Active Forensics Tracking Exploiting Logical Effects of HPEM

José Lopes Esteves
Wireless Security Lab, National Cybersecurity Agency of France (ANSSI)
e-mail: jose.lopes-esteves@ssi.gouv.fr

For several decades, the effects of high power electromagnetic (HPEM) [1] on electronic devices and complex electronic systems have been studied [2], mostly for the characterization of mission critical effects for both designing offensive and defensive strategies. The exploitability of the effects and their consideration in risk analysis has also been investigated, both from a functional safety and an information security [3] perspective. In this study, a novel HPEM effect exploitation technique is investigated. It is proposed to focus on effects which have a logical impact on the target system and which impact is somehow stored by the target. The exploitation of this kind of effects opens the way to embedding information into the target.

In order to characterize the type of effects that are suitable for such kind of exploitation, we consider the classification of the HPEM effects on electronic devices based on their duration that has been proposed in [4]. When effects from categories (E) and (T) lead to logical impacts that can be observed by a piece of software, it becomes possible to take advantage of HPEM effects to create a unidirectional physical covert communication channel. If the logical repercussion of an effect directly or indirectly alters the state of the target, then it can be exploited as a storage channel.

As a proof of concept, this technique is applied to an unmanned aerial vehicle (UAV) as a way to insert a mark allowing an a posteriori proof of its presence during an incident, in the case neutralization techniques failed or could not be used. In this case, the persistence mechanism in use is the raw sensor measurements stored in the flight logs, as schematized in Fig. 1.

During the presentation, the whole methodology for the realization of such electromagnetic watermarking will be presented in detail, from the characterization of the effects on the target to their exploitation in a context of forensic tracking.

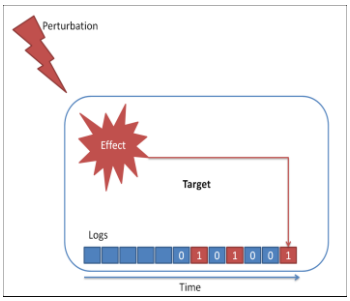

Figure 1. electromagnetic watermarking exploiting system logs for persistence

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] M. G. Bäckström and K. G. Lövstrand, "Susceptibility of electronic systems to high-power microwaves: Summary of test experience," IEEE Transactions on Electromagnetic Compatibility, vol. 46, no. 3, 2004.
[3] C. Kasmi and J. Lopes Esteves, "IEMI threats for information security: Remote command injection on modern smartphones," *IEEE Transactions on Electromagnetic Compatibility*, vol. 57, no. 6, pp. 1752–1755, 2015.
[4] F. Sabath and D. Nietsch, "Electromagnetic Effects on Systems and Components," in *American Electromagnetics International Symposium AMEREM 2006*, Santa Barbara, CA, USA, 2006.