2nd URSI AT-RASC, Gran Canaria, 28 May – 1 June 2018

Software Instrumentation of an Unmanned Aerial Vehicle for HPEM Effects Detection

J. Lopes-Esteves[(1)], E. Cottais[(1)], and C. Kasmi[(2)]
(1) French Network and Information Security Agency-ANSSI, Wireless Security Lab., 75007 Paris, France, www.ssi.gouv.fr,
e-mail: jose.lopes-esteves@ssi.gouv.fr
(2) TV Labs, Dark Matter LLC, Abu Dhabi, UAE

Abstract

Unmanned aerial vehicles are spreading and their malicious use considered as a plausible threat against critical infrastructures. Their neutralization is of high interest for security aware organizations and high power directed energy weapons have been proposed. Therefore, the analysis of the susceptibility of such devices is of fundamental interest for both offensive and defensive purposes. Many studies were devoted to detecting the effects of electromagnetic interference on electronic devices and a recently proposed approach as shown to provide insight on the impact of hardware effects at the software level on tested targets. In this study, the application of this approach on a civilian unmanned aerial vehicle is proposed, consisting of designing and running specific software on the target in order to monitor well chosen observables during susceptibility testing. The methodology to run arbitrary software and to identify interesting observables is detailed. Interesting effects were detected, opening the scope to both neutralization and hardening strategies.

1. Introduction

Unmanned aerial vehicles (UAV) are getting more and more deployed for both military and civilian applications. As some categories of UAVs are available to the public, the possibility of using them for malicious purposes is considered as a realistic threat and the problem of their neutralization is of high interest for security aware organizations. Among the solutions considered to take them down, like using hawks or traditional ballistic weapons, high power electromagnetic (HPEM) directed energy weapons have been proposed [1]. Therefore, the analysis of the electromagnetic (EM) susceptibility of specific UAVs, and particularly the characterization and the analysis of the effects of intentional EM interference (IEMI), is of fundamental interest for both offensive and defensive purposes [2].

Many studies were devoted to the test [3] and the analysis [4] of effects induced by intentional electromagnetic interferences on electronic systems, including UAVs [5]. Publicly known effects of such devices are motor disruption and radio frequency (RF) communication link disruption, but the root causes and internal mechanisms of those effects were not explained.

More recently, an operating system centric approach for detecting such effects on computers and smartphones has been proposed, relying on a software instrumentation of the target turning it into a multi-sensor system [6]. This however requires a high privileged access to the target, which can be hard to obtain on complex embedded devices.

In this study, the aforementioned methodology has been applied to a civilian quadcopter UAV, which showed to be a very interesting target enclosing a lot of embedded sensors. The target was first deeply analyzed, from the hardware to the software layer, in order to identify ways to gain a privileged access and run arbitrary software. Then, specific software was designed and deployed in order to enable a real time monitoring of a set of observables during parasitic exposure.

This paper is organized as follows: in Section 2, the target system topology is presented and its main components are defined. In Section 3, the main observables which have been identified on the target are introduced. The hardware and software analysis that led to the ability to monitor those observables is summarized in Section 4. The experimental setup and the preliminary results are described in detail in Section 5 and discussed in Section 6.

2. Target topology

The targeted UAV is a common off the shelf quadcopter which is marketed as a photo and video acquisition device. The system as a whole is composed of the flight vector (FV), the remote controller (RC) and a proprietary smartphone application (SA). The flight vector encloses a digital camera (DC).

In operation, the system is organized around the RC. The RC implements a Wi-Fi 2.4 GHz access point. It is also in charge of routing IP packets between all the parts of the system. This network is mainly used for the communication from the FV and the DC to the SA. The RC and the FV also communicate over a proprietary radio frequency protocol in the 5.8 GHz band.

The FV encloses a main microcontroller running a MIPS version of OpenWRT [7], a well known Unix distribution dedicated to wireless routers. Besides, a couple of other microcontrollers are in charge of the avionics functions and real-time interactions with the sensors and the motors. Those microcontrollers communicate with the main microcontroller over an asynchronous serial link with a proprietary protocol, in order to both send status information about the sensors and receive commands. The main microcontroller then forwards those packets through the Wi-Fi link to the RC, the SA or the DC.

The RC has a very similar topology. The main differences concern the mechanical sensors and actuators, which are dedicated to the control buttons instead of the gimbal and the motors drive.

3. Identification of observables

Following the methodology described in [6], the target is first decomposed into several coupling interfaces. The front-door coupling interfaces are the Wi-Fi front-end, the proprietary 5.8 GHz interface and the GPS receiver interface.

The interesting back-door coupling interfaces can be summarized as follows: the motor driving cables, the several ribbon cables for internal printed circuit board (PCB) to PCB communication, the embedded sensors and their analog or digital communication links, the power supply network, the analog and digital integrated circuits and components.

As the target is an UAV, it encloses several components which are related to the autopilot and other avionics functions. A lot of sensor information is displayed on the SA main view, such as GPS latitude, longitude and altitude, gyroscope measurements, accelerometer measurements, gimbal movements, battery charge, voltage, motor states, etc.

4. Software instrumentation

One of the main challenges with the proposed approach for analyzing final products (instead of development boards or open prototypes) is to find ways to have access to the observable data gathered by the target. In this case, several options were possible, starting with relying solely on the SA, by visually exploiting the view or by modifying the smartphone operating system to retrieve data. Unfortunately, all the information accessible through the SA is not contained in one view, so one would have to interact physically with the smartphone during the tests. Furthermore, the SA does not gather all the information that is available.

The strategy that was chosen consisted in gaining a privileged access on the FV main microcontroller and to run a specific piece of software to gather information, store it locally and send it to a remote monitoring computer. Indeed, as stated in Section 2, this main microcontroller is in charge of forwarding the messages coming from the sensors and actuators enclosed on the FV to the RC or the SA. As such, it seems to be a relevant observation spot. In order to achieve this, the hardware architecture has been analyzed in detail. Each part of the FV has been reverse engineered and a serial console port has been found, providing a root access to the OpenWRT.

This privileged access has allowed to perform an in depth analysis of the operating system configuration to determine the most efficient ways to gather the information about the observables. In particular, a proprietary piece of software is manipulating serial packets coming from the different parts of the drone (sensors, etc.), probably containing interesting data. Also, it supported a special configuration flag enabling a debugging mode, resulting in writing all those packets in the system log files. After enabling remote system logging in the operating system configuration, all those packets were streamed in real time towards the monitoring computer.

In order to extract and interpret the data contained in the packets, the proprietary serial communication protocol had to be analyzed and reverse engineered. This has been performed by a partial analysis of the SA in order to identify the way the packets are processed and to implement a custom parser on the monitoring computer.

This strategy presents several benefits. First, it gives access to raw measurements from the different parts of the target which may not be accessible otherwise (through the SA for example). Secondly, some information can be obtained from several sources at the same time (e.g. altitude information computed by the flight controller and the one received by the GPS). Finally, integrity checking mechanisms are provided in the packets, so that it also becomes possible to detect the presence of interference on the serial busses.

5. Susceptibility testing

5.1 Setup

The experiments were run in a Faraday cage following the setup depicted in Figure 1. The complete target system, namely the FV, the RC and the smartphone running the SA, was started in a nominal operation mode. In order to route the gathered data to the monitoring computer outside the cage, a device has been linked to the Wi-Fi access point of the RC acting as a Wi-Fi to Optical Fiber bridge.

During the experiments, the target was illuminated with continuous waves in the 100 MHz – 2 GHz frequency band modulated in amplitude with a repetition rate in the range 1 Hz – 20 kHz. The use of this source is related to the following main advantages: building this type of source is less expensive as it is using common RF devices, it can be reconfigured easily to neutralize multiple targets with different frequency of susceptibility and critical frequencies can be avoided (e.g.. law enforcement communication frequency band, GPS frequency band).

The target has been immobilized on a table1 m away from the emitting antenna. The engines were not started during the tests and the propellers were dismantled. Furthermore, in the Faraday cage, the legitimate GPS signals could not be received by the UAV. This implies that the results obtained under these conditions may not be completely representative of the behavior of the target during an outdoor flight. In what follows, the most responsive observables and the observed effects of IEMI exposure are summarized.

Electric field levels were also recorded in the vicinity of the drone in order to link the severity of the effects with the parasitic exposure. Nevertheless, results are shown based on the source's parameter modification in order to highlight the most important ones with are the AM modulation rate and the repetition rate as demonstrated in [8]. Tuning the electric field level remains an easiest part as the RF source can be easily enhanced with solid-state amplifiers. It is worth to mention how the physical observables are affected by intentional exposure.

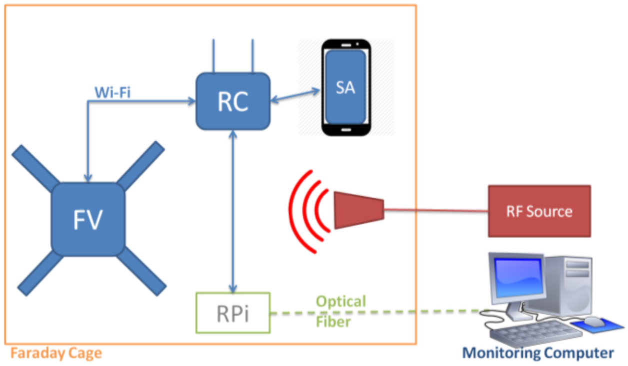

Figure 1. Experimental setup: the flight vector (FV), the remote controller (RC), the smartphone application (SA) are placed in a Faraday cage, and a Raspberry Pi (RPi) relays the logs to a monitoring computer.

5.2 First results

During the tests, several observables were notably sensitive to the RF pulses. In this section, only the most significant results are summarized. In a small number of experiments, it was possible to rapidly identify both front-door and back-door effects, as well as both transient effects and persistent effects (present until reboot).

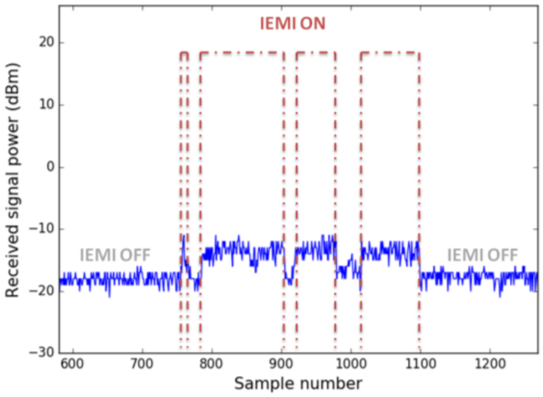

Figure 2. Received signal power on the 2.4 GHz Wi-Fi interface of the UAV showing the presence of sub harmonic (300 MHz) parasitic signal by a +7dBm variation.

The front-door coupling interfaces, namely the Wi-Fi 2.4 GHz link, the 5.8 GHz remote control link and the GPS receiver were observed during parasitic exposure. As expected, the Wi-Fi interface characteristics have shown to be reliable observables for sub harmonic perturbations. As shown in Figure 2, the received signal power at the target increases (+7dBm) when a 300 MHz carrier frequency signal is emitted. Simultaneously, the bit rate of the Wi-Fi link decreases (not shown). This has been observed for several 2.4 GHz sub harmonics.

Among the observables that were identified in Section 3, some have shown to be reacting simultaneously to the RF pulses. However, it could sometimes be explained by the fact that some values are derived from others. It seems to be the case regarding the behavior of the altitude and the vertical speed. As illustrated in Figure 3, the sensor in charge of measuring the vertical speed is recording erroneous variations during parasitic exposure.

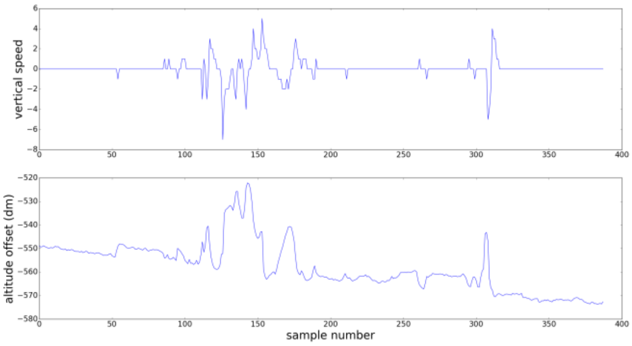

Figure 3. Effects on the measured vertical speed (top) and the altitude (bottom) reported by a still target during parasitic exposure.

These variations have an immediate impact on the altitude reported by the target. It can be noted that when the RF source is off, the vertical speed is null and the altitude is naturally drifting. This drift might be corrected in real time using the GPS data in normal flight conditions.

Several other symptoms have been observed during the experiments and should be further investigated in order to fully understand their origin or their impacts on the target, such as perturbations of the battery temperature and charge reading or significant compass errors (mostly on the yaw angle) including offset values corresponding to demodulated RF pulses.

6. Limitations and further work

As it has already been pointed in [6], one of the main limitations of this approach is that the equipment under test is in charge of gathering data and routing it to a monitoring computer. Therefore, if there is a service disruption due to the IEMI, some data can be lost. Furthermore, in this case, the link for logging the data is somehow fragile as it relies on an unprotected hardware (the Raspberry Pi) and on a Wi-Fi link. During the tests, several interruptions of this link have occurred and as a consequence, some frequencies could not be correctly tested.

As a corrective measure, a local logging mechanism could be implemented on the target. However, it would require remapping the partitions as there is no space for such huge amount of data. An interesting solution would be to be able to store the data on the camera external SD card.

This paper mostly contributes to validate the relevance of the proposed approach on UAVs by presenting several preliminary results. Meanwhile, several other observables can be instrumented on the FV, such as information related to the motors, the inertial measurement unit or the GPS positioning. The identification of malformed or corrupted serial packets could also allow detecting effects on the serial link or on one or several entities communicating on this bus. Several unexplored symptoms are expected to appear with motors on and GPS. This will be further investigated by either having a GPS emulated signal or to switch the test environment in an open area test setup. Furthermore, the RC and the SA could also be modified in order to provide complementary information on the FV susceptibility to IEMI.

7. Conclusion

As the presence of drones spreads out, both their neutralization and their hardening are deeply being investigated. The use of directed energy HPEM weapons is a realistic neutralization solution and therefore the susceptibility of UAVs to IEMI is of high interest. In this paper, a software instrumentation of a common off the shelf civilian quadcopter has been proposed in order to facilitate testing its susceptibility to RF pulses.

To this end, an in depth hardware and software analysis of the target has allowed to identify ways to obtain a fully privileged access to the operating system and to obtain raw data coming from the different sensors and actuators composing the target. Among this data, several observables have been identified and monitored in real time during RF exposure. Several observables have shown to be highly responsive to the parasitic signals.

In particular, the effects observed on the vertical speed sensor and on the compass measurements seem to be quite promising for neutralization purposes, as they could lead to unexpected reactions from the stabilization feedback loop. Therefore, these functions should be hardened in priority in order to protect operation critical UAVs.

8. References

1. DIEHL, “HPEMcounterUAS system,” online: http://drohnenabwehr.de/en/integrated-system/effectors/hpem/, accessed: 2018/01/30.

2. 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, doi: 10.5194/ars-13-141-2015.

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, doi:10.1109/TEMC.2004.831814.

4. 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, doi: 10.1109/URSIGASS.2014.6929514.

5. Q. Zhijun, P. Xuchao, H. Yong, C. Hong, S. Jie, Y. Cheng, “Damage of high power electromagnetic pulse to unmanned aerial vehicles,” *High Power Laser and Particle Beams*, vol. 29, no. 11, November 2017, doi: 10.11884/HPLPB201729.170216.

6. 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, doi: 10.1109/URSI-AT-RASC.2015.7303039.

7. OpenWRT, online: https://openwrt.org, accessed 2018/01/30.

8. R. L. Gardner, C. Kasmi, M. Hélier, M. Darces, “Electromagnetic Security: Risks Management. Improvement using Statistics,” ID 01. *AMEREM 2014, Conference*, Albuquerque, New-Mexico, USA, 2014.