Cooperative Intelligent Transport Systems Security

Pierre-Marie Bajan*, Aymen Boudguiga*, Nabil Bouzerna*, Pierpaolo Cincilla*, Arnaud Kaiser*, Flavien Quesnel*
*IRT SystemX, 8 avenue de la Vauve 91120–Palaiseau, *firstName.lastName@irt-systemx.fr*

By the end of the last century, transportation systems and especially vehicles replaced some of their mechanical functions by electronic controlled applications. Such applications include automatic window control, fuel injection supervision and car headlight automatic activation. By the end of 2010, cars relied on software containing millions lines of code executing on 70 to 100 microcontrollers, namely *Electronic Control Units* (ECUs) [1]. New generation of cars includes *intelligent* functions such as Adaptive Cruise Control (ACC). ACC adapts automatically vehicle's speed to maintain a safe distance with respect to in front vehicles. Nowadays, we are entering a new era with the appearance of self-driving cars such as Google car, new Hyundai Genesis or Volvo Drive me car. These cars are *autonomous* as they do not need human attention during cruise. In addition, they *cooperate* with other cars to communicate information about their actual speed or position and to relay data about traffic jams. These new vehicles ensure emergency braking, auto-parking, platooning and lane keeping. Together, they form a Cooperative Intelligent Transport Systems (C–ITS).

C–ITS rely on a special network architecture where roads and vehicles are equipped with Communication Units (CUs). CUs serve to exchange information about vehicles position and speed, traffic congestion and road's state. CUs installed on roads are called Road Side Units (RSUs), while those embedded in vehicles are referred to as On-Board Units (OBUs). Figure 1 depicts a simplified view of an autonomous vehicle architecture. It contains an OBU which serves as the Input/Output interface with extra-vehicle network (such as IEEE802.11p [2], 3G/4G, small range radio or GPS) and can offer in-car Wi-Fi. OBU provides also an Ethernet connection to Vehicle Control Unit (VCU), Infotainment Control Unit (ICU), Image Processing Unit (IPU) and cameras. VCU and IPU are gateways for Powertrain & Chassis Controller Area Network (CAN) which contains ECUs that provide vital functions such engine starting and brakes control. ICU is a gateway for Comfort CAN which ensures entertainment functions, lights activation and air conditioning control. Cameras provide video to IPU via Ethernet. IPU processes the video and informs VCU about the car position with respect to its neighborhood. Based on position information, VCU adapts the car speed in a self-driving context. Note that there is also an On Board Diagnostics plug (OBD). This plug provides diagnostics about ECU during a car technical control in garage. Autonomous vehicles communicate with the infrastructure via RSUs.

As vehicles communicate with external networks, they become the prey of hackers and malicious users. That is, new communications interfaces and embedded electronics created many attack surfaces. These interfaces not only suffer from classical IT attacks such as Denial of Services (DoS) but are also vulnerable to new C-ITS specific attacks. For example, an attacker can broadcast falsified IEEE802.11p frames with wrong identification to lure its neighboring cars and impersonate as an emergency vehicle. In addition, connected vehicles communicate permanently their position to the infrastructure. Position information can be used by a malicious attacker to track the driver. As a consequence, it becomes compulsory to provide reliable security mechanisms for personal data protection. In 2010, Koscher et al. [3] presented an outstanding analysis of CAN and ECUs security. In fact, they succeeded on hacking different ECUs and executing attacks such as CAN sniffing, spoofing and installing malware on safety related ECUs. They noticed that security recommendations have not been taken into consideration when implementing CAN standard. That is, no security mechanisms were applied during software updates or during the processing of bad command requests on some specific ECUs. In 2011, Checkoway et al. [4] extended Koscher et al. analysis to external attack surfaces on a modern vehicle. The results were again alarming. In fact, they compromised car radio using a tampered CD. They even controlled the car telematics via a call to car's integrated cellular phone. Then, they were able to unlock car doors, start engine and inhibit anti-theft measures.

I. IRT SystemX C-ITS Security Projects

IRT SystemX has started three projects that tackle different topics related to C-ITS security:

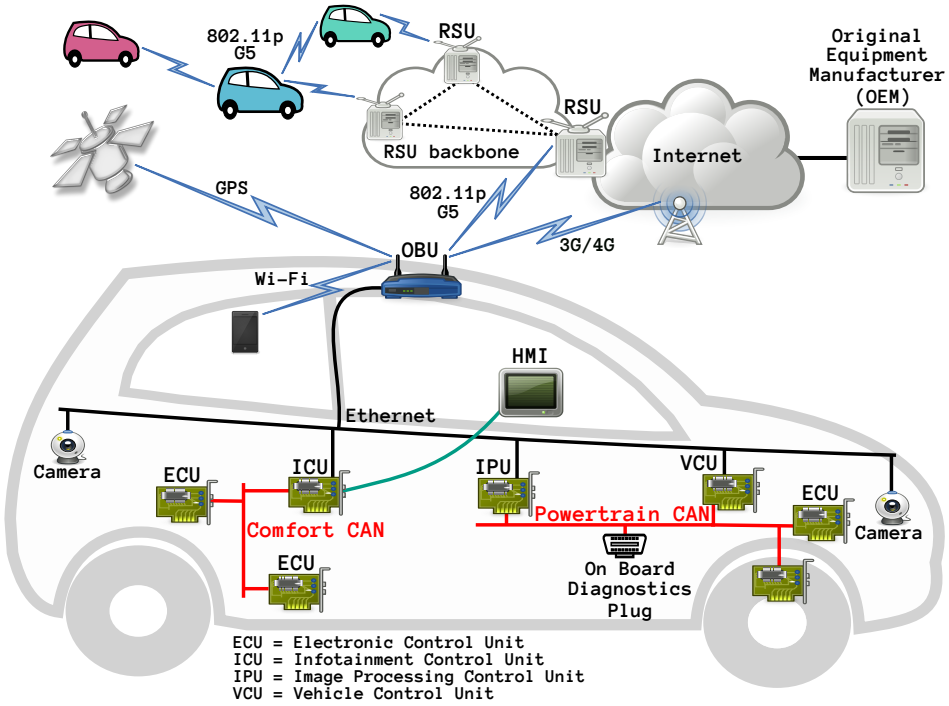

Fig. 1. An example of C-ITS architecture

- **Automotive Electronics and Software (ELA)**[1] project investigates different aspects related to *in-vehicle* embedded network and electronics. The R&D activities in this project concern four subjects: hypervison, image processing, RTOS portage to multi-core architecture and security.
- **ITS Security (ISE)** project studies security challenges related to Intelligent Transport Systems (ITS) communication and messages authentication. The project main concern is privacy preserving identity management system. ISE implements an identity management system based on a Public Key Infrastructure (PKI). The PKI makes use of short-term pseudonym certificates in order to preserve ITS privacy.
- **Environment for Interoperability and Integrity in Cybersecurity (EIC)** project develops several platforms for pentesting and evaluating the security of smart grids, IoT, C-ITS, cyber-physical and big data architectures.

II. IRT SystemX C-ITS Security Research Topics

In the aforementioned projects, our team is investigating the following topics:

- **C-ITS Risk Analysis**: As C-ITS security is mandatory for users safety, it becomes compulsory to make a risk analysis of C-ITS infrastructure. Risks refer to security breaches and weaknesses provided by system assets. Risk estimation methods require the definition of attack *likelihoods* (or *probabilities*) and *impacts* (or *severities*). The impact of an attack refers to its harm and possible damages. Meanwhile, an attack probability is computed as the inverse of its potential i.e., difficulty. In fact, the more difficult to realize the attack is, the less important is its likelihood.
  We have proposed *RACE*, a Risk Analysis method for Cooperative Engines which is more advantageous than current risk analysis methods such as EVITA and TVRA. RACE provides a clean way for attack description and risk evaluation.
- **CAN Security**: Attacks on CAN bus can be life threatening. You can imagine, for example, the fatal consequences of an attack on the Brakes Control Unit to activate the car brakes suddenly while running at high speed, or to release brakes while descending a mountain.
  We are currently working on the proposal of ECUs authentication and intrusion detection mechanisms that aim at thwarting this kind of attacks.

[1]ELA is the project acronym in French: Électronique et Logiciels pour L'Automobile

- **Hardware Security Components**: New automotive ECUs embed Hardware Security Modules (HSMs). HSMs aim at providing security services but without decreasing ECUs global performances and adding supplementary costs. In practice, a HSM will include a tamper resistant memory, a cryptographic acceleration module and optionally a security dedicated processor.
  We are currently studying the performances of Boundary Devices Nitrogen6X and SabreLite cryptographic acceleration and assurance module. In addition, we investigate the feasibility of some security concepts such as secure boot or trustzone usage.
- **PKI Scalability and Interoperability**: Entities involved in message exchanges must be authenticated without violating their privacy. Our Public Key Infrastructure (PKI) ensures privacy (non–traceability) by using short–term pseudonym certificates. In addition, our PKI tackles the scalability challenge in order to be able to distribute thousands of new digital identities each second and manage billions of those digital identities. Compliance with European Telecommunications Standards Institute (ETSI) and Committee for European Normalisation (CEN)/International Organization for Standardization (ISO) security standards is considered to ensure our PKI interoperability.
- **Pseudonym Change Policy**: For privacy reasons, a vehicle should be able to use pseudonym identities, and pseudonyms have to be changed frequently to prevent vehicles tracking. The use of pseudonyms introduces a trade-off between security and privacy: for security reasons (e.g., to prevent sybil attacks) we have to minimize the number of pseudonym that a vehicle can have at a time, while for privacy reasons (e.g., avoid vehicle tracking) we need vehicles to change pseudonym as often as possible.

Readers interested in C-ITS security can refer to our paper *"Cooperative–ITS Architecture and Security Challenges: a Survey"* to get more details about our research topics. Note that the aforementioned paper will be presented at Bordeaux ITS World Congress 2015.

REFERENCES

[1] C. Robert, "This car runs on code: http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code," 2009.

[2] "IEEE standard for information technology– local and metropolitan area networks– specific requirements– part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 6: Wireless access in vehicular environments," *IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007)*, pp. 1–51, July 2010.

[3] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *Proceedings of the 2010 IEEE Symposium on Security and Privacy*. Washington, DC, USA: IEEE Computer Society, 2010.

[4] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *Proceedings of the 20th USENIX Conference on Security*. Berkeley, CA, USA: USENIX Association, 2011.