design). Hence they are not safe to transmit confidential information.

1.3 Structure of the Paper

Section 2 describes some basics on compromising electromagnetic emanations. In Section 3 we present our acquisition method based on Short Time Fourier Transform. In Section 4 we present four different setups used for the measurements, from a semi-anechoic chamber to

real environments. In Section 5 we give the complete procedure used to detect the compromising electromagnetic emanations. Then, we detail the four different techniques. In Section 6, we give the results of our measurements in different setups. In Section 7, we describe some countermeasures to avoid these attacks. In Section 8, we give some extensions and improvements. Finally we conclude.

2 Electromagnetic Emanations

Electromagnetic compatibility (EMC) is the analysis of electromagnetic interferences (EMI) or Radio Frequency Interferences (RFI) related to electric devices. EMC aims at reducing unintentional generation, propagation and reception of electromagnetic energy in electric systems. EMC defines two kinds of unwanted emissions: conductive coupling and radiative coupling. Conductive coupling requires physical support such as electric wires to transmit interferences through the system. Radiative coupling occurs when a part of the internal circuit acts as an antenna and transmits undesired electromagnetic waves. EMC generally distinguishes two types of electromagnetic emissions depending on the kind of the radiation source: differential-mode and common-mode.

Differential-mode radiation is generated by loops formed by components, printed circuit traces, ribbon cables, etc. These loops act as small circular antennas and eventually radiate. These radiations are generally low and do not disturb the whole system. Differential-mode signals are not easily influenced by external radiations. Moreover they can be easily avoided by shielding the system.

Common-mode radiation is the result of undesired internal voltage drops in the circuit which usually appear in the ground loop. Indeed, ground loop currents are due to the unbalanced nature of ordinary transmitting and receiving circuits. Thus, external cables included in the ground loop act as antennas excited by some internal voltages. Because these voltage drops are not intentionally created by the system, it is generally harder to detect and control common-mode radiations than differential-mode radiations.

From the attacker's point of view there are two types of compromising emanations: direct and indirect emanations.

Direct Emanations. In digital devices, data is encoded with logic states, generally described by short burst of square waves with sharp rising and falling edges. During the transition time between two states, electromagnetic waves are eventually emitted at a maximum frequency related to the duration of the rise/fall time. Because these compromising radiations are provided straight by the wire transmitting sensitive data, they are called direct emanations.

Indirect Emanations. Electromagnetic emanations may interact with active electronic components which induce new types of radiations. These unintended emanations manifest themselves as modulations or inter-modulations (phase, amplitude or frequency) or as carrier signals e.g. clock and its harmonics. Non-linear coupling between carrier signals and sensitive data signals, crosstalk, ground pollution or power supply DC pollution may generate compromising modulated signals. These indirect emanations may have better propagation than direct emanations. Hence, they may be captured at a larger range. The prediction of these emanations is extremely difficult. They are generally discovered during compliance tests such as FCC [15], CISPR [10], MIL-STD-461 [22], NACSIM-5000 [37], etc.

3 Electromagnetic Signal Acquisition

Two techniques are generally used to discover compromising electromagnetic emanations.

3.1 Standard Techniques

A method consists in using a spectral analyzer to detect signal carriers. Such a signal can be caught only if the duration of the carrier is significant. This makes compromising emanations composed of peaks difficult to detect with spectral analyzers.

Another method is based on a wide-band receiver tuned on a specific frequency. Signal detection process consists in scanning the whole frequency range of the receiver and to demodulate the signal according to its amplitude modulation (AM) or frequency modulation (FM). When an interesting frequency is discovered, narrow-band antennas and some filters are used to improve the Signal-to-Noise Ratio (SNR) of the compromising emanations. In practice, wide-band receivers such as R-1250 [19] and R-1550 [12] from Dynamic Sciences International, Inc. are used, see [17, 1]. Indeed, these receivers are compliant with secret requirements for the NACSIM-5000 [37] also known as *TEMPEST*. These devices are quite expensive and unfortunately not owned by our lab. Hence, we used a cheaper and open-source solution based on the USRP (Universal Software Radio Peripheral) [14] and the GNU Radio project [35]. The USRP is a device which allows you to create a software radio using any computer with USB port. With different daughterboards, the USRP is able to scan from DC to 2.9 GHz with a sample rate of 64 MS/s at a resolution of 12 bits. The full range on the ADC is 2 volts peak to peak and the input is 50 ohms differential. The GNU

Radio project is a powerful software library used by the USRP to process various modulations (AM, FM, PSK, FSK, etc.) and signal processing constructs (optimized filters, FFT, etc.). Thus, the USRP and the GNU Radio project may act as a wide-band receiver and a spectral analyzer with software-based FFT computation.

3.2 Novel Techniques

Some direct and indirect electromagnetic emanations may stay undetected with standard techniques, especially if the signal is composed of irregular peaks or erratic frequency carriers. Indeed, spectral analyzers need significantly static carrier signals. Similarly, the scanning process of wide-band receivers is not instantaneous and needs a lot of time to cover the whole frequency range. Moreover the demodulation process may hide some interesting compromising emanations.

In this paper, we use a different method to detect compromising electromagnetic emanations of keyboards. First, we obtain the raw signal directly from the antenna instead of a filtered and demodulated signal with limited bandwidth. Then, we compute the Short Time Fourier Transform (STFT), which gives a 3D signal with time, frequency and amplitude.

Modern analog-to-digital converters (ADC) provide very high sampling rates (Giga samples per second). If we connect an ADC directly to a wide-band antenna, we can import the raw sampled signal to a computer and we can use software radio libraries to instantly highlight potentially compromising emanations. The STFT computation of the raw signal reveals the carriers and the peaks even if they are present only for a short time.

Unfortunately there is no solution to transfer the high amount of data to a computer in real time. The data rate is too high for USB 2.0, IEEE 1394, Gigabit Ethernet or Serial ATA (SATA) interfaces. However, with some smart triggers, we can sample only the (small) interesting part of the signal and we store it in a fast access memory. Oscilloscopes provide triggered analog-to-digital converters with fast memory. We used a Tektronix TDS5104 with 1 Mpt memory and a sample rate of 5 GS/s. It can acquire electromagnetic emanations up to 2.5 GHz according to the Nyquist theorem. Moreover, this oscilloscope has antialiasing filters and supports IEEE 488 General Purpose Interface Bus (GPIB) communications. We developed a tool to define some specific triggers (essentially peak detectors) and to export the acquired data to a computer under GNU/Linux over Ethernet. Thus the signal can be processed with the GNU Radio software library and some powerful tools such as Baudline [29] or the GNU project Octave [13]. The advantage of this method is to process the raw signal, which is directly sampled from the antenna without any demodulation. Moreover, all compromising electromagnetic emanations up to a frequency of 2.5 GHz are captured. Thus, with this technique, we are able to highlight compromising emanations quickly and easily. This solution is ideal for very short data burst transmissions used by computer keyboards.

4 Experimental Setup

The objective of this experiment is to observe the existence of compromising emanations of computer keyboards when a key is pressed. Obviously electromagnetic emanations depend on the environment. We defined four different setups.

Setup 1: The Semi-Anechoic Chamber. We used a professional semi-anechoic chamber (7×7 meters). Our aim was not to cancel signal echos but to avoid external electromagnetic pollution (Faraday cage). The antenna was placed up to 5 meters from the keyboard connected to a computer (the maximum distance according to the echo isolation of the room). The tested keyboard was on a one meter high table and the computer (PC tower) was on the ground.

Setup 2: The Office. To give evidence of the feasibility of the attacks with background noise, we measured the compromising emanations of the keyboards in a small office (3×5 meters) with two powered computers and three LCD displays. The electromagnetic background noise was quite important with a cluster of 40 computers 10 meters away from the office, more than 60 powered computers on the same floor and a 802.11n wireless router at less than 3 meters away from the office. The antenna was in the office and moved back through the opened door up to 10 meters away from the keyboard in order to determine the maximum range.

Setup 3: The Adjacent Office. This setup is similar to the office setup but we measured the compromising emanations of the keyboards from an adjacent office through a wall of 15 cm composed of wood and plaster.

Setup 4: The Building. This setup takes place in a flat which is in a building of five floors in the center of a mid-size city. The keyboard was in the fifth floor. We performed measurements with the antenna placed on the same floor first. Then, we moved the antenna as far as the basement (up to 20 meter from the keyboard).

Antennas. Since the compromising emanations were found on frequency bands between 25 MHz and 300 MHz, we used a biconical antenna (50 Ohms VHA 9103 Dipol Balun) to improve the Signal-to-Noise Ratio (SNR). We also tested if these compromising emanations can be captured with a smaller antenna such as a simple loop made of a wire of copper (one meter long).

Keyboards. We picked 12 different keyboard models present in our lab: 7 PS/2 keyboards (Keyboard A1-A7), 2 USB keyboards (Keyboard B1-B2), 2 Laptop keyboards (Keyboard C1-C2) and 1 wireless keyboard (Keyboard D1). They were all bought between 2001 and 2008. We also collected measurements with the keyboard connected to a laptop with battery to avoid possible conductive coupling through the power supply. For obvious security reasons, we do not give the brand name and the model of the tested keyboards.

5 Discovering and Exploiting Emanations

To discover compromising emanations, we placed Keyboard A1 in the semi-anechoic chamber and we used the biconical antenna. A diagram of the experiment is depicted in Figure 1. We acquired the raw signal with the oscilloscope as explained above. Since the memory of the oscilloscope is limited, we have to precisely trigger data acquisition. First, we used the earliest falling edge of the data signal sent when a key is pressed . We physically connected a probe on the data wire of the cable between the keyboard and the computer.

Figure 2 gives the STFT of the captured raw signal when the key E is pressed on an American keyboard. With only one capture we are able to represent the entire spectrum along the full acquisition time. In addition, we have a visual description of all electromagnetic emanations. In particular we clearly see some carriers (vertical lines) and broadband impulses (horizontal lines). The three first techniques are based on these compromising emanations and are detailed in the following sections.

Our objective is to use an electromagnetic trigger, since we normally do not have access to the data wire. The discovered broadband impulses (horizontal lines) can be used as a trigger. Thus, with only an antenna, we are able to trigger the acquisition of the compromising electromagnetic emanations. More details are given below.

Some keyboards do not emit electromagnetic emanations when a key is pressed. But with a different trigger model, based on peak detector as well, we discovered another kind of emission, continuously generated (even if no key is pressed). This is the last technique, detailed in Section 5.4.

5.1 The Falling Edge Transition Technique

To understand how direct compromising emanations may be generated by keyboards, we need to briefly describe the PS/2 communication protocol. According to [9], when a key is pressed, released or held down, the keyboard sends a packet of information known as a *scan code* to the computer. In the default scan code set[1], most of the keys are one-byte long encoded. Some extended keys are two or more bytes long. These codes can be identified by the fact that their first byte is 0xE0. The protocol used to transmit these scan codes is a bi-directional serial communication, based on four wires: Vcc (5 volts), ground, data and clock. For each byte of the scan code, the keyboard pulls down the clock signal at a frequency between 10 KHz and 16.7 KHz for 11 clock cycles. When the clock is low, the state of the signal data is read by the computer. The 11 bits sent correspond to a start bit (0), 8 bits for the scan code of the pressed key (least significant bit first), an odd parity check bit on the byte of the scan code (the bit is set if there is an even number of 1's), and finally a stop bit (1). Figure 3 represents both data and clock signals when the key E is pressed. Note that the scan code is binded to

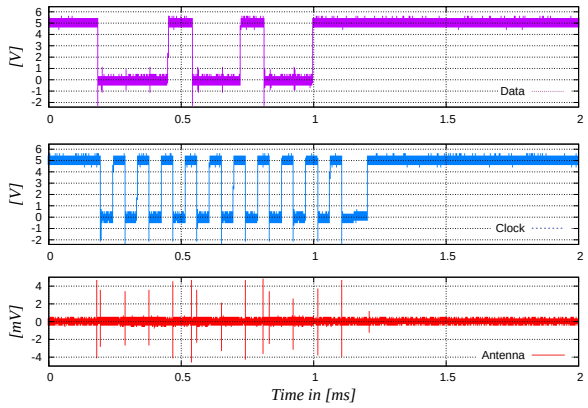

Figure 3: Data, clock and the compromising emanation captured (semi-anechoic chamber, Keyboard A1) with the loop antenna at 5 meters (a wire of copper, one meter long) when the key E (0x24) is pressed. Data signal sends the message: 0 00100100 1 1.

a physical button on the keyboard, it does not represent the character printed on that key. For instance, the scan code of E is 0x24 if we consider the American layout keyboard.

Logic states given by data and clock signals in the keyboard are usually generated by an open collector coupled to a pull-up resistor. The particularity of this system is that the duration of the rising edge is significantly longer (2 μs) than the duration of the falling edge (200 ns). Thus, the compromising emanation of a falling edge should be much more powerful (and with a higher maximum frequency) than the rising edge. This property is known and has been already noticed by Kuhn [17, p.35]. Clock and data signals are identically generated. Hence,

[1] There are three different scan code sets, but the second one is commonly used by default.

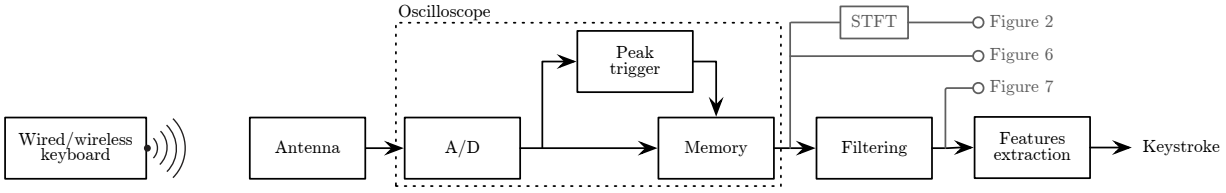

Figure 1: Diagram of our equipment for the experiments.

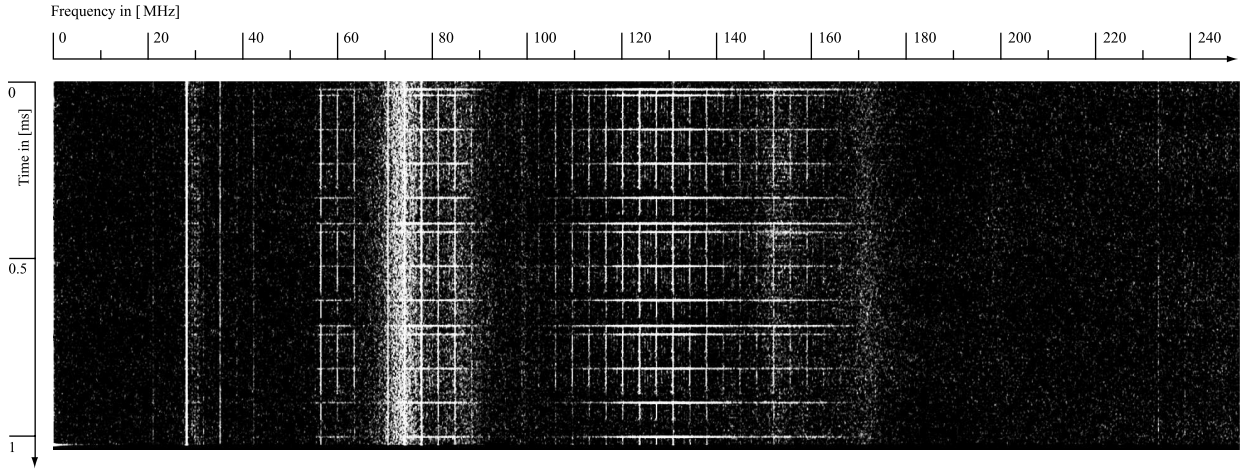

Figure 2: Short Time Fourier Transform (STFT) of the raw signal depicted in Figure 6 (Kaiser windowing of 40, 65536 points)

the compromising emanation detected is the combination of both signals. However (see Figure 3), the edges of the data and the clock lines are not superposed. Thus, they can be easily separated to obtain independent signals.

Since the falling edges of clock signal will always be at the same place, contrary to the falling edges of data signal, we can use them to improve our trigger model. Indeed we consider the detection of a signal based on 11 equidistant falling edges.

Indirect Emanations. If we compare the data signal and the compromising emanation (see Figure 4) we clearly see that the electromagnetic signal is not directly related to the falling edge, as described by Smulders. Indeed, the durations are not equivalent. Thus, the peaks acquired by our antenna seem to be indirectly generated by the falling edges of the combination of clock and data signals. They are probably generated by a peak of current when the transistor is switched. Nevertheless, these emanations, represented by 14 peaks, 11 for the clock signal and 3 for the data signal (see the horizontal lines in Figure 2 or the peaks in Figure 3) partially describe the logic state of the data signal and can be exploited.

Collisions. Because only the falling edges are detected, eventually collisions occur during the keystroke recovery process. For instance, both E (0x24) and G (0x34)

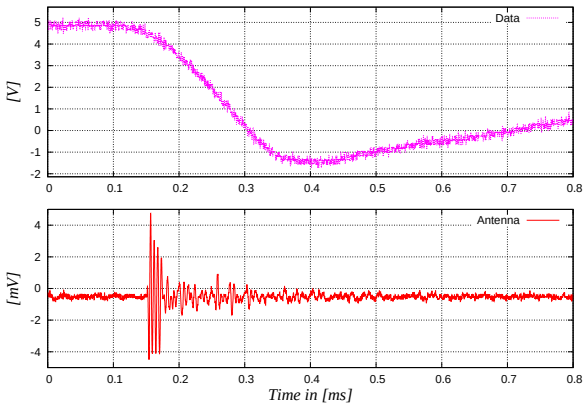

Figure 4: A falling edge of the data signal (upper graph) and the electromagnetic emanation of the keyboard (lower graph). The compromising emission is not directly generated by the data signal such as described by Smulders in [30].

share the same trace if we consider only falling edges. We define the falling edge trace as '2' when both data and clock peaks are detected and '1' when only a clock peak is captured. The letters E (see lower graph in Figure 3) and G may be described by the string `21112112111`.

In Figure 5 we grouped every one byte-long scan code, according to their shared falling edge-based traces.

Trace	Possible Keys
21111111111	<non-US-1>
21111111121	<Release key>
21111111211	F11 KP KP0 SL
21111112111	8 u
21111121111	2 a
21111121211	Caps_Lock
21111211111	F4 ‘
21111211211	- ; KP7
21111212111	5 t
21112111111	F12 F2 F3
21112111121	Alt+SysRq
21112111211	9 Bksp Esc KP6 NL o
21112112111	3 6 e g
21112121111	1 CTRL_L
21112121211	[
21121111111	F5 F7
21121111211	KP- KP2 KP3 KP5 i k
21121112111	b d h j m x
21121121111	SHIFT_L s y
21121121211	’ ENTER]
21121211111	F6 F8
21121211211	/ KP4 l
21121212111	f v
21211111111	F9
21211111211	, KP+ KP. KP9
21211112111	7 c n
21211121111	Alt_L w
21211121211	SHIFT_R \
21211211111	F10 Tab
21211211211	. KP1 p
21211212111	Space r
21212111111	F1
21212111211	0 KP8
21212112111	4 y
21212121111	q
21212121211	=

Figure 5: The one byte-long scan codes classification, according to the falling edges trace for an American keyboard layout.

Even if collisions appear, falling edge traces may be used to reduce the subset of possible transmitted scan codes. Indeed, the average number of potential characters for a falling edge trace is 2.4222 (2.0556 if we consider only alpha-numeric characters and a uniform distribution). For example, an attacker who captured the falling edge-based trace of the word `password` obtains a subset of $3 \cdot 2 \cdot 3 \cdot 3 \cdot 2 \cdot 6 \cdot 2 \cdot 6 = 7776$ potential words, according to Figure 5. Thus, if the objective of the attacker is to recover a secret password, he has significantly reduced the test space (the initial set of $36^8 \approx 2^{41}$ is lowered to 2^{13}). Moreover, if the eavesdropped information concerns an e-mail or a text in English, the plaintext recovery process can be improved by selecting only words contained in a dictionary.

Feature Extraction. The recovery procedure is firstly based on a trigger model, able to detect 11 equidistant peaks transmitted in less than 1 ms. Then, we compute the number of peaks, using a peak-detection algorithm and the GNU Radio library. The feature extraction is based on the number of peaks correlated to the most probable value of the table depicted in Figure 5. The main limitation of the recovery procedure is the ability to trigger this kind of signal.

5.2 The Generalized Transition Technique

The previously described attack is limited to a partial recovery of the keystrokes. This is a significant limitation. We know that between two ’2’ traces, there is exactly one data rising edge. If we are able to detect this transition we can fully recover the keystrokes.

To highlight potential compromising emanations on the data rising edge, we use a software band-pass filter to isolate the frequencies of the broadband impulses (e.g. 105 MHz to 165 MHz of the raw signal in Figure 2). Figure 7 corresponds to the filtered version of the raw time-domain signal represented in Figure 6. We remark

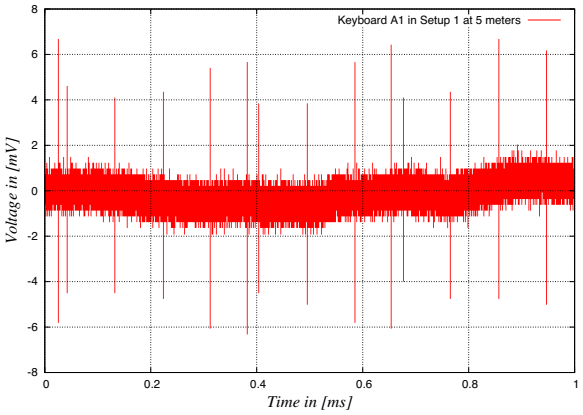

Figure 6: Raw signal (Keyboard A1, Setup 1 at 5 meters with the biconical antenna) when the key E is pressed.

that the filtering process significantly improves the SNR. Thus, the peak detection algorithm is much more efficient.

Furthermore, we notice that the energy of the peaks of the clock falling edges is not constant. Empirically, clock peaks have more energy when the state of data signal is high. Indeed, the data signal pull-up resistor is open. When the clock signal is pulled down, the surplus of energy creates a stronger peak. Hence, the peaks generated by the falling edge of the clock signal intrinsically encode the logic state of the data signal. Because

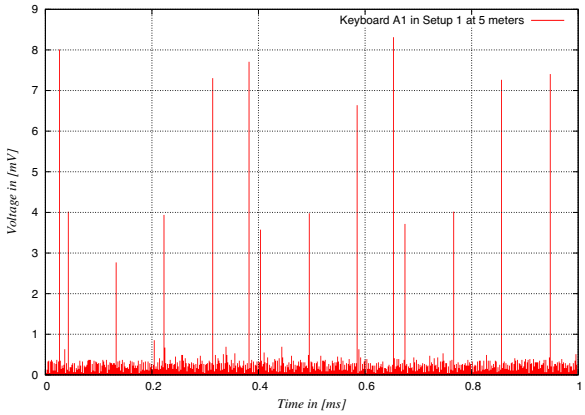

Figure 7: Band-pass (105-165MHz) filtered signal of Figure 6.

there is exactly one rising edge between two falling edge traces of '2', we simply consider the highest clock peak as the rising edge data transition. For example in Figure 7, the rising edge data transitions are respectively at peaks 5 and 9. Thus, the complete data signal is 0010 0100 which corresponds to 0x24 (E). Thus, we manage to completely recover the keystrokes. Note that the band-pass filter improves the previous attack as well. However, the computation cost prevents real time keystroke recovery without hardware accelerated filters.

Feature Extraction. The recovery procedure is firstly based on the same trigger model described previously (11 equidistant peaks detected in less than 1 ms). Then, we filter the signal to consider only the frequency bands containing the peak impulses. The feature extraction is based on the detected peaks. First, we define the threshold between a high peak and a low peak thanks to the two first peaks. Indeed, because we know that data and clock are pulled down, the first one corresponds to a state where clock is high and data is low and the second one describes the state where both signals are low. Then, we determine the potential (and colliding) keystrokes with Figure 5. In our example, it corresponds to the keys 3,6,E,G. Then, we select some bits which differentiate these keys. According to their scan code 3=0x26, 6=0x36, E=0x24, G=0x34 we check the state of the peaks 4 and 8 in Figure 7, which correspond to respectively the second and the fifth bit of the scan codes. Because they are both low, we conclude that the transmitted key is E.

5.3 The Modulation Technique

Figure 2 highlights some carriers with harmonics (vertical lines between 116 MHz and 147 MHz). These compromising electromagnetic emissions come from unintentional emanations such as radiations emitted by the clock, non-linear elements, crosstalk, ground pollution, etc. Determining theoretically the reasons of these compromising radiations is a very complex task. Thus, we can only sketch some probable causes. The source of these harmonics corresponds to a carrier of approximately 4 MHz which is very likely the internal clock of the microcontroller inside the keyboard. Interestingly, if we correlate these harmonics with both clock and data signals, we clearly see modulated signals (in amplitude and frequency) which fully describe the state of both clock and data signals, see Figure 8. This means that the scan code can be completely recovered from these harmonics.

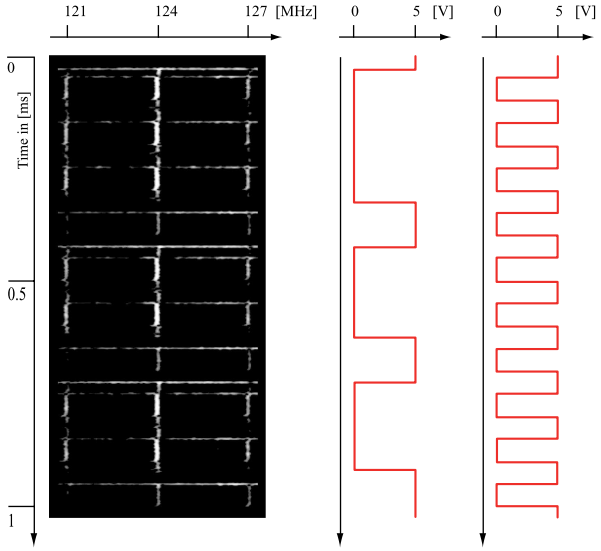

Figure 8: The amplitude and frequency modulations of the harmonic at 124 MHz correlated to both data and clock signals (Keyboard A1, semi-anechoic chamber at 5 meters).

Note that even if some strong electromagnetic interferences emerge, the attacker may choose non-jammed harmonics to obtain a clear signal. It is even possible to superpose them to improve the SNR. Compared to the previous techniques, the carrier-based modulation is much more interesting for distant reception. Indeed, AM and FM transmissions are generally less disrupted by noise and obstacles such as walls, floors, etc. Moreover this technique is able to fully recover the keystrokes. These indirect emanations – which have no formal explanation, but are probably based on crosstalk with the ground, the internal clock of the microcontroller, data and clock signals – let the attacker recover the keystrokes of a keyboard.

This experiment shows that cheap devices such as keyboards may radiate indirect emanations, which are much

more compromising than direct emanations. Even if the SNR is smaller, the use of a frequency modulation significantly improves the eavesdropping range. Moreover, the attacker may avoid some noisy frequency bands by selecting only the clearest harmonics. Furthermore, indirect emanations completely describe both clock and data signals.

Feature Extraction. The feature extraction is based on the demodulation in frequency and amplitude of the captured signal centered on the strongest harmonic. In our example and according to Figure 8 the carrier corresponds to 124 MHz. We used the GNU Radio library to demodulate the signal. However, we still need to use the trigger model based on peak detector since the memory of the oscilloscope is limited. Another option is to directly capture the signal with the USRP. Indeed, the lower but continuous sampling rate of the USRP is sufficient to recover the keystrokes. Unfortunately, the sensitivity of the USRP is weaker than the oscilloscope and the eavesdropping range is limited to less than 2 meters in the semi-anechoic chamber.

5.4 The Matrix Scan Technique

The techniques described above are related to the use of PS/2 and some laptop keyboards. However, new keyboards tend to use USB or wireless communication. In this section, we present another compromising emanation which concerns all keyboard types: PS/2, USB, Notebooks and even wireless keyboards. This attack was previously postulated by Kuhn and Anderson [20] but no practical data has appeared so far in the open literature.

Almost all keyboards share the same pressed key detection routine. A major technical constraint is to consider a key as pressed if the button is pushed for 10 ms, see US Patent [31]. Thus every pressed key should be detected within this time delay. From the manufacturer's point of view, there is another main constraint: the cost of the device. A naive solution to detect pressed keys is to poll each key in a row. This solution is clearly not optimal since it requires a large scan loop routine and thus longer delays. Moreover important leads (i.e. one circuit for each key) increase the cost of the device.

A smart solution [31] is to arrange the keys in a *matrix*. The keyboard controller, often a 8-bit processor, parses columns one-by-one and recovers the state of 8 keys at once. This *matrix scan* process can be described as 192 keys (some keys may not be used, for instance modern keyboards use 104/105 keys) arranged in 24 columns and 8 rows. Columns are connected to a driver chip while rows are connected to a detector chip. Keys are placed at the intersection of columns and rows. Each key is an analog switch between a column and a row. The keyboard controller pulses each column through the driver (using the address bus and the strobe signal). The detector measures the states of the 8 rows. Note that a row is connected to 24 keys, but only one may be active, the one selected by the driver. Suppose we pressed the key corresponding to column 3 and row 5. The controller pulses columns . . ., 22, 23, 24, 1, 2 with no key event. Now, the controller pulses column 3. Row 5, which corresponds to the pressed key, is detected. The keyboard starts a subroutine to transmit the scan code of the key to the computer. This subroutine takes some time. Thus, the next column pulse sent by the scan routine is delayed.

Columns in the matrix are long leads since they connect generally 8 keys. According to [31], these columns are continuously pulsed one-by-one for at least 3μs. Thus, these leads may act as an antenna and generate electromagnetic emanations. If an attacker is able to capture these emanations, he can easily recover the column of the pressed key. Indeed, the following pulse will be delayed.

To figure out if these emanations can be captured, we picked Keyboard A6 and acquired the signal being one meter from the keyboard in the semi-anechoic chamber with a simple one meter long wire of copper as antenna. Figure 9 gives the repeated peak burst continuously emitted by the keyboard. Figure 10 shows the zoomed compromising emanations when the key C resp. key H is pressed.

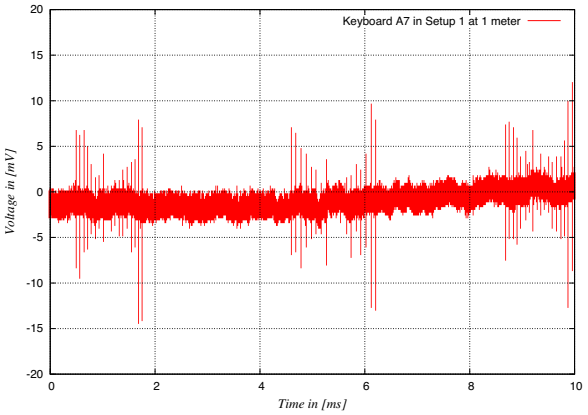

Figure 9: A large view of compromising emanations exploited by the Matrix Scan Technique, (Keyboard A7, semi-anechoic chamber at 1 meter).

The key matrix arrangement may vary, depending on the manufacturer and the keyboard model. We dismantled a keyboard and analyzed the key circuit layout to retrieve the matrix key specifications. The right part of the keyboard layout is depicted on Figure 11. We clearly identify a column (black) and fours rows.

Figure 12 represents the groups of alphanumeric scan codes according to their indirect compromising emana-

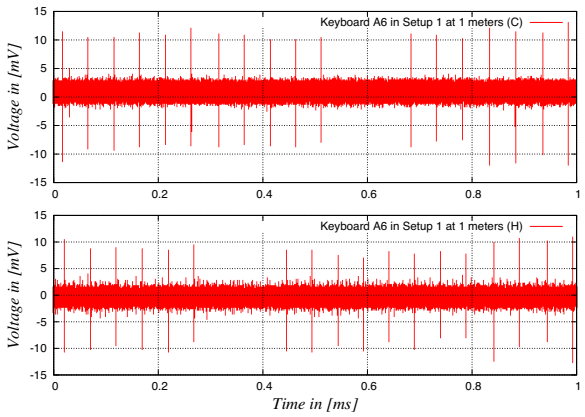

Figure 10: The matrix scan emanations for the letters C and H (Keyboard A6, Setup 1 at 1 meter).

tions (or column number) for Keyboard A6. We describe each electromagnetic signal as a number corresponding to the delayed peak. For example, in Figure 10, the key C is described as 12 and the key H as 7.

Even if this signal does not fully describe the pressed key, it still gives partial information on the transmitted scan code, i.e. the column number. So, as described in the Falling Edge Transition Technique, collisions occurs between key codes. Note that this attack is less efficient than the first one since it has (for this specific keyboard) in average 5.14286 potential key codes for a keystroke (alpha-numeric only). However, an exhaustive search on the subset is still a major improvement.

Note that the matrix scan routine loops continuously. When no key is pressed, we still have a signal composed of multiple equidistant peaks. These emanations may be used to remotely detect the presence of powered computers.

Concerning wireless keyboards, the wireless data burst transmission can be used as an electromagnetic trigger to detect exactly when a key is pressed, while the matrix scan emanations are used to determine the column it belongs to. Moreover the ground between the keyboard and the computer is obviously not shared, thus the compromising electromagnetic emanations are stronger than those emitted by wired keyboards. Note that we do not consider the security of the wireless communication protocol. Some wireless keyboards use a weakly or not encrypted channel to communicate with the computer, see [8, 23].

Feature Extraction. To partially recover keystrokes, we continuously monitor the compromising emanations of the matrix scan routine with a specific trigger model. According to Figure 12 the six first peaks are always present, as well as the last three peaks. Indeed, these peaks are never missing (or delayed). Thus, we use this

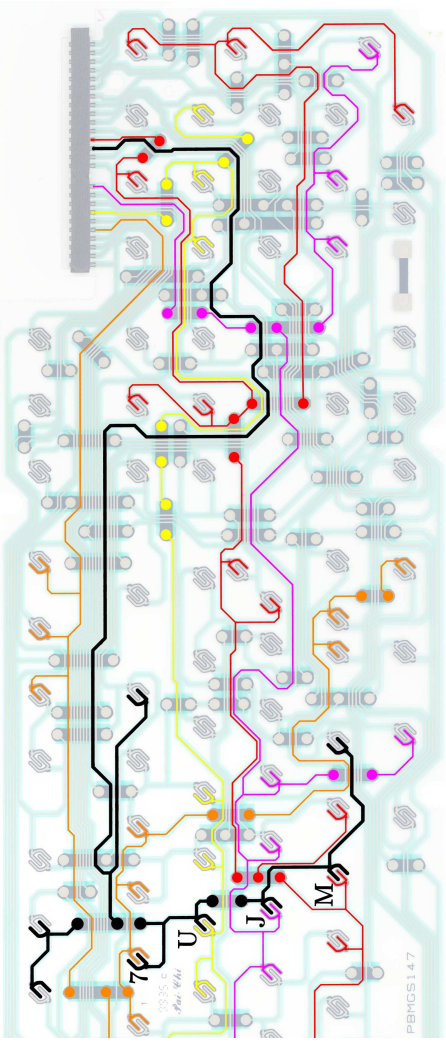

Figure 11: Scan matrix polls columns one-by-one. We are able to deduce on which column the pressed key belongs to. On this keyboard, there will be a collision between keystrokes 7, U, J, M, and others non alpha-numeric keys such as F6, F7, ^, and the dot.

Peak trace	Possible Keys
7	6 7 h J M N U Y
8	4 5 B F G R T V
9	Backspace ENTER
10	9 L O
11	0 P
12	3 8 C D E I K
13	1 2 S W X Z
14	SPACE A Q

Figure 12: The alpha-numeric key classification according to the key scanning routing compromising emanations (Keyboard A6 with American layout).

fixed pattern to define a trigger model. Moreover, the matrix scan continuously radiates compromising emanations since the key is pressed. When a keystroke subset is detected, we acquire multiple samples until another pattern is detected. Therefore, we pick the most often captured pattern.

5.5 Distinguishing Keystrokes from Multiple Keyboards

The falling edge-based traces are distinguishable depending on the keyboard model. Indeed, according to the frequency of the peaks, the clock frequency inconsistencies, the duration between clock and data falling edges, we are able to deduce a specific *fingerprint* for every keyboard. When multiple keyboards are radiating at the same time, we are able to identify and differentiate them. For example, we measured a clock frequency of 12.751 KHz when a key was pressed on a keyboard and the clock frequency was 13.752 KHz when a key was pressed on another keyboard. Thus, when an emanation is captured, we measure the time between two falling edges of the clock and then we deduce if the scan code comes from first or the second keyboard. In practice, we were able to differentiate all the keyboards we tested, even if the brand and the model were equivalent.

This method can be applied to the Falling Edge Transition Technique, the Generalized Transition Technique and the Modulation Technique since they rely on the same kind of signal. The distinguishing process for the Modulation Technique can even be improved by using the clock frequency inconsistencies of the microcontroller as another identifier. For the Matrix Scan Technique, the compromising electromagnetic emanation burst emitted every 2.5 ms (see Figure 9) can be used as a synchronization signal to identify a specific keyboard emission among multiple keyboards. Additionally, the duration between the scan peaks is different, depending on the keyboard model. Thus, it may be used to identify the source keyboard. However, the continuous emission significantly deteriorates the identification process.

Another physical element can be used to distinguish keystrokes from multiple keyboards. For the three first techniques, the broadband impulse range is determined by the length of the keyboard cable, which forms a resonant dipole. Thus, we can use this particularity to identify the source of a compromising emanation. An interesting remark is that the length of the wire connecting the computer to the keyboard is shorter in notebooks. The frequency band of the compromising emanation is higher and the SNR smaller. The Matrix Scan Technique emanates at a higher frequency since the leads of the keyboard layout, acting as an antenna, are shorter.

6 Evaluation in Different Environments

While we have demonstrated techniques that should be able to extract information from keyboard emanations, we have not studied how they are affected by different environments. In this section we study the accuracy of our approaches in all the environments described. Our analysis indicates that keyboard emanations are indeed problematic in practical scenarios.

Evaluating the emission risks of these attacks is not an easy task. Indeed, these results highly depend on the antenna, the trigger model, pass-band filters, peak detection, etc. Moreover, we used trivial filtering processes and basic signal processing techniques. These methods could be significantly improved using beamforming, smart antennas, better filters and complex triggers. In addition, measurements in real environments but the semi-anechoic chamber were subject to massive change, depending on the electromagnetic interferences. Figure 13 gives the list of vulnerable keyboards in all setups, according to the four techniques previously described. Note that all the tested keyboards (PS/2, USB, wireless and laptop) are vulnerable to at least one of these attacks. First, we present the measurements in Setup 1 (semi-anechoic chamber) to guarantee some stable results.

Keyboard	Type	FETT	GTT	MT	MST
A1	PS/2	✓	✓	✓	✓
A2	PS/2	✓	✓		✓
A3	PS/2	✓	✓	✓	✓
A4	PS/2	✓	✓	✓	
A5	PS/2	✓	✓	✓	
A6	PS/2	✓	✓		✓
A7	PS/2	✓			✓
B1	USB				✓
B2	USB				✓
C1	LT	✓	✓		✓
C2	LT				✓
D1	Wi				✓

Figure 13: The vulnerability of the tested keyboards according to the Falling Edge Transition Technique (FETT), the Generalized Transition Technique (GTT), the Modulation Technique (MT) and the Matrix Scan Technique (MST).

6.1 Results in the Semi-Anechoic Chamber

We consider an attack as successful when we are able to correctly recover more than 95% of more than 500 keystrokes. The Falling Edge Transition Technique, the Generalized Transition Technique and the Modulation Technique are successful in the semi-anechoic chamber

for all vulnerable keyboards. This means that we can recover the keystrokes (fully or partially) to at least 5 meters (the maximum distance inside the semi-anechoic chamber). However, the Matrix Scan Technique is limited to a range of 2 to 5 meters, depending on the keyboard. Figure 14 represents the probability of success of the Matrix Scan Technique according to the distance between the tested keyboard and the antenna.

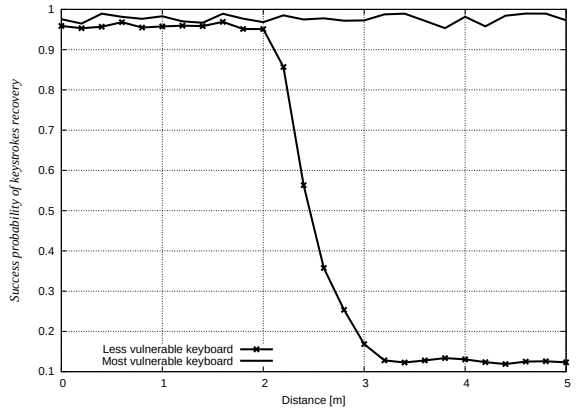

Figure 14: The success probability of the Matrix Scan Technique in the semi-anechoic chamber according to the distance.

We notice that the transition between a successful and a missed attack is fast. Indeed, The correctness of the recovery process is based on the trigger of the oscilloscope. If a peak is not detected, the captured signal is incomplete and the recovered keystroke is wrong. Thus, under a SNR of 6 dB there is nearly no chance to successfully detect the peaks. The SNR is computed according to the average value of the peaks in volts divided by the RMS of the noise in volts.

Considering 6 dB of SNR as a minimum, we are able to estimate the theoretical maximum distance to successfully recover the keystrokes for all techniques in the semi-anechoic chamber. Figure 15 gives the estimated maximum distance range according to the weakest and the strongest keyboard.

In Figure 16 the upper graph gives the SNR of the Falling Edge Transition Technique and the Generalized Transition Technique on Keyboard A1 from 1 meter to 5 meters. The middle graph details the SNR (in dB) of the strongest frequency carrier of the Modulation Technique for the same keyboard. Thus, we can estimate the maximum range of these attacks according to their SNR. The lower graph gives the SNR of the Matrix Scan Technique for the same keyboard. All the measurements were collected in the semi-anechoic chamber.

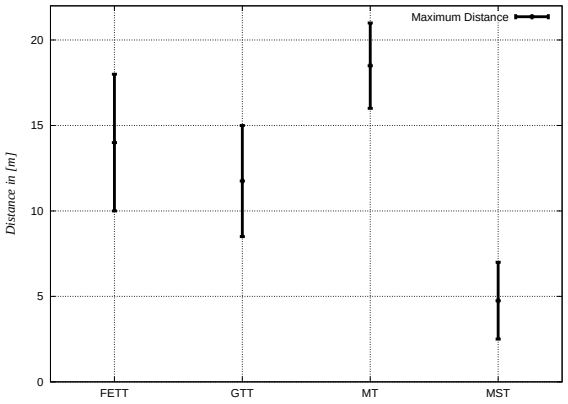

Figure 15: The theoretically estimated maximum distance range to successfully recover 95% of the keystroke according the four techniques in the semi-anechoic chamber, from the less vulnerable to the most vulnerable keyboard.

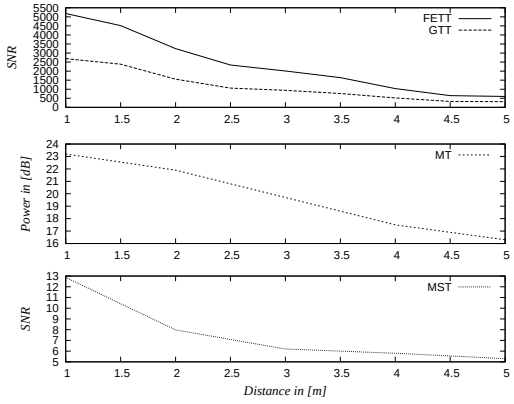

Figure 16: Signal-to-Noise ratio of the peaks [V] / RMS of the noise [V] for the Falling Edge Transition Technique and the Generalized Transition Technique (upper graph). SNR [dB] of the compromising carrier of the Modulation Technique (middle graph). SNR of the peaks [V] / RMS of the noise [V] for Matrix Scan Technique (lower graph).

6.2 Results in Practical Environments

The second phase is to test these techniques in some practical environments. The main difference is the presence of a strong electromagnetic background noise. However, all the techniques remain applicable.

Setup 2: The Office. Figure 17 gives the probability of success of the Generalized Transition Technique on Keyboard A1 measured in the office according to the distance between the antenna and the keyboard. We notice that the sharp transition is present as well when the SNR of the peaks falls under 6 dB. The maximum range of this at-

tack is between 3 and 7.5 meters depending on the tested keyboard. Note that these values were unstable due to a changing background noise. They correspond to an average on multiple measurements.

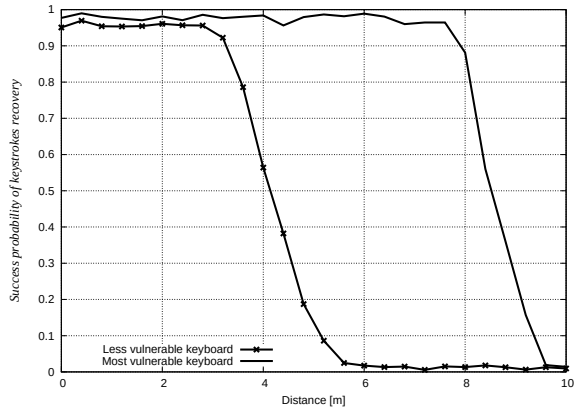

Figure 17: The success probability of the Generalized Transition Technique in the office, according to the distance between the keyboard and the antenna (biconical).

The Modulation Technique is based on a signal carrier. The SNR of this carrier should determine the range of the attack. However, we obtained better results with the same trigger model used in the Falling Edge Transition Technique and the Generalized Transition Technique than one based on the carrier signal only.

Because the Matrix Scan Technique is related to the detection of the peaks, we noticed the same attenuation when the SNR falls under 6 dB. Figure 18 gives the maximum range for the four techniques measured in the office.

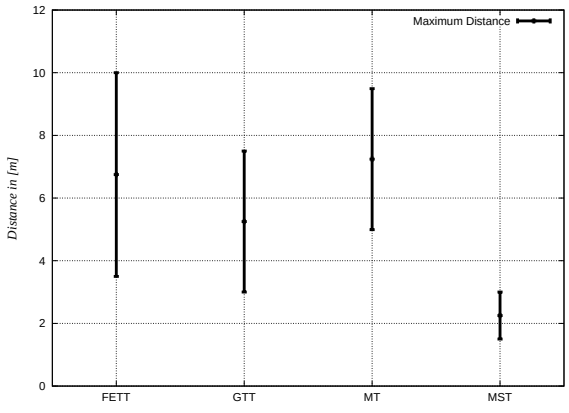

Figure 18: Maximum distance ranges, from the least vulnerable keyboard to the most vulnerable keyboard, to successfully recover 95% of the keystroke according to the techniques (in the office with the biconical antenna).

Setup 3: The Adjacent Office. Results on this setup are basically the same as the previous setup (the office), except that the wall made of plaster and wood removes 3 dB to the SNR.

Setup 4: The Building. We notice some unexpected results in this setup. Indeed, we are able to capture the signal and successfully recover the keystroke with a probability higher than 95% 20 meters away from the keyboard (i.e. the largest distance inside the building). Sometimes the environment can be extremely favorable to the eavesdropping process. For example, metallic structures such as pipes or electric wires may act as antennas and significantly improve the eavesdropping range. In this case, the compromising emanations are carried by the shared ground of the electric line. Thus, the range is defined by the distance between the keyboard and the shared ground and the distance between the shared ground and the antenna. Note that the Matrix Scan Technique is easily disrupted by a noisy shared ground, since the trigger model is more complicated and the emanations weaker. For this technique, we were only able to successfully capture compromising emanations when the keyboard is at less than one meter away from the shared ground. This setup is interesting because it corresponds to a practical scenario where the eavesdropper is placed in the basement of a building and tries to recover the keystrokes of a keyboard at the fifth floor. Unfortunately, it was impossible to provide stable measurements since they highly depend on the environment. We noticed that the main (metallic) water pipe of the building acts as an antenna as well and can be used in place of the shared ground. Furthermore, this *antenna* is less polluted by electronic devices.

Perfect Trigger. We tried the same experiment in the office, but the background noise was too strong. Indeed, we were not able to successfully detect the compromising emissions. However, with a probe physically connected to the data wire, we correctly triggered the emanations. Indeed, the electromagnetic compromising emissions are present in the shared ground. The limitation concerns only the trigger. All the techniques were applicable on the whole floor (about 20 meters) with the keyboard one meter away from the shared ground.

Obviously, you can directly connect the oscilloscope to the shared ground of the building to eavesdrop the keystrokes. Note that an old PC tower used to supply tested keyboards carries the compromising emanations directly through the shared ground. But, this is out of the scope of this paper since we focused our research on electromagnetic emanations only. To avoid such conductive coupling through power supply, we performed our measurements with the keyboards connected to a battery powered laptop.

7 Countermeasures

In this Section, we suggest some possible countermeasures to protect keyboards against the four attacks.

The first solution to avoid the compromising emanations seems trivial. We should shield the keyboard to significantly reduce all electromagnetic radiations. Many elements inside the keyboard may generate emanations: the internal electronic components of the keyboard, the communication cable, and the components of the motherboard inside the computer. Thus, to eliminate these emanations, we have to shield the whole keyboard, the cable, and a part of the motherboard of the computer. We discussed with a manufacturer and he pointed out that the price to shield the entire keyboard will at least double the price of the device. This solution may not be applicable for cost reasons. One can find on the market some keyboards which respect the NATO SDIP-27 standard. All these documents remain classified and no information is available on the actual emission limit or detailed measurement procedures. Another solution is to protect the room where vulnerable keyboards are used. For example, the room can be shielded or a secure physical perimeter can be defined around the room, for instance 100 meters. Attacks 1, 2 and 3 are directly related to the PS/2 protocol. One solution to avoid unintended information leaks is to encrypt the bi-directional serial communication, see [3]. In modern keyboards, one chip contains the controller, the driver, the detector, and the communication interface. So, the encryption may be computed in this chip and no direct compromising emanations related to the serial communication will appear. Attack 4 is related to the scan matrix loop. A solution could be to design a new scanning process algorithm. Even if keyboards still use scan matrix loop routine, there exists some applicable solutions. As described by Anderson and Kuhn [3], the loop routine can be randomized. Actually columns are scanned in the incremental order 1, 2, 3, . . ., 23, 24, but it seems possible to change the order randomly. Moreover, we can add some random delays during the scanning loop process to obfuscate the execution of the subroutine. Both solutions do not avoid electromagnetic emanations, but makes the keystrokes recovery process theoretically impossible. Paavilainen [27] also proposed a solution. It consists in high-frequency filtering matrix signals before they are fed into the keyboard. This will significantly limits compromising electromagnetic emanations.

8 Extensions

Our study has shown that electromagnetic emanations of modern wired and wireless keyboards may be exploited from a distance to passively recover keystrokes. In this section, we detail some extensions and remarks.

The main limitation of these attacks concerns the trigger of the data acquisition. This can be improved with an independent process, using specific filters between the antenna and the ADC. Additionally, other compromising emanations such as the sound of the pressed key could be used as trigger. Furthermore, modern techniques such as beamforming could significantly improve the noise filtering.

Another improvement would be to simultaneously leverage multiple techniques. For keyboards that are vulnerable to more than one technique, we could correlate the results of the different techniques to reduce uncertainty in our guesses.

Another extension would be to accelerate these attacks with dedicated hardware. Indeed, the acquisition time (i.e. the transfer of the data to a computer), the filtering and decoding processes take time (about two seconds per keystroke). With dedicated system and hardware-based computation such as FPGAs, the acquisition, filtering and decoding processes can obviously be instantaneous (e.g. less than the minimum time between two keystrokes). However, the keystrokes distinguishing process when multiple keyboards are radiating is still difficult to implement especially for the Matrix Scan Technique, since the acquisition process should be continuous.

We spend time experimenting with different types of antennas and analog-to-digital converters. In particular, we used the USRP and the GNU Radio library to avoid the need of an oscilloscope and to obtain a portable version of the Modulation Technique. Indeed, we can hide the USRP with battery and a laptop in a bag, the antenna can be replaced by a simple wire of copper (one meter long) which is taped on the attacker's body hidden under his clothes. With this transportable setup, we are able to recover keystrokes from vulnerable keyboards stealthily. However the eavesdropping range is less than two meters.

9 Conclusion

We have provided evidence that modern keyboards radiate compromising electromagnetic emanations. The four techniques presented in this paper prove that these inexpensive devices are generally not sufficiently protected against compromising emanations. Additionally, we show that these emanations can be captured with relatively inexpensive equipment and keystrokes are recovered not only in the semi-anechoic chamber but in some practical environments as well.

The consequences of these attacks is that compromising electromagnetic emanations of keyboards still represent a security risk. PS/2, USB laptop and wireless

keyboards are vulnerable. Moreover, there is no software patch to avoid these attacks. We have to replace the hardware to obtain safe devices. Due to cost pressure in the design, manufacturers may not systematically protect keyboards. However, some (expensive) secure keyboards already exist but they are mainly bought by military organizations or governments.

The discovery of these attacks was directly related to our method based on the analysis of the entire spectrum and the computation of Short Time Fourier Transform. This technique has some pros such as the human-based visual detection of compromising emanations, the large spectrum bandwidth, the use of the raw signal without RF front-ends and the post-demodulation using software libraries. The cons are the limited memory and the difficulty to obtain efficient triggers. However, for short data bursts, this solution seems relevant.

Future works should consider similar devices, such as keypads used in cash dispensers (ATM), mobile phone keypads, digicodes, printers, wireless routers etc. Another major point is to avoid the use of a peak detection algorithm since it is the main limitation of these attacks. The algorithms of the feature extractions could be improved as well. The correlation of these attacks with non-electromagnetic compromising emanation attacks such as optical, acoustic or time attacks could significantly improve the keystroke recovery process.

We discussed with a few agencies interested by our videos [36]. They confirmed that this kind of attack has been practically done since the 1980's on old computer keyboards, with sharp transitions and high voltages. However, they were not aware on the feasibility of these attacks on modern keyboards. Some of these attacks were not known to them.

Acknowledgments

We gratefully thank Pierre Zweiacker and Farhad Rachidi from the Power Systems Laboratory (EPFL) for the semi-anechoic chamber and their precious advices. We also thank Eric Augé, Lucas Ballard, David Jilli, Markus Kuhn, Eric Olson and the anonymous reviewers for their extremely constructive suggestions and comments.

References

[1] AGRAWAL, D., ARCHAMBEAULT, B., RAO, J. R., AND ROHATGI, P. The EM Side-Channel(s). In *CHES* (2002), B. S. K. Jr., Çetin Kaya Koç, and C. Paar, Eds., vol. 2523 of *Lecture Notes in Computer Science*, Springer, pp. 29–45.

[2] ANDERSON, R. J., AND KUHN, M. G. Soft Tempest – An Opportunity for NATO. *Protecting NATO Information Systems in the 21st Century, Washington, DC, Oct 25-26* (1999).

[3] ANDERSON, R. J., AND KUHN, M. G. Lost Cost Countermeasures Against Compromising Electromagnetic Computer Emanations. United States Patent US 6,721,324 B1, 2004.

[4] ASONOV, D., AND AGRAWAL, R. Keyboard Acoustic Emanations. In *IEEE Symposium on Security and Privacy* (2004), IEEE Computer Society, pp. 3–11.

[5] BACKES, M., DÜRMUTH, M., AND UNRUH, D. Compromising reflections-or-how to read lcd monitors around the corner. In *IEEE Symposium on Security and Privacy* (2008), P. McDaniel and A. Rubin, Eds., IEEE Computer Society, pp. 158–169.

[6] BALZAROTTI, D., COVA, M., AND VIGNA, G. Clearshot: Eavesdropping on keyboard input from video. In *IEEE Symposium on Security and Privacy* (2008), P. McDaniel and A. Rubin, Eds., IEEE Computer Society, pp. 170–183.

[7] BERGER, Y., WOOL, A., AND YEREDOR, A. Dictionary attacks using keyboard acoustic emanations. In *ACM Conference on Computer and Communications Security* (2006), A. Juels, R. N. Wright, and S. D. C. di Vimercati, Eds., ACM, pp. 245–254.

[8] BRANDT, A. Privacy Watch: Wireless Keyboards that Blab, January 2003. http://www.pcworld.com/article/108712/privacy_watch_wireless_keyboards_that_blab.html.

[9] CHAPWESKE, A. The PS/2 Mouse/Keyboard Protocol. http://www.computer-engineering.org/.

[10] CISPR. The International Special Commitee on Radio Interference. http://www.iec.ch/zone/emc/emc_cis.htm.

[11] CORRELL, J. T. Igloo White - Air Force Magazine Online 87, 2004.

[12] DYNAMIC SCIENCES INTERNATIONAL, INC. R-1550a tempest receiver, 2008. http://www.dynamicsciences.com/client/show_product/33.

[13] EATSON, J. GNU Octave, 2008. http://www.gnu.org/software/octave/.

[14] ETTUS, M. The Universal Software Radio Peripheral or USRP, 2008. http://www.ettus.com/.

[15] FCC. Federal Communications Commission. http://www.fcc.gov.

[16] GANDOLFI, K., MOURTEL, C., AND OLIVIER, F. Electromagnetic analysis: Concrete results. In *CHES* (2001), Çetin Kaya Koç, D. Naccache, and C. Paar, Eds., vol. 2162 of *Lecture Notes in Computer Science*, Springer, pp. 251–261.

[17] KUHN, M. G. Compromising Emanations: Eavesdropping risks of Computer Displays. *Technical Report UCAM-CL-TR-577* (2003).

[18] KUHN, M. G. Security limits for compromising emanations. In *CHES* (2005), J. R. Rao and B. Sunar, Eds., vol. 3659 of *Lecture Notes in Computer Science*, Springer, pp. 265–279.

[19] KUHN, M. G. Dynamic Sciences R-1250 Receiver, 2008. http://www.cl.cam.ac.uk/ mgk25/r1250/.

[20] KUHN, M. G., AND ANDERSON, R. J. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations. In *Information Hiding* (1998), D. Aucsmith, Ed., vol. 1525 of *Lecture Notes in Computer Science*, Springer, pp. 124–142.

[21] LOUGHRY, J., AND UMPHRESS, D. A. Information leakage from optical emanations. *ACM Trans. Inf. Syst. Secur. 5*, 3 (2002), 262–289.

[22] MIL-STD-461. Electromagnetic Interference Characteristics Requirements for Equipment. https://acc.dau.mil/ CommunityBrowser.aspx?id=122817.

[23] MOSER, M., AND SCHRODEL, P. 27MHz Wireless Keyboard Analaysis Report, 2005. http://www.blackhat.com/presentations/bh-dc-08/ Moser/Whitepaper/bh-dc-08-moser-WP.pdf.

[24] MULDER, E. D., ÖRS, S. B., PRENEEL, B., AND VERBAUWHEDE, I. Differential power and electromagnetic attacks on a FPGA implementation of elliptic curve cryptosystems. *Computers & Electrical Engineering 33*, 5-6 (2007), 367–382.

[25] NALTY, B. C. *The war against trucks: aerial interdiction in southern Laos, 1968-1972*. Air Force History and Museums Program, United States Air Force, 2005.

[26] NATIONAL SECURITY AGENCY. TEMPEST: A Signal Problem, 2007. http://www.nsa.gov/public_info/_files/ cryptologic_spectrum/tempest.pdf.

[27] PAAVILAINEN, R. Method and device for signal protection. United States Patent US 7,356,626 B2, 2008.

[28] QUISQUATER, J.-J., AND SAMYDE, D. Electromagnetic analysis (ema): Measures and countermeasures for smart cards. In *E-smart* (2001), I. Attali and T. P. Jensen, Eds., vol. 2140 of *Lecture Notes in Computer Science*, Springer, pp. 200–210.

[29] SIGBLIPS DSP ENGINEERING. Baudline, 2008. http://www.baudline.com.

[30] SMULDERS, P. The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables. *Computers and Security 9*, 1 (1990), 53–58.

[31] SONDERMAN, E. L., AND DAVIS, W. Z. Scan-controlled keyboard. United States Patent US 4,277,780, 1981.

[32] SONG, D. X., WAGNER, D., AND TIAN, X. Timing analysis of keystrokes and timing attacks on ssh. In *SSYM'01: Proceedings of the 10th conference on USENIX Security Symposium* (Berkeley, CA, USA, 2001), USENIX Association, pp. 25–25.

[33] TANAKA, H. Information leakage via electromagnetic emanations and evaluation of tempest countermeasures. In *ICISS* (2007), P. D. McDaniel and S. K. Gupta, Eds., vol. 4812 of *Lecture Notes in Computer Science*, Springer, pp. 167–179.

[34] VAN ECK, W. Electromagnetic radiation from video display units: an eavesdropping risk? *Comput. Secur. 4*, 4 (1985), 269–286.

[35] VARIOUS AUTHORS. The GNU Software Radio, 2008. http://www.gnuradio.org/.

[36] VUAGNOUX, M., AND PASINI, S. Videos of the Compromising Electromagnetic Emanations of Wired Keyboards, October 2008. http://lasecwww.epfl.ch/keyboard/.

[37] YOUNG, J. NSA Tempest Documents, 2008. http://cryptome.info/0001/nsa-tempest.htm.

[38] ZHUANG, L., ZHOU, F., AND TYGAR, J. D. Keyboard acoustic emanations revisited. In *ACM Conference on Computer and Communications Security* (2005), V. Atluri, C. Meadows, and A. Juels, Eds., ACM, pp. 373–382.