Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Towards a distributed secure in-vehicle communication architecture for modern vehicles

Constantinos Patsakis [a,*], *Kleanthis Dellios* [b], *Mélanie Bouroche* [a]

[a] *Distributed Systems Group, School of Computer Science & Statistics, Trinity College, College Green, Dublin 2, Ireland*
[b] *Department of Informatics, University of Piraeus, Greece*

ARTICLE INFO

Article history:
Received 11 March 2013
Received in revised form
29 October 2013
Accepted 10 November 2013

Keywords:
Immobilizer
In-vehicle communication
Security
Authentication
ECU
ECM

ABSTRACT

Modern automotive vehicles are becoming a collection of interconnected embedded subsystems, where the mechanical parts are controlled by electronic ones and the vehicle is transformed into a mobile information system. However, the industry standards for in-vehicle communication are not following long-established computer security policies. This trend not only makes vehicles prone to thefts and automated attacks, but also endangers passengers safety.

This paper analyzes current practices and standards of the automotive industry, highlighting several vulnerabilities that stress the need to change the way that in-vehicle communication is handled. To this end, we present a novel vehicle security architecture that supports two new features; users with different access rights and roles, and mutual authentication of ECUs. These features can enable a more distributed security architecture and prevent many attacks, or at least trigger adequate alarms to detect and mitigate them, or allow backtracking.

1. Introduction

The evolution of Applied Sciences made the automotive industry one of the largest economic sectors, and the latest modern vehicles come equipped with new levels of functionality, safety, performance and comfort (Naver and Simonot-Lion, 2009; Fuhs, 2009). A modern vehicle can be viewed as an operating platform via a collaborative environment (Bonnick, 2001) due to the simultaneously running tasks and functions of many embedded subsystems over CAN, LIN, Most and other protocols, interconnected together into a networked system (Naver and Simonot-Lion, 2009).

The immobilizer system (Heisler, 2002) is an embedded system that was added to modern vehicle components to protect the vehicle against thefts. Its adoption immediately caused a significant decrease in such acts (Larmtjanst, 2007; Wire, 2010). Immobilizers are still being used nowadays, preventing an engine's ignition unless the correct key is placed. After a drastic decrease in the amount of stolen vehicles, recently their number is increasing, as reported by several sources, such as the FBI in its Uniform Crime Report[1] or Australia's National Motor Vehicle Theft Reduction Council (NMVTRC).[2] This increase can be in many cases justified by the disclosure of vulnerabilities in immobilizer or in vehicles peripherals. While these trends might be temporary, the fact that new vehicles are still being stolen indicates that current immobilizer are not adequate. Therefore, we argue towards the development of a new more secure in-vehicle architecture, that provides other means, beyond the immobilizer, to prevent vehicle attacks.

* *Corresponding author*. Tel.: +353 18963789.
E-mail addresses: patsakik@scss.tcd.ie (C. Patsakis), kdellios@unipi.gr (K. Dellios), melanie.bouroche@scss.tcd.ie (M. Bouroche).

[1] http://www.fbi.gov/about-us/cjis/ucr/ucr.
[2] http://www.carsafe.com.au/images/stories/pdfs/Annual-Reports/NMVTRCAnnualReport2012.pdf.

0167-4048/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2013.11.003

The recent trend towards "computerizing" vehicles, by adding new services with gadgets/devices connected to the vehicle itself, is extending the attack layer (Checkoway et al., 2 011; Bailey, 2010). Major organizations and security firms are trying to alert the public to the possibility of vehicles becoming the next hacking platforms. These concerns have also been pointed out through several public awareness reports, like McAfee (2011) and FBO (2011). In the first, we have a "Request for Information", issued by the US Department of Transportation, while in the latter McAfee issued an information bulletin. In both cases, the risks for Homeland Security are being highlighted, as large-scale cyber-attacks of this form may cripple transportation infrastruc tures, leading to unmeasurable damages or even civilian casualties. Several literature surveys have already highlighted the risks that vehicles have been exposed to Kleberger et al. (2011). Many researchers have already shown that a wide range of attacks is feasible with reasonable resources, as will be discussed in following sections. Independently, when asked to discuss the possibility of such attacks, officials such as the chief technology officer of the US Cyber Consequences Unit,[3] admit their severity.

1.1. Problem setting

The industrial approach towards in-vehicle communication differs from current computer science approaches in the field of network and communications. Even though plenty of methods for securing communication between two entities have been known in computer science for decades, they do not seem to be adopted by the automotive industry, or have been adopted only with lengthy delays. Quite peculiarly, this problematic approach only involves in-vehicle communications and not vehicular networks. The only way to justify it is that it is driven by the budget cost of replacing and redesigning current and old vehicles components, nevertheless the security implications should always be considered. If the vehicle, considered as a node of a network, cannot be considered secure, then the network that it belongs to cannot be considered secure either. So, before widely adopting vehicular networks, cloud services for vehicles and other sophisticated approaches to the networked vehicle, it is essential to rethink the security of each node itself.

Summarizing our literature survey, the problems from which most vulnerabilities are derived, are the following:

- Lack of cryptographic algorithms or problematic implemen tations.
- Lack of different roles/users in vehicle. All users and devices have the same privileges, therefore, all users can plug in any device, which will have the same rights as any other device.
- "Plug 'n' play" devices. Devices can be easily plugged into the vehicle and automatically become available.

1.2. Contribution of the article

This work is an extension of Patsakis and Dellios (2012) and can be considered as a step towards redesigning the conventional security system of vehicles, without compromising the performance or safety levels that have already been achieved by automotive vendors. The focus of the article is mainly on cars, nevertheless, as it will become apparent, the proposed scheme is suitable for all automotive vehicles. Unfortunately, as H. Teso showed recently at the "Hack In The Box" conference, the same concepts and architectures can be exploited in airplanes as well (Teso, 2013).

Addressing the sources of the highlighted vulnerability issues, we propose a more networked vehicle (Heisler, 2002), where the security of the vehicle is distributed among its components, all participating with a vital role. In this context, the proposal is twofold. On one hand, we aim to block arbitrary use of devices, by enforcing mutual authentication of the ECUs. This measure can stop attacks that are based on plugging malicious or vulnerable devices to vehicles in order to gain access to it. If devices fail to authenticate then they are blocked from the network, so these attacks are stopped. On the other hand, we create roles/users in the vehicle, so that each of them has specific privileges. These rights enable them to perform specific tasks and trigger alarms in the case of possible violations or privilege escalation attacks. The security policies that govern each user enable different access levels to vehicle modules and functionality, subject to time and geographical constraints.

We believe that the aforementioned measures can lead to the development of a more secure environment, which is more robust against many current attacks and furthermore lead to the development of new more customizable IT services for vehicles and automotive vendors.

1.3. Structure of the article

The next section illustrates the computerized architecture of modern vehicles, showing how the automotive industry has gradually embraced computer science methods and architectures. Moreover, this section provides an overview of the role of the Immobilizer and how it works. The third section presents the current industry standards in automotive industry, pinpointing several of their inherent vulnerabilities. Afterwards, we present the state of the art in securing in-vehicle communication, arguing why they should be redesigned. Section 4 highlights several vulnerabilities, their extensions, and users exposure through currently adopted industrial schemes. Section 5 discusses our proposal, which is divided in two parts. The first part discusses the need for creating roles/users in current vehicles and how to apply policies on vehicle's usage and functionality based on their credentials, subject to time or even geographical constraints. The second part introduces the proposed protocol, discusses the problems that it addresses and how it solves them. Finally, we conclude with some ideas for future work. The appendix contains the implementation of the proposed protocols in Scyther (Cremers, 2012) that enable easy formal verification of the provided security by the reader.

2. Vehicle's architecture and communication standards

The first modern vehicles were already controlled by numerous power electronic units (Ribbens et al., 2003).

[3] http://www.pcpro.co.uk/news/376480/intel-sets-team-on-thwarting-car-hackers.