MBNA Publishing House Constanta 2021

Proceedings of the International Scientific Conference SEA-CONF

SEA-CONF PAPER • OPEN ACCESS

Keyboards, sitting duck for intercepting sensitive data

To cite this article: Radu MOINESCU, Ciprian RĂCUCIU, Cătălin ALBIȘORU, Daniel-Iulian COSTIA, Dragoș GLĂVAN and Sergiu EFTIMIE, Proceedings of the International Scientific Conference SEA-CONF 2021, pg.189-198.

Available online at www.anmb.ro

ISSN: 2457-144X; ISSN-L: 2457-144X

doi: 10.21279/2457-144X-21-024

Keyboards, sitting duck for intercepting sensitive data

Radu MOINESCU, Ciprian RĂCUCIU, Cătălin ALBIȘORU, Daniel-Iulian COSTIA, Dragoș GLĂVAN, Sergiu EFTIMIE

Military Technical Academy "*Ferdinand I*"
radu.moinescu@gmail.com

Abstract. A real danger for the compromise of sensitive information processed with electronic data processing, storage or transmission equipment is represented by the secondary electromagnetic signals carrying useful information emitted by them. Protection for such threats is achieved by implementing specific security measures, referred to by the generic term TEMPEST. One of the possible channels of information leakage is radiation are the computer keyboards. Since they contain electronic components, keyboards eventually emit electromagnetic waves. These emanations could reveal sensitive information that we are trying to protect such as passwords.

1. Brief history

History has shown many times that information is a weapon. It allows the person who uses it to prevent, counteract risks or threats or to offer an advantage over an opponent. We can point out that there are two main means of gathering information, which has been the case since human societies have been concerned with such activity in order to ensure their survival. A first means of gathering and securing information is human sources (*e.g., paid informants, interrogators or under the influence of various pressures to provide information*), is the case of HUMINT (Human Intelligence) which, until the twentieth century, was dominant. A second means of information is the sources in the form of signals, SIGINT (Signals Intelligence), information resulting from listening to communications or electronic messages. This type of particular information collected by technical means has progressed continuously since the twentieth century. Thus, SIGINT has progressively specialized in three branches: COMINT (Communication Intelligence), ELINT (Electronic Intelligence) and FISINT (Foreign Instrumentation Signals Intelligence). The First World War is the event that marks the decisive increase in the means devoted to gathering information of this nature. In 1914 the German army used the return current to intercept enemy campaign telephones (*Fig.1*). The interception method consisted of connecting electrodes, inserted in the wet soil of the battlefield, to portable valve amplifiers, in order to make the voltages generated all over the field to be perceptible as intercepted speech signals. [1]

In 1918, the United States Army recruited Herbert Osborn Yardley and his team to develop methods for detecting, intercepting, and analyzing signals from military phones and radio stations. Initial research revealed that the equipment emits electromagnetic radiation, which can be used to intercept classified information. [2]

However, by the end of World War II, the relatively weak development of telecommunications technologies did not sufficiently stimulate research into compromising electromagnetic radiation, and there were other ways of intercepting information.

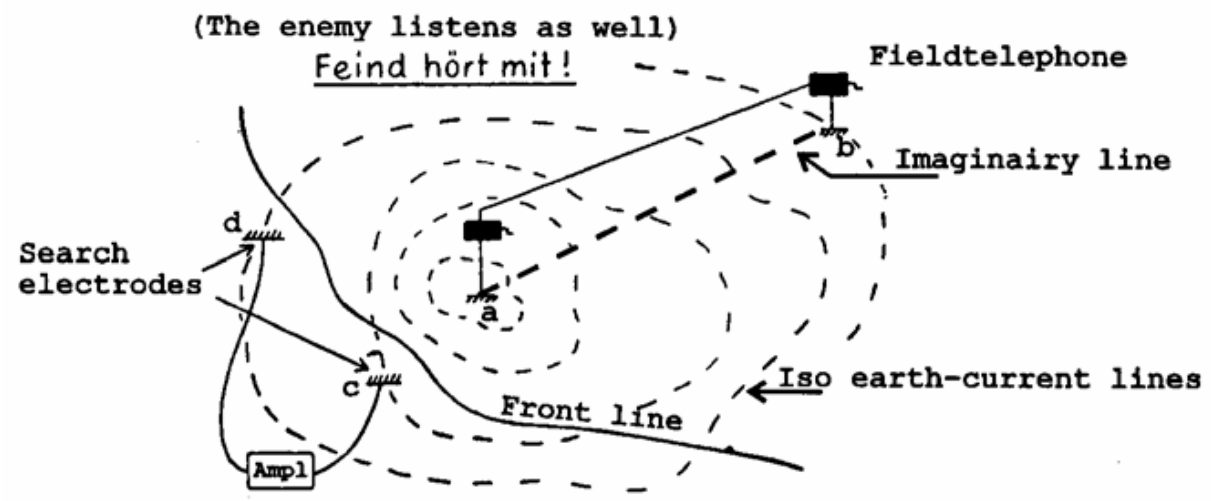

Fig.1 The danger of using the ground in a return circuit [1]

The development of telecommunications networks and the use of computer systems to process transmitted information in the early 1950s stimulated research into parasitic electromagnetic radiation. The memoir of former MI-5 intelligence officer Peter Wright, entitled "Spycatcher", talks about the most famous operation of exploiting compromising electromagnetic radiation in the twentieth century. In the late 1960s, Britain was negotiating accession to the European Economic Community (EEC), and information on France's position on the issue was very important to the British government. The British MI-5 employees constantly intercepted the encrypted messages of French diplomats, but all British efforts to decipher them failed. However, at one point, Peter Wright, when analyzing the electromagnetic radiation coming from the French embassy in London, noticed that, along with the main signal, there was another signal, very weak. British engineers managed to adjust the receiver equipment on this signal and demodulate it. This proved to be a clear message. Like any electrical equipment, French cryptographic equipment emitted parasitic electromagnetic radiation, which was modulated into an informational signal before the actual encryption. So, by intercepting and analyzing the spurious emissions of French encryption equipment, the British government, even without a key to decrypt encrypted messages, received all the necessary information. [3]

In the late 1960s and early 1970s, the concept of TEMPEST (Transient Electromagnetic Pulse Emanation Standard) was developed when methods were developed to prevent information leakage through various types of hidden channels and parasitic electromagnetic emissions from electronic equipment.

For a long time, everything related to the TEMPEST concept was secretly shrouded. The first unclassified paper on the subject, which reveals, for the first time, certain data on the danger posed by information compromise, TEMPEST radiation emitted by cathode ray tube monitors of computer systems, is published in 1985 by Dutch engineer Wim van Eck in Computers & Security magazine, article entitled "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?". [4] Since then, gathering information from radio signals and electronic equipment has become an indispensable necessity in espionage activities. As technology developed, both TEMPEST attacks and TEMPEST defense tools developed.

In Romania, the first regulations regarding parasitic electromagnetic radiation appeared in 2002, together with the Government Decision no. 585 of June 13, 2002 for the approval of the National Standards for the protection of classified information in Romania.

2. TEMPEST, the concept

The trend of recent years shows a worrying upward trend in the number and variety of information attacks, and detecting and defending against them is becoming increasingly difficult. The entities behind

these attacks have shown that they can also enter organizations considered safe. Information is considered in modern organizations an asset, and consequently, it is coveted by opponents/adversaries. For this reason, organizations use various measures to prevent the leakage of sensitive information, and one of them is the isolation (disconnection) both physically and logically from public computer networks. This isolation is commonly used in military defense systems, in critical infrastructure, in the financial-banking sector and in other types of industry.

Even in spite of this high degree of isolation, compromising critical information is possible due to the cliché thinking of information security specialists or system administrators: "if the computer system is disconnected from the network then the information is secure". True, in this case the information stored on the hard disk or other memory media will remain inaccessible. But if the information is open in an application, its content will reach the ether, because the components of computer and communication systems produce electromagnetic radiation. They can be intercepted, analyzed and processed in order to reconstruct the information conveyed through this equipment. This aspect of information security is known as TEMPEST.

The 1994 CIA report, entitled Redefining Security, explicitly stated: "The fact that electronic devices - such as computer systems, printers - emit electromagnetic waves is a threat to the US government. Attackers ... can intercept classified information."

The TEMPEST protection concept combines the criteria of remote propagation of compromising electromagnetic radiation with the technological safety measures applied since the design-manufacture phase of the equipment. Along with the modifications to the equipment for ensuring the electromagnetic shielding of certain components and/or the introduction of filters on the power and data lines, so that the parasitic emissions are canceled or at least reduced, the TEMPEST concept also considers the zoning of the space in around the place where the equipment is installed and operates to establish vulnerabilities, reduce the risks and threats of compromising the information stored, processed or transmitted by it.

3. TEMPEST attacks

Depending on the control that the threat agent has over the calculation process, TEMPEST attacks can be divided into two main categories: passive attacks and active attacks.

Passive TEMPEST attacks refer to the exploitation by a threat agent (adversary) of secondary electromagnetic signals carrying information, without the latter making any effort to create them. There are two categories of this type of attack:

- the compromising signal is directed on a kind of circuit (such as a power line or a telephone line);
- the compromising signal can be radiated as radio frequency energy.

These two types of attack are not mutually exclusive. For example, electromagnetic signals emitted by a computer system can be picked up by power supply circuits and routed to neighboring buildings.

Active TEMPEST attacks refer to the ability of a threat agent to enhance/intensify or create electromagnetic signals from target hardware using malicious software. The concept first exposed to the public in 1998 by Markus Kuhn is essentially similar to steganography.

The main danger of active TEMPEST attacks is the secret activity of malware. Unlike classic malware, it does not corrupt data, does not interfere with the functionality of the computer system or network equipment and does not spread through the network, which means that it can remain undetected for a long time. In this way, a threat agent can filter data from a computer and communications system even if it is stand-alone.

The TEMPEST channel that allows the exfiltration of information is characterized by the size of the three-dimensional physical space surrounding the information processing equipment and the space limit beyond which the actual reception of parasitic electromagnetic radiation is impossible due to attenuation in the given environment of the emitted signal. For example, the NATO model divides the space around equipment used to process information classified into three security zones numbered 0 to 2.

4. The computer keyboard, source of information leakage through the TEMPEST channel

One of the most dangerous ways in which a computer system works, in terms of leaking information through the TEMPEST channel, is entering data from the keyboard.

The keys on the keyboard can be divided into several groups, based on their function:

- *typing keys* (*alphanumeric*) - these include the same keys for letters, numbers, punctuation and symbols as those of a traditional typewriter;
- *control keys* - these keys are used individually or in combination with other keys to perform certain actions. The most commonly used control keys are Ctrl, Alt, Windows logo key and Esc;
- *function keys* - function keys are used to perform certain activities. These are labeled as F1, F2, F3, ..., F12. The functionality of these keys differs from one program to another;
- *navigation keys* - these keys are used for scrolling through documents or web pages and for editing text. These include arrow keys, Home, End, Page Up, Page Down, Delete and Insert;
- *numeric keypad* - the numeric keypad (if available) is useful for entering numbers quickly. The keys are grouped together in a block, like a conventional computer or a calculating machine.

To generate the action of each key, current keyboards use several types of switches. Most keyboards use a version of the mechanical key switch. A mechanical key switch is based on a momentary mechanical contact, which, at the time of typing, makes the electrical contact that closes a circuit. Some keyboards use a completely different model, which is not mechanical, and is based on capacitive switches. The most common type of cup switch is the mechanical one, available in four variants: purely mechanical, with a spongy element, with a rubber cap or with a membrane. In the keyboard, the symbol codes displayed on the keys are generated by the controller, which sequences all the keys. The scan code is a one-byte number, of the least significant 7 bits is the identification number assigned to each key. The type of information signal via the keyboard depends on its interface (PS/2 or USB).

4.1 Measurement method

To observe, measure and evaluate the parasitic electromagnetic emissions from the keyboards, the test bench shown in *Fig. 2*. The measurements were performed in an anechoic chamber, where the assembly was performed. To make the measurements, two configurations were used in terms of the data cable that connects the computer system and the keyboard, more precisely the keyboard wires were left in the original shape, only with their coat of different shades, and in the second test of on them the mantle was removed so that the contact was full between them and the probe. However, the reception of parasitic electromagnetic emissions from keyboards can also be achieved with equipment for measuring electromagnetic compatibility.

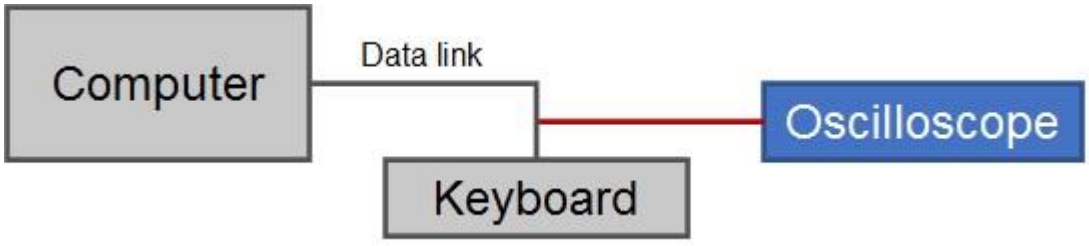

Fig. 2. Measurement configuration

It should be noted that this installation removes from the spectrum all compromising emissions from the computer system. By comparison, the display of the code for an oscilloscope key from the capture of compromising emissions using antennas is deficient in identifying the key without first knowing its code.

This setup helped eliminate any problems in terms of key identification from the start, providing security in analyzing the data provided during the study. The code packets that are transmitted between the keyboard and the computer system are easily observable, which allowed it to be established at the

beginning of the whole spectrum which sequence represents the presence, synchronization and transmission signals.

The type of packet displayed at the time of this assembly shows each area separately, the analysis of the presence and synchronization packets provides us that the amplitude level of the entire signal is 3.4V. It should be noted that the way the keyboard communicates with the computer system is quite interesting, when using a key, a package automatically appears that tells the computer system that a key has been pressed (a kind of flag for example) and immediately the key code is attached to this sequence.

4.2 The structure and spectrum of the signal of parasitic electromagnetic emissions from the keyboard

The PS/2 interface is the original serial protocol for keyboards and mice, later replaced by the USB interface. The data exchange between the keyboard and the controller is performed asynchronously using a serial protocol when a certain key is activated. Two lines are used for data exchange - KBData and KBSync. When transmitting scan codes, the keypad sets the next bit of data on the KBData line and confirms the transfer by changing the signal from "1" to "0" on the KBSync line. When it receives data from the controller, the keyboard reads bits from the KBData line and issues an acknowledgment by transferring the signal on the KBSync line from "1" to "0". The controller may signal that it is not ready to transmit/receive low-level data on the KBSync line. The rest of the time, when there is no data to transmit, both lines have a high signal level. The pulse rate of the KBSync line is approximately 10-25 KHz. (*Fig. 3*)

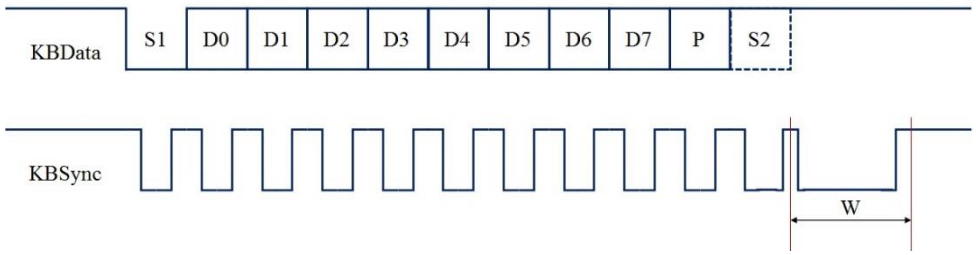

Fig.3. Keyboard data transmission overview

The order of data transmission is: a start bit "0", a data byte, parity bit (sum of all bits +1), a stop bit - "1". After receiving each byte of data, the controller sets a low level on the KBSync line signaling that it is busy processing the received data and is not ready to accept the next one. This can be considered a confirmation of acceptance. The keyboard confirms each byte of the command received with the code 0FAh. If an error occurs during transmission, the controller may request that the last byte be transmitted again by issuing the 0FEh command. The keyboard behaves differently - it simply ignores errors. Each PS/2 keyboard key has a unique scan code, which is sent each time the corresponding key is pressed.

When a signal pulse passes from the keyboard to the motherboard through the connecting cable, an alternating electromagnetic field (parasitic electromagnetic radiation) appears around it, the spectrum of which will be determined by the type of pulse signal. The analysis showed that the pulse sequence is close to the periodic duty cycle $Q = \frac{T}{\tau} = 2$ (*where τ represents the sampling period*) is entered in the data line of the PS/2 keyboard when the "=" key is pressed. When this key is pressed, a sequence of pulses 01010101011 is sent to the line. This mode of operation indicates that PS/2 keyboards have a high risk of intercepting parasite electromagnetic radiation.

Key:	Packet synchronization frequency in kHz	Data line frequency in kHz	The type of signal transmitted
=	12,35	6,25	10101010
1	12,35	3,10	01101000

Key:	Packet synchronization frequency in kHz	Data line frequency in kHz	The type of signal transmitted
2	12,35	6,25	01111000
Tab	12,35	6,25	10110000
Left Shift	12,35	4,11	01001000

Table 1. Frequencies of data transmission when certain keys are pressed

Simultaneously with the data, a synchronization signal is transmitted via the keyboard, which has an alternating sequence "0" and "1" - 01010101010101010101. Since the pulse duration of the synchronization signal is twice less than the duration of the data pulse, the frequency of the synchronization pulses must be twice as high as the data transmission frequency, $F = 16{,}5\ kHz$. In *Fig. 4* shows the harmonics of the synchronization signal: signals at frequencies of 16.5 kHz, 49.5 kHz and 82.5 kHz. From the point of view of intercepting data entered from the keyboard, the clock signal is not informative.

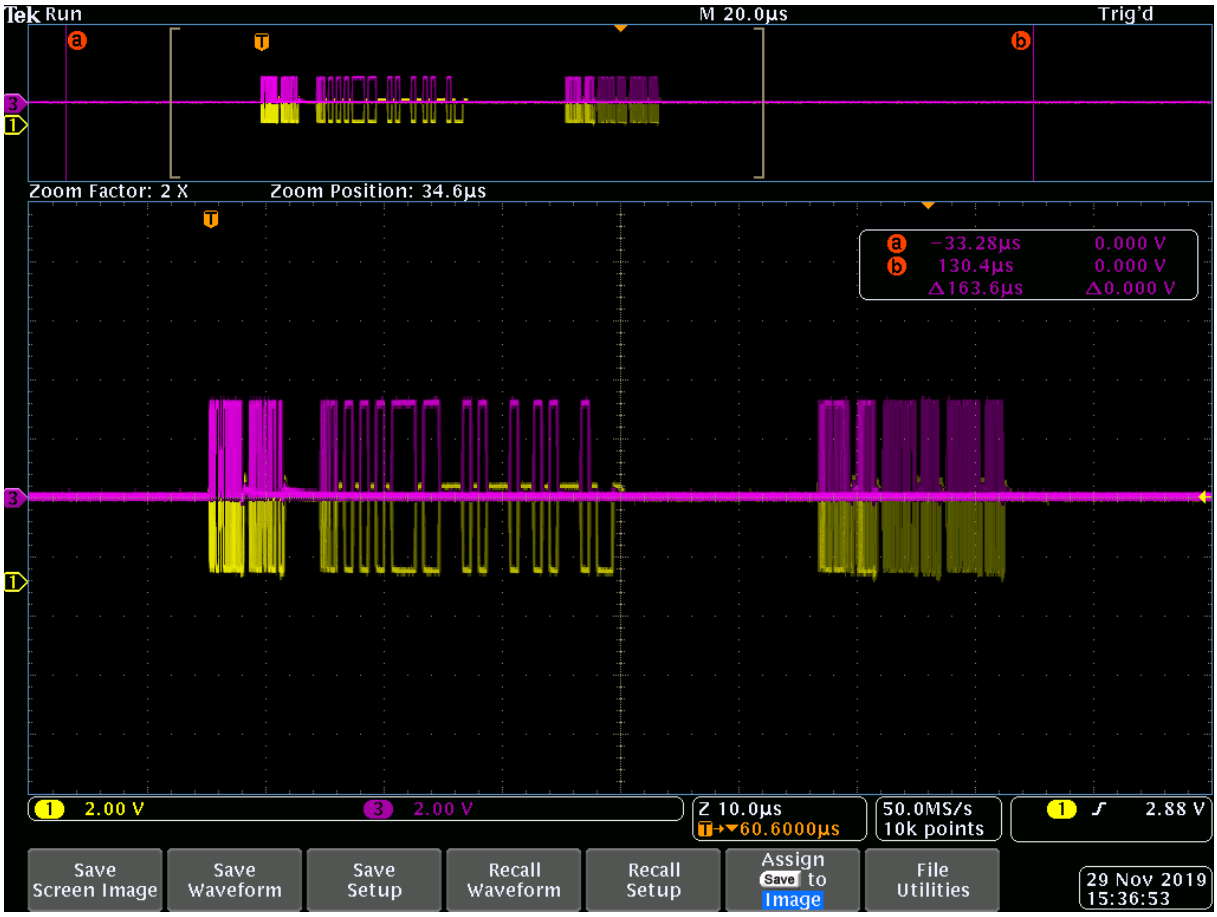

Fig.4. Overview of the transmission of the original package

The USB interface is distinguished from the PS/2 both by the large number of peripheral devices that can be connected, which can reach 127, and by the transfer rate offered by its bus. Initially (at versions 1.0 and 1.1), the bus offered two categories of speeds: Low-speed (1.5 Mb/s) and Full-speed (12 Mb/s). In versions 2.0 and 3.0, the High-speed (480 Mb/s) and Super-High-speed (5 Gb/s) speed categories are defined.

In the case of the USB interface, all information exchanges, hereinafter referred to as transactions, are initiated by the host. A transaction consists of two to three packages. Four types of packets are used in data transactions (*Fig.5*):

- *token packets* - represent the control packets and are transmitted only by the host;
- *data packets* - used to transfer the payload, used by the host and the USB device;
- *handshake packets* - represents the confirmation of the received data packet, used by both the host and the device;
- *start of frame packets* - issued by the host at a nominal rate of 1 every 1.00 ms ± 0.05 on a maximum speed connection. This packet type is used to send messages that are larger than the maximum payload of the data packet.

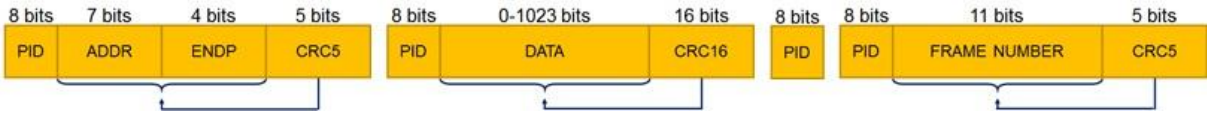

Fig.5. Package format: *a) token packets*; *b) data packets*; *c) handshake packets*; *d) start of frame*

USB bus communication uses Non-Return to Zero Inverted (NRZI) encoding. In this method, a bit of 1 is represented by a lack of voltage level change, and a bit of 0 is represented by a change in voltage level, without returning to the reference voltage (zero) between the encoded bits. Additional bits are inserted into the transmitted data to ensure sufficient signal transitions to ensure proper synchronization. A bit of 0 is inserted after every six consecutive bits of 1 before encoding the data, to force a transition in the data string. Each data packet is preceded by a synchronization field to allow the receivers to synchronize the reception clocks. (Fig. 6) [5]

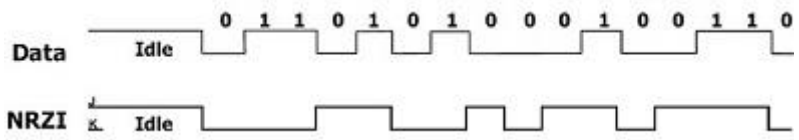

Fig.6. NRZI coding [5]

The host probes the USB device every 8 ms with a packet with the following data: [10101011] SYNC, [1011] PID in 1001_2, [0001] Check PID 0110_2, [1010101] ADDR 0000001_2, [1010] ENDP 0001_2, [00110] CRC, [00] EOP.

The SYNC and EOP fields are not significant, they are needed to synchronize and initialize the data exchange. When EOP (end of packet) is transmitted, both differential pairs go to zero for two cycles, which means the end of packet transmission. The PID field defines the packet type, the CRC field is the inverse representation of the PID field, it is necessary for error control. The ADDR field is the address of the function (device) assigned by the host. All devices must respond to address zero. The ENDP (Endpoint) field is the endpoint number of the function, and provides more flexible addressing. The CRC field checks the ADDR and ENDP fields. In the following we will neglect the SYNC and EOP fields when describing the packages, because they are not information carriers and are present in any type of package.

The USB device responds after 8 clock cycles per byte ≈ 5.3 ms. If the device has nothing to transmit, then send a confirmation packet without content: PID NAK 1010_2 - the device cannot receive or transmit data, Check PID. The only packages that do not have a checksum are the dialog packages. Error checking is performed by the Check field. [5]

The way to transmit the information regarding the event of pressing a key is the following (*Fig. 7*)

SYNC	PID data1	Check PID	DATA 0x00	DATA 0x00	DATA 0x04	DATA 0x00	DATA 0x00	DATA 0x00	DATA 0x00	DATA 0x00	CRC 0xCE	CRC 0x78
10101011	1101	0111	01010101	01010101	01101010	10101010	10101010	10101010	10101010	10101010	11111100	10100001

Table 2. Transmitting "A" key event information

A maximum of 8 bytes are allocated in the data field on a low-speed connection. The field size may be smaller, but the tested USB keyboard had the following configuration: the first 2 bytes are zero, the next byte is the HID code of the key, and the remaining 5 bytes are zero. [6] The checksum is calculated on the data field.

Information about the keystroke event is transmitted only once. Press time, uppercase/lowercase, layout, key combinations - all calculated by the keyboard driver that determines what to do.

Fig.7. "A" key press event

If the data is accepted without errors, the host sends a dialog packet to confirm receipt. [0010] PID ACK 0010_2, the receiver accepts the data packet without errors and [0111] Check. When several keys are pressed simultaneously, the scan codes will be transmitted sequentially. When one of the pressed keys is released, the HID codes of the keys that are still pressed will be transmitted. The maximum number of keys at a time is seven, pressing the eighth key is ignored. When the last key is pressed, 8 null bytes of data are transmitted. [5]

In the tests performed, it was found that, in order to intercept the parasitic electromagnetic emissions emitted by the keyboard, the operating frequency range of the complex should be from 3-6 kHz to several tens and even hundreds of MHz. The bandwidth of the receiving device must be adjusted in the range 1 kHz-10 MHz in steps of 1 kHz or less. The noise level of the receiving device, measured at the bandwidth of the receiver $\Delta F = 1Hz$, shall not exceed 165 dBm. [7]

The possibility of detecting a deterministic signal S_0 is calculated by the following formula:

$$S_0 \approx \Phi\left[q_c - \Phi^{-1}(1 - S_{fp})\right]$$

where $q_c = \sqrt{2\frac{E_p}{N_o}}$, represents the signal-to-noise ratio at the output of the appropriate filter (optimal receiver). The calculation formula for S_0 gives the relationship between the probability of a correct detection, the probability of a false alarm and the signal-to-noise ratio at the appropriate filter output and defines the detection curves (Neyman-Pearson curves).

To recognize the keystroke event, the scan code sent by the keyboard controller to the data cable must be intercepted. Assuming that the probabilities of correctly detecting each pulse in the scan code signal are independent, the probability of intercepting the scan code S can be calculated by the formula:

$$S_{sc} = \prod_{i=1}^{m} S_{0_i} \approx (S_0)^m$$

where S_{0_i} represents the probability of correctly detecting the pulse *i* of the scan code, and *m* represents the number of bits used to transmit the scan code.

For example, in the case of PS/2 keyboards that use a byte to transmit the scan code of a key, the probability of intercepting it will be $S_{sc} \approx (F_0)^8$. Given the threshold value of the probability of intercepting the scan code S_{sci} and the probability of a false-positive value S_{fp} from the two formulas stated above, the maximum allowed value of the signal-to-noise ratio σ can be calculated for a deterministic signal as follows.

$$\sigma \approx \Phi^{-1}\left(\sqrt[m]{S_{sci}}\right) + \Phi^{-1}\left(1 - S_{fp}\right)$$

For a random phase signal:

$$\sigma \approx \Phi^{-1}\left(\sqrt[m]{S_{sci}}\right) + \sqrt{2\log_e\left(\frac{1}{S_{fp}}\right)}$$

The threshold value of the signal-to-noise ratio can also be determined by the Neyman-Pearson curves. Thus, in order to evaluate the possibilities of intercepting the parasitic radiation emitted by the keyboard, it is necessary to calculate the signal-to-noise ratio of the voltage at the output of the appropriate filter (optimal receiver) q and compare it with the threshold value σ.

Given that for an optimal receiver the filter bandwidth is $\Delta F = \frac{1}{\tau}$ and assuming that the pulse shape is rectangular, the signal-to-noise voltage ratio at the output of the appropriate filter (optimal receiver) q can be calculated by the formula:

$$q_c = \sqrt{\frac{2E_p}{N_0}} \approx \sqrt{\frac{2S_p \cdot \tau}{N_0}} = \sqrt{\frac{2S_p}{N_0 \cdot \Delta F}}$$

where S_p represents the power of a single pulse at the input of the recognition receiver. Assuming that the input impedance of the antenna and receiver match, we can write the above formula as

$$q_c = \frac{U_p}{\sigma_n \cdot \sqrt{\Delta F}}$$

where U_p represents the signal voltage at the input of the recognition receiver, and σ_n represents the average square root of the noise voltage, reduced at the input of the recognition receiver and measured at a bandwidth of 1 Hz.

5. Conclusions

This paper shows that it is possible to create a receiver outside the inspectable space[1]. Because the parameters that allow interception have been identified, measures can be taken to protect the keyboard. The first way to protect it is to shield the keyboard which can be done either by spraying a metal layer on its plastic body, or replacing it with a thin metal body. The data cable is also replaced with a shielded one. The second way is to implement the dynamic change of the scan code table from the keyboard, and vice versa decoding into a standard table with a special decoder. Because the main transmitter is the keyboard data cable, which acts as an antenna, even if it is possible to intercept the signal with the scan code, it will be difficult to pair it with the key it has encoded.

We can conclude that the TEMPEST phenomenon is extremely complex and that the methods of protection against compromising electromagnetic radiation are expensive. The TEMPEST zonal protection model is one of the most effective measures for the protection of equipment that processes, stores or transmits classified information, as it correlates the degree of TEMPEST vulnerability of equipment with the protection provided by the environment in which such equipment is installed and operated. However, certain factors may change the electromagnetic characteristics of the location,

[1] the three-dimensional physical space surrounding equipment that processes classified information in which the operation of TEMPEST is not considered practical or where there is no structure capable of identifying and / or removing a potential operation of TEMPEST

possibly as a result of: changes in the structure of the location, interior adjustments (partitioning, etc.) or changes in the size of the inspectable space.

References:

[1] Arthur O. BAUER, *Some aspects of military line communications. The History of Military Communications*, Proceedings of the Fifth Annual Colloquium, Centre for the History of Defence Electronics, Bournemouth University, 24 septembrie 1999

[2] Fabio GARZIA, *Handbook of Communications Security*, WIT Press, 2013, pg. 617-619, ISBN 978-1-84564-768-1

[3] Peter WRIGHT, *Spycatcher – The Candid Autobiography of a Senior Intelligence Officer*, Heinemann Publishers, Australia, 1987, ISBN 0-85561-166-9

[4] Wim van ECK, *Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?*, Computers & Security, nr. 4, 1985, https://cryptome.org/emr.pdf, accessed on February 13, 2021

[5] USB 2.0 Specification, *Universal Serial Bus Specification, Revision 2.0*, April 27, 2000, pag.157, https://www.usb.org/sites/default/files/usb_20_20190524.zip, accessed on August 31, 2020

[6] Microsoft, *USB HID to PS/2 Scan Code Translation Table*, https://download.microsoft.com/download/1/6/1/161ba512-40e2-4cc9-843a-923143f3456c/translate.pdf, accessed on August 31, 2020

[7] Martin VUAGNOUX, Sylvain PASINI, *Compromising Electromagnetic Emanations of Wired and Wireless Keyboards*, 18th USENIX Security Symposium 2009, Montreal, Canada, August 2009, https://www.usenix.org/legacy/events/sec09/tech/full_papers/vuagnoux.pdf, accessed on August 31, 2020