Vehicular Communications ••• (••••) •••–•••

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom

Security and privacy in vehicular communications: Challenges and opportunities

Cesar Bernardini [a], Muhammad Rizwan Asghar [b], Bruno Crispo [c,d]

[a] Department of Computer Science, Aalto University, Finland
[b] Department of Computer Science, The University of Auckland, New Zealand
[c] Department of Computer Science, KU Leuven, Belgium
[d] Department of Information Engineering and Computer Science, University of Trento, Italy

ARTICLE INFO

Article history:
Received 12 June 2017
Received in revised form 12 September 2017
Accepted 30 October 2017
Available online xxxx

Keywords:
Modern cars
Infotainment
EV
AUTOSAR
On-Board Diagnostic
Intra-vehicle communication
In-vehicle communication
Inter-vehicle communication
Privacy
Security

ABSTRACT

Modern cars have become quite complex and heavily connected. Today, diverse services offer infotainment services, electric power-assisted steering, assisted driving, automated toll payment and traffic-sharing information. Thanks to recent technologies, which made it possible to enable these services. Unfortunately, these technologies also enlarge the attack surface. This survey covers the main security and privacy issues and reviews recent research on these issues. It summarizes requirements of modern cars and classifies threats and solutions based on the underlying technologies. To the best of our knowledge, this is the first survey offering such an overall view.

1. Introduction

The increasing use of electronic components and technology in cars has radically changed the mean of transportation in the last couple of decades. Modern cars became very complex and sophisticated systems after having been equipped with several on-board microcontrollers. The basic unit of computation is the Electronic Control Unit (ECU). Most ECUs are organized and interconnected to monitor and control different subsystems such as the interaction between the braking system, airbags and the Antilock Braking System (ABS). However, the interconnection is not limited to internal car's ECUs; ECUs interconnect to other vehicles' ECUs and microcontrollers available in the roads to provide active safety, infotainment services, electric power-assisted steering, airbags, antilock braking system, assisted driving, cruise controls, automated toll payment and to simplify interaction with the environment.

To provide such a wide range of services, modern cars enable several means of communication. First, different ECUs and subsystems are interconnected to form *intra-vehicle networks*. These subsystems may use different networking technologies depending on the diverse constraints. For instance, a mirror adjusting system has a lower priority compared to the system controlling the braking system. Second, modern cars provide different *gateways* to interact with the external entities. Gateways represent the entry and exit points of the intra-vehicle network and provide a wide range of services. These services include support for self-diagnostics, toll and petrol payment, remote access to various features of the car, the Bluetooth hands-free and the USB media player are few important ones among many others. A communication port, On-Board Diagnostics 2 (OBD2), exchanges test information with intra-vehicle ECUs and reports their status. The petrol and electrical stations could exchange payment information with the car [1]. Third, cars enhance car safety by means of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication that we will call *inter-vehicle* communication.

With such a broader range of communication, it is essential to understand the security and privacy aspects of such a complex Cyber-Physical System (CPS). Indeed, Miller [2] has already demonstrated examples of attacks in modern cars. Petit and Shladover [3] reviewed potential attacks that autonomous vehicles may suffer

E-mail addresses: mesarpe@gmail.com (C. Bernardini), r.asghar@auckland.ac.nz (M.R. Asghar), bruno.crispo@cs.kuleuven.be (B. Crispo).

https://doi.org/10.1016/j.vehcom.2017.10.002
2214-2096/

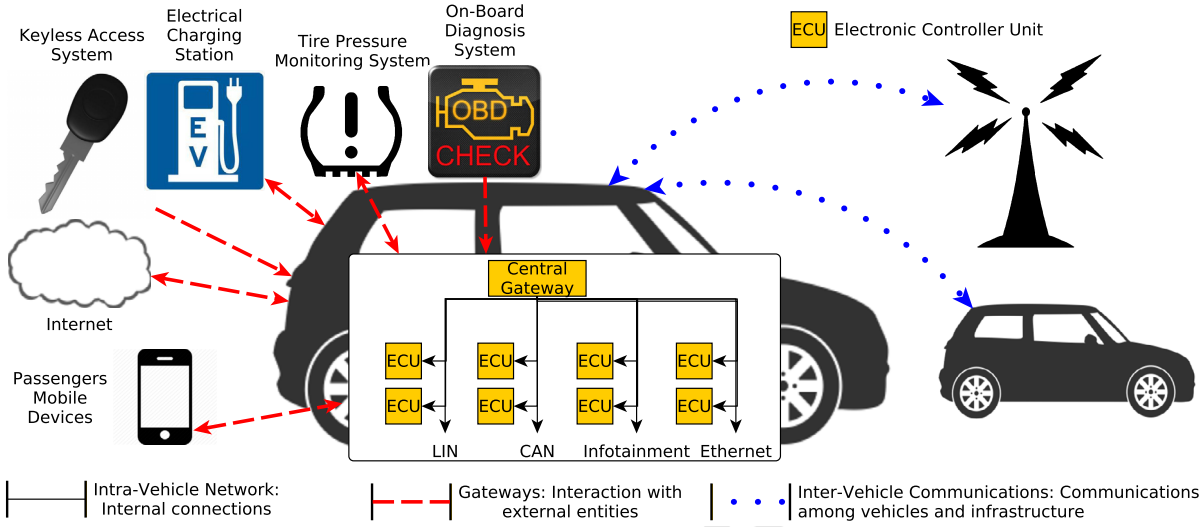

Fig. 1. Overview of networking in modern cars, illustrating our proposed classification: interconnection of components in a modern car; inter-vehicle communications; and communication with external entities through gateways.

from. Kleberger et al. [4] revisited security aspects of the intra-vehicle network. Nevertheless, existing surveys neither comprehend essential aspects of modern cars nor address potential attacks and proposed solutions in a holistic fashion. This survey reviews the recent technical research on security and privacy in modern cars. It revisits threats and solutions based on the interconnection technologies.

Fig. 1 illustrates the classification presented in this survey. A modern car is represented with its intra-vehicle network. The network is composed of multiple ECUs that are interconnected using different communication buses (i.e., LIN, CAN, infotainment – MOST and FlexRay), represented using solid black arrows in Fig. 1. The interaction of the car through gateways is represented using dashed red arrows. A modern car may interact with the Electric Charging Stations, the Keyless Access System, the Tire Pressure Monitoring System and the On-Board Diagnosis system. Further, modern cars can also directly connect to the Internet, cloud services and smartphones. The V2V and V2I communications are represented using dotted blue arrows.

The rest of the survey is organized as follows. First, we list security, safety, standardization and architectural requirements for modern cars in Section 2. Section 3 describes security and privacy issues that emerge in intra-vehicle networks. In Sections 4 and 5, we explain challenges caused by the use of gateways and inter-vehicle communication. Section 6 concludes this survey and provides research directions for future work.

2. Requirements for modern cars

From the security and privacy perspective, modern cars must respect a set of requirements. In this section, we list this set of requirements that we classify into three categories: security requirements, safety requirements, and standardization and architectural requirements.

2.1. Security requirements

Security requirements are constraints that emerge from security concerns. Some of these requirements are based on use cases proposed in literature [5,6]. In the following, we list core security requirements:

- *Authentication.* In vehicular networks, various entities (e.g., drivers, cars and different service providers) interact with each other. If we consider interactions within the car, software and hardware components from different Original Equipment Manufacturers (OEMs) communicate with each other. This openness provides an opportunity to adversaries who may disrupt normal behavior of the car or trigger sophisticated attacks. To overcome this problem, communicating entities must authenticate each other to make sure that they are the ones they claim to be. Further, different car components must establish authenticity of incoming data and their origins.
- *Intellectual Property Protection.* Modern cars must be protected against cloning and reverse engineering. Their software and configuration parameters must remain protected. Moreover, they must be protected even during software updates and upgrades.
- *Confidentiality.* In vehicular networks, confidentiality refers to the protection of information exchanged between or stored by different components and entities. Loss of such protection could lead to leaking sensitive information.
- *Integrity.* In the context of vehicular networks, integrity refers to the property that if the data exchanged between or stored by components and entities is manipulated by an adversary, it must be detected. It must also be possible to detect injection of messages by an adversary. Moreover, it must be possible to detect any modification while the system boots or a piece of software is running. This equally applies to software upgrades and updates.
- *Access Control.* Modern cars must grant selective access to its components. A car must ensure that only authorized components are able to gain access. These components must only be repaired by authorized maintenance partners. Moreover, each component (or subcomponent) must be able to access memory allocated to it. In other words, secure software code must be written to avoid vulnerabilities, such as preventing buffer overflow or string format vulnerability attacks. Besides, entities must get access if they are authorized. The principle of least privilege should be applied while providing access to components or entities.
- *Message Freshness.* Modern cars must ensure that network messages are not being replayed or delayed. Assuring freshness avoids replay attacks, which otherwise could be mounted by adversaries.
- *Privacy.* Modern cars must protect sensitive information that may compromise privacy of users (say drivers or passengers). Tracking the geographical position of the car is a typical ex-