


COMPROMISING ELECTROMAGNETIC RADIATION - CHALLENGES, THREATS AND PROTECTION

Milorad S. Markagić

University of Defence in Belgrade, Military Academy, Department of
Telecommunications and Informatics, Belgrade, Republic of Serbia,
e-mail: milmarkag@yahoo.com,
ORCID iD:  <http://orcid.org/0000-0001-6981-7973>

<http://dx.doi.org/10.5937/vojtehg66-8691>

FIELD: Telecommunications, IT

ARTICLE TYPE: Professional Paper

ARTICLE LANGUAGE: English

Summary:

The aim of this paper is to open up problems regarding parasitic radiation, both inductive and conductive one, originating from devices for data transmission, processing, generation and data protection as well as from their assemblies.

All devices that are used today, both in everyday use at home and in communication between individuals or institutions, contain, other than useful electromagnetic radiation, a part of useless, but also inevitable signals that are outside the control of manufacturers. Devices used for encrypting information are particularly vulnerable to this phenomenon, because every form of protection is meaningless if any part of useful information is accessible, and one of the most important segments of reaching them is monitoring parasitic radiation.

Keywords: radiation, eavesdropping, security of information.

Introduction

We live in a time of mass generation, flow and use of information, which is conditioned by the development of information and communication technologies.

The question of contemporary society is not who rules capital, but who rules information. Namely, the information has become the most appreciated and sought-after commodity.

A great deal of information and data is common goods and serves for public use; it is neither subject to financial expense, nor is subject to the interests of intelligence services - therefore, there is no need to protect it.

The other kind of information is a kind of a secret, it has a special usable value and is often a subject of trade or attempts to acquire it in an illegal manner.

No matter what kind of information or data is in question - secret, commercial, or information and data relevant to the field of defense and security of an institution or state authority - there are two possible scenarios:

- non-conformity of supply and demand in the price and terms of delivery of information, and
- inability to provide information due to the violation of the integrity of an institution or the state.

Such data and information are protected in different ways, from their source to destination, using physical technical protection measures, access restrictions, special handling and storage, cryptographic protection (Markagić, 2010), and other methods.

Bearing in mind that digitization has entered almost all human activities, it is understandable that a large amount of information is processed, transmitted and stored in a digital form, thus increasing a possibility of access to information by an unconventional path.

Although encryption methods have reached a high degree of confidentiality, and although the integrity and the protection of information seem to be "absolute", it must be borne in mind that much information can be compromised and accessible to unauthorized individuals on its way from the sender to the recipient.

Phenomena of CER and TEMPEST

The phenomenon of interest in electromagnetic radiation (EMR) and electromagnetic eavesdropping dates back to the middle of the last century. Almost all armies of the world and the intelligence services have always known that electromagnetic devices, without proper protection, generate a certain level of radio frequency (RF) signals that can be recorded, and then easily read as clear information by simple methods.

Since there is a lack of expertise related to the topic of Compromising Electromagnetic Radiation - CER (KEMZ in Serbian), this issue is not sufficiently focused on (Blandova, 2001), especially in the field of information technology.

The occurrence of massive use of information technology equipment with information of great sensitivity and significance highlights, first of all, the problem of protection of state, military, and other secrets.

The problem of unauthorized access to information through CER has been present in military, diplomatic and intelligence circles for more than 50 years (Markagić, 2010). In Western literature, this problem is most often dealt with in the Transient Electro Magnetic Pulse Emanation Standard (TEMPEST) (Horev, 1998), although there are opinions that this is just a code name without any special meaning. In any case, these are strictly confidential standards which define the permissible limits and measurement methods of TEMPEST or CER (National Security Agency, 2007), (TEMPEST workshop presentation, RIGA, 2008).

The notion of compromising radiation is primarily related to devices where the cryptographic protection of information is carried out. (Ward, 1993)

History of parasitic radiations

The initial forms of the present CER or TEMPEST occurred sometime before the end of the 19th century. The first scientists in the field of telecommunications became aware of the problem which was later called crosstalk. This name was related to the effect of one wire's signal on the signals of the other wire, which would result in unwanted consequences such as signal transmission from one wire to another.

The first documented appearance of the above-mentioned problem occurred during the war in 1914. The phone, as a relatively new invention at that time, was used in communication between soldiers on the battlefield and their command posts. The cable lines sometimes stretched along the entire battlefield, at a distance of several kilometers. In some cases, they would go directly to hostile trenches, and the idea of using the leakage of the signal emerged in order to get to the enemy's confidential information.

To this end, the stations for eavesdropping in key locations were developed to monitor the hostile activity.

This technique brought a great advantage to those who eavesdropped, and by 1915, it progressed to such an extent that signals "leaking" into the ground could be eavesdropped at a distance of nearly 100 meters for the phone and at more than 250 meters for the telegraph.

This was a major problem for the Antanta forces because the Germans thus inflicted huge losses on them. The following year, the

telephone equipment had to be moved two and a half miles from battlefields.

In 1918, the US military hired top cryptologist Herbert Jardley to develop methods for detecting, intercepting and exploiting compromised radiation of telephone lines and radio receivers used on the battlefield.

Already at that time, something similar to TEMPEST began to be developed. The official date of the creation of TEMPEST is not known to the general public, but the assumption is that it was in 1950.

Because of the American Government's awareness of the dangers of losing information, it launched the TEMPEST program with the primary goal - fight against espionage. The WW2 aftermath and the Cold War between the United States and its allies and the USSR were considered to be the beginning of a race in technological development between the two world powers and the two antagonistic blocs. There was a massive development of spying activities, so the need for information security and secure communication was becoming greater than ever. At that time, NATO discovered a German underground tunnel with equipment for wiretapping wire communication where the Germans intercepted Soviet messages.

After several years, one of the most famous TEMPEST attacks in history occurred. Namely, in 1957, the British Prime Minister issued an order to oversee the French Embassy in order to determine their position on accession to the European Economic Community. In addition to encrypted traffic that was transmitted via a crypto device from the embassy to the headquarters in Paris, MI5 intelligence agents discovered a very small and weak secondary signal, which in some way "leaked" from the device, that is, the device itself acted as an emitter. It was a signal that did not contain encrypted text, so there was no need for a cryptanalysis, but only for a simple reconstruction.

Already in 1965, TEMPEST was publicly mentioned for the first time at a conference on computer devices and systems. Then a TEMPEST memorandum was published, which was later replaced with the NACSIM 5000 manual (TEMPEST manual). In 1982, it officially stopped being confidential and became available to the general public, although there are still darkened lines considered to be secret (Kuhn & Anderson, 1998).

Source of CER

Each electrical device creates an electromagnetic field and transmits electromagnetic signals. Simple kitchen appliances - mixer, fridge, electric

cooker, toaster, home appliances - TV and radio, computer, and equipment for telecommunication and cryptographic devices are all sources of EMR.

On each of these devices, even in the production process, and before the sale, certain tests are carried out about whether they can have an impact on other electrical and electronic devices.

In commercial appliances and devices, besides the requirements for physical protection of the environment and people, the problem of radiation is not studied in more detail; however, computer and communication devices take into account the requirements of TEMPEST.

Even not specially skilled and qualified individuals with appropriate and often commercial and cheap equipment, from the remote and safe place, are able to intercept the already mentioned compromising radiation from which a large amount of usable data can be obtained by analysis and reconstruction.

It is understandable that the methods and procedures are still kept in strict secrecy to achieve security through obscurity and many things are still under question (NSA, 2004).

Attacks, information disclosure and protection

It is impossible to separate the concept of electromagnetic radiation and attacks on ICT systems from the concept of protection from CER. Certainly, the focus in both cases is to protect the confidentiality of information and data without neglecting the physical and technical requirements for the design and configuration of the device. Attacks are defined as a wide range of activities that aim to get information by tapping, or by monitoring radiation at the source of processing and / or encryption of information. When considering protection against attacks, and therefore protection from them, it is necessary to know the structure and the methods of attacks in order to prepare an appropriate way of defence and protection against malicious individuals or theft of information. By the way of execution, all attacks can be divided into active and passive attacks.

Passive attacks

Passive attacks are a type of attacks that does not have a third party's impact on the sender, recipient, or information. The third party only monitors the movement of signals through the transmission path, collects

them with the listening equipment and devices, and then analyzes them and attempts to find out the open / desired information.

It is very difficult, almost impossible to detect the presence of an attacker because its presence does not affect the flow of processing or transmission of information, leaves no traces of its activities and is often located at a certain distance from those involved in the generation and transmission of information.

A large number of passive TEMPEST attacks are attacks by side channel attacks. This term is taken from the field of cryptography. From the very name it can be concluded that this attack goes roundabout. As the name itself says, these attacks are going to be bypassing roads (Markagić, 2010). The most common idea is to use an "unbreakable" algorithm, and then a failure to implement it is required.

Based on the vulnerability of the systems for generating, processing, protecting and transmitting data, information attacks are also divided as:

- monitoring the amount of radiation on the computer - the most striking attack on the basis of which one of the more prominent TEMPEST experiments emerged,
- time attacks - monitoring of the time needed to perform a certain computer operation,
- architectural attacks by a secondary channel - the use of failures in the architecture of computers,
- acoustic cryptanalysis - the analysis and use of sounds that arise as side effects in computer use,
- control of computer energy consumption - the amount of energy a computer uses during operation, listening to sounds - an attack that monitors pressing of buttons,
- emissions from the monitor and other computer components.

Active attacks

From the very name it can be seen that active attacks involve the attacker's engagement and its impact on information either at the place of generation, processing, cryptography or transmission, thereby increasing the possibility that an attacker will be detected. Apart from a higher risk, these attacks can bring a greater advantage to a malicious individual or allow eavesdropping in cases where this would not be possible with passive methods.

The first known form of active attacks was an attack by the TEMPEST virus that occurred in the early seventies of the last century. This is one

aspect of the impact of a program on a computer that behaves as a radio emitter whose tones are data carriers.

Then there was the idea of writing TEMPEST viruses, malicious codes that infect computers so that they transmit secret data to a radio frequency that is later intercepted by a conventional radio receiver (Atkinson, 2010). It is even not necessary for this type of attack that a computer is connected to the public network. Using modern signal reception devices, attacks can be carried out from long distances.

Another type of active TEMPEST attacks is an attack on smart cards. The most famous attack of this type is the exploitation of program errors (glitching), or the exploitation of hardware failures in the card itself. In the literature, there are often some other terms such as: EMSEC (Emission Security) HIJACK (type of attacks aimed at intercepting and using signals traveling through a communication line, cable or wireless, or via a power cable and NONSTOP (Kuhn & Anderson, 1998) (radiation monitoring that accidentally induces nearby radio transmitters and similar devices). In this way it is possible to cause compromising radiation of a device containing classified information and intercept and radiate these radiations.

There is also the third, most commonly used category of attacks, which is a combination of active and passive methods.

Protection

Preventing data leakage by compromising electromagnetic radiation in order to protect the device against unwanted loss of information is the core of protection from CER or TEMPEST.

Two basic postulates to be considered when applying the CER methods and procedures for protecting information are:

1. Technical and technological characteristics of equipment that meets the standards:

- a) preventing the correlation between RED signals and BLACK equipment, RED / BLACK separation (RED devices, i.e. connections that transmit confidential, secret information and BLACK devices and connections that transmit open information).
- b) amount of radiation generated by the equipment, and
- c) preventing leakage of signals through electromagnetic and acoustic radiation.

2. Appropriate use of equipment.

The RED / BLACK separation separates these two systems in order to avoid mixing RED (safe) and BLACK (unstable) devices, because then there may be a combination of signals, i.e. transmission of confidential data along an uncertain line and intercepting and detecting this information.

Equipment

In the standards worldwide, it has been concluded that it is necessary to distinguish three levels of approval for the use of CER protection equipment:

1 - Devices of this level do not exist for commercial purposes, and the electromagnetic radiation emitted by such devices is almost non-existent; they are used for the protection and secure transmission of data of national importance.

2 - Equipment used to transfer standard but partially confidential data.

3 - Classic equipment publicly available and easily made by handy means.

Protection against compromising radiation or TEMPEST is dealt with by almost all important institutions and state authorities.

Conclusion

Through the consideration of the harmful effects of uncontrolled radiation, it can be concluded that the fear of such radiation is justified and not a figment of imagination.

Eavesdropping and monitoring primarily state authorities but also companies are everyday occurrences, and even individuals are not immune to this phenomenon. It is a matter of concern that the losses are estimated by billions of dollars this way, and that part of the data thus lost represents permanent and irreparable damage.

However, although the danger is real, there are methods for data, information and device protection. Lately, it has been concluded that the investment in protection should be adapted to the situation in order to minimize possible compromising radiation. Methods are different and protection is achieved by using special metal enclosures and special filtered power supplies. One of the ways is to ensure the entire area around the used equipment, although in most cases it is difficult or impractical to implement it. Between protection and a real danger there should certainly be a happy medium so one needs to consider the

profitability of such investments and acts accordingly. Of course, there is a big difference between private, business, state, and public sectors.

Nowadays, information security is at the forefront. Although attacks pose a potentially major threat to information security, it is clear that individuals can have very little influence on the protection against them. Although CER / TEMPEST is a topic that does not affect most citizens' daily functioning, any leakage of confidential information should nevertheless be prevented.

References

Atkinson, J.M., 2010. *Tempest 101*. Granite Island Group. [Internet]. Available at: <http://www.tscm.com/TSCM101tempest.html>. Accessed: 01 July 2015.

Blandova, E.S., 2001. Pomehopodavljajushhie izdelija. Rekomendacii po vyboru i primeneniju. Special"aja tehnika (in Russian).

Horev, A.A., 1998. *Sposoby i stedstva zashhity informacii, uchebnoe posobie*, Moskva: MoD of Russian Federation (in Russian).

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

Markagić, M.S., 2010. KEMZ i informaciona bezbednost. Zbornik radova, ZT10. Belgrade: Military Academy (in Serbian).

-National Security Agency, 2007. *TEMPEST: A Signal Problem*. [Internet]. Available at: <https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/assets/files/tempest.pdf>. Accessed: 01 July 2015.

TEMPEST workshop presentation, RIGA, 2008. [Internet]. Available at: http://1010.co.uk/org/tempest_presn.html. Accessed: 01 July 2015.

Ward, G., 1993. *TEMPEST in a Teapot. A note discussing the prevention of electromagnetic eavesdropping of personal computers*. [Internet]. Available at: <http://www.austinlinks.com/Crypto/tempest.html>. Accessed: 01 July 2015.

КОМПРОМЕТИРУЮЩЕЕ ЭЛЕКТРОМАГНИТНОЕ ИЗЛУЧЕНИЕ – ВЫЗОВЫ, УГРОЗЫ И ЗАЩИТА

Милорад С. Маркагич

Университет обороны в г. Белград, Военная академия, Отдел телекоммуникаций и информатики, г. Белград, Республика Сербия

ОБЛАСТЬ: телекоммуникации, информационные технологии

ВИД СТАТЬИ: профессиональная статья

ЯЗЫК СТАТЬИ: английский

Резюме:

Целью данной работы является освещение проблемы паразитных индуктивных и кондуктивных излучений. Устройства, используемые в повседневном быту, а также в коммуникации между людьми и учреждениями, кроме полезных магнитных излучений содержат и паразитные излучения, в том числе и неминуемый сигнал, который производитель не в состоянии контролировать. Устройства, которые используются в криптообработке данных особенно чувствительны к этому явлению, поскольку каждая форма защиты теряет смысл, если хоть малейшая часть полезной информации становится доступной. Одним из наиболее важных сегментов приобретения полезной информации является контроль побочных излучений.

Ключевые слова: излучение, прослушивание, информационная безопасность.

КОМПРОМИТУЈУЋА ЕЛЕКТРОМАГНЕТНА ЗРАЧЕЊА – ИЗАЗОВИ, ПРЕТЊЕ И ЗАШТИТА

Милорад С. Маркагић

Универзитет одбране у Београду, Војна академија, Катедра
телекомуникација и информатике, Београд, Република Србија

ОБЛАСТ: телекомуникације, информационе технологије

ВРСТА ЧЛАНКА: стручни чланак

ЈЕЗИК ЧЛАНКА: енглески

Сажетак:

Циљ овог рада јесте да се сагледа проблематика паразитских зрачења, како индуктивних, тако и кондуктивних, која емитују уређаји за пренос података, уређаји за обраду, генерисање и заштиту података и њихови склопови.

Уређаји који се користе у свакодневној кућној употреби и у комуникацији међу појединцима или институцијама, осим корисног електромагнетног зрачења садрже и део некорисног, али и неизбежног сигнала који је ван контроле произвођача. Уређаји који служе за криптообработку информација посебно су осетљиви на ову појаву, јер сваки вид заштите губи смисао ако се у ма ком делу дође до дела корисне информације, а један од битнијих сегмената доласка до њих подразумева и праћење паразитских зрачења.

Кључне речи: зрачење, прислушкивање, сигурност информација.

Paper received on / Дата получения работы / Датум пријема чланка: 12.07.2015.
Manuscript corrections submitted on / Дата получения исправленной версии работы /
Датум достављања исправки рукописа: 27.07.2017.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум
коначног прихватања чланка за објављивање: 29.07.2017.

© 2018 The Author. Published by Vojnotehnički glasnik / Military Technical Courier
(www.vtg.mod.gov.rs, втг.мо.упр.срб). This article is an open access article distributed under the
terms and conditions of the Creative Commons Attribution license
(<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2018 Автор. Опубликовано в «Военно-технический вестник / Vojnotehnički glasnik / Military
Technical Courier» (www.vtg.mod.gov.rs, втг.мо.упр.срб). Данная статья в открытом доступе и
распространяется в соответствии с лицензией «Creative Commons»
(<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2018 Аутор. Објавио Војнотехнички гласник / Vojnotehnički glasnik / Military Technical Courier
(www.vtg.mod.gov.rs, втг.мо.упр.срб). Ово је чланак отвореног приступа и дистрибуира се у
складу са Creative Commons licencom (<http://creativecommons.org/licenses/by/3.0/rs/>).

