SCREEN READING: ELECTROMAGNETIC INFORMATION LEAKAGE FROM THE COMPUTER MONITOR

Milena M. Grdović[a], *Danijela* D. Protić[b], *Vladimir* D. Antić[c], *Boriša* Ž. Jovanović[d]

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

[a] e-mail: milena.grdovic@gmail.com,
ORCID iD: https://orcid.org/0000-0003-4310-7935

[b] e-mail: danijelaprotic318@gmail.com, **corresponding author**;
ORCID iD: https://orcid.org/0000-0003-0827-2863

[c] e-mail: vladimirantic2013@gmail.com,
ORCID iD: https://orcid.org/0000-0001-9843-0743

[d] e-mail: borisa.jovanovic@vs.rs,
ORCID iD: https://orcid.org/0000-0002-9353-724X

DOI: 10.5937/vojtehg70-38930; https://doi.org/10.5937/vojtehg70-38930

FIELD: Computer sciences, Electronics, Telecommunications, Mechanical engineering
ARTICLE TYPE: Original scientific paper

Abstract:

Introduction/purpose: The security of systems can be jeopardized by compromising emanations. This paper provides an overview of computer screen attacks. New technologies can be used to exfiltrate sensitive data from computer screens. Emission security is the prevention of electromagnetic signal attacks that are conducted or radiated.

Methods: This paper examines the impact of a side-channel attack that intercepts compromised information from a computer screen. The leakage of electromagnetic data is also explained. Software-defined radios are described to explain malicious attacks on computer monitors.

Results: The source of the electromagnetic signal determines the nature of the side-channel information they carry. The most well-known issue associated with revealing emissions is the possibility of intercepting visual information displayed on computer monitors.

Conclusion: Visual data displayed on computer monitors could be intercepted by a software-defined radio which can digitize the desired frequency spectrum directly from an antenna, present it to a digital signal processor, and output it to an application for revealing sensitive data. A

variety of countermeasures, such as shielding, zoning, soft TEMPEST, and similar techniques, can be used to prevent data leakage.

Key words: electromagnetic emission, information leakage, computer monitor.

Introduction

In recent years, new technologies have made it possible to exfiltrate sensitive data from a computer by monitoring the computer screen in a variety of novel ways that do not require network connectivity or physically contacting devices via the invisible channel determined by the computer screen. Because the user does not have a visual perception of what is happening, malware on the compromised computer can obtain sensitive data such as files, images, or passwords. The prevention of attacks using electromagnetic (EM) signals that are either conducted or radiated is referred to as emission security. By formulating that "changing electrical currents induce changing magnetic fields, which induce changing currents and induce a changing magnetic field that propagates as an EM wave through surrounding space," Oersted, Faraday, and Henry discovered the physics of EM emanation (Rowe, 2006). This field can be picked up by nearby electrical conductors and, through EM interference, can impede the operation of other electromagnetic devices. As a result, an antenna with an amplifier can pick up some signal from a computer and reconstruct generated electrical signals (Rowe, 2006). Military and commercial organizations are very concerned about the Transient Electro Magnetic Pulse Emanation Standard (TEMPEST) defence which prevents the stray EM pulses emitted by computers and other electronic devices from being picked up and used to reconstruct the sensitive data (Markagić, 2018, pp.143-153). TEMPEST has recently become a commercial issue for electronic voting machines and smart cards used for digital signatures. Side-channel attacks refer to a variety of attacks that take advantage of optical, thermal and acoustic emanations from the equipment. This happens when information leaks through a channel that is not intended for communication. Electromagnetic eavesdropping attacks can cause a computer to emit a stronger signal than usual and modulate the signal so that it can pass through the firewall.

Electromagnetic compatibility (EMC) and radio frequency interference (RFI) are closely related to EM security measures. All emission security issues are expected to worsen as more devices connect to wireless networks and processor speeds increase into the gigahertz range. There are two types of electromagnetic attacks that are not mutually exclusive:

1) when the signal is transmitted over a circuit such as a power line or phone line, it is known as Highjack and 2) when the signal is transmitted as radio frequency (RF) energy, it is known as TEMPEST. Properly shielded equipment is typically limited in quantity and designed specifically for defence markets, making it extremely expensive. The operating rooms must also be properly filtered.

Screen signals can be found in a variety of locations across computer networks. These signals may contain multiple harmonics, some of which radiate more effectively than others, owing to the designed equipment being certified to not emit any signals beyond a certain distance. Spying on the surface of a screen with a powerful telescope is a very basic approach to spying on the content displayed on it (Lavaud et al, 2021). Khun (2002), Backes et al (2008), and Backes et al (2009), on the other hand, describe several more efficient ways to attack computer monitor content. Computer monitors leak electromagnetic information as a result of three key factors used to reproduce video images: (1) refresh rate, (2) horizontal frequency, and (3) pixel frequency, which is the display principle (Mao et al, 2017). One method for estimating the risk of information leakage is to use multi-resolution spectrum analysis to distinguish and match the spectrum interval from the radiated EM signals.

This paper investigates the impact of how a side-channel attack causes compromised information to be taken from a computer screen. This paper also discusses the leakage of electromagnetic information from computer screens. To explain potential malicious attacks on computer monitors, software-defined radios (SDRs) are described.

Side-channel attacks

The security of a cryptosystem (cryptographic algorithms and protocols, cryptographic keys, and cryptographic devices used for implementation) is dependent on more than just using robust algorithms and parameters, certified protocols, and cryptographic keys that are long enough. Physical attacks on a system can also be used to compromise it. Side-channel attacks are generally physical attacks in which malicious parties extract confidential and protected data by observing how systems physically behave (Barthe et al, 2018). These attacks use the dependency between secret information used in the cryptosystem and physical values measured on/around the cryptosystem (e.g. power consumption, electromagnetic radiation, timing information) to break a system (Mangard et al, 2007). Table 1 depicts the classification of side-channel emanation (Lavaud et al, 2021). Each side-channel attack seeks to exploit an

unintentional emission. As a result, the subject of side-channel attacks covers a broad range of techniques (Sayakkara et al, 2018). Side-channel information sources, such as EM emanations from a chip (Agrawal et al, 2003) and timings for various operations performed (Kocher, 1996, pp.104-113) have also been demonstrated to be exploitable (Mangard et al, 2007). Hayashi et al (2014, pp.954-965) conducted a thorough examination of EM emanations from a chip in-depth, including countermeasures. Their primary focus, however, was on recovering sensitive information from inside the computer systems (cryptographic keys, not-the-screen content). Kinugawa et al (2019, pp.62-90) demonstrate how to increase the EM leakage with a (cheap) hardware modification added to potentially any device and spread the attack over a greater distance. The authors show that the additional circuitry (interceptor) increases leakage and forces leakage in devices that are not susceptible to EM leakage.

Table 1 – Side channel emanation
Таблица 1 – Утечка по стороннему каналу
Табела 1 – Еманација успед споредних ефеката

SIDE-CHANNEL EMANATION	
Power line	Keyboard Internal components Cryptosystems
Sound	Speakers Internal components External components
Light	Status LED Internal components Screens
Electromagnetic	Radio radiation Forced broadcast

Goller & Sigl (2015, pp.255-270) proposed to perform side-channel attacks on smartphones using standard radio equipment. The authors also show the ability to distinguish between squaring and multiplications. This discovery may result in the complete recovery of the Rivest, Shamir, and Adelman (RSA) key (Jonsson & Kaliski, 2003). Their setup gathered electromagnetic leaks from an Android phone. Genkin et al (2015, pp.95-112), and Genkin et al (2019, pp.853-869) present the extraction of cryptographic keys such as RSA or ElGamal from laptops using various side channels such as power and EM radiation (Will & Ko, 2015). Furthermore, an adversary may be able to monitor a device's power

consumption while it performs secret key operations (Kocher et al, 2011, pp.5-27). Acoustic emanation from various computer system components can be used to exfiltrate data. Genkin et al (2014, pp.444-461) demonstrated that, by listening for acoustic emanation, it is possible to distinguish between CPU operations, resulting in an attack on an RSA algorithm encryption key. Fenkin et al (2019) show how to extract screen content using the acoustic side channel. Microphones can pick up sound from webcams or screens and transmit it during a video conference call or archived recordings. Berger et al (2006, pp.245–254) demonstrated a dictionary attack using keyboard acoustic emanation. Backes et al (2010) investigated acoustic side channels in printers. Asonov and Agrawal (2004) used the sound emitted by different keys to recover information typed on a keyboard. The contribution of Liu et al (2021, pp.1-15) is a side-channel attack analysis that exploits the EM emanations of the display cable from a mobile phone. These signals are more difficult to obtain and may be significantly weaker than those examined in more traditional TEMPEST technique attacks. TEMPEST is a side-channel technique for spying on computer systems via unintentional radio or electrical signals, sounds, and vibrations (Kuhn & Anderson, 1998, pp.124-142). The possibility of intercepting visual information displayed on an electronic device screen is the most well-known issue associated with EM revealing emissions. Van Eck (1985, pp.269-286) is the first to present an unclassified analysis of the feasibility and security risks of computer monitor emanations. He was able to listen in on a real system from hundreds of meters away by measuring electromagnetic emanations with only $15 in equipment and a Cathode-Ray Tube (CRT) television set.

Side-channel attacks have a variety of countermeasures because they are among the most serious threats to embedded crypto devices and frequently target the secret (cryptographic) key in a device that secures sensitive data. The countermeasures' primary goal is to eliminate reliance on sensitive data and the side channel. One method attempts to separate the actual data processed by the device from the data on which the computation is performed (masking) (Prouff & Rivian, 2013, pp.142-159). Another approach attempts to separate the device's computed data from the power consumed by the computations (hiding). One of the countermeasures is also flattening the power consumption of a device. Hardware-based countermeasures propose microarchitecture-based solutions such as providing hardware support for advanced encryption standard (AES) instructions or making caches security-sensitive. Hardware countermeasures are effective, but they can be difficult to implement. In contrast, software countermeasures are simple to

implement solutions that can be implemented at the program language level (secure programming guidelines, program transformations). They can also be supported by strict enforcement methods (Bernstein, 2005; Molonar et al, 2005; Barthe et al, 2018).

Electromagnetic information leakage from the computer monitor

EM radiation is the underlying technology for wireless communication, and it is selected based on the distance to be covered, data throughput rate, signal frequency, amount of bandwidth required, modulation technique, power of the transmitted signal, and other factors (Sayakkara et al, 2018). Although wireless communication devices are designed to generate EM radiation at the appropriate frequency and amplitude for the communication technology, as a by-product of their internal operations, these devices also generate EM radiation at unintended frequencies (Genkin et al, 2014, pp.444-461). Unintentional EM emissions from computers can be caused by a variety of factors. The source of each EM signal determines the nature of these EM signals as well as the type of side-channel information they carry. The possibility of intercepting visual information displayed on computer monitors is the most well-known issue associated with the issue of EM revealing emissions. Van Eck (1985, pp.269-286) demonstrated a modified television set that was capable of capturing and visualizing video streams displayed on a nearby television screen. To transmit video data to computer monitors, various protocols are used, necessitating more flexibility than a dedicated hardware-based attack. This article was about CRT monitors. It should be noted that liquid-crystal displays (LCD), which are common output components of computers and currently dominate the market, are not immune to this threat because they are equipped with digital video data (DVD) transmission interfaces. This is not the case, because digital signals, like analogue signals, are susceptible to electromagnetic infiltration and enable non-invasive data acquisition. There is a risk of eavesdropping on the leaked signal because the leakage of the displayed information is quite high. In 2002, Kuhn expands on this eavesdropping concept by conducting an analysis of EM side-channel eavesdropping on modern video display technologies (Kuhn, 2002, pp.3-18). This study employs RF acquisition hardware with fast sampling rates to monitor EM emissions from computer displays. Sekiguchi (2010, pp.127-131) describes receiving EM noise and reconstructing a display image on a touch screen monitor on a personal computer. The experimental results showed that the reconstructed display image can recognize the image of the touched button on the touch screen

monitor. Elibol et al (2012, pp.1767-1771) demonstrated a monitor eavesdropping system that remotely reconstructs screen images using RF acquisition hardware. The signal acquisition hardware is a portable platform that can operate at a variety of RF frequencies. In this work, the averaging of adjacent frames is used to improve the readability of the text. In 2016, Lee et al demonstrated the possibility of display information leakage by analysing electromagnetic emissions from desktop and laptop monitors (Lee et al, 2016). By analysing the display mechanism, the characteristics of the leaked signal from the LCD monitor are verified, and electromagnetic emanations are measured over a long distance using an eavesdropping experiment. Using a variety of signal processing techniques, the authors recovered display information.

Software-defined radio: How to spy on?

There have been practical challenges in the more demanding SDR applications, primarily due to analogue to digital conversion (ADC) and digital to analogue conversion (DAC) limitation trade-offs. Many of these compromises are being limited to higher frequencies due to faster ADC/DACs and higher resolution. To avoid being limited to single-frequency ranges and to deal with multiple channels at once, SDR requires a wideband. Wideband performance is required to allow for dynamic spectrum and radio parameter management. The SDR should be able to digitize the desired frequency spectrum directly from an antenna, present it to a DSP processor, and output it to an application, as well as the reverse for a transmitter. The following benefits are provided by SDR: (1) flexibility, (2) interoperability, (3) ease of upgrade, (4) efficiency, and (5) higher-level interfaces. Figure 1 depicts the basic structure of an SDR receiver (Benks, 2016, pp.1-16).

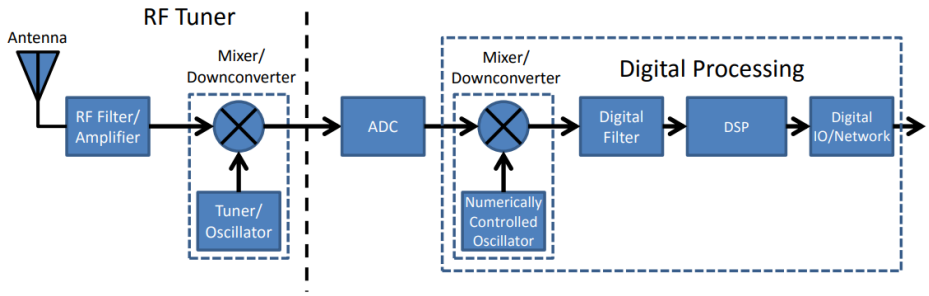

Figure 1 – SDR Receiver (Benks, 2016)
Рис. 1 – SDR приемник (Benks, 2016)
Слика 1 – SDR пријемник

The sampling rate of the RF acquisition hardware is the most important factor in the accuracy of the screen image reconstruction. SDRs provide greater flexibility at a lower cost, but their sampling rate is lower than that of dedicated RF acquisition hardware. Digital processors give radio equipment the flexibility of a programmable system, allowing a communication system to be changed simply by changing its software. Under the SDR paradigm, the task of configuring the radio's behaviour is transferred to software, leaving the hardware only to implement the radiofrequency front end. As a result, the radio is transformed into a dynamic element capable of changing its operational characteristics (bandwidth, modulation, coding rate) based on software configuration. The SDR is defined as "*radio in which some or all physical layer functions are defined by software*" (Garcia Reis et al, 2012). SDR devices use real-time software module execution on microprocessor platforms or digital signal processors, fast programmable gate arrays (FPGA) are commonly used for transmitting or receiving radio signals, the main operational characteristics of SDRs are modified at runtime, and the system can be easily reconfigured to perform different functions (Chamran et al, 2020). SDRs apply to a wide range of radiofrequency technologies, and their standards have made base station software updates more appealing than costly base station replacements. The SDR expands the possibilities by making it easier to implement existing radio applications and enabling new types of applications. The availability of low-cost devices that receive and digitize radiofrequency signals has brought the SDR to both professional and home engineering desks (Stewart et al, 2015, pp.64-71). In their work, Molina-Tenorio et al (2021, pp.1-21) describe the characteristics of the SDR-RTL (Nooelec, 2021), HackRF One (Great scott gadgets, 2021), and LimeSDR Mini (Lime microsystems, 2021) devices. Table 2 lists the main characteristics of these devices.

Table 2 – SDR device characteristics
Таблица 2 – Характеристики устройства SDR
Табела 2 – Карактеристике SDR уређаја

Device	HackRF One	RTL-SDR	LimeSDR Mini
Frequency range	1 MHz-6 GHz	22 MHz-2.2 GHz	10 MHz-3.5 GHz
RF bandwidth	20 MHz	3.2 MHz	30.72 MHz
Sample depth	8 bit	8 bit	12 bit
Sample rate	20 MSPS	3.2 MSPS	30.72 MSPS
Tx channels	1	0	1
Rx channels	1	1	1
Duplex	Half	-	Full
Transmit power	- 10 dBm	-	Max 10 dBm

Rugeles Uribe et al (2021, pp.1-13) compare 19 more commercially available SDR platforms in terms of ADC/DAC, Tx/Rx, Fmin-Fmax and Max RF Bandwidth, all of which were collected in 2019 and 2020: FUNcube Dongle, RSPduo, Airspy-mini, Airspy-R2, Pluto, BladeRF 2.0 Micro, AD-FMCOMMS4-EBZ, USRP-1, PicoSDR, WARP-V3, USRP-N210, TMDSSFFSDR, USRP X310, USRP-2974, AIR-T, Sidekiq X4, USRP N320 and CRIMSON Cyan, all of them being commercially available SDR platforms. The authors also discuss how hardware is evolving to increase computational capacity. Furthermore, the authors present the Bastille Network classification and descriptions of wireless vulnerabilities (Bastille Networks, 2020).

Electromagnetic compatibility standards and regulations in consumer products address emerging threats from eavesdropping attacks using EM side-channels. According to the International Organization for Standardisation (ISO) ITU-T advisory notice K.841, when considering the EMC requirements of consumer devices, information leakage from EM emissions must be considered (ITU, 2014). Many hardware-software tools, however, use SDR platforms for side-channel attacks on computer monitors. TempestSDR, an open-source software library that uses SDR platforms for EM side-channel attacks on computer monitors, is one of the most well-known. It is capable of automatically detecting the dimensions and frame rate of a target when the target monitor details are unknown by identifying repeating patterns in the EM signal that correspond to the individual frames of the video (see Figure 2).

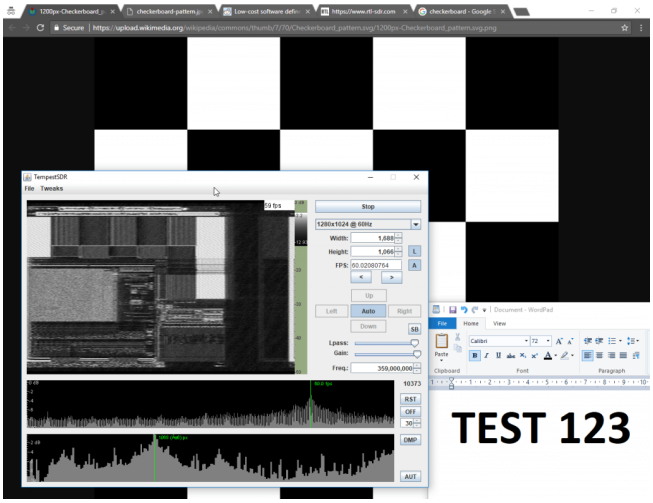

Figure 2 – TempestSDR (RTL-SDR, 2017)
Рис. 2 – TempestSDR (RTL-SDR, 2017)
Слика 2 – Tempest SDR (RTL-SDR, 2017)

TempestSDR allows the user to use any SDR that supports ExtIO (such as those described in Table 2) to receive unintentional signal radiation from the screen and convert that signal back into a live image, allowing them to see what is on screen without a direct connection (RTL-SDR, 2017).

How to defend against computer monitor attacks?

Electronic security protection, like all security measures, must be cost-effective, that is, it must eliminate security issues without interfering with system performance (Doychev, 2016; Rowe, 2006). The sources of unwanted signals must be protected by implementing solutions that effectively prevent the infiltration process from taking place (Levina et al, 2019, pp.393-400; Ometov et al, 2017, pp.2591-2601). Rowe summarizes the suitability of various electronic security methods for mitigating various threats. Table 3 shows the results for the monitor, power, and cables.

Table 3 – Summary of electronic protection methods (Rowe, 2006)
Таблица 2 – Краткое изложение методов электронной защиты (Rowe, 2006)
Табела 2 – Резиме метода електронске заштите (Rowe, 2006)

Threat	Monitor	Cable	Power
Electromagnetic shielding	Yes	Yes	No
Source suppression	Yes	Yes	Yes
Noise generation and encryption	Yes	Yes	Yes
Signal irregularity	Yes	Yes	Yes
Deliberate deception	Yes	Yes	No
Bug detectors	Yes	Yes	Yes

It is essential to emphasize the significance of differences in military and civil security standards. In 2006, Khun predicted that simple eavesdropping tools for compromising emanations would soon be available for free download from the Internet. For today's information security professionals, the question is: What protective countermeasures are available for computers that display extremely sensitive data regularly? These could be jamming devices used to intentionally increase environmental noise, metal shielding, zoning, soft TEMPEST, and other similar techniques. Today, jamming devices are rarely used because the jamming signal must be carefully selected and synchronized with the signal to be covered, and jamming devices may draw the attention of eavesdroppers to the location of equipment. The EM shielding protects devices, cables and rooms against compromising emanations (Kuhn,

2005, pp.265-279; Kuhn, 2006, pp.1-10). To eliminate emanations, the source of the emanations should be placed in metal boxes made of conductive materials (copper, aluminium, steel), also known as Faraday cages. However, perfect protection requires that the conductive enclosure remain intact. Because gaps are required for ventilation, power lines, keyboards, and network connections, these gaps may allow signals to leak out (Warne & Chen, 1992, pp.173-182). Molyneux-Child (1997) recommends at least one-tenth to prevent significant radiation from escaping and one-hundredth to provide a 60 dB reduction. Creating meandering channels through the gaps, as well as using waveguides in the form of conductive pipes through the gaps, can help to reduce the emanations at these gaps. Power lines can be filtered through these gaps, and fibfibretic cables can transmit data without requiring an electromagnetic channel. A conductive film can be applied to monitor screens, but keyboards are more difficult to protect. Due to the difficulty of shielding, both devices and their locations can be classified to indicate how close an eavesdropper can get (Zone 0: eavesdropper can be within 1–20 m; Zone 1: eavesdropper can be within 20–100 m; Zone 2: eavesdropper can be 100 m to 1 km; Zone 3: eavesdropper cannot be closer than a kilometre). These measurements are based on the assumption that only space exists between the eavesdropper and the target. Przybysz et al (2021, pp.1-15) discuss publicly available fragments of the American military requirements NSTISSAM TEMPEST/1-92 (Cryptome, 2008) and NSTISSAM TEMPEST/2-95 (Cryptome, 2000), which define three levels of security for devices that could be used in information processing zones and whose R rays meet the following conditions: R 20 m, R 100 m, and R > 100 m. (Emission levels must be measured from a distance of one meter). The MIL-STD-461G document (EverySpec, 2015) also recommends this measurement distance. The authors concluded promising emission signals emitted by commercial devices can be detected from a few dozen meters away. De Meulemeester et al (2020) confirmed this by demonstrating that visual information could be recovered from a distance of approximately 80 m. Various software countermeasures, such as deliberate softening of font edges or randomization of less significant bits in the frame buffer, can be used to protect against EM leakage from the computer monitor (Duc et al, 2019, pp.1263-1297). Safe fonts are one of the security measures developed using Kubiak's safety criteria (Kubiak, 2020), and they have the following characteristics: (1) The lines that form the characters intersect at right angles, implying that each character is made entirely of vertical and horizontal lines, (2) font characters are devoid of decorative and diagonal

elements, and (3) the general contour of safe font characters is rectangular. In the case of a graphic source of valuable emissions, safe fonts protect processed information from EM penetration. These fonts safeguard the Video Graphics Array (VGA) and Digital Video Interface (DVI).

Conclusion

New technologies enable malicious scanning of information emitted by the computer monitor. The TEMPEST defence, which prevents stray EM pulses emitted by computers and other electronic devices from being picked up and used to reconstruct sensitive data, is causing concern among military and commercial organizations. There are two types of EM attacks: highjack and RF energy attacks. Screen signals contain multiple harmonics, some of which radiate more effectively than others. The refresh rate, horizontal frequency, and pixel frequency of computer monitors all leak electromagnetic information. This paper describes how a side-channel attack causes compromised information to be taken from a computer screen. The SDR is used to explain how visual data can be intercepted. To describe the possibility of protecting the data radiated from the computer monitor, a variety of countermeasures such as shielding, zoning, soft TEMPEST, and similar techniques are described.

References

Agrawal, D., Archambeault, B., Rao, J. & Rohatgi, P. 2003. The EM Side—Channel(s). In: Kaliski, B.S., Koç, ç.K. & Paar, C. (Eds.) *Cryptographic Hardware and Embedded Systems - CHES 2002. CHES 2002. Lecture Notes in Computer Science*, 2523, pp.29-45. Berlin, Heidelberg: Springer. Available at: https://doi.org/10.1007/3-540-36400-5_4.

Asonov, D. & Agrawal, R. 2004. Keyboard acoustic emanations. In: *IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, pp.3-11, May 12. Available at: https://doi.org/10.1109/SECPRI.2004.1301311.

Backes, M., Chen, T., Duermuth, M., Lensch, H.P.A. & Welk, M. 2009. Tempest in a Teapot: Compromising Reflections Revisited. In: *2009 30th IEEE Symposium on Security and Privacy*, Oakland, CA, USA, pp.315-327, May 17-20. Available at: https://doi.org/10.1109/SP.2009.20.

Backes, M. Dürmuth, M., Gerling, S., Pinkal, M. & Sporleder, C. 2010. Acoustic side-channel attacks on printers. In: *19th USENIX Security Symposium (USENIX Security 10)*, Washington, DC, pp.307-322, August 11-13 [online]. Available at: https://www.usenix.org/legacy/event/sec10/tech/full_papers/Backes.pdf [Accessed: 25 June 2022].

Backes, M., Dürmuth, M. & Unruh, D. 2008. Compromising Reflections-or-How to Read LCD Monitors around the Corner. In: *2008 IEEE Symposium on Security and Privacy (sp 2008)*, Oakland, CA, USA, pp.158-169, May 18-22. Available at: https://doi.org/10.1109/SP.2008.25.

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 9-12. Available: https://doi.org/10.1109/CSF.2018.00031.

-Bastille Networks. 2020. *Top Internet of Radios Vulnerabilities* [online]. Available at: https://www.bastille.net/research/top-10-internet-of-radios-vulnerabilities [Accessed: 25 June 2022].

Benks, J. 2016. Using Software Defined Radio for Faster Speeds And Increased Bandwidth. Technology white paper. *Curtis-Wright Defence Solutions* [online]. Available at: https://www.curtisswrightds.com/resources/white-papers/using-software-defined-radio-for-faster-speeds-and-increased-bandwidth [Accessed: 25 June 2022].

Berger, Y, Wool, A. & Yeredor, A. 2006. Dictionary attacks using keyboard acoustic emanations. In: *CCS '06: Proceedings of the 13th ACM conference on Computer and communications security*, Alexandria, Virginia, USA, pp.245-254, October 30. Available at: https://doi.org/10.1145/1180405.1180436.

Bernstein, D.J. 2005. *Cache-timing attacks on AES* [online]. Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.140.2835&rep=rep1&type=pdf [Accessed: 25 June 2022].

Chamran, M.K., Yau, K.-L.A., Noor, R.M.D. & Wong, R. 2020. A Distributed Testbed for 5G Scenarios: An Experimental Study. *Sensors*, 20(1), art.number:18. Available at: https://doi.org/10.3390/s20010018.

-Cryptome. 2008. *NSTISSAM TEMPEST/1-92* [online]. Available at: https://cryptome.org/nt1-92-1-5.htm [Accessed: 25 June 2022].

-Cryptome. 2000. *NSTISSAM TEMPEST/2-95* [online]. Available at: https://cryptome.org/tempest-2-95.htm [Accessed: 25 June 2022].

De Meulemeester, P., Scheers, B. & Vandenbosch, G.A.E. 2020. Eavesdropping a (Ultra-)High-Definition Video Display from an 80 Meter Distance Under Realistic Circumstances. In: *2020 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI)*, Reno, NV, USA, pp.517-522, July 28-August 28. Available at: https://doi.org/10.1109/EMCSI38923.2020.9191457.

Doychev, G. 2016. *Tools for evaluation of choice of countermeasures against side-channel attacks*. PhD Thesis. Madrid: Universidad Politecnica de Madrid. Escuela Tecnica Superior de Ingenieros Informaticos. Available at: https://doi.org/10.20868/UPM.thesis.42965.

Duc, A., Faust, S. & Standaert, F-X. 2019. Making Masking Security Proofs Concrete (Or How to Evaluate the Security of Any Leaking Device), Extended Version. *Journal of Cryptology*, 32, pp.1263-1297. Available at: https://doi.org/10.1007/s00145-018-9277-0.

Elibol, F., Sarac, U. & Erer, I. 2012. Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system. In: *2012 Proceedings of the 20th European Signal Processing Conference (EUSIPCO)*, Bucharest, Romania, pp.1767-1771, August 27-31 [online]. Available at: https://ieeexplore.ieee.org/abstract/document/6334179 [Accessed: 25 June 2022].

-EverySpec. 2015. *MIL-STD-461G, Department of Defense Interface Standard: Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment* [online]. Available at: http://everyspec.com/MIL-STD/MIL-STD-0300-0499/MIL-STD-461G_53571/ [Accessed: 25 June 2022].

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.

Genkin, D., Pattani, M., Schuster, R. & Tromer, E. 2019. Synesthesia: Detecting screen content via remote acoustic side channels. In: *IEEE Symposium on Security and Privacy*, San Francisco, CA, USA, pp.853-869, May 19-23. Available at: https://doi.org/10.1109/SP.2019.00074.

Genkin, D., Pipman, I. & Tromer, E. 2015. Get your hands off my laptop: Physical side-channel key-extraction attacks on PCs. *Journal of Cryptographic Engineering*, 5(2), pp.95-112. Available at: https://doi.org/10.1007/s13389-015-0100-7.

Genkin, D., Shamir, A. & Tromer, E. 2014. RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. In: Garay, J.A., Gennaro, R. (Eds.) *Advances in Cryptology – CRYPTO 2014. CRYPTO 2014. Lecture Notes in Computer Science,* 8616*,* pp.444–461*.* Berlin, Heidelberg: Springer*.* Available at: https://doi.org/10.1007/978-3-662-44371-2_25.

Goller, G. & Sigl, G. 2015. Side channel attacks on smartphones and embedded devices using standard radio equipment. In: Mangard, S., Poschmann, A. (Eds.) *Constructive Side-Channel Analysis and Secure Design. COSADE 2015. Lecture Notes in Computer Science,* 9064, pp.255-270*.* Springer, Cham*.* Available at: https://doi.org/10.1007/978-3-319-21476-4_17.

-Great scott gadgets. 2021. *HackRF* [online]. Available at: https://greatscottgadgets.com/hackrf/one/ [Accessed: 25 June 2022].

Hayashi, Y., Homma, N., Miura, M., Aoki, T. & Sone, H. 2014. A Threat for Tablet PCs in Public Space: Remote Visualization of Screen Images Using EM Emanation. In: *CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, Scottsdale, Arizona, USA, pp.954-965, November 3-7. Available at: https://doi.org/10.1145/2660267.2660292.

-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: 25 June 2022].

Jonsson, J. & Kalinski, B. 2003. *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1* [online]. Available at: https://datatracker.ietf.org/doc/html/rfc3447 [Accessed: 25 June 2022].

Kinugawa, M., Fujimoto, D. & Hayashi, Y. 2019. Electromagnetic Information Extortion from Electronic Devices Using Interceptor and Its Countermeasure. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2019(4), pp.62-90. Available at: https://doi.org/10.13154/tches.v2019.i4.62-90.

Kocher, P.C. 1996. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: Koblitz, N. (Ed.) *Advances in Cryptology — CRYPTO '96. CRYPTO 1996. Lecture Notes in Computer Science,* 1109, pp.104-113. Berlin, Heidelberg: Springer. Available at: https://doi.org/10.1007/3-540-68697-5_9.

Kocher, P., Jaffe, J., Jun, B. & Rohatgi, P. 2011. Introduction to differential power analysis. *Journal of Cryptographic Engineering*, 1, pp.5-27. Available at: https://doi.org/10.1007/s13389-011-0006-y.

Kubiak, I. 2020. Electromagnetic Eavesdropping. In: Mitra, P. (Ed.) *Recent Trends in Communication Networks,* pp.593-653. London, UK: IntechOpen. Available at: https://doi.org/10.5772/intechopen.83215.

Kuhn, M.G. 2002. Optical Time-Domain Eavesdropping Risks of CRT Displays. In: *Proceedings 2002 IEEE Symposium on Security and Privacy,* Berkeley, CA, USA, pp.3-18, May 12-15. Available at: https://doi.org/10.1109/SECPRI.2002.1004358.

Kuhn, M.G. 2005. Security Limits for Compromising Emanations. In: Rao, J.R., Sunar, B. (Eds.) *Cryptographic Hardware and Embedded Systems – CHES 2005. CHES 2005. Lecture Notes in Computer Science*, 3659, pp.265-279. Springer, Berlin, Heidelberg. Available at: https://doi.org/10.1007/11545262_20.

Kuhn, M. G. 2006. *Eavesdropping attacks on computer displays* [online]. Available at: https://www.semanticscholar.org/paper/Eavesdropping-attacks-on-computer-displays-Kuhn/96c1ddf18dbadfa3a9e81ef0bf238511292cab8f [Accessed: 25 June 2022].

Kuhn, M. & Anderson, R. 1998. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations. In: Aucsmith, D. (Ed.) *Information Hiding. IH 1998. Lecture Notes in Computer Science*, 1525, pp.124-142. Berlin, Heidelberg: Springer. Available at: https://doi.org/10.1007/3-540-49380-8_10.

Lavaud, C., Gerzaguet, R., Gautier, M., Berder, O., Nogues, E. & Molton, S. 2021. Whispering Devices: A Survey on How Side-channels Lead to Compromised Information. *Journal Hardware and Systems Security*, 5, pp.143-168. Available at: https://doi.org/10.1007/s41635-021-00112-6.

Lee, H., Sim, K., Oh, S. & Yook, J-G. 2016. Analysis of the Electromagnetic Leakage from Liquid Crystal Display Monitors. *The Journal of Korean Institute of Electromagnetic Engineering and Science*, 27(9), pp.844-853. Available at: https://doi.org/10.5515/KJKIEES.2016.27.9.844.

Levina, A., Mostovoi, R., Sleptsova, D. & Tcvetkov, L. 2019. Physical model of sensitive data leakage from PC-based cryptographic systems. *Journal of Cryptographic Engineering,* 9, pp.393-400. Available at: https://doi.org/10.1007/s13389-019-00215-5.

-Lime microsystems. 2021. *LimeSDR Mini* [online]. Available at: https://limemicro.com/products/boards/limesdr-mini/ [Accessed: 25 June 2022].

Liu, Z., Samwel, N., Weissbart, L., Zhao, Z., Lauret, D., Batina, L. & Larson, M. 2021. Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an Electromagnetic Side Channel. In: *Network and Distributed System Security (NDSS) Symposium*, virtual, pp.1-15, February 21-25. Available at: https://doi.org/10.14722/ndss.2021.23021.

Mangard, S., Oswald, E. & Popp, T. 2007. *Power analysis attack: revealing the secrets of smart cards*. Springer-Verlag US. Available at: https://doi.org/10.1007/978-0-387-38162-6.

Mao, J., Liu, P., Liu, J. & Han, Z. 2017. Method for detecting electromagnetic information leakage from computer monitor. *Mechatronic System and Control*, 45. Available at: http://doi.org/10.2316/Journal.201.2017.1.201-2791.

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., Perieto-Guerrero, A. & Aguilar-Gonzales, R. 2021. Real-Time Implementation of Multi-Band Spectrum Sensing Using SDR Technology. *Sensors*, 21(10), art.number:3506, pp.1-21. Available at: http://doi.org/10.3390/s21103506.

Molyneux-Child, J.W. 1997. *EMC Shielding Materials, Second Edition: A design guide 2nd Edition*. Oxford, UK: Newnes. ISBN-13: 978-0750635486.

-Nooelec. 2021. *NESDR SMArt v4 SDR—Premium RTL-SDR w/Aluminum Enclosure, 0.5PPM TCXO, SMA Input. RTL2832U & R820T2-Based—Software Defined Radio* [online]. Available at: https://www.nooelec.com/store/sdr/nesdr-smart-sdr.html [Accessed: 25 June 2022].

Ometov, A., Levina, A., Borisenko, P., Mostovoy, R., Orsino, A. & Andreev, S. 2017. Mobile social networking under side-channel attacks: Practical security challenges. *IEEE Access***,** 5, pp.2591-2601. Available at: https://doi.org/10.1109/ACCESS.2017.2665640.

Prouff, E. & Rivian, M. 2013. Masking against Side-Channel Attacks: A Formal Security Proof. In: Johanson, T. & Nguyen, P.Q. (Eds.) *Advances in Cryptology EUROCRYPT 2013. Lecture Notes in Computer Science*, 7881, pp.142-159. Berlin, Hiedelberg: Springer. Available at: https://doi.org/10.1007/978-3-642-38348-9_9.

Przybysz, A. Grzesiak, K. & Kubiak, I. 2021. Electromagnetic Safety of Remote Communication Devices – Videoconference. *Symmetry,* 13(2), art.number:323. Available at: https://doi.org/10.3390/sym13020323.

Rowe, N.C. 2006. Electronic protection II-7. In: Bidgoli, H. (Ed.) *The Handbook of Information Security*. New York: Wiley [online]. Available at: https://faculty.nps.edu/ncrowe/eprotect_final.htm [Accessed: 25 June 2022].

-RTL-SDR. 2017. *TempestSDR: An SDR tool for eavesdropping on computer screens via unintentionally radiated RF* [online]. Available at: https://www.rtl-sdr.com/tempestsdr-a-sdr-tool-for-eavesdropping-on-computer-screens-via-unintentionally-radiated-rf/ [Accessed: 25 June 2022].

Rugeles Uribe, J.J., Gullien, E.P. & Cardoso, L.S. 2021. 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.

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.

Sekiguchi, H. 2010. Information leakage of input operation on touch screen monitors caused by electromagnetic noise. In: *2010 IEEE International Symposium on Electromagnetic Compatibility*, Fort Lauderdale, FL, USA, pp.127-131, July 25-30. Available at: https://doi.org/10.1109/ISEMC.2010.5711258.

Stewart, R.W., Crockett, L., Atkinson, D., Barlee, K., Crawford, D., Chalmers, I., Mclernon, M. & Sozer, E. 2015. A low-cost desktop software defined radio design environment using MATLAB, simulink, and the RTL-SDR. *IEEE Communications Magazine.* 53(9), pp.64-71. Available at: https://doi.org/10.1109/MCOM.2015.7263347.

Van Eck, W. 1985. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security*, 4(4), pp.269-286. Available at: https://doi.org/10.1016/0167-4048(85)90046-X.

Warne, L.K. & Chen, K.C. 1992. A simple transmission line model for narrow slot apertures having depth and losses. *IEEE Transactions on Electromagnetic Compatibility,* 34(3), pp.173-182. Available at: https://doi.org/10.1109/15.155827.

Will, M.A. & Ko, R.K.L. 2015. Chapter 5 - A guide to homomorphic encryption. In: Ko, R. & Choo, K-K.R. (Ed.) *The Cloud Security Ecosystem Technical, Legal, Business and Management Issues*, pp.101-127. Available at: https://doi.org/10.1016/B978-0-12-801595-7.00005-7.

ЧТЕНИЕ С ЭКРАНА: ЭЛЕКТРОМАГНИТНАЯ УТЕЧКА ИНФОРМАЦИИ С КОМПЬЮТЕРНОГО МОНИТОРА

Милена М. Грдович, *Даниела* Д. Протич, **кореспондент**,
Владимир Д. Антич, *Бориша* Ж. Йованович

Вооруженные силы Республики Сербия, Генеральный штаб,
Управление информатики и телекоммуникаций (J-6),
Центр прикладной математики и электроники,
г. Белград, Республика Сербия

РУБРИКА ГРНТИ: 20.23.25 Информационные системы с базами знаний,
30.03.17 Физические проблемы механики,
30.19.17 Оболочки,
47.01.11 Современное состояние и перспективы развития,
47.43.21 Влияние различных факторов среды на распространение радиоволн,
47.53.35 Электростатические системы записи и воспроизведения сигналов
ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: Безопасность систем может оказаться под угрозой компрометирующих излучений. В данной статье представлен обзор различных атак на информацию, излучаемую компьютерным монитором. Новые технологии отслеживания излучения экрана могут быть использованы в извлечении (эксфильтрации) конфиденциальных данных с экранов компьютеров. Меры по безопасности способствуют предотвращению электромагнитных атак на излучаемую или передаваемую информацию.

Методы: В данной статье исследуется воздействие атак по сторонним каналам, которые перехватывают скомпрометированную информацию с экрана компьютера. Также в статье объясняется утечка данных вследствие электромагнитных излучений. Программно-определяемые радиосистемы описаны с целью объяснения вредоносных атак на компьютерные мониторы.

Результаты: Источник электромагнитного сигнала определяет характер передаваемой им информации по побочному каналу. Наиболее известная проблема, связанная с выявлением излучений, заключается в возможности перехвата визуальной информации, отображаемой на мониторах компьютеров.

Выводы: Визуальные данные, отображаемые на компьютерных мониторах, могут быть перехвачены программно-определяемой радиосистемой, которая может оцифровывать нужный частотный спектр непосредственно с антенны, передавать его в цифровой сигнальный процессор и выводить в приложение для выявления конфиденциальных данных. Для предотвращения утечки данных можно использовать различные контрмеры, такие как: экранирование, зонирование, программный комплекс TEMPEST и прочие аналогичные методы.

Ключевые слова: электромагнитное излучение, утечка информации, компьютерный монитор.

ЧИТАЊЕ СА ЕКРАНА: ЦУРЕЊЕ ЕЛЕКТРОМАГНЕТНИХ ИНФОРМАЦИЈА СА МОНИТОРА РАЧУНАРА

Милена М. Грдовић, *Данијела* Д. Протић, **аутор за преписку,**
Владимир Д. Антић, *Боршша* Ж. Јовановић

Војска Србије, Генералштаб, Управа за телекомуникације и информатику (J-6), Центар за примењену математику и електронику, Београд, Република Србија

ОБЛАСТ: рачунарске науке, електроника, телекомуникације, информационе технологије, машинство
КАТЕГОРИЈА (ТИП) ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Безбедност система може бити угрожена компромитујућим зрачењем. У раду је приказан преглед напада на информације које зрачи монитор рачунара. Праћењем зрачења са екрана рачунара, нове технологије се могу користити за ексфилтрацију осетљивих података. Емисиона безбедност представља начин за спречавање напада електромагнетних сигнала који настају зрачењем или се преносе.

Методе: У раду се испитује утицај side-channel напада који пресреће компромитоване информације са екрана рачунара. Објашњено је „цурење" података услед електромагнетног зрачења. Софтверски дефинисани радио описан је како би били објашњени злонамерни напади на мониторе.

Резултати: Извор електромагнетног сигнала одређује природу информација које оне носе. Најпознатији проблем повезан са откривањем емисија јесте могућност пресретања визуелних информација приказаних на мониторима рачунара.

Закључак: Визуелни подаци приказани на мониторима могу бити пресретнути софтверски дефинисаним радиом, који може дигитализовати жељени спектар директно са антене, у дигиталном облику га представити процесору и проследити апликацији за откривање осетљивих података. За спречавање цурења података могу се користити разне противмере заштите, као што су зонирање, софт TEMPEST и сличне технике.

Кључне речи: електромагнетна емисија, цурење информација, монитор.

Paper received on / Дата получения работы / Датум пријема чланка: 30.06.2022.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 10.10.2022.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 12.10.2022.