Compromising Electromagnetic Emanations of Wired USB Keyboards

Alexandru Boitan[1](✉), Razvan Bărtuşică[1], Simona Halunga[2],
Mircea Popescu[1], and Iulian Ionuţă[1]

[1] The Special Telecommunications Service, Bucharest, Romania
boitanalexandru@yahoo.com, rbartusica@yahoo.com,
mpopescu@sts.ro
[2] University Politehnica of Bucharest, Bucharest, Romania
simona.halunga@upb.ro

Abstract. The TEMPEST methods and procedures focus on classified information carriers generated by any electronic devices through electromagnetic radiation. Any electromagnetic radiation-carrying information is called compromising emanation. In this paper we will exemplify the keystroke information recovery by receiving compromising emanations emitted by the USB keyboards and the possibility of automatic detection of compromising emanation by using the autocorrelation function as well as the risk assessment of information vulnerability.

Keywords: USB · Keyboard · TEMPEST · Compromising emanations

1 Introduction

We live in the era of digital communications, and no matter how traditional we are, we still have a personal computer or laptop, a smart phone or a tablet PC in our possession.

All electronic equipment emits electromagnetic radiations that can propagate in free space at considerable distances, in the order of meters or even tens of meters. This aspect has been known for decades and is being standardized by Electromagnetic Compatibility (EMC) rules and regulations [1]. A part of the electromagnetic signals emitted by electronic equipment consist in information carriers, meaning that, if they are received with specialized equipment, processed and analyzed by specialists, who possess the specific hardware and knowledge, they can partially or totally recover the information processed or manipulated by the targeted electronic equipment. These electromagnetic signals are known in the specialty TEMPEST regulations as compromising emanations (CE). The set of standardized methods and procedures necessary to protect against information leakage represent the Tempest standards. Like EMC, the TEMPEST domain has its own regulations which are in continuous updating process due to emerging technologies and the need for information security assurance. There are TEMPEST regulations both on EU and NATO level [2, 3]. The TEMPEST domain is a military-specific domain and it only applies to the protection of classified information. Therefore, all TEMPEST regulations are classified information also.

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2018
O. Fratu et al. (Eds.): FABULOUS 2017, LNICST 241, pp. 39–44, 2018.
https://doi.org/10.1007/978-3-319-92213-3_6

Recent research shown that the keyboard and its connection to the computer is one of the most critical points. In [4] the authors proposed a method to analyze the electromagnetic radiation from USB keyboard and, using signal processing algorithms, shown that the signal can be reconstructed, while in [5] an automatic control system for reception of the compromising emanations has been developed. In [6] the authors propose a method that jams the emanations and in [7] a number of general protection guidelines are proposed. In some of their previous work [8, 9] the authors have shown that the PS/2 keyboard uses a low-speed serial cable communication (10–15 kHz) is considered outdated and should not be used in the future. One can also use a virtual keyboard as an input method but this falls under the video signal display eavesdropping that was approached by Wim van Eck for the first time in 1985 [10].

We will focus our attention on the USB signal with the bit duration of 600 [ns] or 80 [ns], used by the USB keyboard communication as it is a more complex signal than the PS/2 communication with the bit duration of 100 µs, and, therefore harder to recover from the CE radiation but also because most of the keyboards currently used are USB type. In this work we will exemplify that the USB signal can be rebuild from CE signal at the bit level in laboratory conditions, which has not been achieved in the past, as well as the possibility of automatic detection of the compromising signal. We will also try to evaluate the level of risk of disclosing the information from the compromising signal radiated by USB keyboards.

This paper is organized on 5 sections: Sect. 2 presents the measurement configuration testbed, in Sect. 3 some examples of USB keyboard codes recovery are illustrated. In Sect. 4 a number of examples will be presented to highlight the difficulty of CE detection, while Sect. 5 contains the conclusions of this paper.

2 The Measurement Setup

In order to observe, evaluate and measure the reception of compromising signals coming from USB keyboards, the testbed described in Fig. 1 has been used. The measurements were performed in a semi-anechoic chamber and reception equipment is located outside the test room.

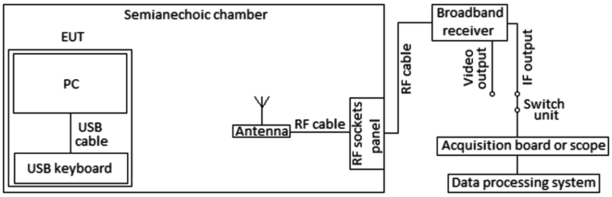

Fig. 1. Measurement setup

The TEMPEST laboratory measurements need much higher resolution bandwidth. However, the reception of compromising signals from the USB 1.0 and USB 1.1 keyboards can also be achieved with EMC receivers.

The CE detection tests were performed using a Rohde & Schwarz FSET 7 test receiver with 10 MHz resolution bandwidth (RBW) and a HL223 passive logperiodic antenna. For signal processing, we used an acquisition board with a sampling frequency of 125 MHz and 12-bit Resolution, controlled by a computer with a dedicated software package for TEMPEST evaluations.

The testing equipment (EUT) was a commercial Jujitsu Siemens desktop, CELSIUS W350 type, installed in normal working conditions, at a distance of 1 m from the receiving antenna (EMC test distance according to MIL461F standard).

3 CE from USB Keyboard Communication

In order to highlight the CE detection for USB 1.0 and USB 1.1 signals performed with the receiver system described above we used a Tektronix type DPO70804B.

If we monitor the USB bus through an oscilloscope and galvanic probing we will see two types of USB packets: synchronization and data packets. The data packet is illustrated in Fig. 2.

The USB communication uses Non Return to Zero Inverted (NRZI) encoding, in which "0" represents transition and "1" means no transition. All USB packets start with a synchronization field (SYNC), used by the receiver circuits to synchronize with the transmitter. The SYNC field is 8 bits long at low speed (USB 1.0) and full speed (USB 1.1) USB communications "11111100", where the last two bits indicate the end of the SYNC field, according to the USB standard [11].

Using the measurement setup described in Sect. 2, we were able to receive the Compromising Emanations (CE) generated by data packet, as shown in Fig. 3. As one can see, only the transitions are reflected in the compromising emanations.

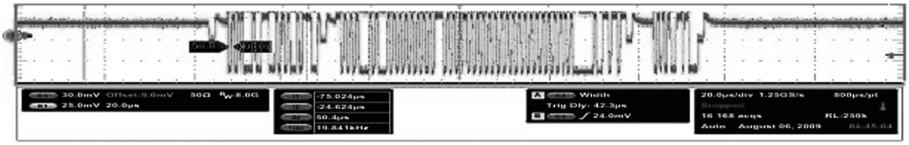

Fig. 2. USB data packet (by pressing the "c" key)

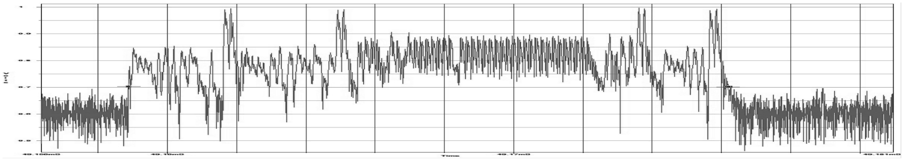

Fig. 3. CE from USB data packet (by pressing the "c" key)

From the comparative analysis of the USB waveforms captured galvanically with the oscilloscope and the accidentally radiated signals of the EUT and received by the measurement system it resulted that these types of signals can be intercepted by an attacker and the information can be compromised by restoring the data.

4 CE Propagation

To analyze the risk level of information leakage through the low speed USB (USB 1.0) we used CE generated by a desktop keyboard and we evaluated the maximum distance from which such signals can be detected under the most disadvantageous conditions for the targeted computer, namely a reduced ambient electromagnetic noise (provided by the semi-anechoic chamber) and the use of commercial equipment as equipment under test (EUT), without any TEMPEST protection measures (shielding, data lines filtering, power lines filtering etc.).

In some situations, the CE detection process is hampered due to the complexity of the electromagnetic waves propagation phenomenon, since it has a broadband spectrum and its different frequency components may propagate differently. In Fig. 4 is illustrated the most advantageous situation, in which the payload is received at a much higher level than the USB-specific packaging fields. However, the opposite might happen as well.

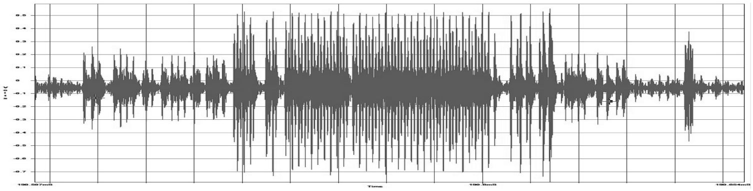

Fig. 4. CE from USB data packet (“m” keystroke)

For measurement and evaluation of CE the testbed described in Sect. 2 has been used. The “p” keystroke has been repeated with an operator’s typed frequency. A compromising signal was received on the 212.3 [MHz] frequency, and, after filtering and time correlation, it was confirmed to be the USB 1.0 waveform corresponding to the “p” key, as illustrated in Fig. 5. We can observe the searched signal in the left-upper side of Fig. 5 and the data acquisition we are looking for at the top right. At the bottom of Fig. 5 we can see the result of the time correlation function.

The maximum CE and noise level were evaluated in time domain and the corresponding signal-to-noise ratio resulted to be 20.8 [dB]. To prevent detection and interception of this signal, the SNR ratio should be less or equal to 0 [dB], hence, in this setting, the received signal should be reduced by 20.8 [dB].

The CE can be reduced either by electromagnetic shielding of the computer system, or by increasing the separation distance between the target computer equipment and the minimum protection area from which an attacker can intercept the CE. The shielding effectiveness is larger than or equal to 20.8 [dB], resulting from the evaluation presented above. To determine the minimum radius of the TEMPEST protection area (around the IT system), the worst case scenario is assumed, where the attenuation of the building is 0 [dB] and the free space attenuation formula is used:

$$L_{bf} = 32.4 + 20 * \log\left(f_{[\mathrm{MHz}]}\right) + 20 * \log\left(d_{[\mathrm{Km}]}\right). \tag{1}$$

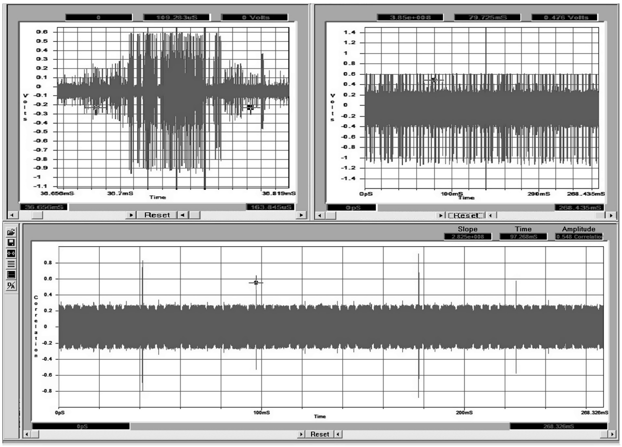

Fig. 5. CE time correlation (“p” keystroke)

Using this, it resulted a minimum distance of 11 meters for the TEMPEST protection area around the targeted computer system in order to prevent leakage of information through USB signals accidentally emitted by computer equipment. However, this value does is covering and does not represent a danger of compromising the information processed by the targeted electronic equipment because, in reality, the ambient radio noise is much higher than the one considered in the tests performed, and this falls within the TEMPEST minimum protection area according to the current TEMPEST regulations.

5 Conclusions

In this paper we presented several examples of CE recovery and demonstrated that it is possible to restore the keystroke information from the CE radiation of the USB keyboards. We also illustrated an example of time correlation process used for automatic detection of CE.

Since people are asked to be as open as possible in terms of working time, one may get to work on a computer not only in our office but also at home, in a car on the way to work or even outdoors, in green parks, at the playground of our children. This may be efficient from time optimization point of view, but may lead to significant flows with respect to security. One is not protected against security TEMPEST attacks when our workspace is located in free space or a car and not even if we’re in an office but right next to the window. In fact, we are the least protected. The window offers small electromagnetic waves attenuation. It is very important how much a possible attacker can approach us without being visible and obviously what physical obstacles (distance in free space, perimeter delimitation fencing, vegetation, building elements, etc.) are between us and the attacker. Another important technical aspect is represented by fortuitous conductors leaving our workspace represented by any conductor that may provide an unintended propagation path for CE signals (water and gas pipes, wires, cables, and any metal building structure). They can override any propagation pattern, and in this case the estimation of the propagation can be unrealistic and it is necessary to make specific measurements to assess the site attenuation in a certain frequency range imposed by the TEMPEST regulations.

In this paper we exemplified the estimation of the maximum risk of information vulnerability from USB keyboard CE, which can be an important component of the risk analysis that is required during the implementation of the TEMPEST protection measures. Similar risk analysis should be also performed for the others CE signals corresponding to the latest technologies like USB 3.0, HDMI, Ethernet 1 GB/s, etc.

We can conclude that the TEMPEST phenomenon is complex and the methods of protection against CE are expensive. If protection against CE is needed, a TEMPEST security officer will be able to provide customized technical expertise, according to the equipment, location and the information classification level.

References

1. The Electromagnetic Compatibility Regulations (2016). http://www.legislation.gov.uk/uksi/2016/1091/pdfs/uksi_20161091_en.pdf. Accessed 20 Mar 2017
2. NATO Standard, SDIP-27/1: NATO TEMPEST Requirements and Evaluation Procedures (NATO CONFIDENTIAL), NATO Military Committee Communication and Information Systems Security and Evaluation Agency (SECAN) 2009
3. EU Standard, IASG 07-03: Information assurance security guidelines on EU TEMPEST requirements and evaluation procedures (EU CONFIDENTIAL), General Secretariat of the Council of the European Union (GSC) (2013)
4. Choi, H.J., Lee, H.S., Sim, D., Yook, J.G., Sim, K.: Reconstruction of leaked signal from USB keyboards. In: URSI Asia-Pacific Radio Science Conference (URSI AP-RASC), pp. 1281–1283. IEEE, August 2016
5. Sokolov, R.I., Abdullin, R.R., Dolmatov, D.A.: Development of synchronization system for signal reception and recovery from USB-keyboard compromising emanations. In: IEEE International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), pp. 1–4, May 2016
6. Ahsan, M.A., Islam, S.R., Islam, M.A.: A countermeasure for compromising electromagnetic emanations of wired keyboards. In: 17th IEEE International Conference on Computer and Information Technology (ICCIT), 22 Dec 2014, pp. 241–244 (2014)
7. Zhou, C., Yu, Q., Wang, L.: Investigation of the risk of electromagnetic security on computer systems. Int. J. Comput. Electrical Eng. **4**(1), 92 (2012)
8. Popescu, M., Bîndar, V., Crăciunescu, R., Fratu, O.: Estimate of minimum attenuation level for a TEMPEST shielded enclosure. In: 11th International Conference on Communications – COMM 2016, Politehnica University of Bucharest, Military Technical Academy, Bucharest, pp. 521–526 (2016)
9. Bîndar, V., Popescu, M., Crăciunescu, R.: Aspects of electromagnetic compatibility as a support for communication security based on TEMPEST evaluation. In: 10th International Conference on Communications - COMM 2014, Politehnica University of Bucharest, Military Technical Academy, Bucharest, pp. 529–532 (2014)
10. van Eck, W.: Electromagnetic radiation from video display units: an eavesdropping risk? Comput. Secur. **4**(4), 269–286 (1985)
11. Universal Serial Bus Specification-USB 2.0: Released in 27 April 2000. http://www.usb.org/developers./docs/usb20_docs/#usb20spec/usb_20.pdf. Recommendation ITU-R P.525-2. https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.525-3-201611-I!!PDF-E.pdf. Accessed 10 May 2017