Software development and hardware means of hidden usb-keylogger devices identification

I I Barankova, U V Mikhailova and G I Lukyanov

Nosov Magnitogorsk State Technical University, 38 Lenina avenue, Magnitogorsk, 455000, Russia

Abstract. Identifying keylogger is a simple task implemented by analyzing program code and identifying suspicious activity. The keylogger identification made as a technical device is a difficult operation in connection with hiding the electromagnetic fields of such devices. Therefore, the implementation of a firmware module for detecting hidden USB-keylogger devices is very relevant at present. The article presents the technical modules and block diagram of the developed device. An algorithm for detecting hidden devices is demonstrated and the analysis of the device operation is done. Conclusions and recommendations for identifying hidden keylogger devices were formulated.
Keywords: firmware system, information security, USB-keylogger, hidden devices detection, analysis of electrical indicators

1. Introduction

The modern world development in the field of information and digital technologies is conducive to the old methods improvement and the emergence of new spy intelligence methods. A vast variety of information on software and hardware solutions implementing leak channels and information on their implementation is available on the Internet. All this allows an attacker to easily use the necessary device or program without difficulty. One of these solutions is a keylogger, which everyone is known as a software keylogger that allows you to register various user actions – keystrokes on a computer keyboard, movement and mouse clicks, etc.

After analyzing the Internet, you can get a huge software developments list that implements the keylogger functionality, which is updated and increase every day. Protection from such software keylogger consists in updating the operating system, the presence of antivirus with an updated database and the use of other software solutions. But, as everyone knows, an attacker is always one step ahead than means of protection. In addition to the software implementation of the keylogger, there are also hardware implementations. Such devices are small-sized equipment that can be located in near the cable using non-contact reading, or inside the system unit, keyboard, using a mechanical connection. The detection of such devices is possible by detecting the electromagnetic field and determining the wireless communication channel. However, shielding and the lack of wireless connectivity make keylogger detection is difficult.

2. Problem statement

Improving the hardware keylogger will allow you to hide the device from the basic detection methods. In this connection, a required method is not based on the identification of the electromagnetic field or wireless channel of the device. Therefore, we had a task to develop a new method for detecting a keylogger.

Identifying keyloggers in manual mode is very inconvenient, as it is caused by a significant expenditure of time for searching. Therefore, the automation of the implemented method is an integral part of the project. As a result, we decided to implement a portable device with autonomous power, which allows us to search for keyloggers.

3. Experimental methodology

Hardware keyloggers differ in functionality and location in the keyboard-PC circuit. Figure 1 shows the possible location options of the funds in question.

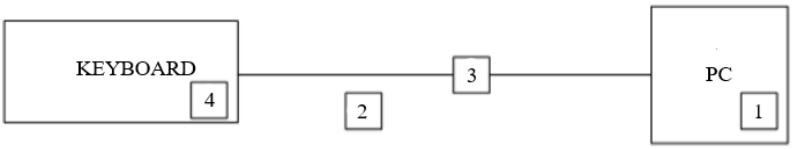


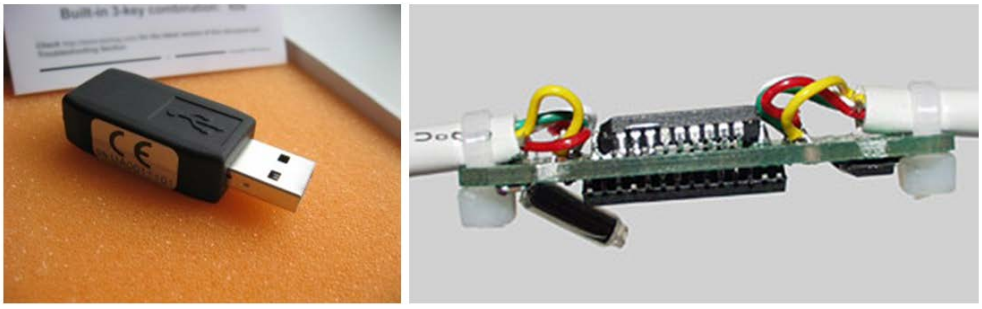
Figure 1. Keylogger location options**.**

Let's consider in more detail the implementation of keyloggers per under the location. The first possible location is the PC. These keyloggers can be located on a printed circuit board or in the peripheral port module (USB, PS/2) of the motherboard. This method of installing a keylogger is difficult. This is due to the complexity of replacing the motherboard, and if the PC is sealed, then these actions will be easily detected [1-3].

If mechanical intervention is not possible, then the attacker can use the non-contact option (Figure 2), which receives the useful signal from the keyboard wire using electromagnetic interference and can be located near the cable, as shown in Figure 1 (2). Such an information retrieval device is easy to detect since it must be at a short distance from the wire. Also, due to its design features, it is impossible to hide electromagnetic radiation on this device [4-9]

Figure 2. Contactless hardware keylogger.

The last way to arrange the keylogger is to install it in the keyboard in several ways. One option is to install it in a cable under the guise of a filter (Figure 3a) or between the cable and the connector in a PC (Figure 3b). Another option is to install it inside the keyboard. The latter option is more common, because the keyboard body has a lot of space, and therefore the implementation of the keylogger is simplified. The design of the keylogger inside the keyboard is similar to the keylogger installed in the cable break.



a) b)

Figure 3. Contact hardware keyloggers.

Identification of the latter keyloggers type is possible by visual inspection of the cable or the keyboard insides. However, careful concealment of such devices will not make it possible to visually determine the presence of a keylogger. As mentioned earlier, in the presence of shielding and the absence of a wireless communication channel, it will not be possible to identify the keylogger by technical means. Therefore, we proposed to perform keylogger detection by keyboard voltage-current characteristics [10-11].

Consider the structure of the developed device that allows you to analyze the keyboard. As mentioned earlier, one of the tasks was the implementation of a portable device that allows automated inspection. Modules of the Arduino family or other devices capable of working with a serial asymmetric I2C bus are suitable for this task. Per under the set requirements, we chose the raspberry pi 3 device. This choice is due to a possible subsequent modernization and implementation of a multifunctional device. Since this device cannot independently measure voltage-current characteristics, the INA219 module was selected (Figure 4), which makes it possible to carry out such measurements and transfer data to the raspberry via the I2C bus [12–13].

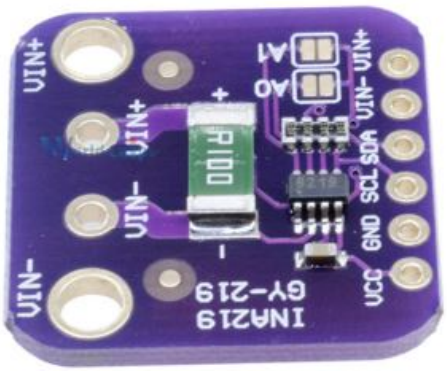


Figure 4. INA219 module.

The INA219 module allows measurements of current values up to 3A and voltages up to 36V, and the interface speed is 3.4MHz. The serial interface of the version up to USB 2.0 inclusive provides power to peripherals up to 0.5A, and the isochronous channel delivers packets at a maximum speed of 8kHz.

After analyzing the schemes for connecting keyloggers to the keyboard, two typical schemes can be distinguished. One installation scheme is made into a cable break, the second uses a parallel connection. However, both equally affect the electrical performance of the general USB connection scheme (Figure 5). Having performed the analysis of keyboards with installed keyloggers, the keyloggers influence only on the supply circuit was revealed.

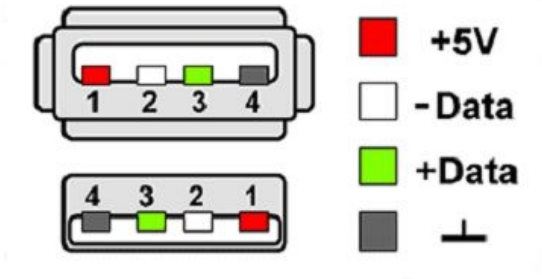


Figure 5. USB 2.0 pinout.

Consider the scheme of the developed portable device for identifying keyloggers (Figure 6). To connect the INA219, (use) the GPIO connector located on the raspberry pi board is used. To power the sensor we use 3.3V power. The connection diagram can be seen in the presented figure (Figure 6). The

current consumption of the keyboard is measured by breaking the power circuit of the USB port. The power failure was realized by introducing the "1" jumper module (Figure 6). An important note is that the installation of the module is performed in front of the USB tower interface and its installation in the general power supply circuit of the interface is not allowed. This module implementation allows you to switch the interface operating modes. Mode "a" (Figure 6) disables the INA219 and measurements aren't made. In the position of jumpers "b" (Figure 6), the readings of the power circuit are supplied to the measuring sensor and readings of the consumed current indicators are made.

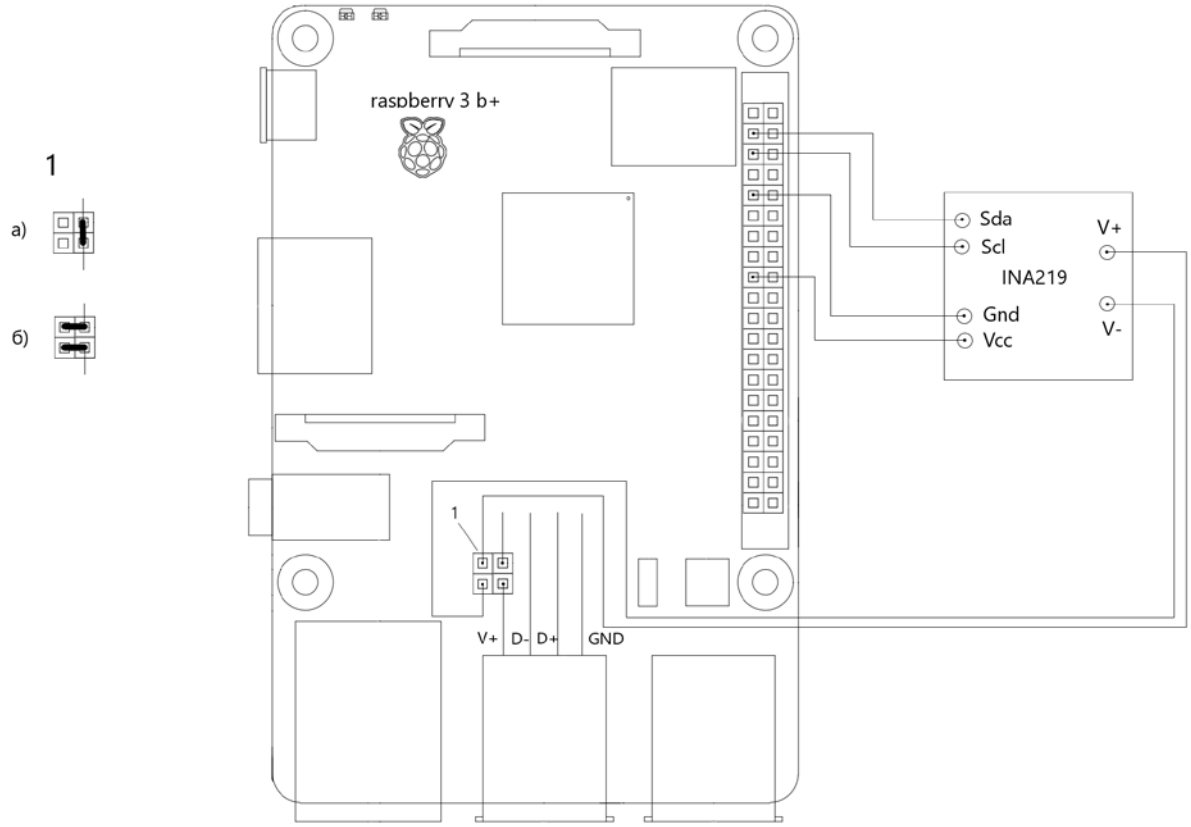


Figure 6. Connection diagram of a portable device.

The keyboards were analyzed using the developed scheme. For testing, we chose keyboards with a minimum set of functionality, namely, without additional backlighting, with a missing USB hub and audio interfaces. Table 1 shows the current consumption of the keyboards.

Table 1. USB keyboards consumption.

Company	Model	Passport current consumption, mA	Consumption current, mA
Microsoft	CCK 2000 v1	100	99
Defender	HM-830 RU	100	100
	HM-710	100	95
	UltraMate SM-530	110	102
Genius	Smart KB-101	100	94
	Genius KB-110	100	104
	SlimStar 130	100	100
Logitech	K120	120	112
	K200	110	105

The analysis shows that the keyboard consumption corresponds to the passport data with the indication of all Numlock, Shift, ScrollLock buttons on only two models. This result is due to the measurement error, as well as the averaged values indicated by the manufacturer. For the further experiment, we will use the Microsoft CCK 2000 v1 keyboard and two versions keyloggers (used for educational purposes). One version is installed in the gap between the PC and the keyboard, the second is soldered in parallel to the keyboard controller.

4. Experimental results

When keyloggers were introduced into the PC keyboard connection, it was revealed that the keylogger was not identified by the PC as a third-party device. Further analysis was carried out after installing the keyboard in the raspberry pi OS and ready for full operation. Figure 7 shows the graphs of the current consumption with the installed keylogger of different versions.

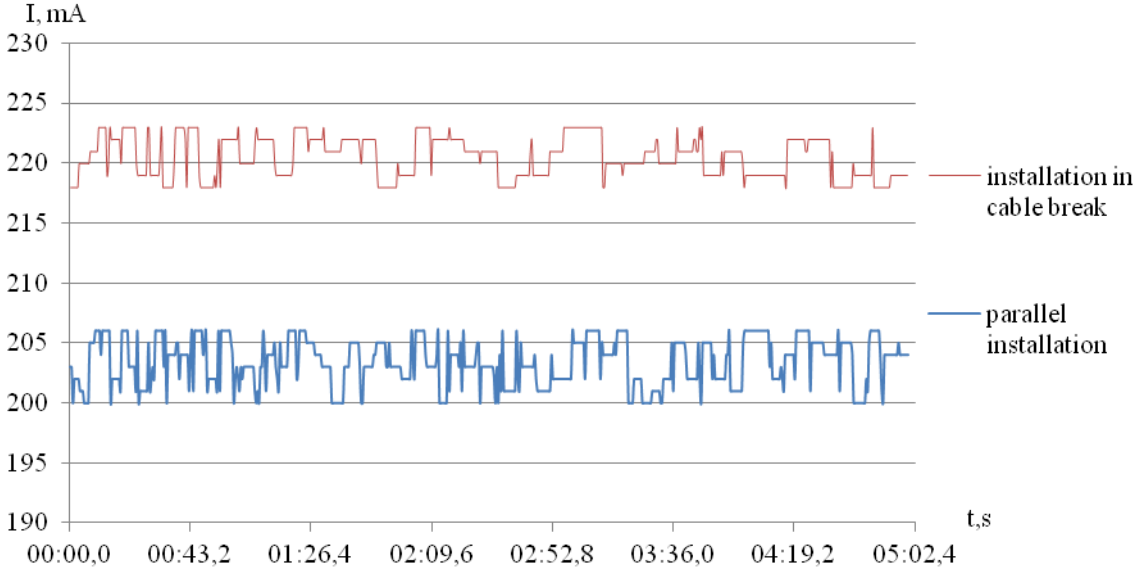


Figure 7. Current consumption of keylogger keyboard.

The data obtained show that if there is a keylogger into the keyboard connection circuit, there is an increased current consumption of more than 2 times the passport value of the keyboard without a keylogger. The difference in values when a keylogger installing in cable break or parallel is explained by different device schemes.

5. Results and discussion

Identifying a hardware keylogger is possible by determining the current consumption of the keyboard. As described above, when there is a device in the circuit, it significantly changes the passport current consumption indications of the keyboard. During an additional experiment, the essence of which was measurements with the key held down, an additional increase in the current consumption by 5..10 mA was revealed. This proves the presence of side consumers in the connection diagram.

The developed complex allows you to determine the presence of keyloggers, but at this stage, its difference from the USB tester is not significant. Further promising development of this device is software development, which forms a research protocol with a conclusion about a keylogger presence. In particular, it is planned to expand the device functionality. Since raspberry pi allows you to connect multiple sensors, it is possible to additionally introduce an electromagnetic field indicator and an analyzer of wireless information transfer into the device. Such a device modernization will allow a full analysis of the presence of hidden keyloggers installed in the keyboard.

6. Conclusions

Using any type of keylogger as espionage may result in criminal liability. At the same time, the development of the market for such devices doesn't stand still and the issue of identification doesn't lose its relevance. The analysis showed a variety of types of keyloggers scanning user activity on the

keyboard. During the study, a complex based on raspberry pi and INA219 was developed to identify hardware keyloggers installed in a cable or inside a keyboard. The principle of the complex is based on measurements of current consumption by the keyboard interface. Further development of this device allows you to supplement it with survey logging software. In particular, it is planned to implement a multifunctional device to perform complete technical measures to detect keyloggers, which allows the demonstrated platform.

References

[1] Somova E V and Dunaevsky A S 2017 *Keyloggers as an actual information security problem* (Innovative development of modern science: problems, patterns, prospects, collection of articles of the V International Scientific and Practical Conference: at 3 parts) pp 60–62
[2] Shlykova A V and Khaitzhanov A 2014 *Special equipment used in the commission of crimes* (Science. Society. State) **2 (6)** pp 120–130
[3] Bashly I P and Chernysheva N I 2015 *Information security as a key factor in ensuring national economic interests* (Logistics in the portfolio of import-substituting industrialization resources: anti-crisis growth and development strategies under conditions of sanctions restrictions materials of the international scientific and practical XI South Russian logistics forum) pp 243–246
[4] Blokhina E E 2018 *Software and hardware keyboard spies* (In the world of scientific discoveries Materials of the II International Student Scientific Conference) pp 160–162
[5] Horev A A 2010 *Technical channels of information leakage processed by computer technology* (Special equipment) **2** pp 39–57
[6] Kopyrulina O A and Ustyuzhanin E.V. 2018 *Keylogger as a protection means at the enterprise* (Bulletin of modern research) **10.1 (25)** pp 301–303
[7] Xiao Y, Vrbsky S V, Li C C Lei M 2014 *Differentiated virtual passwords, secret little functions, and codebooks for protecting users from password theft* (IEEE Systems Journal) **8** pp 406-416.
[8] Tuli P and Sahu P 2013 *System monitoring and security using keylogger* (IJCSMC) **2** pp 106 – 111
[9] Sagiroglu S and Canbek G 2009 *Keyloggers increasing threats to computer security and privacy* (IEEE Technology and Society Magazine) **28(3)** pp 10 – 17
[10] Creutzburg R 2017 *The strange world of keyloggers – an overview, Part I* (Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications) pp 139–148
[11] Yadav S and Randale R 2015 *Detection and prevention of keylogger spyware attack* (International Journal of Advance Foundation and Research In Science & Engineering (IJAFRSE)) **1** pp 1–5
[12] Texas instruments 2008 *INA219 Zero-drift, bi-directional current/power monitor with I2C interface* p 33
[13] Dorofeev A V and Rautkin Yu V 2017 *Applied aspects of security testing* (CEUR Workshop Proceedings conference proceedings) pp 49–53