# Security of embedded automotive networks: state of the art and a research proposal

Ivan Studnia, Vincent Nicomette, Eric Alata, Yves Deswarte, Mohamed Kaâniche, Youssef Laarouchi

# Security of embedded automotive networks: state of the art and a research proposal

Ivan Studnia[1], Vincent Nicomette[2,3], Eric Alata[2,3], Yves Deswarte[2,4]
Mohamed Kaâniche[2,4], Youssef Laarouchi[1]

[1] Renault S.A.S., 1 Avenue du Golf, F-78288 Guyancourt, France
[2] CNRS, LAAS, 7 Avenue du colonel Roche, F-31400 Toulouse, France
[3] Univ. Toulouse, INSA, LAAS, F-31400 Toulouse, France
[4] Univ. Toulouse, LAAS, F-31400 Toulouse, France
{ivan.studnia, youssef.laarouchi}@renault.com, {deswarte,nicomett,kaaniche,ealata}@laas.fr

**Abstract.** Embedded electronic components are nowadays a prominent part of a car's architecture. Moreover, modern cars are now able to communicate with other devices through many wired or wireless interfaces. As a consequence, the security of embedded systems in cars has become a main concern for the manufacturers. This paper aims at 1) presenting a short overview of the current attacks already known and experimented against vehicles as well as the current state of the art of the protection mechanisms; 2) presenting an overview of our contribution to these protection mechanisms: the design and implementation of a stateful intrusion detection system for CAN-based automotive networks.

## 1 Introduction

The embedding of electronic components into cars is now a well established fact: modern vehicles may comprise up to 70 ECUs (Electronic Control Units, the embedded computers monitoring and controlling the different subsystems of a car). In order to exchange data between them, some ECUs are connected to a bus where any message is broadcast to all the connected nodes. Communication between nodes can be done using several different protocols according to the needs (safety, performance, cost, etc.). Currently, CAN (Controller Area Network) is the most used protocol in automotive networks, existing in several standards according to one's needs, with data rates up to 1Mb/s. Other protocols, designed to fit specific uses may also be used, such as LIN, MOST or FlexRay. An automobile embeds several of such networks, interconnected together through gateway ECUs.

Moreover, modern vehicles are now able to exchange data with external sources, via USB, Bluetooth, Wifi or even 3G/4G networks. The emergence of V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure) communications will also amplify this trend. These technologies will for example allow a car braking abruptly to alert the following vehicles so that their drivers could react more quickly, or even to automatically trigger an emergency brake. Therefore, car's internal networks are now complemented by communication means with external devices. Figure 1 shows a summary of those different possible external connections.

However, all these new features also potentially expose the internal network to the outside world. As we will see in the next section, the aforementioned internal protocols are very vulnerable to attacks relying on a malicious use of the network. As long as such attacks required a prolonged physical access to the car's wiring, these vulnerabilities were a minor concern for the manufacturers.

However, with the addition of ECUs able to access data from external sources, a car can no longer be considered as a closed network and becomes a potential target for remote computer attacks.

This paper is organised as follows. In Section 2, we give an overview of documented attacks against an automotive network. Section 3 is devoted to a short summary of the works aiming at implementing security mechanisms in the connected car. A more comprehensive survey on the works presented in Sections 2 and 3 can be found in [19]. Then, Section 4 presents our planned research contribution to this topic. Finally, Section 5 concludes this paper.

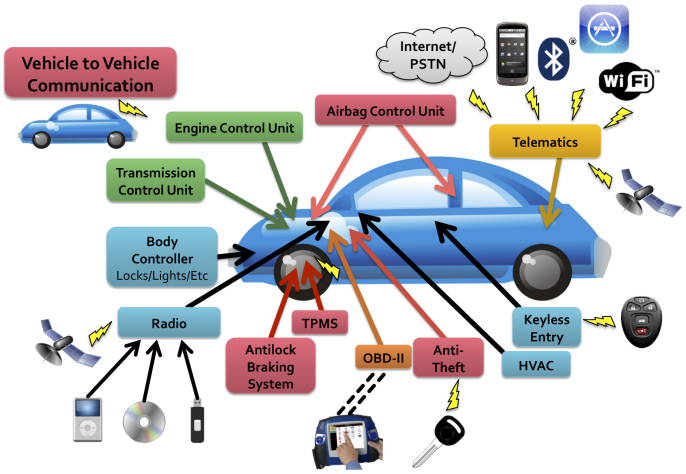


**Fig. 1.** Possible connections of a modern car (from [4])

## 2 Examples of attacks

An attacker can have many reasons to launch an attack against a car's network: car theft, electronic tuning (unauthorized modifications in the code of ECUs in order to, for instance, gain more engine power), sabotage (deterioration of the vehicle capacities through the deactivation of ECUs), privacy breach (retrieval of personal information stored in some ECUs), or just for the intellectual challenge. For that purpose, an attacker may carry out local or remote attacks. The following subsections give a brief overview of these attacks.

### 2.1 Local attacks

Analyses on the CAN bus [11] showed that this protocol, cannot guarantee the usual security properties. For instance, by design, every message sent on the CAN is physically broadcast to every node, which obviously cannot guarantee the confidentiality property. A basic CRC is used to check if a message has been modified by a transmission error, which is insufficient to guarantee the integrity property, as an attacker can forge a CRC corresponding to any message he may send. Arbitration rules in CAN make it easy for an attacker to cause a denial of service on the bus, thus violating the availability property. Moreover, CAN frames do not include a field to authenticate the sender nor a way for an ECU to sign its messages. Hence, the authenticity and non-repudiation properties cannot be guaranteed.

Some attacks were performed by directly sending packets on an embedded bus, either by plugging an additional device on the targeted bus or by using the OBD port (On Board Diagnostics, which refers to a vehicle's ability to identify and report existing problems in its infrastructure). This port is now mandatory in the United States and the European Union. OBD dongles used to connect a computer to a car's OBD port can be legally bought by anyone. The OBD port can therefore be turned into a plug-in entry point into the CAN bus for an attacker, who can use it to eavesdrop and send frames on the bus. For example, after having identified the meaning and effects of some frames [11], an attacker could send control instructions to other ECUs on the bus [10] or reflash them over the network [13], thus leaving the vehicle in a compromised state after the attacker's intervention. Moreover, Koscher et al. [13] were able to successfully target an ECU that was not on the same bus segment as their entry point by previously targeting and reprogramming the ECUs acting as gateways between the buses. This means that an ECU located on a low-speed, non critical CAN bus has been able to send control sequences on a safety critical, high-speed CAN bus. Therefore, if an attacker controls one single node of a car's network, he may be able to take over any other ECU of the vehicle.

### 2.2 Remote attacks

While the previous examples are quite impressive, one could object that they imply a previous security breach that gave the attacker a physical access to the car's network. Moreover, in such cases, there may be quicker and easier non electronic ways for an attacker to reach its goals (e.g. cutting the brake wires). However, by leveraging the wireless communication capacities of modern cars, a physical access to the targeted car may no longer be required by the attacker. This section shows examples of such attacks.

In [4] Checkoway et al. were able to remotely reproduce the attacks described in [13] by exploiting vulnerabilities in a car's communication interfaces (through wireless communications or via a compromised third party device plugged into the car). They were able to take over the vehicle's network via all kinds of remote accesses. For example, they used indirect physical channels such as a CD causing the CD player to send frames on the bus while reading it, short range wireless access by exploiting a vulnerability in the ECU handling Bluetooth communications or even performed long range wireless attacks by hacking the telematics unit through GSM communications. Other examples of documented remote attacks include attacks against the Tire Pressure Monitoring System [17] or relay attacks against a Passive Keyless Entry and Start (PKES) system [5] where a car has been unlocked and its engine started while the keys were actually 50 meters away from the car.

## 3 Protection mechanisms

As seen previously, an attacker may need to exploit only one vulnerability related to the management of the communications with an external device to be able to entirely compromise a vehicle. Therefore, a first step in order to protect the embedded system is to secure those external communication channels. The security of the automotive networks have become a main concern for the manufacturers, as evidenced by a large number of projects between industrial and academic partners. For example, projects such as SEVECOM [12], PRESERVE [1] or EVITA [9] aim at designing secure communication architectures for internal or intervehicular communications while the goal of OVERSEE [6] is to devise a unified, open and secured multimedia interface managing all the communication protocols. The other step in order to protect the embedded system is to secure

the internal communications channels, i.e., the communications on the CAN bus. These protection mechanisms can be classified into three categories (cryptography, software integrity and anomaly detection) that are discussed in the following sub-sections.

### 3.1 Cryptography

The use of cryptographic solutions can enable ECU authentication, integrity checks and encryption of the emitted frames, preventing their reading by nodes not possessing the appropriate keys. Such features are for example described in [7] or [8]. However, the computation required to perform strong enough encryption or decryption can be time and resource consuming. This problem can be addressed by using a hardware module dedicated to cryptographic operations, such as the Hardware Security Module [20] (HSM) from the EVITA project, to free the ECUs computational capacities.

### 3.2 Software integrity

This category refers to other works that aim at ensuring ECU software integrity, in a way similar to the secure boot mechanisms implemented in traditional computers. This can be done through security modules like EVITA's HSM or a Trusted Platform Module [2]. Integrity of the critical software can also be done via virtualization in order to isolate critical software from non trusted modules such as external communication interfaces by putting them into distinct virtual machines. This is one of the main goals of OVERSEE, based on the XtratuM hypervisor.

### 3.3 Anomaly detection

Other techniques that have been investigated consist in implementing anomaly detection on the automotive network by monitoring the data transmitted on the bus and asserting their legitimacy. These works include for example : i) a module preventing a node from sending its messages at a too fast rate [3] in order to avoid bus flooding, ii) a system where each node tries to detect if other nodes are impersonating it by checking the frames headers [14] or iii) a tainting tool used to mark and track the data as they are sent and processed by the ECUs [18]. Moreover, the implementation of Intrusion Detection (resp. Prevention) Systems (IDS, resp. IPS) is also considered, either from a signature-based [16] or an anomaly-based [15] approach. If a well defined signature-based IDS raises very few false positives, it requires regular updates to maintain its signature base up to date. On the other hand, anomaly-based intrusion detection may be able to detect previously unknown attack patterns, but the high complexity of an automotive network makes it difficult to design a model that is precise enough to prevent false negatives while still allowing exceptional but perfectly legitimate situations.

## 4 Designing a stateful IDS

As highlighted by the previous sections, the design and implementation of security mechanisms in the automotive embedded network are currently a very important issue for automotive manufacturers. Our work on this topic currently focuses on the implementation of a stateful intrusion detection system over several CAN buses. To the best of our knowledge, current implementations of IDS-based solutions in an automotive network are still at a preliminary stage. While some of

the proposed solutions are investigating correlation between different frames [16], to the best of our knowledge, they do not seem to take into account the operational context in which those frames are emitted. In other words, our goal is to check if a message being sent on a bus is legitimate in accordance with the current operational state of the car (simple examples could be: parked, normal driving, emergency procedures during a crash, etc.).

The proposed IDS will be implemented on a test platform composed of distinct ECUs with different levels of criticality (for example, the Body Control Module is not as safety critical as the ABS) plugged on the same CAN bus (CAN-V, for Vehicle), a multimedia unit (MM) plugged on a second bus (CAN-M, for Multimedia) as well as a Telematics Control Unit (TCU) and a gateway (GW) ECU connected to both buses. Interaction with this platform can be done by connecting a computer to an OBD port linked to the CAN-V bus. Figure 2 gives an overview of such a test platform with 4 distinct ECUs on the CAN-V and 2 levels of criticality. To be as efficient as possible, our IDS should be able to read from both buses and should therefore be located in a gateway ECU.

To do so, we plan to pursue the following steps:

- Model each ECU with a state diagram in which the transitions between states can be characterized through a message (or a sequence of messages) emitted on the bus.
- Characterize attacks by 1) a message (or sequence) read on the bus and 2) the current state of the ECUs.
- Implement this approach on our test platform in order to be able to raise an alert whenever an attack is detected, or even to block the malicious messages if possible.

A challenging issue that will be investigated consists in taking into account in the design of the proposed IDS the criticality of the different ECUs that are targeted by potential attacks.

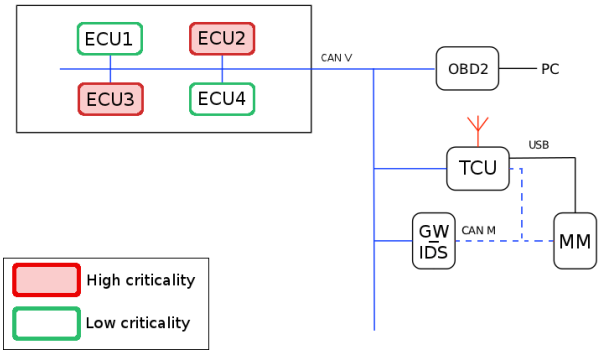


**Fig. 2.** Overview of our test platform

## 5 Conclusion

In this paper, we have presented 1) a short overview of current attacks against computers embedded in cars as well as the corresponding protection mechanisms and 2) an overview of a novel stateful intrusion detection system for CAN bus. We are currently developing a test plateform, composed of several ECUs with different levels of criticality, in order to assess this IDS, by means of real experimentations.

## References


1. About PRESERVE. http://www.preserve-project.eu/about (2011), [Online; accessed February-2013]
2. TPM main specification. http://www.trustedcomputinggroup.org/resources/tpm_main_specification (2011), [Online; accessed February-2013]
3. Broster, I., Burns, A.: An analysable bus-guardian for event-triggered communication. In: Real-Time Systems Symposium. pp. 410–419. IEEE (2003)
4. Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., Kohno, T., et al.: Comprehensive experimental analyses of automotive attack surfaces. In: Proc. 20th USENIX Security. San Francisco, CA (2011)
5. Francillon, A., Danev, B., Capkun, S.: Relay attacks on passive keyless entry and start systems in modern cars. IACR ePrint Report 2010/332 (2010)
6. Groll, A., Holle, J., Ruland, C., Wolf, M., Wollinger, T., Zweers, F.: Oversee a secure and open communication and runtime platform for innovative automotive applications. In: 7th Embedded Security in Cars Conf. (ESCAR). Düsseldorf, Germany (2009)
7. Groza, B., Murvay, S., Van Herrewege, A., Verbauwhede, I.: Libra-can: a lightweight broadcast authentication protocol for controller area networks. In: Proc. 11th Int. Conf. Cryptology and Network Security, CANS. Darmstadt, Germany (2012)
8. Hartkopp, O., Reuber, C., Schilling, R.: Macan - message authenticated can. In: 10th Int. Conf. on Embedded Security in Cars (ESCAR 2012) (2012)
9. Henniger, O., Ruddle, A., Seudié, H., Weyl, B., Wolf, M., Wollinger, T.: Securing vehicular on-board it systems: The evita project. In: 25th VDI/VW Automotive Security Conf. Ingolstadt, Germany (2009)
10. Hoppe, T., Dittman, J.: Sniffing/replay attacks on can buses: A simulated attack on the electric window lift classified using an adapted cert taxonomy. In: Proc. 2nd Workshop on Embedded Systems Security (WESS). Salzburg, Austria (2007)
11. Hoppe, T., Kiltz, S., Dittmann, J.: Automotive it-security as a challenge: Basic attacks from the black box perspective on the example of privacy threats. Computer Safety, Reliability, and Security pp. 145–158 (2009)
12. Kargl, F., Papadimitratos, P., Buttyan, L., Muter, M., Schoch, E., Wiedersheim, B., Thong, T.V., Calandriello, G., Held, A., Kung, A., et al.: Secure vehicular communication systems: implementation, performance, and research challenges. Communications Magazine 46(11), 110–118 (2008)
13. Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H.: Experimental security analysis of a modern automobile. In: 2010 IEEE Symp. Security and Privacy. pp. 447–462. Oakland, CA (2010)
14. Matsumoto, T., Hata, M., Tanabe, M., Yoshioka, K., Oishi, K.: A method of preventing unauthorized data transmission in controller area network. In: Vehicular Technology Conf. (VTC Spring). pp. 1–5. IEEE, Yokohama, Japan (2012)
15. Muter, M., Asaj, N.: Entropy-based anomaly detection for in-vehicle networks. In: Intelligent Vehicles Symposium (IV). pp. 1110–1115. IEEE, Baden Baden, Germany (2011)
16. Muter, M., Groll, A., Freiling, F.C.: A structured approach to anomaly detection for in-vehicle networks. In: 6th Int. Conf. Information Assurance and Security (IAS). pp. 92–98. IEEE, Atlanta, GA (2010)
17. Rouf, I., Miller, R., Mustafa, H., Taylor, T., Oh, S., Xu, W., Gruteser, M., Trappe, W., Seskar, I.: Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In: Proc. USENIX Security Symposium. pp. 323–338. Washington, DC (2010)
18. Schweppe, H., Roudier, Y.: Security and privacy for in-vehicle networks. In: Vehicular Communications, Sensing, and Computing (VCSC). pp. 12–17. IEEE, Seoul, Korea (2012)
19. Studnia, I., Nicomette, V., Alata, E., Dewarte, Y., Kaâniche, M., Laarouchi, Y.: Survey on security threats and protection mechanisms in embedded automotive networks. In: 2nd Workshop on Open Resilient Human-aware Cyber-Physical Systems. Budapest, Hungary (2013)
20. Wolf, M., Gendrullis, T.: Design, implementation, and evaluation of a vehicular hardware security module. Information Security and Cryptology-ICISC 2011 pp. 302–318 (2012)