Susceptibility testing of COTS Sensors to RF Pulses with focus on widespread electronics for Information Security risks management and mitigation

E. Al Shahhi(1), M. Bluhm(1), A. Garipov(1) and C. Kasmi(1)
(1) TV Labs, Xen1thLabs, DARK MATTER LLC, Abu Dhabi, United Arab Emirates
chaouki.kasmi@darkmatter.ae

During the last decades, high interest has been shown to the analysis of the susceptibility of electronic devices to intentional electromagnetic interference. One of the recent main contributions is the link between the Electromagnetic Compatibility (EMC) and Interference (EMI) testing and the Information Security needs [1-2]. Using appropriate health monitoring agents, it has been demonstrated that a fine-grained analysis of effects induced by parasitic fields can be obtained. Having at hand a precise list of effects for a given excitation defined by a set of characteristics (e.g., type of source, PHY layer parameters), risks management can be enhanced by taking into account threats of electromagnetic attacks for improving the resilience and the integrity of an infrastructure and the provided services.

While many challenges remain for non-experts in electronics to completely design embedded systems, low cost boards and sensors have been made available. Users have the possibility to implement software applications to combine and control electronic actuators and sensors with development platform like the Arduino [3]. Considering the popularity of these easily accessible tools for building embedded solutions in the Internet-Of-Things (IoT), the Electromagnetic Compatibility of such solutions becomes questionable as their implications may affect our daily lives due to low immunity (e.g. devices may experience malfunctions due to parasitic exposures) or a high emissivity (e.g. devices may emit higher level of noise than the defined levels by standards). In [4], the Arduino motherboard has been tested and EMC issues have been raised. Nevertheless, as far as we know, the shields composed of sensors connected to the Arduino board have not been tested.

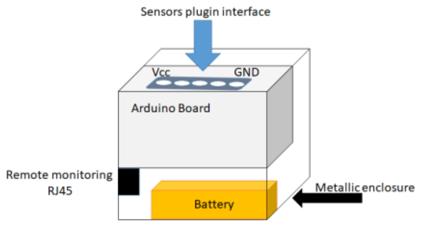

Figure 1. Experimental test set-up for the susceptibility testing of COTS sensors

While many sensors may have been tested with regards to EMC standards, it is very common to buy counterfeits of electronic devices in online markets. The likeliness of the EMC testing of these counterfeits is known to be very low. As a result, when inserted in custom applications, these counterfeits introduce a risk to the EMC compliance of the built system. In this presentation, we propose to analyze the susceptibility of low-cost sensors to RF pulses with a dedicated test set-up as depicted in Figure 1, which only exposes the set of sensors. From the induced malfunctions and measurement errors, it will be shown that unexpected behaviors can be encountered putting an embedded system at risk. As an additional outcome, it will demonstrated that part of failures induced by measurement errors and malfunctions can be mitigated by following some basic programming rules.

1. C. Kasmi, J. Lopes Esteves, “Electromagnetic Threats for Information Security: Ways to Chaos in Digital and Analogue Electronics,” *34c3 Chaos Communication Congress*, 28, December 2017, Leipzig, Germany.
2. C. Kasmi and J. Lopes Esteves, “IEMI Threats for Information Security: Remote Command Injection on Modern Smartphones,” in IEEE Transactions on Electromagnetic Compatibility, vol. 57, no. 6, pp. 1752-1755, Dec. 2015.
3. Arduino Project, online documentation, https://www.arduino.cc/, 2018.
4. S. Kovar, V. Mach, J. Valouch and M. Adámek, “Electromagnetic Compatibility of Arduino Development Platform in Near and Far-Field”, International Journal of Applied Engineering Research, vol. 12, 15, pp. 5047-5052, 2017.