Addressing Man-In-The-Middle threat in automotive wireless links

Luca Crocetti, Luca Baldanzi and Luca Fanucci
Department of Information Engineering, University of Pisa

Connected cars is one of the hot topic in automotive field, because it is a fundamental step along the roadmap to autonomous driving. Wireless communication links such as Wi-Fi 802.11p and 5G are expected to be integrated in next-generation vehicles, in order to extend the capabilities and the range of traditional in-vehicle networking. Thus a connected car will result to act as a node of many and heterogeneous networks and thus being exposed to the typical threats of the IT field. If not properly addressed, the communication threats and vulnerabilities could cause hazards and dangerous situations affecting the human safety.

In this demonstrator, we imagine a realistic near-future scenario in which a citizen calls back its own vehicle by a public car park, by means of a smartphone application. The demand is forwarded to a public service infrastructure node whose Wi-Fi range is able to reach the citizen's vehicle. A malicious and unauthorized entity can interfere in the Wi-Fi link of the communication bridge, altering the content of the messages. For instance the attacker could manipulate the GPS coordinates sent by the citizen and make move the car to an isolated place to steal it. A such kind of attack can be classified as a Man-In-The-Middle (MITM) attack.

Inspiring to WAVE (Wireless Access in Vehicle Environment), that regulates the automotive communication over Wi-Fi 802.11p links, we developed a countermeasure to address such issue. The proposed solution aims to protect the communication against intruders and unauthorized entities, by providing a set of suitable security services based on cryptographic algorithms and functions. Recently cryptographic algorithms require high computational power commonly not available in embedded microprocessors. Hence hardware accelerators play a fundamental role in such kind of applications, accordingly to the real-time context requirements of automotive field.

The demo uses two FPGA boards and a laptop to emulate the described scenario: the two FPGA boards act, respectively, as the car (called OBU, On Board Unit, from WAVE standard) and as an infrastructure unit (called RSU, Road Side Unit, from WAVE standard), while the laptop acts as the malicious entity performing the Man-In-The-Middle attack.

The demo consists in three phases:

1. OBU and RSU are not equipped with security countermeasures and thus the malicious entity performs the attack successfully;
2. OBU and RSU are equipped with security countermeasures implemented in software only, hence blocking the malicious entity attack, but with a high response time.
3. OBU and RSU are equipped with hardware accelerators to implement the required security countermeasures, realizing an embedded SoC (System-on-Chip), blocking the attack with a tiny response time.