An Improved Technique to Discover Compromising Electromagnetic Emanations

Martin Vuagnoux [*1], Sylvain Pasini [*2]

[*] *EPFL, Lausanne, Switzerland*
[1] martin.vuagnoux@epfl.ch [2] sylvain.pasini@epfl.ch

***Abstract*—The techniques generally used to detect compromising emanations are based on a wide-band receiver tuned on a specific frequency or a spectral analyzer with a limited bandwidth. However, these methods may not be optimal since a significant amount of information is lost during the signal acquisition. In this paper, we propose a straightforward but efficient approach which acquires raw signal directly from the antenna and processes the entire captured electromagnetic spectrum thanks to the computation of short time Fourier transforms. We applied this approach to detect potential compromising electromagnetic emanations radiated by modern keyboard. Since keyboards are often used to transmit confidential data such as passwords, these emanations could remotely reveal sensitive information such as keystrokes. 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.**

I. Introduction

Most of the practical attacks on computers exploit software vulnerabilities from both operating systems and third party software. Every day, dozens of new security weaknesses are discovered and disclosed. To reduce this risk, patches and workarounds are commonly delivered within a few days by the company developing the flawed products. Since a few years, most of the software tend to use online update processes to automatically deliver these patches and to secure computers as fast as possible.

When a vulnerability is based on hardware, there is sometimes no firmware update to avoid the exposure: the device must be changed. Because of the cost of the device or due to the lack of the user awareness (no automatic update process), vulnerable hardware is not replaced quickly and the vulnerability may stay exploitable for a long time.

Thus, there are two main interests for an attacker to focus his research on hardware security. Contrarily to software-based weaknesses, hardware vulnerabilities may be exploited for a much longer period of time. Additionally, side channel cryptanalysis is an interdisciplinary study which requires knowledges in different fields. Academic researchers tend to become specialists focused on a specific domain. Hence, an attacker may easily find new weaknesses in interdisciplinary fields, since they are less studied.

II. Electromagnetic Signal Acquisition

Detecting and capturing unattended electromagnetic emanations is not a new research field.

A. Electromagnetic Compatibility

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.

1) Differential-mode: Differential-mode radiation is generated by loops formed with 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.

2) Common-mode: 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.

Note that the undesired common-mode currents that are found on external cables can be some percentage of the signal currents that would normally be expected on this interface but, more often, cables are found to carry high-frequency harmonics that are not at all part of the intentional signal. Rather they have been picked up inside the equipment from internal clock signal or its harmonics by crosstalk, ground pollution or power supply DC pollution.

Mardiguian in [1] concludes that the identification of the common-mode current source is so complicated, that it is often only during FCC [2], CISPR [3], MIL-STD-461 [4] or other compliance testing that they are discovered.

B. EM from an Attacker's Point of View

From the attacker's point of view there is a simpler way to describe these radiations. Indeed, the attacker has no real interest to determine the source of the emanations, since he aims only at exploiting them. He may look for correlations

between the signal carrying the sensitive information and the compromising emissions. Thus, we redefine the classification of these compromising electromagnetic emanations accordingly.

1) 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.

2) 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 because they are mainly based on common-mode radiations.

III. Standard Method for Signal Acquisition

In this section, we define two commonly used techniques to discover compromising electromagnetic emanations. These methods come from the electromagnetic compatibility standards.

A. Spectral Analyzer

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.

B. Wide-band Receiver

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 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 [5] and R-1550 [6] from Dynamic Sciences International, Inc. are used, see [7], [8]. Indeed, these receivers are compliant with secret requirements NACSIM-5000 [9] 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) [10] and the GNU Radio project [11].

IV. Full Spectrum Acquisition Technique

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 research, we used 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 peaks detector) and to export the acquired data to a computer under GNU/Linux over Ethernet. Hence, the signal can be processed with the GNU Radio software library and some powerful tools such as Baudline [12] 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[1]. Thus, with this technique, we are able to highlight compromising emanations quickly (with only one capture) and easily (with a visual representation of the signal). This solution is ideal for very short data burst transmissions used by computer keyboards.

A. Using an ADC with Fast Data Storage

Since oscilloscopes have limited memory, we implemented a data storage system based on RAM and linked to an ADC.

[1]Multiple antenna models may be used to cover the entire spectrum without any signal loss.

Thus, compared to the previous solution, storage is only limited by the amount of RAM. With this system, we are able to capture a large portion of the electromagnetic spectrum for seconds instead of milliseconds.

B. Removing Antialiasing Filter

To improve the detection of frequencies higher than the bandwidth, we removed all antialiasing filters, to have a wider spectrum. Remember that our objective is to exploit compromising electromagnetic emanations, not to identify the source of these radiations.

V. Case Study: Modern Keyboards

To provide a practical example of the technique described above, we analyzed the compromising electromagnetic emanations of modern keyboards (both wired and wireless).

A. Experimental Setup

Obviously electromagnetic emanations depend on the environment. We defined four different setups.

a) The Semi-Anechoic Chamber (Setup 1): We used a professional semi-anechoic chamber (7×7 meters). 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.

b) The Office (Setup 2): 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)

c) The Adjacent Office (Setup 3): 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.

d) The Building (Setup 4): This setup takes place in a flat which is in a building of five floors in the center of a mid-size city.

e) Antennas: We mainly 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). Indeed, our objective was to demonstrate that easy-to-hide antennas can be used as well.

f) Keyboards: We picked more than 30 keyboards which share 12 different 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.

g) Power Supply: To guarantee that only electromagnetic emanations were exploited, we collected measurements with the keyboard connected to a laptop with battery.

B. Discovering Compromising Emanations

To discover compromising emanations, we placed Keyboard A1 in the semi-anechoic chamber and we used the biconical antenna. We acquired the raw signal with the method described above.

Figure 1 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 to recover keystrokes are based on these compromising emanations and are detailed in the following sections. They can all be discovered from this figure.

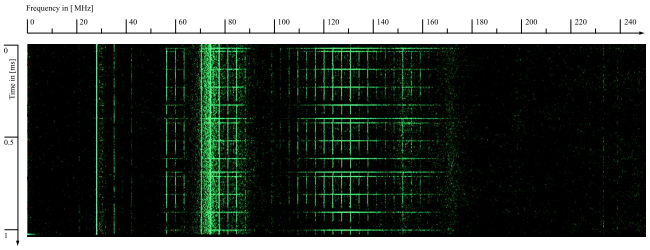

Fig. 1. Short Time Fourier Transform (STFT) up to 250 MHz of the compromising electromagnetic emanation of Keyboard A1 when the key E is pressed (Kaiser windowing of 40, 65536 points).

Some keyboards continuously emit electromagnetic emanations, even when no key is pressed. These radiations were detected with our method as well and are depicted in Figure 2.

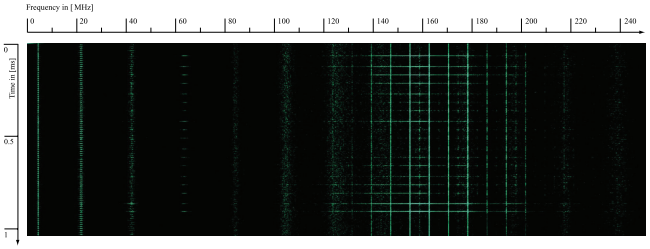

Fig. 2. Short Time Fourier Transform (STFT) up to 250 MHz of the continuously radiated compromising electromagnetic emanation of Keyboard A7 when no key is pressed (Kaiser windowing of 40, 65536 points).

With these two figures, we are able to discover and describe four different techniques to fully or partially recover keystrokes from PS/2, USB, laptop and wireless computer keyboards. The next step is to exploit these emanations. Our first approach was to highlight potential direct emanations. It means that we tried to correlate these radiations with the internal protocol used in keyboards.

VI. Exploiting Compromising Emanations

To understand how direct compromising electromagnetic emanations may be generated by keyboards, we need to briefly describe the PS/2 communication protocol.

When a key is pressed, released or held down, the keyboard sends a packet of information known as a *scan code* to the computer. 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 and finally a stop bit (1). Note that the scan code is binded to 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. Figure 3 represents data, clock signals and the signal captured by a simple wire of copper (one meter long as antenna) when the key E is pressed. We notice that the falling edges of both clock and signal data radiate some compromising peaks. They correspond to the horizontal lines in Figure 1. The exploitation of these peaks defines the first keystroke recovery technique.

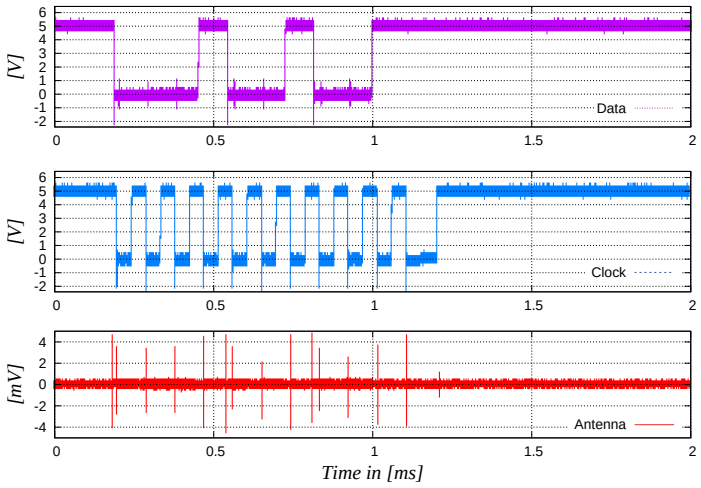

Fig. 3. Data, clock and the compromising emanation captured (semi-anechoic chamber, Keyboard A1) with the loop antenna at 5 meters (a wire of copper, one meter long) when the key E (`0x24`) is pressed. Data signal sends the message: `0 00100100 1 1`.

A. The Falling Edge Transition Technique (FETT)

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 [7, p.35]. Clock and data signals are identically generated. Hence, 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.

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

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. 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.

B. The Generalized Transition Technique (GTT)

The previously described attack is limited to a partial recovery of the keystrokes. However, it may be possible to improve the attack. We know that between two '2' traces, there is exactly one data rising edge. Indeed, the data signal is pulled up exactly one time between two falling edges. Thus, if we are able to detect when this transition occurs, we can fully recover the keystrokes.

To highlight potential compromising emanations on the data rising edge, we use a software band-pass filter on the raw signal to isolate the frequencies of the broadband impulses (e.g. 105 MHz to 165 MHz of the raw signal in Figure 1). Our objective is to visually highlight some information on the rising edge of the data signal.

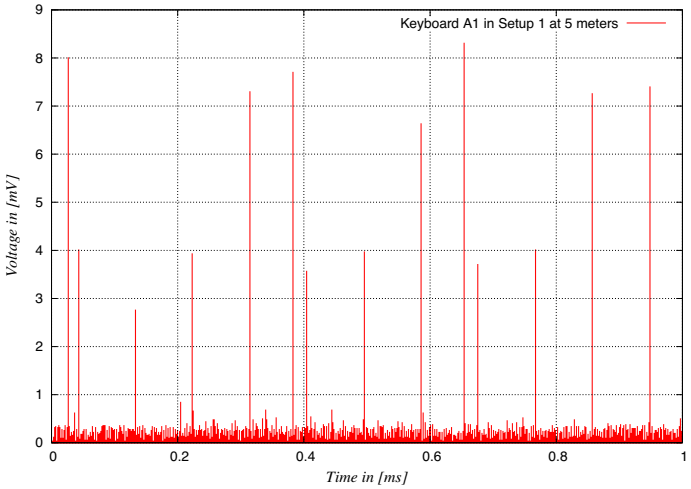

Fig. 4. Band-pass (105-165 MHz) filtered signal of Figure 3.

We notice that the energy of the peaks generated by the falling edges of the clock is not constant. Empirically, clock peaks have more energy (i.e. the peaks are higher) 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 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 4, the rising edge data transitions are respectively at the 5^{th} and the 9^{th} peaks. Thus, the complete data signal is `0010 0100` which corresponds to E (`0x24`).

C. The Modulation Technique (MT)

Figure 1 draws attention to 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 fundamental frequency of 4 MHz, which is very likely the internal clock of the microcontroller inside the keyboard.

If we correlate these harmonics with both clock and data signals (see Figure 5), we clearly see modulated signals (in amplitude and frequency) which fully describe the state of both clock and data signals. This means that the scan code can be completely recovered from these harmonics.

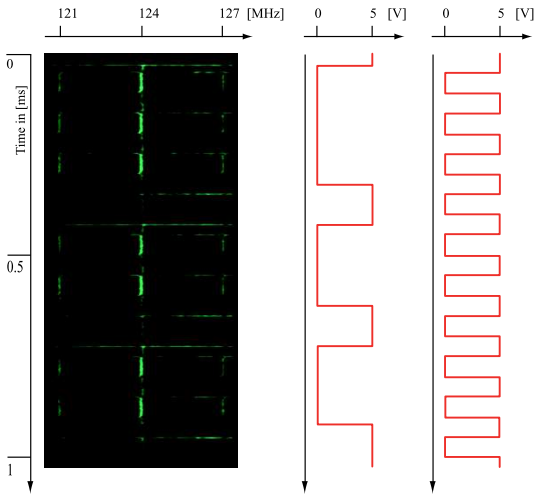

Fig. 5. The amplitude and frequency modulations of the harmonic at 124 MHz correlated to both data and clock signals (Keyboard A1, semi-anechoic chamber at 5 meters).

D. The Matrix Scan Technique (MST)

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 emanations which concern all keyboard types: PS/2, USB, Notebooks and even wireless keyboards. This attack was previously postulated by Kuhn and Anderson [14] but no practical data has appeared so far in the open literature.

Columns in the matrix are long leads since they connect several keys. According to [15], 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 pulse following the pressed column will be delayed by the time taken to process the scan code transmission.

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 6 shows the compromising emanations when the key C resp. key H is pressed.

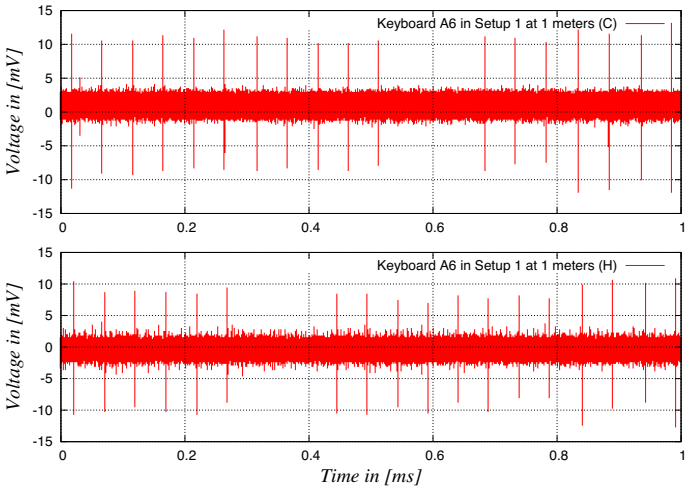

Fig. 6. The matrix scan emanations for the letters C and H (Keyboard A6, Setup 1 at 1 meter).

The key matrix arrangement may vary, depending on the manufacturer and the keyboard model.

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. Thus, 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.

VII. Results

We consider an attack as successful when we are able to correctly recover more than 95% of more than 500 keystrokes.

A. Semi-Anechoic Chamber

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). The Matrix Scan Technique is limited to a range of 2 to 5 meters, depending on the keyboard. 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 7 gives the estimated maximum distance range according to the weakest and the strongest keyboard.

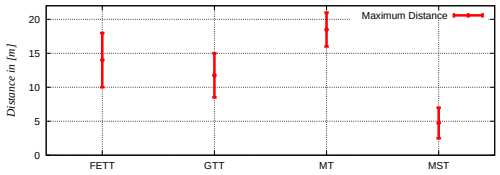

Fig. 7. The theoretically estimated maximum distance range to successfully recover 95% of the keystroke according the four techniques in the semi-anechoic chamber, from the less vulnerable to the most vulnerable keyboard.

B. The Office (Setup 2)

All the results are summarized in Figure 8, which gives the maximum range for the four techniques measured in the office.

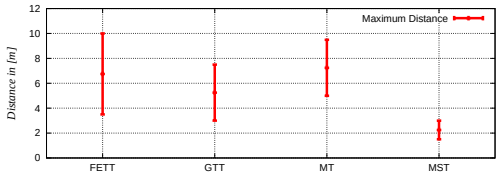

Fig. 8. Maximum distance ranges, from the least vulnerable keyboard to the most vulnerable keyboard, to successfully recover 95% of the keystroke according to the techniques (in the office with the biconical antenna).

C. The Adjacent Office (Setup 3)

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.

D. A Flat in a Building (Setup 4)

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.

VIII. 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 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. The main interest of this technique is the human-aided visual detection of potential compromising electromagnetic emanations. Indeed, once these signals identified, it is trivial to develop some filters which efficiently recover the sensitive information. But with this technique, we are able to interpret these signals quickly and intuitively with our eyes and our brain.

Acknowledgment

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 and Eric Olson.

References

[1] M. Mardiguian, *Controlling Radiated Emissions by Design*. Kluwer Academic Publishers, ISBN 0-7923-7978-0, 2001.
[2] FCC, "Federal Communications Commission," http://www.fcc.gov.
[3] CISPR, "The International Special Commitee on Radio Interference," http://www.iec.ch/zone/emc/emc_cis.htm.
[4] MIL-STD-461, "Electromagnetic Interference Characteristics Requirements for Equipment," https://acc.dau.mil/CommunityBrowser.aspx?id=122817.
[5] M. G. Kuhn, "Dynamic Sciences R-1250 Receiver," http://www.cl.cam.ac.uk/ mgk25/r1250/, 2008.
[6] Dynamic Sciences International, Inc., "R-1550a tempest receiver," http://www.dynamicsciences.com/client/show_product/33, 2008.
[7] M. G. Kuhn, "Compromising Emanations: Eavesdropping Risks of Computer Displays," *Technical Report UCAM-CL-TR-577*, 2003.
[8] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM Side-Channel(s)," in *CHES*, ser. Lecture Notes in Computer Science, B. S. K. Jr., Çetin Kaya Koç, and C. Paar, Eds., vol. 2523. Springer, 2002, pp. 29–45.
[9] J. Young, "NSA Tempest Documents," http://cryptome.info/0001/nsa-tempest.htm, 2008.
[10] M. Ettus, "The Universal Software Radio Peripheral or USRP," http://www.ettus.com/, 2008.
[11] Various authors, "The GNU Software Radio," http://www.gnuradio.org/, 2008.
[12] SigBlips DSP engineering, "Baudline," http://www.baudline.com, 2008.
[13] J. Eatson, "GNU Octave," http://www.gnu.org/software/octave/, 2008.
[14] M. G. Kuhn and R. J. Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations," in *Information Hiding*, ser. Lecture Notes in Computer Science, D. Aucsmith, Ed., vol. 1525. Springer, 1998, pp. 124–142.
[15] E. L. Sonderman and W. Z. Davis, "Scan-controlled keyboard," United States Patent US 4,277,780, 1981.