Vojnotehnicki glasnik/Military Technical Courier
ISSN: 0042-8469
ISSN: 2217-4753
vojnotehnicki.glasnik@mod.gov.rs
University of Defence
Serbia

Security of wireless keyboards: Threats, vulnerabilities and countermeasures

Jovanovi#, Siniša V.; Proti#, Danijela D.; Anti#, Vladimir D.; Grdovi#, Milena M.; Baji#, Dejan A.
Security of wireless keyboards: Threats, vulnerabilities and countermeasures
Vojnotehnicki glasnik/Military Technical Courier, vol. 71, no. 2, 2023
University of Defence, Serbia
Available in: https://www.redalyc.org/articulo.oa?id=661774773004
DOI: https://doi.org/10.5937/vojtehg71-43239

Original scientific papers

Security of wireless keyboards: Threats, vulnerabilities and countermeasures

Безопасность беспроводных клавиатур: угрозы, уязвимость и меры противодействия

Безбедност бежичних тастатура: претње, рањивости и мере заштите

Siniša V. Jovanović a
Serbian Armed Forces, Serbia
sinisa.jovanovic711@gmail.com
https://orcid.org/0009-0002-6088-9553

Danijela D. Protić b
Serbian Armed Forces, Serbia
danijelaprotic318@gmail.com
https://orcid.org/0000-0003-0827-2863

Vladimir D. Antić c
Serbian Armed Forces, Serbia
vladimirantic2013@gmail.com
https://orcid.org/0000-0001-9843-0743

Milena M. Grdović d
Serbian Armed Forces, Serbia
milena.grdovic@gmail.com
https://orcid.org/0000-0003-4310-7935

Dejan A. Bajić e
Serbian Armed Forces, Serbia
strelacyu@yahoo.com
https://orcid.org/0009-0007-5283-4110

DOI: https://doi.org/10.5937/vojtehg71-43239
Redalyc: https://www.redalyc.org/articulo.oa?id=661774773004

Received: 06 January 2023
Revised document received: 24 March 2023
Accepted: 26 March 2023

Abstract:

Author notes

a Serbian Armed Forces, General Staff, Telecommunications and Information Security Directorate (J-6), Centre for Applied Mathematics and Electronics, Belgrade, Republic of Serbia

b Serbian Armed Forces, General Staff, Telecommunications and Information Security Directorate (J-6), Centre for Applied Mathematics and Electronics, Belgrade, Republic of Serbia

c Serbian Armed Forces, General Staff, Telecommunications and Information Security Directorate (J-6), Centre for Applied Mathematics and Electronics, Belgrade, Republic of Serbia

d Serbian Armed Forces, General Staff, Telecommunications and Information Security Directorate (J-6), Centre for Applied Mathematics and Electronics, Belgrade, Republic of Serbia

e Serbian Armed Forces, General Staff, Telecommunications and Information Security Directorate (J-6), Centre for Applied Mathematics and Electronics, Belgrade, Republic of Serbia

danijelaprotic318@gmail.com

Introduction/purpose: This paper provides an overview of research on computer system vulnerabilities caused by compromised electromagnetic radiation by wireless keyboards. Wireless devices that use event-triggered communication have been shown to have critical privacy issues due to the inherent leakage associated with radio frequency emissions. Wireless connectivity technology is a source of signal emanation that must be protected in terms of performance and security.
Methods: Wireless device vulnerabilities and side-channel attacks are observed, along with electromagnetic emission of radio waves.
Results: The findings highlight a specific wireless keyboard's security and encryption flaws. The results of penetration testing reveal vulnerabilities of targeted wireless keyboards in terms of outdated firmware, encryption, wireless reliability, and connection strength.
Conclusion: Wireless keyboards have security flaws that disrupt radio communication, giving a malicious user complete access to the computer to which the keyboard is connected. An attacker can steal sensitive data by observing how the system works using compromised electromagnetic emissions.
Keywords: wireless keyboard, radio frequency, electromagnetic emission, software defined radio.

Р е з ю м е :

Введение/цель: В данной статье представлен обзор исследований уязвимости компьютерных систем, вызванных побочным электромагнитным излучением беспроводных клавиатур. Было показано, что беспроводные устройства, использующие связь, инициируемую триггерами, сталкиваются с серьезными проблемами конфиденциальности вследствие утечки, связанной с радиочастотным излучением. Технология беспроводной связи является источником излучения сигнала, который необходимо защищать с точки зрения производительности и безопасности.
Методы: Наблюдаются уязвимости беспроводных устройств и атаки по сторонним каналам, а также электромагнитное излучение радиоволн.
Результаты: В результате исследования выявлены недостатки безопасности и шифрования конкретных беспроводных клавиатур. Результаты тестирования на проникновение показали уязвимость беспроводной клавиатуры, связанной с устаревшим встроенным программным обеспечением, шифрованием и надежностью беспроводной связи.
Выводы: Недостатки безопасности беспроводных клавиатур приводят к нарушению радиосвязи, предоставляя злоумышленникам полный доступ к компьютеру, к которому подключена клавиатура. Таким образом, благодаря наблюдению за работой системы, у злоумышленников появляется возможность украсть конфиденциальные данные, используя побочное электромагнитное излучение.
К л ю ч е в ы е с л о в а : беспроводная клавиатура, радиочастота, электромагнитное излучение, программно-определяемое радио.

Abstract:

Увод/циљ: Рањивост рачунарских система узрокована је компромитујућим електромагнетским зрачењем са бежичних тастатура. Показано је да бежични уређаји који користе комуникацију базирану на тригерима имају проблеме који се односе на приватност, што је узроковано електромагнетским отицањем повезаним са емисијом радио-таласа. Технологија бежичних веза извор је еманације сигнала који мора бити заштићен у погледу перформанси и безбедности.
Методе: Уочавају се рањивости бежичних уређаја и напади на бочне канале, упоредо са електромагнетском емисијом радио-сигнала.
Резултати: Указано је на грешке у безбедности и енкрипцији за одређене бежичне тастатуре. Резултати пенетрационих тестова откривају рањивости циљане бежичне тастатуре у погледу застарелог фирмвера, енкрипције и поузданости бежичне мреже.
Закључак: Бежичне тастатуре имају безбедоносне пропусте који омогућују ометање радио-комуникације, дајући злонамерном кориснику потпун приступ рачунару на који је тастатура повезана. Стога он може да украде осетљиве податке посматрајући рад система и користећи електромагнетску емисију.
Keywords: бежична тастатура, радио-фреквенције, електромагнетска емисија, софтверски дефинисани радио.

Introduction

Manipulation and compromise of wireless devices are not new concepts. Wireless devices that use event-triggered communication have been shown to have critical privacy issues due to the inherent leakage associated with radio frequency (RF) emissions (Oligeri et al, 2020, pp.231-241). Wireless keyboards allow users to move keyboards to a more comfortable or visually pleasing position, resulting in a mess-free

workspace. These keyboards, on the other hand, are not typically selected or used with security in mind, and a surprising number of wireless keyboards affected by multiple vulnerabilities can allow malicious users to completely compromise the computers to which these devices are connected.

This paper advances the attack frontier by reviewing inexpensive, easy-to-implement, efficient, and effective attacks capable of detecting typing on a wireless keyboard. Such attacks are particularly harmful because they succeed even when an eavesdropping antenna is several meters away from the target keyboard, regardless of the encryption scheme, communication protocol, radio noise, or physical obstacles. We also discuss attacks on wireless capabilities, such as wireless access points, routers, mice, and keyboards. However, it is critical to understand that of all wireless risks, not just those associated with network connectivity must be considered (Sheimo, 2021). In terms of performance and security, wireless connectivity technology is also a source of signal emanation and must be protected (Logitech, 2023). Furthermore, we offer some recommendations for mitigating attacks.

This paper is organized as follows. Wireless keyboard layouts and standards are covered in the second chapter. The third chapter discusses wireless security, vulnerabilities, and threats. The fourth chapter is about penetration testing. The final chapter concludes the paper.

Computer keyboards

The computer keyboard is a primary component needed while working on desktops. There are various types of keyboards available in the market, and choosing the best one is dependent on the user's requirements. Selecting a layout such as QWERTY, QWERTZ or AZERTY can influence the decision on what type of keyboard should be used for a specific purpose.

Computer keyboard layout

A keyboard is a type of input, a peripheral device that allows users to enter text into another electronic device and communicate with a computer in the simplest way possible. It is made up of a number of buttons that generate numbers, symbols, letters, and special keys. The design of the keyboard is inspired by typewriter keyboards, and the arrangement of numbers and letters on the keyboard aids in typing speed. Table 1 shows the most commonly used keyboard layouts.

TABLE 1
Keyboard layouts (WebNots, 2022)

Keyboard layouts	Description
Ergonomic	Designed to reduce wrist and arm pain. Curvy to accommodate palms and provide a comfortable experience.
Flexible	Foldable and portable. Made of rubber-like material resistant to water and dust. Bluetooth keyboards with a connector. Require a hard surface to be placed on and typed on.
Mechanical	Designed for heavier usage. Keys are placed on spring-activated switches. An electric circuit sends signals to the computer based on the pressed keys. Produces more noise than rubber membrane keyboards, but they reduce the possibility of accidentally pressing a different key.
Membrane	Keys tightly packed and occasionally protected by a transparent membrane. Lightweight and resistant to dust. Error-prone nature when typing.
Multimedia	Include multimedia keys for play, pause rewind, forward, and volume adjustments. May be useful if the user frequently watches videos or listens to music. The keyboard replaces the controls on a computer's video/audio player apps. Some may include gaming controls.
Projection	Come with a default onscreen or touchscreen monitors. Eliminates need for a physical keyboard. Lack physical components in the layout section. Necessitates use of a small handheld device connected to the computer via Bluetooth or USB cable. When turned on, the device displays a laser projection of the keyboard layout.
Wireless	Connect to computers via Bluetooth or USB RF. To use it, customer should insert a small connector into the USB port and turn on Bluetooth

Таблица 1 – Раскладка клавиатуры (WebNots, 2022)
Табела 1 – Тастатура (WebNots, 2022)

Keyboard standards

The keyboard is primarily used to enter the alphabet, numbers, commands, and other data into a computer (see Table 2). It has over 100 keys (see Figure 1) (Chauhan, 2020). Most keyboards today use one of three different physical layouts by the (1) worldwide International Standard Organization/International Electrotechnical Commission ISO/IEC 9995-2 standard, (2) American National Standard Institute ANSI-INCITS 154-1988 standard, and (3) Japanese Industrial Standard (JIS) X 6002-1980 (ANSI webstore, 1999).

TABLE 2
Key type description (Chauhan, 2020)

Keyboard keys	Description
Navigation	Turn the page up and down (arrows, Home, End, Insert, Delete, Page Up, Page Down)
Function	Used to perform specific tasks (F1-F12)
Control	Mostly used in combination with other keys to perform specific tasks (Ctrl, Alt, Windows key, Esc)
Typing	Alphanumeric keys, symbols and punctuation marks
Numeric	Equal to calculator keys, at the right side of the keyboard
Special	Used to perform special functions related to the computer system (Shift, Enter, Alt, Ctrl, Esc)

Таблица 2 – Описание клавиш (Chauhan, 2020)
Табела 2 – Опис тастера (Chauhan, 2020)

FIGURE 1
Keyboard keys (Chauhan, 2020)
Рис. 1 – Клавиши (Chauhan, 2020)
Слика 1 – Тастери (Chauhan, 2020)

Figure 2 shows physical division and a reference grid defined by ISO/IEC 9995 standard series. The sections are further subdivided into zones as follows:

· alphanumeric section:
o alphanumeric zone (green),
o function zone (blue),
· numeric section:
o numeric (dark red),
o function (lighter red),
· editing/function section:
o cursor keys (darker grey),
o editing function zone (lighter grey).

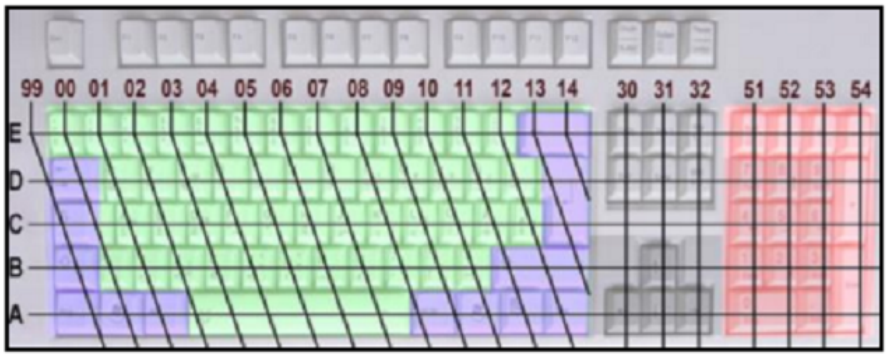

FIGURE 2
ISO/IEC keyboard (ISO, 2009)
Рис. 2 – Клавиши ISO/IEC (ISO, 2009)
Слика 2 –Тастатура ISO/IEC (ISO, 2009)

Each key can be identified using the reference grid by a unique combination of a letter (indicating the row) and a two-digit sequence (indicating the column). The labelling rules allow for function keys to be arranged in rows other than above the alphanumeric section (thus, an AT keyboard is compliant with the standard):

- Columns containing editing/function keys should be numbered from 60 onwards if they are placed beyond a right numeric section, or from 80 onwards if they are placed left of the alphanumeric section.
- Rows above the alphanumeric section should be labelled beginning with K, and rows below the space key should be labelled beginning with Z.
- The grid can be angled or squared.

The characters that can be entered using the keys in the alphanumeric section are organized in levels. Level 1 contains lower-case letters, while Level 2 contains capital letters (e.g. unshifted/shifted). There are no rules governing the distribution of non-letter characters, while digits are most commonly found in Level 1. The standard allows for a third level (characters are selected by the means of an AltGr key). If the three-level organization of the keyboard is insufficient to accommodate all characters to be contained in a specific layout, "groups" may be defined as a higher hierarchical unit than levels. The Japanese keyboard layout, as well as the Canadian Quebec layout and the German T2 layout, are common examples of layouts that allow characters from different scripts to be input (ISO/IEC 9995-1, 2009).

ANSI-INCITS 154-1988 standard describes the layout of the 48 keyboard basic keys as well as the upper- and lower-case characters that can appear on the keys (ANSI webstore, 1999). In recognition of the various graphic character requirements of each application, the character assignments are divided into five application areas.

The Japanese Industrial Standard specifies the layout of a keyboard used for information processing with both hands that implements the JIS X 0201 7-bit alphanumeric-katakana code (JSAJIS, 2018). This standard specifies the relative positions of keys on a keyboard but does not specify key spacing, keyboard inclination, keytop and space bare shapes, or else. This standard makes no mention of character representation on keytops.

Keyboard prevalence

The QWERTY keyboard is widely used in the Americas and parts of Europe. In German-speaking countries, the QWERTZ keyboard, also known as the Swiss keyboard, is used, whereas in France and Belgium, the AZERTY keyboard is standard. American keyboards used to be alphabetically organized. This layout, while logical, presented some technical challenges. Some of the most commonly used keys were placed near one another, their mechanisms too close next to each other. As a result, the letters and the QWERTY keyboard

had to be rearranged. Because the most commonly used characters vary from language to language, a slightly different layout was chosen in certain non-English-speaking areas. German speakers adopted the QWERTZ keyboard because the letter Z is more common than the letter Y. New keys have also been added in several countries. For example, the keys needed to enter French accents were added to the traditional English QWERTY layout. QWERTY was retained in Spain and Latin America, but with the addition of Ñ, a commonly used character in Spanish.

Wireless keyboard security

Because wireless signals travel through the air and can be intercepted and read by a skilled attacker, wireless devices are almost always a security risk. The wireless link is usually encrypted with an encryption algorithm such as the Advanced Encryption Standard - AES (NIST, 2001), which is widely used to protect the majority of wireless keyboards. However, using a Software Defined Radio (SDR), for example, encrypted signals can be recorded. Wireless Universal Serial Bus (USB) dongles are also at risk. Unencrypted input can still be sent to the dongle and used to access the attached computer and send signals while the keyboard is connected to the dongle in an encrypted session (Weiss, 2023).

Wireless communication

Wireless communications are globally regulated, but certain bands are reserved for unlicensed users. The industrial, scientific, and medical (ISM) bands which range from 2.4 GHz to 2.5 GHz and are defined as such by the International Telecommunication Union Radio Regulation are one example. Wireless keyboards also use the ISM band (Tomsic, 2022). Analog RFs are used to transmit digital data using various modulation techniques such as frequency shift keying (FSK). Because the use of two distinct discrete frequencies allows for the transmission of either zero or one, binary data can be transmitted over an analogue channel. The digital data transmitted by a radio transceiver will have limitations on how frequently a new symbol can be sent, which will affect the data rate. To convey the correct data, a transmitter and a receiver must use the same data rate and be synchronized. A protocol must be used to structure the data transmitted between devices. The protocol stack typically defines a logical link frame as a preamble (a series of bits) to allow the receiver's clock to be synchronized with that of the transmitter, a destination address, and data. Some protocols make use of other fields, and the exact protocol specifications vary greatly between manufacturers and devices (Pohl & Noack, 2019). Because software-defined radios are devices in which many radio components are replaced with software variations of them, it is possible to control the radio flexibly through software and adapt it to a wide range of applications and scenarios. This, however, makes it useful in debugging and research situations where the system under investigation by a malicious user is not completely known (Sadiku & Akujuobi, 2004, pp.14-15).

Wireless keyboard security vulnerabilities, threats, and countermeasures

Every wireless device has weaknesses that malicious users can take advantage of. The top ten sources of vulnerability, as identified by Bastille Networks in 2020 and presented by de Jesus Rugeles Uribe et al. in 2022, include, among other things, wireless peripherals that are open to Keystroke injection attacks on keyboards without data encryption. A hacked wireless keyboard could reveal sensitive information because of the wireless keyboard flaws such as:

- Flaws in encryption: the signal travels unprotected through the air and is easily intercepted.

• Firmware flaws: even if a wireless keyboard is encrypted, firmware bugs can be used to read the wireless signal.

• Keylogger: a type of spyware that records every keystroke and sends the stolen information back to the attackers.

• Keysniffer: a set of security flaws affecting non-Bluetooth wireless keyboards from eight different vendors (Anger, EagleTec, General Electric, Hewlett-Packard, Insignia, Kensington, Radio Shack and Toshiba) since they use unencrypted radio communication protocols enabling an attacker to eavesdrop on all the keystroke typed (Bastille Networks Internet Security, 2023).

• A compromised access point: cybercriminals can install rogue access points in public places with the intent of stealing data from unsuspecting users who connect to them.

To help in the prevention of wireless keyboard attacks, the connections must be as secure as possible. The first step is to ensure that the firmware of the keyboard is up to date and that the connections it establishes are encrypted. Bluetooth devices should also use the Secure Connection only mode, which is compliant with the Federal Information Processing Standard (FIPS) developed by the National Institute of Standards and Technology (NIST). Furthermore, an anti-rollback feature for security-based device firmware upgrades should be considered for keyboards that connect via a USB dongle. This prevents critical security patches from being unintentionally removed while still allowing non-security-related updates to be rolled back. Third, the encryption algorithms, such as AES which is the most known symmetric algorithm today, should be used. When two devices connect, a key is generated and shared between them. The key is then used by the devices to encrypt and decrypt the data they transmit and receive (Griskenas, 2023).

Side channel attacks over USB connection

The most common standard used to connect wired peripheral devices to a main host and transmit data is the USB standard. The standard has evolved over the years, going from version 1.1 to the most recent version 4.0, which supports a transmission rate of up to 40 Gbps (Liu et al, 2021). Different plugs, transmission speeds, and power delivery capacities define each standard. The ability to power or recharge standalone devices is just one example of the new features that could be integrated thanks to the evolution of the USB standard over time. As a result, the USB standard is now used for a variety of purposes, expanding the range of peripheral devices that are mutually compatible, while also exposing brand-new vulnerabilities. Malicious users today take advantage of the default trust on USB ports to extract sensitive data from wireless devices. Despite efforts by security experts and manufacturers to detect and block threats to a wireless keyboard, an even more subversive approach to compromising user privacy relies on a USB side-channel attack (Liu et al, 2021).

According to Barthe et al (2018, pp.328-343), side-channel attacks are typically physical intrusions in which malicious parties steal protected and confidential data by observing how the system operates physically. To defeat a cryptographic system, these attacks use specific factors like electromagnetic (EM) radiation, timing, and power consumption (Mangard et al, 2007). The goal of every side-channel attack is to exploit an unintentional emission (Sayakkara et al, 2018; Grdović et al, 2022, pp.836-855). This problem is also related to Compromising EM radiation (CER), which is primarily associated with devices protected by some of the cryptographic methods (Markagić, 2018, pp.143-153). In general, attacks on user information can be either passive or active, with the former having no effect on the sender, the receiver, or the data transmitted over a communication channel, and the latter involving a malicious user engaging in an attack and affecting one of these. Side-channel attacks are a type of passive attack that involves "listening" to devices, equipment and transmission to monitor communication between two (or more) parties while leaving no traces. As a result of these factors, users are frequently unaware of the attack.

A malicious user can passively and covertly record everything typed on the wireless keyboard from several meters away using an antenna, a wireless dongle, and a few lines of software code in a side-channel attack to

USB. It is a difficult-to-prevent attack that almost no one sees coming. Due to several flaws, low-cost wireless keyboards enable a malicious user to listen in from afar. Though not all wireless keyboards are created equal, and many are not vulnerable to eavesdropping, there is a simple solution to the problems caused by malicious attacks on the wireless keyboard - make use of a wired keyboard (Whittaker, 2016).

Electromagnetic emission and electromagnetic signal acquisition

Electromagnetic compatibility (EMC) is a property of electric equipment that allows it to operate as expected in the presence of other electric/electronic equipment while not interfering with it (ETSI, 2023). EMC is focused on the analysis of EM interferences of RF interferences in electric devices, to reduce the unintentional generation, propagation, and reception of EM energy. Unwanted emissions can be categorized into two groups: conductive coupling and radiative coupling. Through transmit interferences through the system, conductive coupling requires physical support (such as wires). Radiative coupling, on the other hand, occurs when an internal circuit component acts as an antenna and transmits unwanted EM waves. EMC also distinguishes two types of EM emissions based on the type of radiation source: differential mode (generated by loops) and common mode (the result of internal voltage drops) (Vuagnoux & Pasini, 2009). There are several standards, two of which are specifically related to RF, telecommunication network equipment, radio equipment and services, EN 300 386 V16.1, EN 301 489-1 V1.9.2 (ETSI, 2011; ETSI, 2012).

There are two techniques for detecting compromising EM radiation. Standard techniques include using a spectral analyser to detect signal carriers (compromised emanation is composed of peaks) or a wide-band receiver tuned to a specific frequency (scanning a receiver's entire frequency range of the receiver to demodulate the signal based on its amplitude or frequency modulation). Unfortunately, some direct and indirect EM emanations may go undetected using standard techniques, especially if the signal contains irregular peaks or erratic frequency carriers. Indeed, spectral analysers rely heavily on static carrier signals. Similarly, the scanning process of wide-band receivers is not instantaneous and takes a long time to cover the entire frequency range. Demodulation may also conceal some intriguing compromising emanations (Vuagnoux & Pasini, 2009). Novel approaches detect compromising EM emanation by directly collecting raw signals from the antenna and processing the entire captured EM spectrum, which is extremely useful for detecting EM emanations from the keyboards (both wired and wireless).

Software defined radio

SDR is a dynamic radio transmitter and/or receiver, capable of changing operational characteristics, setting or changing RF operating parameters such as frequency range, modulation type, output power, and coding rate, allowing a single hardware platform to be adapted to be a transmitter or a receiver under different technologies, based on software configuration for any type of signal through software or firmware functions (Chamran et al, 2019; Molina-Tenorio et al, 2021; de Jesus Rugeles Uribe et al, 2022). In SDR, software modules execute in real-time on microprocessor platforms. The main operational characteristics of the system can be modified or changed while running, allowing SDR to be easily reconfigured to perform different functions (Garcia Reis et al, 2012). As a result of this, as well as due to relatively low-cost technology, SDR platforms are now frequently used for side-channel attacks.

An ideal SDR has very little hardware at the RF front end, consisting of only an antenna and a very fast sampler capable of capturing and digitizing wideband radio signals. However, relatively long coverage distances may be achieved only by employing amplifiers before both analogue-to-digital and digital-to-analogue conversion (ADC/DAC) stages (see Figure 3). LNA, PA, FPGA, and DSP are acronyms for Low-

Noise Amplifier, Power-Amplifier, Fast Programmable Gate Array, and Digital Signal Processor, respectively (Stewart et al, 2015; Duarte et al, 2019, p.1490).

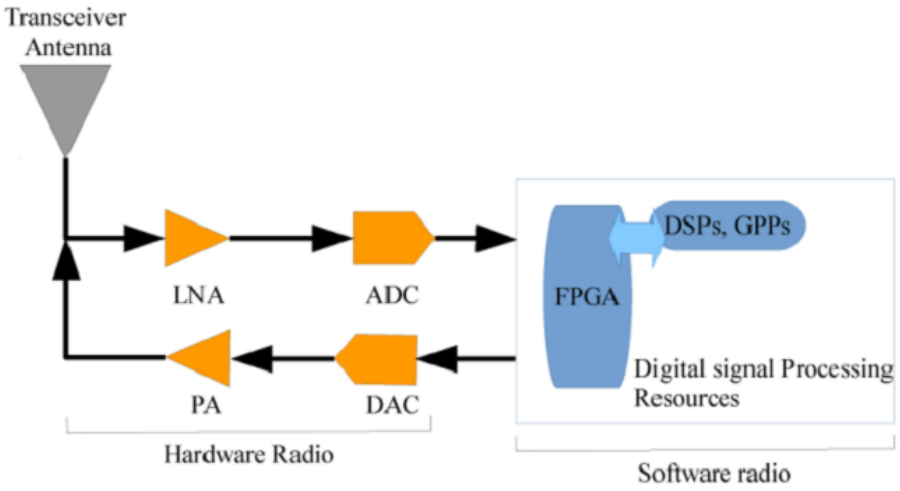

FIGURE 3
Software defined radio (Duarte et al, 2019)
Рис. 3 – Программно-определяемое радио (Duarte et al, 2019)
Слика 3 – Софтверски дефинисани радио (Duarte et al, 2019)

De Jesus Rugeles Uribe et al (2022) compare 19 commercially available SDR platforms in terms of ADC/DAC, Tx/Rx, Fmin-Fmax, Max RF Bandwidth, signal processing platforms (MATLAB, Labview), and GNU radio (free open-source toolkit available for low-cost external RF hardware to create SDRs). The following devices are classified as low-cost hardware: FUNCube, RTL, RSPduo, AirSpy, HackRF, BladeRF, LimeRF, and Pluto. These SDR platforms, together with open-source software and signal processing platforms, have enabled the global advancement of SDR technology. At the same time, the possibility of side-channel attacks increased exponentially. As a result, SDR is now opening up entirely new pathways for penetration testing and security research even though EMC standards and regulations address emerging threats from side-channel attacks. When considering the EMC requirements of devices, the International Organization for Standardization (ISO) advisory notice K.841 states that information leakage from EMC must be considered (ITU, 2014).

Penetration testing

Liu et al (2021) presented the findings of a survey on vulnerabilities and side-channel attacks related to, among other things, wireless devices and the EM emission of radio waves. The results show vulnerabilities of the targeted wireless keyboard in terms of keystrokes as targeted information. Vuganoux and Pasini (2009) conducted a comprehensive study on this type of attack, testing its feasibility on various keyboard technologies, including wireless. The authors specifically rate the Matrix Scan Technique (MST) as the most effective method for keystroke interference over a USB cable. The authors propose three countermeasures against side-channel attacks: (1) shielded cables and wired keyboards to reduce EM emanations (effective but costly), (2) signal-shielded areas (low cost, effective, but valid only within a certain range), and (3) encrypted USB communication (improves communication security but encryption can be cracked). In similar circumstances, a brief study by Sim et al. (2016, pp.518-520) aims to infer keystrokes from wired keyboards solely through signal processing.

Wireless keyboards, on the other hand, have many advantages, but they also have some critical flaws that allow malicious users to take complete control of connected devices. Throughout the years, numerous

test methods have been developed and implemented to identify vulnerabilities and improve the security of wireless keyboards.

Goodin (2019) shows that keystrokes can be recorded, replayed and injected into Fujitsu wireless model. Researchers from the penetration-testing firm SySS created a proof-of-concept attack that takes advantage of the insecure design. They were able to send commands to vulnerable Fujitsu keyboard set LX901 receiver dongles within the range using a small hardware device. The researchers were able to send input that was automatically routed to the connected computer. The distance was about 10 meters.

Gatlan (2019) discovered in 2018 four novel vulnerabilities of the Logitech Unifying USB receivers that allow users to connect wireless keyboards to the same computer via a 2.4 GHz radio connection. The flaws are caused by Logitech's outdated firmware that allowed physical access to the target computer to exploit the bugs and launch keystroke injection attacks, record keystrokes, and take control of the compromised system. Logitech fixed two of them with patches in 2019.

Logitech introduced Logi Bolt, a new standard for secure, robust wireless connections in terms of both security and encryption, in 2022 (Logitech, 2022). Logi Bolt is the next-generation wireless connectivity protocol that ensures compatibility with multiple operating systems while also improving security, wireless reliability, and connection strength. It reduces the risk of cyber-attacks while also addressing the growing security concerns brought on by more mobile workforce. The Logi Bolt provides security through encryption using Elliptic Curve Diffie-Hellman P-256 and AES-128.

Wadell (2016) discusses wireless keyboards that are vulnerable to KeySniffer, all of which are low-end, inexpensive models. Anker, EagleTec, General Electric, Hewlett-Packard, Insignia, Kensington, Radio Shack and Toshiba are among the companies affected (Bastille Networks Internet Security, 2023). Note that, although Bastille Networks has tested these products, the results should not be interpreted as an exhaustive list of all vulnerable keyboards.

Deeg and Klostermeier (2019) present security concerns about wireless keyboards that use 2.4GHz radio communication that they have collected over two years. They began opening keyboards, identifying chips, reading documentation, locating testing points, and analysing data communication with a logic analyser. Then they used SDR (HackRF one), a wireless development platform (Ubertooth One), research firmware (Crazy Radio PA) and GNU radio to record and analyze radio communication to identify used transceivers and communication protocols, among other things. The findings on two Fujitsu wireless keyboard sets (LX901 and LX390) and Cherry B.Unilimited 3.0 (all of which include wireless keyboards and mice) reveal the following flaws: no protection against Replay attacks, no encryption of sensitive data (KeyStroke sniffing attack), and insufficient verification of data authenticity (KeyStroke injection attack).

Tomsic (2022) describes seven steps of penetration testing: (1) pre-engagement (communication with the client about the scope, approvals, and terms), (2) information gathering (post scanning and gathering open source intelligence), (3) threat modelling (threat a plan how to attack targeting system, based on gathered information), (4) vulnerability analysis (developed threat model is used to discover vulnerabilities if any), (5) exploitation (attacking vulnerabilities), (6) post-exploitation (determining the actual impact of the exploit), and (7) reporting (the findings of the penetration test). He used HackRF SDR connected to the computer via high-speed USB 2.0 to conduct the research. Following the SDR analysis, a Crazy Radio PA was used to capture and send data. Furthermore, 10 wireless keyboards from nine different manufacturers (Clas Ohlson, Corsair, Deltaco, Exibel, Siglo, Logitech, Plexgear, Rapoo, and Razer) were subjected to penetration testing. Penetration testing revealed that the majority of protocols contained flaws that allowed for keystroke injection or key sniffing. Eight of the keyboards were found to have previously unknown vulnerabilities that could give an attacker complete control of the computer to which the keyboard was connected. Furthermore, only one of the keyboards promised any type of encryption.

Conclusion

Wireless keyboards have security flaws that disrupt radio communication, giving a malicious user complete access to the computer to which the keyboard is connected. Because malicious users can easily either passively or actively attack the sender, the receiver, or the data transmitted over a communication channel, secure connections and secure communications are required to aid in the prevention of wireless keyboard attacks. Side-channel attacks are physical intrusions in which the attacker steals sensitive data by observing how the system works using compromised electromagnetic emissions. The results of penetration testing presented in this article reveal vulnerabilities of the targeted wireless keyboard in terms of outdated firmware, encryption, wireless reliability, and connection strength.

References

-ANSI webstore. 1999. *ANSI INCTIS 154-1998 (R1999). Office machines and supplies – Alphanumeric machines – Keyboard arrangement (Formerly ANSI X3. 154-1988 (R1999))* [online]. Available: https://webstore.ansi.org/standards/incits/ansiincits1541988r1999 [Accessed: 05 January 2023].

Barthe, G., Gregorie, B. & Laporte, V. 2018. Secure Compilation of Side Channel Countermeasures: The Case of Cryptographic "Constant-Time". In: *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*, Oxford, UK, pp.328-343, July 09-12. https://doi.org/10.1109/CSF.2018.00031.

-Bastille Networks Internet Security. 2023. *KeySniffer affected devices* [online]. Available at: https://keysniffer.net/affected-devices [Accessed: 05 January 2023].

Chamran, M.K., Yau, K.-L.A., Noor, R.M.D. & Wong, R. 2019. A Distributed Testbed for 5G Scenarios: An Experimental Study. *Sensors*, 20(1), art.number:18. Available at: https://doi.org/10.3390/s20010018.

Chauhan, P. 2020. What is keyboard? & Types of keyboard. *RKR Knowledge,* 12 May [online]. Available at: https://rkrknowledge.com/what-is-keyboard-types-of-keyboard/ [Accessed: 05 January 2023].

de Jesus Rugeles Uribe, J., Guillen, E.P. & Cardoso. L.S. 2022. A technical review of wireless security for the internet of things: Software defined radio perspective. *Journal of King Saud University – Computer and Information Sciences*, 34(7), pp.4122-4134. Available at: https://doi.org/10.1016/j.jksuci.2021.04.003.

Deeg, M. & Klostermeier, G. 2019. New tales of wireless input devices. *SlideShare* [online]. Available at: https://www.slideshare.net/proidea_conferences/new-tales-of-wireless-input-devices-matthias-deeg-gerhard-klostermeier [Accessed: 05 January 2023].

Duarte, L., Gomes, R., Riberio, C. & Caldeirinha, R.F.S. 2019. A Software-Defined-Radio for future wireless communication systems at 60 GHz. *Electronics*, 8(12), art.number:1490. Available at: https://doi.org/10.3390/electronics8121490.

-ETSI. 2011. *Final draft EN 301 489-1 V1.9.2. (2011-04) Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements* [online]. Available at: https://www.etsi.org/deliver/etsi_en/301400_301499/30148901/01.09.01_40/en_30148901v010901o.pdf [Accessed: 05 January 2023].

-ETSI. 2012. *ETSI EN 300 386 V16.1. (2012-09) Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; ElectroMagnetic Compatibility (EMC) requirements* [online]. Available at: https://www.etsi.org/deliver/etsi_en/300300_300399/300386/01.06.01_60/en_300386v010601p.pdf [Accessed: 05 January 2023].

-ETSI. 2023. *Electro Magnetic Compatibility* [online]. Available at: https://www.etsi.org/technologies/emc [Accessed: 05 January 2023].

Garcia Reis, A.L., Barros, A.F., Gusso Lenzi, K., Pedroso Meloni, L.G. & Barbin, S.E. 2012. Introduction to the Software-defined Radio Approach. *IEEE Latin America Transactions,* 10(1), pp.1156-1161. Available at: https://doi.org/10.1109/TLA.2012.6142453.

Gatlan, S. 2019. Logitec unifying receivers vulnerable to key injection attacks. *Bleeping Computer* [online]. Available at: https://www.bleepingcomputer.com/news/security/logitech-unifying-receivers-vulnerable-to-key-injection-attacks/ [Accessed: 05 January 2023].

Goodin, D. 2019. How a wireless keyboard lets hackers take full control of connected computers. *arsTECHNICA* [online]. Available at: https://arstechnica.com/information-technology/2019/03/how-a-wireless-keyboard-lets-hackers-take-full-control-of-connected-computers/ [Accessed: 05 January 2023].

Grdović, M.M, Protić, D.D, Antic, V.D. & Jovanovic, B.Ž. 2022. Electromagnetic information leakage from the computer monitor. *Vojnotehnički glasnik/Military Technical Courier*, 70(4), pp.836-855. Available at: https://doi.org/10.5937/vojtehg70-38930.

Griskenas, S. 2023. What is wireless keyboard security? Everything you need to know. *Nord VPN* [online]. Available at: https://nordvpn.com/blog/what-is-wireless-keyboard-security/ [Accessed: 05 January 2023].

-ISO. 2009. *ISO/IEC 9995-1:2009. Information technology – Keyboard layouts for text and office systems – Part 1: General principles governing keyboard layouts*[online]. Available at: https://www.iso.org/standard/51645.html [Accessed: 05 January 2023].

-ITU. 2014. *K.84: Test methods and guide against information leaks through unintentional electromagnetic emission* [online]. Available at: https://www.itu.int/rec/T-REC-K.84/en [Accessed: 05 January 2023].

-JSAJIS. 2018. *JIS X 6002:1980 English Edition Keyboard layout for information processing using the JIS 7 bit coded character set* [online]. Available at: http://www.jsajis.org/index.php?main_page=product_info&cPath=4&products_id=16459 [Accessed: 05 January 2023].

Liu, H., Spolaor, R., Turrin, F., Bonafede, C. & Conti, M. 2021. USB powered devices: A survey of side-channel threats and countermeasures. *High-Confidence Computing,* 1(1), art.ID:100007. Available at: https://doi.org/10.1016/j.hcc.2021.100007.

-Logitech. 2022. *Logi Bolt Secure, robust wireless connections*. Logitech [online]. Available at: https://www.logitech.com/content/dam/logitech/en/business/pdf/logi-bolt-white-paper.pdf [Accessed: 05 January 2023].

-Logitech. 2023. *Setting a new standard in wireless peripheral security. Today's work-from-anywhere workplace demands enhanced protection*. Logitech [online]. Available at: https://www.logitech.com/en-us/business/resources/wireless-peripheral-security.html [Accessed: 05 January 2023].

Mangard, S., Oswald, E. & Popp, T. 2007. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. New York, NY: Springer. Available at: https://doi.org/10.1007/978-0-387-38162-6.

Markagić, M.S. 2018. Compromising electromagnetic radiation–challenges, threats and protection. *Vojnotehnički glasnik/Military Technical Courier,* 66(1), pp.143-153. Available at: https://doi.org/10.5937/vojtehg66-8691.

Molina-Tenorio, Y., Prieto-Guerrero, A. & Aguilar-Gonzales, R. 2021. Real-Time Implementation of Multiband Spectrum Sensing Using SDR Technology. *Sensors,* 21(10), art.number:3506. Available at: https://doi.org/10.3390/s21103506.

-NIST National Institute of Standards and Technology. 2001. *Advanced Encryption Standard (AES). Federal Information Processing Standards*. NIST National Institute of Standards and Technology, NIST Technical Series Publications. Available at: https://doi.org/10.6028/NIST.FIPS.197.

Oligeri, G., Sciancalepore, S., Raponi, S. & Di Pietro, R. 2020. BrokenStrokes: on the (in)security of wireless keyboards. In: *WiSec '20: Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, Linc, Austria, pp.231-241, July 08-10. Available at: https://doi.org/10.1145/3395351.3399351.

Pohl, J. & Noack, A. 2019. Automatic Wireless Protocol Reverse Engineering. In: *Proceedings of 13th USENIX Workshop on Offensive Technologies* (WOOT 19), Santa Clara, CA: USENIX Association, August [online]. Available at: https://www.usenix.org/conference/woot19/presentation/pohl [Accessed: 05 January 2023].

Sadiku, M.N.O. & Akujuobi, C.M. 2004. Software-defined radio: a brief overview. *IEEE Potentials*, 23(4), pp.14-15. Available at: https://doi.org/10.1109/MP.2004.1343223.

Sayakkara, A., Le-Khac, N.-A. & Scanlon, M. 2018. Accuracy Enhancement of Electromagnetic Side-Channel Attacks on Computer Monitors. In: *ARES 2018: Proceedings of the 13th International Conference on Availability,*

Reliability and Security, Hamburg, Germany, August 27-30. Available at: https://doi.org/10.1145/3230833.3234690.

Sheimo, M. 2021. Ahhh! My mouse and keyboard were hacked! *Sikich*, 23 June [online]. Available at: https://www.sikich.com/insight/ahhh-my-mouse-and-keyboard-were-hacked/ [Accessed: 05 January 2023].

Sim, D.-J., Lee, H.S., Yook, J.-G. & Sim, K. 2016. Measurements and analysis of the compromising electromagnetic emanations from USB keyboard. In: *2016 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)*, Shenzhen, pp.518-520, May 17-21. Available at: https://doi.org/10.1109/APEMC.2016.7522785.

Stewart, R.W., Barlee, K.W., Atkinson, D.S.W. & Crockett, L.H. 2015. *Software Defined Radio Using MATLAB & Simulink and the RTL-SDR*. Glasgow, UK: Strathclyde Academic Media. ISBN: 978-0-9929787-2-3.

Tomsic, N. 2022. *Penetration testing wireless keyboards. Are your devices vulnerable? Degree Project in Computer Science and Technology*. Stockholm, Sweden: KTH Royal Institute of Technology [online]. Available at: https://www.diva-portal.org/smash/record.jsf?dswid=-5484&pid=diva2%3A1701492 [Accessed: 05 January 2023].

Vuagnoux, M. & Pasini, S. 2009. Compromising Electromagnetic Emanations of Wired and Wireless Keyboards. *USENIX* [online]. Available at: https://www.usenix.org/legacy/events/sec09/tech/full_papers/vuagnoux.pdf [Accessed: 05 January 2023].

Wadell, K. 2016. Hackers Can Spy on Wireless Keyboards From Hundreds of Feet Away: There's a gaping security hole in eight popular models. *The Atlantic*, 26 July [online]. Available at: https://www.theatlantic.com/technology/archive/2016/07/hackers-can-spy-on-wireless-keyboards-from-hundreds-of-feet-away/492962/ [Accessed: 05 January 2023].

-WebNots. 2022. What are Different Types of Computer Keyboards? *WebNots*, 15 August [online]. Available at: https://www.webnots.com/what-are-different-types-of-computer-keyboards/ [Accessed: 05 January 2023].

Weiss, B. 2023. Can Your Wireless Keyboard Be Hacked? *WyzGuys Cybersecurity* [online]. Available at: https://wyzguyscybersecurity.com/can-your-wireless-keyboard-be-hacked/ [Accessed: 05 January 2023].

Whittaker, Z. 2016. Flaws in wireless keyboards let hackers snoop on everything you type. *ZD Net*, 26 July [online]. Available at: https://www.zdnet.com/article/millions-of-wireless-keyboards-at-risk-of-spying-by-hackers-in-new-attack/ [Accessed: 05 January 2023].

Additional information

FIELD: computer sciences, electronics, telecommunications, mechanical engineering

ARTICLE TYPE: original scientific paper

Alternative link

https://scindeks.ceon.rs/article.aspx?artid=0042-84692302296J (html)
https://aseestant.ceon.rs/index.php/vtg/article/view/43239 (pdf)
https://doaj.org/article/a5931f931d6c49d18df25fc32ff5e101 (pdf)
https://elibrary.ru/item.asp?id=50445622 (pdf)
http://www.vtg.mod.gov.rs/archive/2023/military-technical-courier-2-2023.pdf (pdf)