Analysis of HPEM perturbations induced on the navigation system of a UAV

José Lopes Esteves and Emmanuel Cottais
Wireless Security Lab
French Network & Information Security Agency (ANSSI)
Paris, France
jose.lopes-esteves@ssi.gouv.fr
emmanuel.cottais@ssi.gouv.fr

Chaouki Kasmi
TV Labs
Dark Matter LLC
Abu Dhabi, UAE
chaouki.kasmi@darkmatter.ae

***Abstract*—In this study, a software instrumentation of a UAV has been performed in order to ease the detection of the effects induced by RF pulses on the target and determine potential neutralization strategies. As outcomes, several effects have been observed which could be combined for neutralizing the target or taking control of its flight path.**

***Keywords*—UAV, IEMI, HPEM, susceptibility, neutralization**

I. INTRODUCTION

Unmanned aerial vehicles (UAVs) have been subject to a recent widespread in sectors ranging from military and industrial applications to civilian entertainment. This situation has brought to focus on the susceptibility of UAVs to high power radio frequency (RF) pulses, both for neutralization and hardening purposes. Several studies were devoted to the analysis of the susceptibility of electronic devices, including UAVs [1-3]. However, a fine grain analysis of the local hardware effects and their propagation to the software layer still remains a challenge. We propose in this study to show how EM experts can benefit from Information Security methodologies to unlock targets and enable to detect direct effects (front-door and back-door) as well as cascading effects (from hardware to software failures).

II. ASSESSING SYSTEM LEVEL EFFECTS

An interesting approach has been proposed in [4], which consists in identifying software observables and monitoring them with custom software during parasitic exposure. As a result, the software level symptoms can be analyzed and the effects on critical processes can be inferred. However, this approach can be difficult to apply on a closed system. In order to gain a full access on the target and to be able to run monitoring software, a hardware and software security analysis has been performed.

III. SOFTWARE OBSERVABLES

The target possesses several RF communication interfaces which are seen as the front-door coupling interfaces: a 2.4 GHz Wi-Fi link, a proprietary 5.8 GHz OFDM link and a GPS receiver. When possible, the received signal power, the signal to noise ratio, the transmission rate and the error rate have been monitored. Besides, UAVs possess a lot of sensors gathering data towards a flight controller in charge of positioning and controlling the motors of the propellers. All these actions occur over a serial communication bus which we eavesdropped in order to access raw and derived measurements as well as actuator commands.

IV. OUTCOMES

This study demonstrates the validity of the approach from [4] on UAVs and highlights the difficulty of analyzing closed systems. Several observables have shown to be pretty reactive to RF pulses. Along with the expected perturbations of the front-door coupling interfaces, interesting phenomena occurred on components in charge of the in-flight self-stabilization and positioning of the UAV. During the presentation, the different steps that lead to an unrestricted access to the target will be explained. The instrumented software interfaces will be introduced. Finally, the test results from high power electromagnetic (HPEM) attacks against the targeted UAV will be presented, showing promising strategies for a logical layer neutralization of UAVs by a smart use of HPEM.

REFERENCES

[1] C. Adami, S. Chmel, M. Jöster, T. Pusch., and M. Suhrke, “Definition and Test of the Electromagnetic Immunity of UAS for First Responders,” Adv. Radio Science, 13, 3, November 2015, pp. 141-147.

[2] 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.

[3] Y. V. Parfenov, W. A. Radasky, B. A. Titov, L. N. Zdoukov, “Some Features of the Pulse Electrical Disturbances Influence on Digital Devices Functioning,” URSI General Assembly, August 2014.

[4] C. Kasmi, J. Lopes-Esteves, “Automated analysis of the effects induced by radio-frequency pulses on embedded systems for EMC Functional Safety,” Radio Science Conference (URSI AT-RASC), 16-24 May 2015.