Computer Communications 132 (2018) 17–41

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Review

Security and privacy for innovative automotive applications: A survey

Van Huynh Le[*], Jerry den Hartog, Nicola Zannone

Eindhoven University of Technology, Postbus 513, 5600 MB Eindhoven, The Netherlands

ARTICLE INFO

Keywords:
Automotive
Application
Platform
Security
Privacy
Literature study

ABSTRACT

Software applications play an important role in vehicle innovation, aiming at improved safety, efficiency, and comfort, and creating the new areas of cooperative intelligent transport systems and autonomous vehicles. To accommodate modern applications, vehicles have become increasingly computerized and connected. Despite the benefits that the adoption of these applications bring to the automotive sector and consumers, automotive applications along with the enabling technological innovation open great challenges to security and privacy. Addressing these challenges is a prerequisite for the acceptance and deployment of innovative applications at a large scale. This survey investigates the main security and privacy challenges for the design of automotive applications and platforms. Based on the main security and privacy requirements and threats identified, we review existing protection mechanisms proposed within the automotive domain. We then identify the main gaps in existing research and draw a roadmap for future research.

Contents

1. Introduction 18
2. System overview 19
  2.1. In-vehicle architecture 19
  2.2. External interfaces 21
    2.2.1. Physical access 21
    2.2.2. Short-range wireless access 21
    2.2.3. Long-range wireless access 21
3. Automotive applications 22
  3.1. Application classification 22
  3.2. Review of existing and near future applications 23
4. Application platforms 24
  4.1. Platform classification 24
  4.2. Review of existing application platforms 25
    4.2.1. In-vehicle platforms 25
    4.2.2. Mobile platforms 25
    4.2.3. Internet-based platforms 26
5. Threat analysis 26
  5.1. Terminology 26
  5.2. Security and privacy goals 26
    5.2.1. Security goals 26
    5.2.2. Privacy goals 27
  5.3. Attackers 27
    5.3.1. Attacker capabilities 27
    5.3.2. Impacts caused by attackers 28
  5.4. Vulnerabilities 28
    5.4.1. In-vehicle systems 28
    5.4.2. Vehicular Ad Hoc Networks (VANETs) 30
  5.5. Attacks 30
    5.5.1. In-vehicle systems 30

[*] Corresponding author.
E-mail address: v.h.le.1@tue.nl (V.H. Le).

https://doi.org/10.1016/j.comcom.2018.09.010
Received 7 November 2017; Received in revised form 30 August 2018; Accepted 24 September 2018
Available online xxxx

5.5.2. VANETs 30
6. Security and privacy mechanisms........ 31
6.1. In-vehicle systems........ 32
6.2. VANETs 35
6.2.1. Public key infrastructures (PKIs) 35
6.2.2. Alternatives to PKI........ 35
6.2.3. Detection of and response to misbehaving vehicles........ 36
7. Gap analysis and roadmap for future work........ 36
8. Conclusion 37
Acknowledgments 38
References........ 38

1. Introduction

Modern vehicles have become complex systems containing a large number of interconnected embedded computers, sensors and actuators as well as interfaces to communicate with the outside world. These components are often coupled with an increasing use of software applications that aim to improve safety, efficiency and comfort. This trend is still ongoing; future vehicles will become even more complex and connected to accommodate innovative applications and enable new ways of using vehicles. Despite their benefits, these innovations open new security and privacy challenges. This survey investigates the current state of the art in security and privacy for automotive applications and platforms.

Existing automotive applications cover three main categories: *control systems* that manage physical functions of the vehicle including engine, chassis, body, and passive safety functions; *telematics systems* that provide information and support entertainment as well as financial transactions; and complex *advanced driver assistance systems (ADAS)* that aim to turn vehicles into intelligent systems, improve safety, and enhance driving experience. The complexity that accompanies all these different applications, as well as the need to quickly adopt new applications, is challenging the traditional approach of rigidly building applications into the vehicles during assembly. This approach of adding embedded computers for each new application has reached its cost and complexity limits [1]. Therefore, a current trend is the adoption of application platforms to increase flexibility while reducing cost and complexity.

Application platforms offer easier development and deployment of new services. Flexible software distribution allows applications to be selected according to customers' requirements [2]. By providing common application programming interfaces (APIs) that abstract the underlying hardware, application platforms can also increase software reuse [3] compared to low-level and hardware-specific approaches that are currently largely adopted by the automotive industry. A platform can also reduce hardware complexity and cost by hosting multiple applications on the same hardware [1].

Until recently, most applications and platforms were implemented inside vehicles for control systems with little communication with the outside world. Yet, a vehicle is no longer isolated within intelligent transport systems; information sharing is essential for many advanced applications. Vehicles need to communicate with other entities, such as personal devices, other vehicles, road-side infrastructure, and the Internet. Modern vehicles thus involve three main areas as illustrated in Fig. 1. *In-vehicle systems* were initially designed for applications in control systems but have been extended to support ADAS and telematics. *VANETs* are ad-hoc communication networks among vehicles and between vehicles and road side infrastructures enabling collaborative ADAS as well as telematics applications. Finally, *Internet-based applications* have telematics as main purpose.

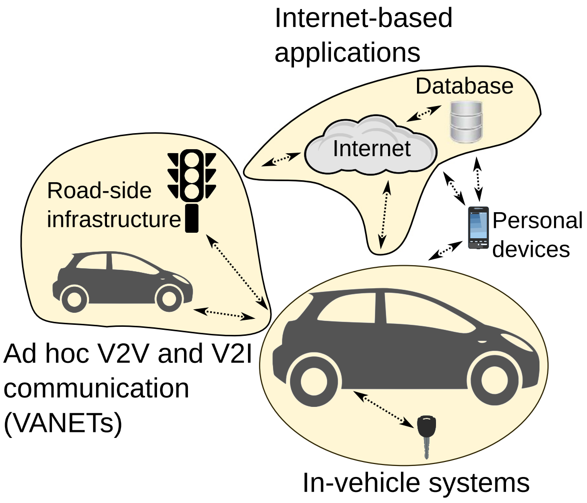

Fig. 1. The anatomy of a connected vehicle.

All these trends of more complex systems, flexible application platforms and increased connectivity also come with significant security and privacy challenges that must be addressed before smart vehicles and innovative applications can be widely adopted and large scale intelligent transport systems can be successfully deployed. In particular, the increasing number of vehicle assets (e.g., more vehicular communication, personal information stored in vehicles, and audio-visual media) along with the ease to interact with modern vehicles has attracted considerable attention to the study of their security, and several attacks have already been demonstrated [4–13]. The potential impact of attacks can range from slight inconvenience to serious safety, financial and/or privacy consequences. For instance, Miller and Valasek [6] demonstrated an attack in which they could remotely track a vehicle and perform various actions, such as changing radio volume, killing the vehicle's engine, and disabling the brakes.

Automotive security and privacy is a wide topic encompassing multiple subjects, such as automotive system architectures, the plethora of applications and platforms with different requirements, attackers with various motivations and levels of skills, and the diversity of threats and their countermeasures. To identify the most important issues and identify research directions that will enable the acceptance and adoption of innovation in the automotive sector, a broad overview of the field is needed. This survey aims to provide such an overview by presenting a literature review on automotive security and privacy. In particular:

- We review automotive system architectures, applications, and application platforms to provide the context for security and privacy analysis. Applications and platforms from all major areas (in-vehicle systems, VANETs, and Internet-based applications) are discussed, as security and privacy issues can arise not only from individual areas but also from their interconnection.