INTERNATIONAL JOURNAL of ENGINEERING TECHNOLOGIES-IJET
Aydın, Vol.5, No.3, 2019

TEMPEST Attacks and Cybersecurity

Hakan Aydın*‡

*Department of Computer Engineering, Faculty of Engineering and Architecture, İstanbul Gelisim University, İstanbul, Turkey
(haaydin@gelisim.edu.tr)

‡ ++90 212 422 70 00 / 231

Received: 19.06.2019 Accepted:23.07.2019

Abstract- Broad usage of Information and Communication Technologies (ICT) and the Internet have made cybersecurity a vital issue. One of the less known threat for cybersecurity is TEMPEST (Transient Electromagnetic Pulse Emanation Standard) which has become more apparent today. TEMPEST is an information security term that refers to the examination and control of unwanted electromagnetic energy emissions caused by electrical and electronic devices. As a result of TEMPEST attacks, confidential information such as state secrets, personal information such as bank passwords, and more information can be passed on to the attackers. Unlike other known cyber-attack methods, TEMPEST attack methods are kept secret and those who are exposed to TEMPEST attacks are not aware of these attacks. The concept of TEMPEST is a less known cybersecurity component which can cause much greater damage if the necessary cybersecurity measures are not taken. The purpose of this study is to present a review of TEMPEST attacks and countermeasures. The study also highlights the importance of using national cybersecurity products that passed the national TEMPEST cybersecurity testing certification.

Keywords Cybersecurity, TEMPEST, Electromagnetic Emission.

1. Introduction

Today, the use of Information and Communication Technologies (ICT) in almost every field increases the quality and speed of information services, thus enabling the relevant institution to work more efficiently and contributing to the increase of the living standards of citizens. However, this situation brings about the cybersecurity phenomenon in information systems. Information services, which have become unpredictable with the use of computer technologies, have left their information systems at risk of cybersecurity. Nowadays, cybersecurity has become an inevitable necessity for everyone. As a matter of fact, cyber-attacks against information systems confirm this situation. It is necessary to be prepared for cyber incidents, to get out of these incidents with the least damage, to keep cybersecurity risks at manageable and acceptable levels in order to ensure both personal information security and corporate information security. In this context, one of the prominent cybersecurity issues is TEMPEST. Especially in terms of providing cybersecurity of confidential information, TEMPEST attacks and countermeasures have become an important cybersecurity issue.

Nowadays, TEMPEST cybersecurity studies are carried out in order to be prepared against TEMPEST cyber-attacks, to get out of these incidents with minimum damage and to keep cybersecurity risks at manageable and acceptable levels. Electrical and electronic devices such as wireless transmitters, mobile telephones, radars, peripherals, wireless data transmission systems, computers, copiers or projectors give off electromagnetic emanations. By unauthorized access, the electromagnetic emissions emitted from these devices can be converted into numerical data to provide remote access to their display, thus creating a security vulnerability. By means of appropriate information systems, these electromagnetic waves can also be recorded at long distances and can be reconstructed by processing the electromagnetic radiation. TEMPEST is defined as the examination and control of electromagnetic energy emissions from electrical or electronic devices. TEMPEST is unwanted electromagnetic emissions from electrical and electronic equipment that process confidential information [1]. According to US NSTISSI-7000 Standard, it is defined as electronic and electromechanical computing equipment can produce transmissions of unintentional intelligence. It is an information security term that refers to the examination and control of unwanted electromagnetic energy emissions caused by electrical and electronic devices. It benefits from electromagnetic pollution to access confidential information [2]. This security can be expressed as information security measures that prevent unauthorized persons from generating information from electromagnetic waves. It identifies standards in order to limit radiation emanations from electronic equipment. It is used to protect data from emanations monitoring. It is a field of EMC (Electromagnetic Compatibility) raises worldwide security concerns [3]. While it offers many advantages in terms of information security, it is a costly technology to implement.

If caught and analyzed, publications from electronic devices may disclose information [4]. If the TEMPEST measures are not taken into account, the electromagnetic emissions emitted from these devices in the cyberspace can be converted into information. The electoral machines used in

voting recently have become vulnerable to these attacks. It was proven that 90% of the electronic selection machines used in an election in the Netherlands in October 2006 could be attacked from tens of meters away [5]. TEMPEST is the set of standards that determine the maximum limits of electromagnetic radiation levels of electronic devices and the methods of shielding [6]. It is protection against the exploitation of electromagnetic emanations [7]. TEMPEST is a non-invasive and virtually undetectable tool which enables to steal secret data from a computer up to a kilometer away [8]. In light of the information given above it can be defined as an information security term that refers to the examination and control of unwanted electromagnetic energy emissions caused by electrical and electronic devices. In TEMPEST, it is aimed to catch electromagnetic signals that are transmitted by the systems from one side and to prevent the enemy from catching their electromagnetic signals from the other side.

Among the basic concepts that should be known about TEMPEST security are cybersecurity, cyberspace, cyber defense, cyber-attack, cyberwar and cyber terrorism. The concept of cybersecurity refers to the protection of the information systems that constitute the cyber environment from attacks, to ensure the confidentiality, integrity, and accessibility of the information/data processed in this environment, to identify them, to activate the reaction mechanisms and to return the systems to the pre-cyber security situation [9]. Cybersecurity practices are based on confidentiality, integrity, and accessibility. Of these concepts, the principle of confidentiality is to ensure that access to information and the system is authorized only by authorized persons; the principle of integrity is that information has not been altered, partially or completely corrupted and destroyed; the principle of accessibility means that the user in need can access information at any time.

Cyberspace is an environment consisting of information systems and networks that connect them all over the world and in space. Countries' armed forces, intelligence organizations, other legal authorities, private sector, individual or group of persons involved in crime are the main actors in cyberspace [10]. It is an electronic and electromagnetic environment used to store and exchange information with network systems and related physical infrastructure [11]. Cyber defense can be defined as protecting cyberspace against cyber-attacks and cyber-terrorism [11]. Cyber defense ensures the survival of the systems [10]. Cyber-attacks are the activities carried out in the cyber environment in order to exploit, corrupt, change, prevent access to systems or damage information in the cyber environment [10]. Cyber threats are now emerging as an asymmetrical warfare type that can damage a country's critical communications systems, computer systems, energy and transport networks, military command and control systems [12]. Cyberwarfare is the cyber-attack activities of states against each other [10]. The first point of attention in this definition is the fact that cyberwar takes place between states and the second is that the aim is to damage and interrupt the systems. Cyber terrorism requires less physical training, psychological investment, less death and travel risk than traditional terrorism, which makes it easier for terrorist organizations to hire and hire followers [13].

The purpose of this study is to present a review of TEMPEST attacks and countermeasures. The study also highlights the importance of using national cybersecurity products that passed the national TEMPEST cybersecurity testing certification in Turkey.

2. The Importance of TEMPEST Information Security

2.1. Cyber Security and TEMPEST

Cyber terrorism is the use of computer networking tools to disable critical national infrastructures or to subjugate a state or intimidate civil society [10]. Since today's societies are increasingly dependent on information systems, intervention or attack on information systems among cyber warfare elements is among the first to come to mind. In this context, devices without TEMPEST protection in cyber space face the threat of cyber warfare and cyber terrorism. Cyber defense is the measures taken and the actions carried out to prevent the negative effects caused by attacks, misuse or harmful software and to prevent the systems from being used in a cyber-environment [10]. The TEMPEST standard has been developed to protect against electromagnetism within the scope of cyber defense measures. The TEMPEST standard includes measures and actions taken to ensure the safety of cyber-attacks against cyberspace information systems. The cyber-attack is an activity carried out in a cyber-environment to exploit, distort, change, inhibit or prevent access to the information contained in the cyber environment [10]. Cyber-attacks by using information obtained from TEMPEST cyber-attacks are activities performed in the cyber environment by using the data obtained from electromagnetic waves belonging to systems in the cyberspace.

Military organizations are largely interested in TEMPEST defense [14]. In the US, over $1 billion dollars is spent per year on TEMPEST security [15]. Prices of the devices which are used intercept electromagnetic emissions start from $3000 up to $250,000 or more [16]. Equipment for protection against TEMPEST on the market is expensive [17]. From the information stated above it is possible to make a conclusion that while TEMPEST offers many advantages in terms of information security, it is a costly technology to implement.

2.2. TEMPEST Attacks

Many institutions and people are unintentionally exposed to TEMPEST attacks. Side-channel attacks are methods of extracting information from security systems and research has focused on TEMPEST. It is possible to take the image on the TV screen by using the radiation of the video imaging units (Fig.1) [18].

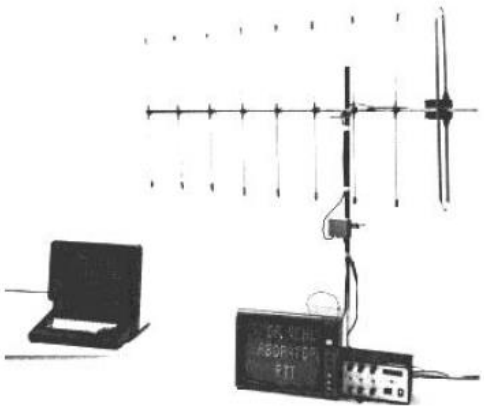

Fig.1. An eavesdropping set-up [18]

TEMPEST is just inherent to electrical or electronic products like computers, servers, etc. A TEMPEST cyber-attack can be performed as follows [19]:

- An attacker runs a TEMPEST virus on the target computer using techniques such as Trojan horses.

- Then the attacker waits until the work hours are over and starts the attack. This may only be possible if the computers are still running.

- The attacker places the radio receiver at a distance where signals can be received, for example in the parking lot of the company.

- It then launches the program and saves the transmission on the radio receiver.

By TEMPEST attacks it is possible to obtain information, messages and other critical security information [20]. Figure 2 below shows the workflow for the attack [21]. In this attack type, an antenna is used for analog measurement.

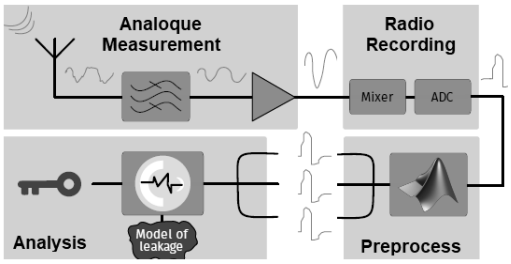

Fig.2. Overview of the attack workflow [21]

Some TEMPEST attacks are among the TEMPEST attacks that are known to exist today (Table 1) [22].

Table 1: Examples of TEMPEST Attacks [22]

Attack Name	Attack Type
Timing Analysis	Leaked side-channel information is utilized by encryption algorithms with variable data processing time periods.
Timing Analysis Attacks	Side channel information leaked by encryption algorithms with variable data processing time periods is utilized.
Timing Analysis Attacks to the RSA Algorithm	Based on the secret key obtained using the timing analysis technique over the RSA algorithm.
Power Analysis Attacks	Based on the principle of inspecting the electric current used by smart cards.
Electromagnetic Analysis Attacks	The attack of TEMPEST by which card and PIN information can be received from an ATM has proven.
Glitch Attacks	Here, the attackers create sudden changes in power or frequency values and try to generate an error that might benefit them.
Y Error Difference Analysis Attacks	These attacks can be easily applied to cards that are not protected against notch attacks, as well as many symmetrical algorithms and protocols.
Optical-Acoustic and Thermal Attacks	It has been shown that the screen data can be read using a photomultiplier tube, telescope, and an appropriate image processing software.
Unified Attacks	Expresses the attack methods in which both active and passive attack methods are used.
Screen Display Listening Attacks	Broadband antenna, oscilloscope and spectrum analyzer, and a system that analyzes the leaked radio signals from computers running in the office environment to obtain a screen image.
Displaying Written Text on the Screen	Electromagnetic propagation may be caused by wideband antennas, tuning mechanisms, band-passive amplifiers, analog-digital converters, etc. systems.

In 1996, it is showed that many public key application algorithms, such as RSA, leak key information over the application run time. The following describes how to obtain the secret key using the timing analysis technique over the RSA algorithm. The process where the secret key is used in the RSA algorithm is as follows:

(1) $R = f(x,y) = y^x \ mod \ n;$

In Eq. (1), the term "n" is a known value and "y" is an input value. The aim of the attacker is to find the secret key information "x". The attack can operate for any structure that includes non-fixed duration operations. For example, if the following algorithm is used to calculate the value of

(2) $R = f(x,y) = y^x \ mod \ n;$

(3) $s_0 = 1,$

(4) $for \ 0 \leq k \leq (w-1);$

(5) $If\ X_k = 1\ then$

(6) $R_k = (S_x \times y) mod\ n,$

(7) $else$

(8) $R_k = S_{k,}$

(9) $S_{k+1} = S_{k^2}\ mod\ n,$

(10) $Result = R_{w-1}$

In this way, all the force term bits are obtained. Since the first "b" bit value is known, the first step b of the algorithm is calculated to find the "sb" value. The next step requires the first unknown bit value. If this bit is '1', then; $R_b = (S_b \times y)$ is performed, if the bit is '0' it is skipped. This branch is used in the attack. Electromagnetic propagation may be caused by wideband antennas, tuning mechanisms, band-passive amplifiers, analog-digital converters, etc. systems. Not only military and civilian institutions but civilian organizations may also be subjected to TEMPEST attacks. Electromagnetic radiation which transmitted can be controlled with computer software for both attack and defense [23].

2.3. TEMPEST Countermeasures

TEMPEST countermeasure is a term for the investigation, capture, analysis, and control of involuntary electromagnetic energy emissions from information and communication technologies that process confidential information. TEMPEST countermeasures provide for a number of improvements and adjustments to the devices, buildings or building installations used. For this purpose, national and international but generally military documents (standards, directives, etc.) are used which explain device and building tests, restrict building installation applications and direct them to the truth. Solutions such as Faraday cage application and grounding are used against electronic information leaks. Leaks caused by conductivity can be overcome by filtering.

One of the best-known methods for TEMPEST attacks is shielding. The only protection against TEMPEST attacks is to use some type of metal shielding [19]. By shielding it is possible to encompass the device in a Faraday Cage. Faraday Cages are not cost-effective or simple to build nor are they readily available to private organizations as a purchasable product [21]. TEMPEST is not taken into consideration by most companies [17]. Using electronic equipment in accordance with standards for emission, using shielded cables, setting up a phone line filter, keeping the length of cables as short as possible are among some of TEMPEST Countermeasures. TEMPEST-certified electronics (computers, servers, etc.) can be used in the context of TEMPEST countermeasures. The copper pipes in a building might be used as conduits for signal emanations, so, even a secure room inside a facility can leak information through the plumbing [21]. Another method is to use different types of fabric produced by using stainless steel wire within the scope of TEMPEST resistance measures [2].

Adding noise to electromagnetic waves is another TEMPEST countermeasure. Noise is added to the electromagnetic waves emitted by this method. In this way, interference occurs in the device that detects the electromagnetic data and no successful TEMPEST result can be obtained. The position of the devices is another TEMPEST protection measure. An example of this countermeasure is that the monitors of the computer should not be turned towards the window. Otherwise, the electromagnetic emission will occur very clearly out of the window. The location of the computer should not be near metal cabinets, radiators or pipes. Because these metals lead to an increase in electromagnetic emissions. These conductors strengthen the propagation of waves. TEMPEST filter products prevent electromagnetic leakage. A TEMPEST filter is a device that allows the signal to pass through a conductor within the limits stipulated by the standards and stops any unwanted signal (TEMPEST leakage). Cybersecurity tempest paint, tempest fabrics, tempest window film, tempest tent, tempest power filters can be counted among these products. By encryption, it is also possible on the software side to prevent reconstructing into anything meaningful [21]. The most reliable solution for protection against TEMPEST leakage is the use of TEMPEST precautionary devices, TEMPEST devices (computers, printers, scanners, keyboards, etc.). These devices are designed and developed nationally within TÜBİTAK UEKAE.

3. Conclusion

The results of our study can be listed as follows:

- Especially information systems that process confidential information may be exposed to TEMPEST attacks. The importance of TEMPEST has become even more important today, in which cybersecurity has increased its value. Nowadays, it is seen that various studies have been carried out both on software and hardware level in order to ensure the TEMPEST security. The information obtained in our research reveals the importance of TEMPEST attacks in cybersecurity and the resistance to these attacks.

- The concept of TEMPEST is relatively less known to other IT Security terms but is a security component that can cause much greater damage if the necessary precautions are not taken. In the electromagnetic energy emitted by devices that process confidential information while operating, there may be leaks that allow this information to be reproduced. The measures to be taken on TEMPEST ensure that these leakages are checked and the security breaches that may occur for this reason are minimized.

- The TEMPEST attack on electoral machines in the Netherlands has once again revealed the need for relevant standards.

- It is of utmost importance to take and implement the necessary TEMPEST cybersecurity measures against cyber threats, vulnerabilities, risks, and attacks.

- While TEMPEST offers many advantages in terms of information security, it is a costly technology to implement.

Based on these results, the following proposal can be presented:

- Continuous and up-to-date training should be provided in order to create TEMPEST awareness in institutions where confidential information is processed.

- Since TEMPEST activities are generally conducted for intelligence purposes, TEMPEST techniques and facilities are kept as confidential as possible. Therefore, when processing confidential information, TEMPEST standards and guidelines should be followed.

- In Turkey, national TEMPEST information technologies and products, which have been subjected to national cybersecurity tests should be used.

References

[1] Resmi Gazete, 4 Haziran 2010. Resmî Gazete, Sayı: 27601, Millî Savunma Bakanlığı Savunma Sanayi Güvenliği Yönetmeliği.

[2] S. Bilgin, Ö. Sarıtaş, G. Okyay, H.G. Örtlek, "Askeri ve Kamu Kuruluşlarına ait Binaların Tempest Güvenliği için Farklı Yapıda Dokuma Kumaşların Geliştirilmesi", Tekstil ve Mühendis, 2013, p.81.

[3] Z. Hongxin, H. Yuewang, W. Jianxin, L. Yinghua, Z. Jinling,. Recognition of electro-magnetic leakage information from com- puter radiation with svm, computers & security 28 (1-2), 2009.

[4] NSTISSI No. 7000, 29 Nov 1993, "TEMPEST Countermeasures for Facilities.", 1993.

[5] B. Jacobs, W. Pieters, "Electronic Voting in the Netherlands: from early Adoption to early Abolishment", Published in: Foundations of Security Analysis and Design V: FOSAD 2007/2008/2009 Tutorial Lectures. Springer LNCS 5705, p. 121-144, 2009.

[6] G. Bayraktar, "Harbin. Beşinci. Boyutunun. Yeni. Gereksinimi: Siber İstihbarat", Güvenlik Stratejileri Dergisi,120-135,. 2014.

[7] F. Cohen, "Information System Attacks: A Preliminary Classification Scheme," Computers & Security, Vol.16, No.1, 1997, pp.127--153.

[8] S. Philippsohn, "Trends in Cybercrime - an overview of current financial crimes on the Internet," Computers &. Security, vol. 20, no. 1, pp. 53-69, 2001.

[9] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, "2016-2019 Ulusal Siber Güvenlik Stratejisi", 2016.

[10] H. Çifci, "Her Yönüyle Siber Savaş", Ankara: Tübitak Popüler Bilim Kitapları, 2013. p.154.

[11] M. Meral. "Siber savunma: Ülkeler ve Stratejiler", 3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, Aralık 2008.

[12] F. Aslay, "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi", IJMSIT (International Journal of Multidisciplinary Studies and Innovative Technologies), vol.1, pp.24-28, 2017.

[13] M.E. Erendor, "Risk Toplumu ve Refleksif Modernleşme Çerçevesinde Siber Terörizm: Tanımlama ve Tipoloji Sorunu", Cyberpolitik Journal, 1(1), 2016, pp.114-134.

[14] Ross J. Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems", 2nd Edition. ISBN: 978-0-470-06852-6. Apr 2008.

[15] P. Shotbolt, "Several compromising-emanations based interception techniques and their implications", June 2003.

[16] D. Garlick, "TEMPEST and Electromagnetic Emanations Security: Is Not Only A Government Standard", GIAC Security Essentials Certification (GSEC) Practical Assignment Option One: Case Study in Information Security, January 27, 2005.

[17] T. Finne, "The information security chain in a company", Computers & Security, 15, 4, 297–316, 1996.

[18] W.V. Eck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?", 1985.

[19] J. Karlsson, "TEMPEST Attacks", Master Thesis in Computer Science, Thesis no: MCS-2003:13. June 2003.

[20] The Federal Information Processing Standard (FIPS) Publication 140-2 (FIPS PUB 140-2), "Security Requirements for Cryptographic Modules", 1994.

[21] F. Mohajer, "Cybersecurity Cyber-Attack Series Side Channel – TEMPEST Attacks", 2016.

[22] H. Altıner, H. ALTINER, E. Şaykol, E. ŞAYKOL, "Veri Güvenliğinde TEMPEST Saldırı Türleri Üzerine Tarihsel Bir İnceleme", Beykent Üniversitesi Fen ve Mühendislik Bilimleri Dergisi, 6 (2), 2015, pp.121-152.

[23] M.G. Kuhn, Markus G. and R.J. Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations.", Berlin Heidelberg, 1998.