URSI AP-RASC 2019, New Delhi, India, 09 - 15 March 2019

Second Order Soft Tempest: from Internal Cascaded Electromagnetic Interactions to Long Haul Covert Channels

J. Lopes Esteves [(1)], E. Cottais[(1)] and C. Kasmi[(2)],
(1) Wireless Security Lab, ANSSI, France
(2) Mobile and Telecom Lab, Darkmatter LLC, UAE

Abstract

Many studies were devoted to the characterization, the analysis, the detection and the mitigation of TEMPEST and soft tempest attacks. Such attacks involve a direct interaction between the information processing in an electronic device and the related spurious electromagnetic emanations. Recently, second order soft tempest has been introduced, involving an indirect interaction through internal cascaded coupling effects. In this paper, a setup for investigating such threat is proposed and a proof of concept second order soft tempest attack is described.

1. Introduction

As it is well established for several decades now by the electromagnetic compatibility (EMC) community, functioning electronic devices radiate energy in the form of an electromagnetic (EM) field [1]. More recently, the information security community has shown a growing interest towards the exploitation of the EM radiation of electronic devices for circumventing security policies and designing attacks [2]. Among those attacks, TEMPEST and soft tempest attacks have been investigated for several decades along with mitigations and detection strategies. More recently, second order soft tempest has been introduced. It involves the exploitation of internal cascading EM interactions of an electronic device in order to create covert communication channel. This paper focuses on the analysis of such new attacks through the design of a dedicated test bench and the implementation of different proof of concept attacks.

The paper is organized as follows: Section 2 is dedicated to the definition of TEMPEST and an extensive literature review. Section 3 defines the concept of soft tempest. In Section 4, the second order soft tempest class of attack is defined and compared to TEMPEST and soft tempest. Section 5 describes the experimental setup and introduces the test scenarios that were performed. Conclusions and security considerations regarding second order soft tempest are proposed in Section 6.

2.TEMPEST

The class of attacks called TEMPEST is based on the exploitation of unintentional interactions between a target electronic device and a physical property of the environment while processing sensitive information. When a direct correlation between the information and the measurable variation of the physical property exists, it is possible to reconstruct the information by processing the physical measurements. Although this class of attacks also considers optical, thermal or acoustical emissions, most studies focused on the EM emissions of several technologies and signals, such as video display units (from CRT to LCD and touch screens) [2-8], keyboards (PS/2 and USB) [9,10], printers [15,16] and communication interfaces (PS/2, USB and ethernet) [11-14].

3. Soft tempest

As TEMPEST attacks are based on unintentional emissions during a legitimate operation, the same EM interactions have been exploited in a different type of scenario. Soft tempest attacks have been formalized in [17] and introduce a specific attacker model. Here, an attacker exploits the EM leakage in order to create an unidirectional covert communication channel for data exfiltration. This supposes that the target is running a malicious piece of software which will perform intentional operations specially crafted to modulate the spurious EM emanations. Such physical covert channels are usually referred to as air-gap covert channels and several studies focused on the design and the analysis of soft tempest attacks involving video signals [17,18], CPU-RAM communication [19], hard drive accesses [20] and USB communication [21]. A famous example of such phenomenon is the “TEMPEST for Elisa” proof of concept, which crafts a video stream radiating an amplitude modulated version of Beethoven’s “Für Elise” track when displayed [18].

4. Second-order soft tempest

As summarized in Table 1, TEMPEST attacks exploit directly unintentional EM leakage of legitimate operations to recover the processed information. Soft tempest attacks aim a creating a covert channel through an intentional leakage caused by a specifically crafted operation.

Table 1: Characteristics of TEMPEST, soft tempest and second order soft tempest attacks

	TEMPEST	**Soft tempest**	**Second order soft tempest**
Operation	Legitimate	Specially crafted (malicious)	Specially crafted (malicious)
EM radiation	Unintentional	Intentional	Intentional
Software-EM interaction	Direct	Direct	Indirect
Attack impact	Information recovery	Covert channel	Covert channel

Second-order soft tempest [22] introduces the possibility of exploiting cascading low and high emission EM interactions in the target electronic device in order to create a long range covert channel. The main process can be summarized as follows:

- An intentional (malicious) operation is performed
- Specially crafted to generate internal EM interactions
- Between low emission and high emission components
- Resulting in an indirect *n*-step soft tempest attack

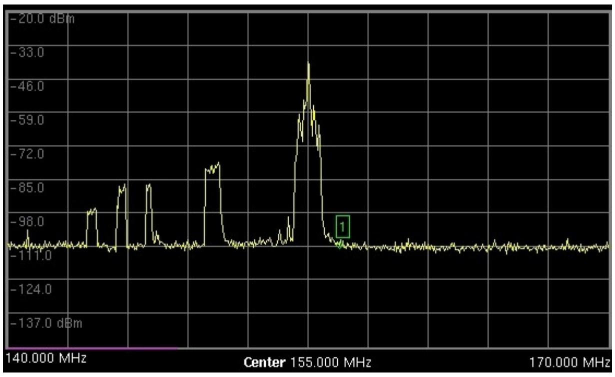

Figure 1. RF output signal of the upconverter containing an upconverted QPSK signal along with parasitic components due to an interaction with a cellular phone sending a text message.

5. Experimental setup

There is a need to characterize second order soft tempest phenomena in order to deeply analyze this class of attacks and design appropriate testing and detection strategies. To this end, a test bench has been set up involving a vulnerable printed circuit board. An unshielded radio frequency (RF) 125 MHz upconverter has been chosen to act as the last-step coupling interface and long haul relay. This board is a low cost and open hardware device, which means that the schematics are known and the design can be easily adapted to our needs.

The upconverter board has been inserted in several configurations together with different low or high emissivity electronic parts, such as graphic cards or cellular radio front ends, allowing observing and analyzing the propagation of the EM interactions of those boards. A legitimate 30 MHz QPSK signal is fed into the RF input of the upconverter. The RF output signal is then analyzed in real time with a spectrum analyzer and a software defined radio receiver. Fig. 1 illustrates an observation of the RF output of the upconverter when a cellular phone in close range is sending a text message.

6. Conclusion

In this paper, second order soft tempest attacks were defined regarding classical TEMPEST and existing soft tempest attacks. In order to analyze this new class of attacks more deeply, a testing strategy has been proposed which allows for a rapid characterization of the propagation of spurious EM emanations towards a RF front-end and their impact on the transmitted output RF signal. During the presentation, the results of different test configurations will be presented and discussed. The indirect interactions and the cascading effects exploitation introduced with the concept of second order soft tempest involve a drastically different approach for both designing attacks and testing against those attacks. Indeed, in the case of a video cable originated leakage, a TEMPEST test will try to recover video signals (first order EM interactions) and other types of signals possibly radiated and originated by cascading effects may not be searched for. Furthermore, second order soft tempest attacks possibly extend significantly the range of the attacker controlled low emission leakage when a high emission component, such as a radio frequency front-end, is in the exploit chain.

7. References

1. C. R. Paul, Introduction to electromagnetic compatibility, vol. 184. John Wiley & Sons, 2006.

2 W. van Eck, “Electromagnetic radiation from video display units: An eavesdropping risk?,” Computers & Security, vol. 4, no. 4, pp. 269–286, Dec. 1985.

3 M. G. Kuhn, “Compromising emanations: eavesdropping risks of computer displays,” University of Cambridge, Computer Laboratory, UCAM-CL-TR-577, Dec. 2003.

4 M. G. Kuhn, “Electromagnetic Eavesdropping Risks of Flat-panel Displays,” in Proceedings of the 4th International Conference on Privacy Enhancing Technologies, Berlin, Heidelberg, 2005, pp. 88–107.

5 M. G. Kuhn, “Compromising emanations of LCD TV sets,” IEEE Transactions on Electromagnetic Compatibility, vol. 55, no. 3, pp. 564–570, 2013.

6 Y. Hayashi, N. Homma, M. Miura, T. Aoki, and H. Sone, “A Threat for Tablet PCs in Public Space: Remote Visualization of Screen Images Using EM Emanation,” in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2014, pp. 954–965.

7 P.-M. Ricordel and E. Duponchelle, “Risques associés aux signaux parasites compromettants : le cas des câbles DVI et HDMI,” in Symposium Sur la sécurité des Technologies de l’Information et des Communications (SSTIC), Rennes, France, 2018.

8 R. Hoad, “Identifying Some Radiated EMSEC Vulnerabilities of Tablet Personal Computers,” in European Electromagnetics International Symposium EUROEM 2016, London, UK, 2016.

9 M. Vuagnoux and S. Pasini, “Compromising Electromagnetic Emanations of Wired and Wireless Keyboards,” in Proceedings of the 18th Conference on USENIX Security Symposium, Berkeley, CA, USA, 2009, pp. 1–16.

10 Y.-L. Du, Y.-H. Lu, and J.-L. Zhang, “Novel Method to Detect and Recover the Keystrokes of Ps/2 Keyboard,” Progress In Electromagnetics Research, vol. 41, pp. 151–161, 2013.

11 P. Smulders, “The threat of information theft by reception of electromagnetic radiation from RS-232 cables,” Computers & Security, vol. 9, no. 1, pp. 53–58, Feb. 1990.

12 L. Nowosielski and M. Wnuk, “Compromising Emanations from USB 2 Interface.,” in PIERS Proceedings, 2014.

13 R. Przesmycki and L. Nowosielski, “USB 3.0 interface in the process of electromagnetic infiltration,” in 2016 Progress in Electromagnetic Research Symposium (PIERS), 2016, pp. 1019–1023.

14 M. Schulz, P. Klapper, M. Hollick, E. Tews, and S. Katzenbeisser, “Trust The Wire, They Always Told Me!: On Practical Non-Destructive Wire-Tap Attacks Against Ethernet,” in WiSec ’16. Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, United States, 2016, pp. 43–48.

15 Cihan U., Aşık U., Cantürk K., Analysis of Information Leakages onLaser Printers in the Media of Electromagnetic Radiation and Line Conductions,International Conference on Information Security and Cryptology; October 2015; Ankara, Turkey

16 Kubiak I., LED printers and safe fonts as an effective protection against the formation of unwanted emission, Turkish Journal of Electrical Engineering and Computer Sciences, 2017; 25: 4268-4279, DOI: 10.3906/elk-1701-128;

17 M. Kuhn, R. Anderson, Soft Tempest: hidden Data Transmission Using Electromagnetic Emanations, Information Hiding: Second International Workshop, IH’ 98 Portland, Oregon, USA, April 14-17, 1998

18 E. Thiele, Tempest For Elisa, 2001, http://www.erikyyy.de/tempest/

19 M. Guri, G. Kedma, A. Kachlon, Y. Elovici, “AirHopper: Bridging the Air-Gap between Isolated Networks and Mobile Phones using Radio Frequencies”, 9th IEEE International Conference on Malicious and Unwanted Software, 2014.

20 M. Guri, A. Kachlon, O. Hasson, G. Kedma, Y. Mirsky, Y. Elovici, “GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies”, 24th USENIX Security Symposium, 2015.

21 M. Guri, M. Monitz and Y. Elovici, "USBee: Air-Gap Covert-Channel via Electromagnetic Emission from USB," no. arXiv:1608.08397.

22 J. Lopes Esteves, E. Cottais, and C. Kasmi, “Second Order Soft-Tempest in RF Front-Ends: Design and Detection of Polyglot Modulations,” in Electromagnetic Compatibility-EMC EUROPE, 2018 International Symposium on, Amsterdam, Netherland, 2018