A Self-monitored Information System for High Power Electromagnetic Attacks Detection

Chaouki Kasmi[1]*, José Lopes-Esteves[1] and Mathieu Renard[2]
Wireless Security Lab[1], Hardware and Software Security Lab[2]
French Network and Information Security Agency
Paris, France
*chaouki.kasmi@ssi.gouv.fr

***Abstract*—The trend in society is to integrate more and more electronic devices in critical infrastructures which make them more vulnerable to high power electromagnetic attacks. Many studies were devoted to the analysis and the detection of electromagnetic attacks against critical electronic systems. In almost all cases, detection devices are additional hardware devices which need to be placed inside the facility. A new approach, considering the target itself as a sensor, is proposed to detect HPEM attacks.**

Keywords-component; HPEM attacks; HPEM detection; Forensic;

I. INTRODUCTION

During the last decades, high power electromagnetic (HPEM) attack [1] against critical systems has become a topic of high interest. The protection from and the detection of such threats becomes of fundamental interest in order to prevent either service disruptions or physical damages. Many studies were devoted to the analysis [2-3] and the detection [4-5] of electromagnetic attacks against electronic systems. Generally, detection devices are additional hardware systems [4-5] which need to be placed inside the facility. In this abstract, it will be shown that the target itself can be naturally used as a sensor and that the statistical analysis of recorded information can be used for HPEM-attacks detection.

II. FAULT DETECTORS

The information system, a computer in what follows, possesses several interfaces (peripherals, communication links) and internal sensors (temperature sensor), as summarized in Table 1, that can be used to monitor any trouble that may occur during its use. The wireless interfaces, known as *front-door* coupling interfaces, can be used to monitor the noise floor, the signal to noise ratio and the received power of the surrounding electromagnetic environment.

Additional parameters can be monitored on the computer using the general commands provided by manufacturers such as CPU load, motherboard sensors status, memory faults or software crashes can provide, when properly correlated, a reliable HPEM-attacks detector system. Mouse deflection errors on a computer running a Microsoft Windows operating system have been reported [5] during immunity testing. In order to obtain further details, we decided to work on a Linux distribution which allows getting deeper in the kernel system logs.

TABLE I. Information available on a computer

	Detectors	Information available
Communication interfaces	2G/3G, NFC, PLC WI-FI, Bluetooth	noise floor signal to noise ratio bit error rate received power data rate
	Ethernet	
Hardware	CPU Memories	fault analysis load temperature
Software	Operating system	software crashes
	Drivers	

III. ONLINE DETECTION AND FORENSIC

The collected data can be analysed in real time or stored, either locally or remotely. Alert messages can be provided to the user of the computer. Moreover, if a computer is physically damaged, a forensic analysis can be applied by extracting and analyzing the collected data in order to estimate if the computer has been hit by HPEM-attacks.

Furthermore, the wide deployment of such software in a large IT-network can lead to the design of a distributed agent mesh which allows increasing the efficiency of HPEM-attacks detection.

During the presentation the test results from HPEM-attacks against a monitored computer will be presented. It will be shown how the proposed method provides a low-cost built-in reliable way to detect HPEM-attacks and their effects on a target.

REFERENCES

[1] W. A. Radasky, C. E. Baum and M. W. Wik, "Introduction to the special issue on high-power electromagnetics and intentional electromagnetic interference," Electromagnetic Compatibility, IEEE Transactions on, vol.46, no. 3, pp. 314-321, Aug. 2004.

[2] J. Mirschberger, F. Sonnemann, J. Urban and R. H. Stark, "High-Power Electromagnetic effects on Distributed and Automotive CAN-bus systems", In Proc. of EUROEM 2012, pp. 85, July, 2012

[3] M. G. Bäckström and K. G. Lövstrand, "Susceptibility of electronic systems to high-power microwaves: Summary of test experience," IEEE Trans. Electromagn. Compat., vol. 46, no. 3, 2004.

[4] A. Kreth, O. Doering. E. Genender and H. Garbe, "Predetection for the identification of electromagnetic attacks against airports", In Proc. of EUROEM 2012, pp. 81, July, 2012.

[5] R. Hoad, L. Sutherland, "The Forensic Utility of Detecting Disruptive Electromagnetic Interference", In Proc. of the 6th European Conference on I-Warfare and Security, pp. 77-87, July, 2007.