BULETINUL INSTITUTULUI POLITEHNIC DIN IAŞI
Publicat de
Universitatea Tehnică „Gheorghe Asachi” din Iaşi
Volumul 62 (66), Numărul 3, 2016
Secția
ELECTROTEHNICĂ. ENERGETICĂ. ELECTRONICĂ

CONSIDERATIONS ON TEMPEST MEASUREMENTS

BY

CRISTIAN ȚURCĂ[1] and CRISTIAN ANDRIESEI[1,2*]

Technical University “Gheorghe Asachi” of Iaşi,
[1]Faculty of Electronics,Telecommunications and Information Technology,
[2]AT&C Technology SRL, Iaşi

Received: September 1, 2016
Accepted for publication: September 30, 2016

Abstract. The fact that electronic equipment radiate unintentional electromagnetic waves has raised concerns about leaking information, especially when dealing with sensitive data. This is the case of government agencies, defense contractors and big corporations which therefore must reduce the RF emissions of their equipment by proper physical shielding. In this regard, our paper reviews the main side channel attacks targeting the emissions of electronic devices, as reported in literature, and details several particular TEMPEST specifications and setup configurations.

Key words: eavesdropping; EMC; leakage; SCA; TEMPEST.

1. Introduction

The history of TEMPEST dates back during the WWII when US Army was interested to exploit weaknesses of enemy combat phones and radio. The development of computing technology and the first computers, yet analog, raised new concerns, primarily for the U.S. government, that information processed by computers could be captured and reconstructed, fact proved to be true. This was already in the ’50s and during the next decades NSA (National Security Agency) specialized in conducting measurements and developing shielding for different electronic devices, electric infrastructure and even

[*]Corresponding author: *e-mail*: candriesei@etti.tuiasi.ro

facilities, all these in accordance with specific TEMPEST standards, known also as EMSESC in NSA terminology, being kept classified until recently. Taking into account that the first computers were built with analog components which radiate even better than the current digital technology, it is obvious that unwanted emissions were of primary interest for intelligence agencies and armies. To avoid confusion, since this topic addresses both the phenomenon of electromagnetic emission and also measurements conducted for shielding development, based on a basic glossary (TEMPEST Glossary) addressing Protective Distribution Systems (NSTISSI 7003), recently replaced by CNSSI 7003 (CNSSI 7003), TEMPEST refers to "investigations and studies of compromising emissions". This is in good agreement with another definition given in (Ayala L., 2016) by a military expert with great experience in battlefield (including espionage) and within Defense Intelligence Agency, where it signifies "investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment.". This glossary further cites FIPS140-2 standard (FIPS140-2, 2001), a supplementary annex issued as draft in 2016 being reported in (Annex A, 2016) and covering also *Electromagnetic Interference/ Electromagnetic Compatibility (EMI/EMC)*. No matter which approach is considered, TEMPEST addresses the phenomenon of emitting and capturing compromising information. The Romanian equivalent of NSA division focused on TEMPEST studies is the Special Telecommunications Service (STS) which shares technical expertise and services not only to Government/State institutions (including embassies) but also to companies willing to protect sensitive data.

Despite of lacking information in this field, many things and standards being classified, this article reviews the main concepts used in the TEMPEST field, with a short description of experimental setups publicly reported in literature by different researchers' groups.

2. 'Red/Black' Separation Principle

This principle simply classifies electronic devices in two classes:

a) 'red' equipment carrying or processing confidential information/data, such as computers, cipher machines, secure workstations;

b) 'black' equipment carrying, processing or transmitting unclassified and/or unencrypted information/data, such as radio modems/routers.

In general, 'red' equipment should be isolated by filters and shields from 'black' equipment while devices with both 'red' and 'black' connectors require specific through testing. In case of sensitive systems currently used by government and not only, quite expensive metallic shielding is employed for individual devices, rooms or even buildings.

According to Red/Black Installation Guidance covered in an unclassified US regulation (NSTISSAM TEMPEST/2-95, 1995), many technical details should be taken into account when dealing with sensitive data, such as:

a) signal cables (shielded metallic cables, cable characteristics, shield termination);

b) optical fiber cables (applications, multifiber cables, cable shielding);

c) signal distribution (wireways, patching, protected distribution systems);

d) signal line isolators and (active, passive) filters;

e) power distribution (including UPS);

f) grounding system (equipotential plane, single point ground, fault protection ground, isolated ground);

g) administrative support equipment (telephone systems, paging, alarm systems, radio transmission, commercial television system installation).

In the same time, the specifications address distinct areas of applications or particular levels where security is stringent: securing voice systems, sensitive compartmented information, transportable systems, aircraft and ships, overall the specifications being split into a set of 9 Recommendations (A – I).

Small details might attract the attention proving the particularities of this field:

a) the existence, development and standardization of RED/BLACK guidance for improved security (and less hazard electromagnetic emissions);

b) the concept of TEMPEST security;

c) (development of) TEMPEST countermeasures to achieve TEMPEST security for a particular physical scenario;

d) equipment TEMPEST zone (ETZ) which is the required secure distance assigned to an equipment based on its TEMPEST electric field radiation characteristic and reported to the limits of NSTISSAM TEMPEST/1-92 (4 zones and 3 levels being defined in this regard);

e) RED/BLACK installation in accordance with TEMPEST security level desired for a new facility (configuration) and, equivalently, a new facility should be designed with TEMPEST specifications in mind if sensitive data will be manipulated inside of this area;

f) an equipment is designated as RED if it processes sensitive unencrypted data that requires protection during electrical/electronic processing while RED lines are optical or metallic wires that carry a RED signal or originate/terminate in a RED equipment;

g) an equipment is designated as BLACK if it processes unclassified or unencrypted information while BLACK lines are optical or metallic wires that carry a BLACK signal or originate/terminate in a BLACK equipment;

h) high-power means radiated power (EIRP = emitted isotropic radiated power) exceeding 100 mW (20 dBm) while low-power means radiated power less than or equal to 100 mW (20 dBm), definition inserted into the revised standard version (CNSSAM TEMPEST/01-13, 2014).

3. TEMPEST Zoning and Separation Recommendations

TEMPEST zoning is a security countermeasure that exploits the inherent free space propagation loss with the attenuation of unwanted emissions by the facility shield. By profiling a facility attenuation, TEMPEST zoning can reduce the costs while allowing equipment operation with less fear of being intercepted, monitored or tracked. In the worst case, a global shielding must be developed for facility, which is the most expensive TEMPEST countermeasure. According to the revised TEMPEST standard (2014), there are two schools of thought about TEMPEST: shielding the entire building and shielding the equipment. The second one seems to be more effective than shielding the building and less expensive, the first one being taken into account even from the very first step of building an official facility (Government, Embassy, etc).

To sketch the facility profile, attenuation plots are measured between 10 MHz and 1 GHz with antennas separated by 20 m in open field. It is obvious that the measured radiation pattern as well as TEMPEST countermeasures depend on the local context, its boundaries and the (free) space surrounding the facility.

There are three security levels (1, 2 and 3) which can be coupled with each of the 3 possible sectors defined as A (less than 20m), B (20m - 100m) and C (more than 100 m), a total of 9 recommendations being defined. As clearly mentioned in the revised standard (CNSSAM TEMPEST/01-13, 2014), the first Level 1 corresponds to the highest containment of classified data. In addition, different colors are associated to cables carrying NSI, such as: green (unclassified), blue (confidential), red (secret), orange (top secret) and yellow (special category).

For example, the security levels 1-3 defined for zone A are defined as follows:

1º Level 1 (Recommendation A) imposes a separation of 50 cm between a RED processor and any BLACK equipment, cable, power line or cable connected to an RF transmitter. In case that this separation can't be maintained, the separation should be at least 5 cm between a RED processor and BLACK power line or cable connected to RF transmitter (or exiting the inspectable area) which should be increased to 15 cm for parallel runs of 30 m. In addition, RED and BLACK wire lines should not use the same distribution vehicle (excepting the case of BLACK optical fiber lines) while shielded cables are mandatory in all applications.

2º Level 2 (Recommendation B) imposes a separation of 1 m between RED processor and BLACK equipment or cable.

3º Level 3 (Recommendation C) imposes a separation of 1 m between RED and BLACK equipment with the plus that administrative support equipment is also part of the BLACK equipment.

In all cases, additional precautions may be necessary in case that the distance is less than 8 m, TEMPEST measurements being necessary to

determine the security level in that zone. Interestingly, these 3 specifications are the same for recommendations D–F and G–I, even though the inspectable space increases up to 100m.

Moreover, RED processors should not be powered from the same source as RF transmitters or BLACK equipment with signal lines exiting the inspectable zone, excepting the case of using powerline filters.

Regarding the distance between RED processor and RF transmitters, the first standard (1995) imposes a separation of 3 m while the revised one (2014) comes with two major improvements (and corresponding distance change):

i) RF transmitters are split in two categories depending on the emitted power: low power and high power;

ii) RF transmitters are split in three categories based on stationarity:

a) stationary transmitter (permanently installed) – 3m for high-power and 1m for low-power RF transmitter;

b) non-stationary (hand held and not docked) – one meter distance for high-power transmitters (such as mobile phones), no particular value for low-power transmitter (such as Bluetooth);

c) special use transmitters (RFID tags, proximity badges) - particular request for recommendations.

Hence, according to these recommendations, separation refers to both physical and electrical separation.

The same recommendations are applicable to aircrafts where one meter should be kept between RED and RF transmitter, RED and BLACK equipment/wirelines connecting to RF transmitter, 30 cm between RED and BLACK wirelines leaving the inspectable space. In this case, TEMPEST design must consider weight, size, power consumption, cooling requirements and available space of the aircraft and solving security issues addressing both airborne operations and ramp operations. A critical TEMPEST issue particular to aircrafts is the ground scheme, since many current paths exist because of seams, material used and static buildup during flight, even though the structure of the aircraft provides an equipotential plane and grounding shouldn't be a problem.

TEMPEST measures should be considered for ships as well, where vulnerabilities address underway (at sea) and in port operation. Similar to aircrafts, one meter should be kept between RED and BLACK equipment.

4. TEMPEST – Threat or Hoax?

Despite of some public assertions of several people working in the engineering field (including telecommunications) or others related to information security, stating that TEMPEST subject would be a hoax as it's rather about cross-interference of electronic devices and not monitoring them, there are several practical facts proving the opposite:

1. There are two civil sectors quite interested of this field, such as banks and law companies, which often impose TEMPEST measures to their architects when building a new facility (USA cases).

2. TEMPEST methods for spying on information systems through leakage emanations are classified by both NSA (NSTISSAM Levels I, II and III) and NATO (such as NATO SDIP-27 Levels A, B and C), just several TEMPEST recommendations for defensive purpose (protection), partially covered in this paper as well, being disclosed, such as Emission Security Countermeasures Reviews (Air Force Manual, 2001). Practically speaking, there is no reason to classify something not useful.

3. Taking into account that national special (secret) services are financially supported by Government, there is no logic in showing interest for TEMPEST shielding if the topic would not be serious for national security and Industry.

4. There are companies, such as SST (Secure Systems & Technologies Ltd) based in UK, specialized in developing and manufacturing electronic equipment for military, in accordance with NATO TEMPEST standard, being certified for Military EMC as well. In addition, it is in charge of securing government organizations throughout NATO and Europe. A short description about their TEMPEST solutions can be found on the website (TEMPEST Introduction, Secure Systems & Technologies).

5. TEMPEST Sources of Vulnerabilities

Computer emissions represent the first serious TEMPEST vulnerability since computers are part of our everyday activity and indispensable tools, no matter if Government, public institutions or private companies is considered. In this regard, electromagnetic radiation of computers was mentioned for the first time in open literature in 1967 (Highland, 1986). It did not attract the attention of the community until 1984 when TEMPEST threat was clearly stated in a Swedish report (Beckman, 1984) and screen capture recovery of a (cathode-ray tube) video display unit was demonstrated one year later (Eck, 1985). In this regard, a clear demonstration of image recovery based on computer emissions, with many screenshots of the results obtained during the experiment, was illustrated in 1998 (Kuhn & Anderson R., 1998). To our knowledge, this is also the single reference proposing TEMPEST monitoring (attacks) to reduce software piracy and copyright infringement, of great help to get physical proofs for obtaining the initial search warrant. Same author, *e.g.* Kuhn M., showed six years later that flat-panel displays were also vulnerable to eavesdropping (Kuhn, 2004). In this regard, the experiments were conducted either in the same room (3 m distance) or several rooms away (10 m). Other successful experiments targeting desktop computers, notebooks and LCD monitors were reported one year later (Hidema, 2005), the authors concluding that for an effective attack, the stealers should be as close as possible to the target or implant some monitoring devices, the last being sufficiently feasible taking into account illegal intrusion in a building and card cloning. Electromagnetic emissions of the keyboards during keystrokes has been successfully studied and reported in

2009 (Vuagnoux, 2009), the experiments being conducted in several setups (semi-anechoic chamber, office, adjacent office and in a building – block of flats). Three years later, successful eavesdropping over computer display from a distance of 46 m (different building) was reported (Elibol, 2012).

The possibility of extracting information by means of optical sources, such as LEDs (light-emitting diode), either modulated or not, was extensively discussed together with several successful experiments (Loughry & Umphress, 2002). The successful information recovery from optical sources impose the development of new regulations and also the introduction of a new type of TEMPEST scenario, such as "optical TEMPEST". According to these surprising results, many electronic and IT devices can be monitored (even link encryption devices with LEDs as monitors), creating many vulnerabilities in a system using LEDs as indicators: computers, workstations, network devices (routers), modems, mass storage devices, peripherals. This method is effective even to 30 meters away of the target.

Another interesting TEMPEST vulnerability is represented by computer keyboard, the keyboard acoustic emanations (different parts of the keyboard plate producing different sounds) helping the attacker to recover the entire text, including password in particular, by studying the keyboard audio registration only. This issue was publicly disclosed and discussed for the first time in 2004 (Asonov & Agrawal, 2004). Soon after, other successful experiments were reported in 2005 (Zhuang, 2005) and 2006 (Berger, 2006). Similar successful acoustic side channel attack targeting printers was reported in 2009, as part of a Master thesis research (Gerling, 2009). As in previous cases, it makes use of feature extraction and (character) recognition. Another acoustic side channel attack was successfully conducted against a notebook CPU as part of a master thesis (Melhus, 2014), the measurements making use of anechoic chamber.

6. TEMPEST Instrumentation

For military purposes, the measuring equipment is by far more sensitive than those targeting civilian applications. However, this should not be a problem as long more sensitive devices are necessary when targeting shielded devices, therefore proving that such measurements are conducted rather from attack perspective than defensive reasons. And this might be the reason why all military TEMPEST setups are classified, as well. In this regard, taking into account that the consumer electronic products are targeted, very sensitive measurement instruments are not necessary.

According to the experiments reviewed in this article, several conclusions addresing the performances of the instruments used to collect data and process it can be drawn, as it follows:

a) Frequency spectrum is monitored from 100 Hz/100MHz/200MHz to 1 GHz, maximum 2 GHz (EMSEC Solutions), depending on the chosen target (TV, monitor, computer/notebook etc).

b) Very sensitive receiver is mandatory, with wideband tuning capability, wide bandwidth (> 20 MHz) and as cheap as possible (professional and expensive instruments suits rather the Army). Dedicated receivers currently sold on the market were preferred for experiments, such asESL Model 400 Tempest Emission Monitor, Dynamic Sciences R-1250 and R-1550, Rohde & Schwarz FSET22.

c) Antennas are crucial for spectrum monitoring, different shapes being reported, such as 4 m dipole (good information recovery even at 10 m), borrowed spiral log conical antenna (more expensive and wideband), log-periodic (broadband, compact, the most preferred and suitable for TEMPEST and eavesdropping).

d) Oscilloscopes are necessary in particular cases for real time measurement and analysis, a sample rate of 5 GS/s being sufficient which is by far more relaxed compared to other cases of side channel attacks (SCA) targeting crypto-processors where oscilloscopes with 20 GS/s are used to ensure good accuracy (Petrvalsky, 2014).

e) Spectrum analyzers are mandatory, the main requirements being larger bandwidth, wide spectrum capability (usually 10 Hz – 2 GHz) and the lowest noise floor as possible (about –165 dBm/Hz). There are some solutions of built-in processing systems, e.g. spectrum analyzers together with oscilloscopes and software for signal processing, such as Z2090B-7XX (Agilent Technologies) and ESI-Z2090B designed by EMSEC Solutions Inc.

7. Conclusions

TEMPEST represents a critical topic in all aspects of national security, addressing information security for public institutions, government, military and intelligence services, small private companies and corporations, all dealing with sensitive data. Experiments conducted so far by researchers from Academia, prove the security vulnerabilities of consumer electronic devices due to electromagnetic radiation since they are not designed with security in mind, TEMPEST protection increasing the product final price otherwise. Looking ahead, the development of new consumer products and services in the context of increasing interest shown to IoT and 5G hot topics, will increase the list with potential vulnerabilities. Hence, extensive TEMPEST measurements of the new electronic devices might be useful and constitute our next step on this topic, making use of the existent University infrastucture, *e.g.* an anechoic chamber working up to 40 GHz, useful for TEMPEST measurements as well.

REFERENCES

Asonov D., Agrawal R., *Keyboard Acoustic Emanations*, Proceedings of the IEEE Symposium on Security and Privacy, SECPRI 2004, Oakland, California, USA, 3-11.

Ayala L., *Cybersecurity Lexicon,* Apress, **158**, 2016.
Beckman, K., *Läckande Datorer [Leaking Computers]*, 1984.
Berger Y., Wool A., Yeredor A., *Dictionary Attacks Using Keyboard Acoustic Emanations*, Proc. of the 13th ACM Conf. on Computer and Communications Security, CCS 2006, Alexandria, Virginia, USA, 245-254.
Eck W., *Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?*, Computers & Security, **4**, 269-286 (1985).
Elibol F., Sarac U., Erer I., *Realistic Eavesdropping Attacks on Computer Displays with Low-Cost and Mobile Receiver System*, Proc. of the 20th European Signal Processing Conf., EUSIPCO 2012, Bucharest, Romania, 1767-1771.
Gerling S., *Acoustic Side-Channel Attacks on Printers*, Saarland University, Department of Computer Science, 2009.
Hidema T., Osamu T., Akihiro Y., *A Trial of the Interception of Display Image using Emanation of Electromagnetic Wave*, Journal of the National Institute of Information and Communications Technology, **52**, 213-223 (2005).
Highland H. J., *Electromagnetic Radiation Revisited*, Computers & Security, **5**, 85-93 and 181-184 (1986).
Kuhn M., Anderson R., *Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations*, Lecture Notes in Computer Science - Information Hiding, **1525**, 124-142 (1998).
Kuhn M., *Electromagnetic Eavesdropping Risks of Flat-Panel Displays*, Proc. of the International Workshop on Privacy Enhancing Technologies, PET 2004, Toronto, Canada, 88-107.
Loughry J., Umphress D., *Information Leakage From Optical Emanations*, ACM Trans. on Information and System Security (TISSEC), **5**, *3*, 262-289 (2002).
Melhus M.K., Mørk H.G., *Analysis of Acoustic Emanations from Computer Systems*, Norwegian Univ. of Science and Technology, Department of Telematics, 2014.
Petrvalsky M., Drutarovsky M., Varchola M., *Differential Power Analysis Attack on ARM Based AES Implementation without Explicit Synchronization*, Proceedings of the 24th Radioelektronika International Conference (RADIOELEKTRONIKA 2014), Bratislava, Slovak Republic, 1-4.
Vuagnoux M., Pasini S., *Compromising Electromagnetic Emanations of Wired and Wireless Keyboards*, Proceedings of the 18th conference on USENIX security symposium, SSYM 2009, Montreal, Canada, 1-16.
Zhuang L., Zhou F., Tygar J.D., *Keyboard Acoustic Emanations Revisited*, Proceedings of the 12th ACM Conference on Computer and Communications Security, CCS 2005, Alexandria, VA, USA, 373-382.
* * * *Annex A: Approved Security Functions for FIPS PUB 140-2,* http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf.
* * * *CNSSI 7003 –Protected Distribution Systems (PDS), September,* 2015, https://cryptome.org/2015/10/cnssi-7003-15-09.pdf.
* * * *Emission Security Countermeasures Reviews, Air Force Manual 33-214,* **2**, (2001), https://cryptome.org/2015/10/cnssi-7003-15-09.pdf.
* * * *EMSEC Solutions LTD*, http://www.emsecsolutions.com/
* * * *FIPS140-2*, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.
* * * *National Security Agency*, https://www.nsa.gov/.
* * * *NSTISSAM TEMPEST/2-95 - RED/BLACK INSTALLATION GUIDANCE*, http://ece.wpi.edu/courses/ee579sw/ECE579S/NSTISSAMTEMPEST2-95.doc.
* * * *CNSSAM TEMPEST/01-13*, https://cryptome.org/2014/10/cnssam-tempest-1-13.pdf.

* * * *NSTISSI 7003 - National Security Telecommunications and Information Systems Technology No. 7003, Protective Distribution Systems, December 13*, 1996, www.dss.mil/documents/odaa/protective_distribution_systems.pdf.
* * * *Secure Systems & Technologies*, http://sst.ws/downloads/SST_insert_TEMPEST_v6.pdf.
* * * *STS, Special Telecommunications Service*, www.sts.ro.
* * * *TEMPEST Glossary*, https://cryptome.org/ncsc-3.htm.
* * * *TEMPEST Introduction, Secure Systems & Technologies*, http://sst.ws/downloads/TEMPEST%20Introduction%20iss%203.pdf.
* * * *Z2090B-7XX*, http://cp.literature.agilent.com/litweb/pdf/5991-1984EN.pdf.

CONSIDERAŢII CU PRIVIRE LA MĂSURĂTORILE TEMPEST

(Rezumat)

Faptul că echipamentele electronice radiază neintenţionat unde electromagnetice a dat naştere la îngrijorări cu privire la scurgerea de informaţii, mai ales când se operează cu date critice. Acesta este cazul agenţiilor guvernamentale, contractorilor privaţi şi marilor corporaţii care, în consecinţă, trebuie să-şi reducă emisiile RF ale echipamentelor folosite printr-o ecranare fizică adecvată. În acest context, articolul nostru rezumă cele mai importante tipuri de atacuri ce vizează emisiile dispozitivelor electronice, după cum au fost menţionate în literatură, detaliind câteva specificaţii TEMPEST particulare şi configuraţii de test.