Chapter 8
Security of In-Vehicle Communication Systems:
A Survey of Possible Vulnerabilities

Dennis Dubrefjord
Chalmers University of Technology, Sweden

Myeong-jin Jang
Chalmers University of Technology, Sweden

Oscar Carlsson
Chalmers University of Technology, Sweden

Hayder Hadi
Chalmers University of Technology, Sweden

Tomas Olovsson
https://orcid.org/0000-0001-9548-819X
Chalmers University of Technology, Sweden

ABSTRACT

The automotive industry has seen remarkable growth in the use of network and communication technology. These technologies can be vulnerable to attacks. Several examples of confirmed attacks have been documented in academic studies, and many vehicular communications systems have been designed without security aspects in mind. Furthermore, all the security implications mentioned here would affect the functionality of decision support systems (DSS) of IoT and vehicular networks. This chapter focuses on in-vehicle security and aims to categorize some attacks in this field according to the exploited vulnerability by showing common patterns. The conclusion suggests that an ethernet-based architecture could be a good architecture for future vehicular systems; it enables them to meet future security needs while still allowing network communication with outside systems.

DOI: 10.4018/978-1-7998-7468-3.ch008

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

Vehicles become smarter and more complicated every day due to the development in automotive electronics, which consists of various subsystems including engine electronics, transmission electronics, chassis electronics, and entertainment systems. The percentage of the electronic systems' cost in an automobile has gradually increased from approximately 1 percent in 1950 to about 30 percent in 2010 (Wagner, 2020). However, along with the rapid growth, security concerns regarding the communication systems in vehicles have not been considered. Therefore, vehicles are no longer in an acceptable state in terms of information security. This can lead to negative consequences for the passengers in the vehicle, but also other road users since a malfunction in one vehicle can cause accidents that harm both passengers and others. Furthermore, the stakes are quickly rising as the evolution towards smart cities means that the vehicles become more connected to other systems, such as decision support systems. In other words, vehicles are becoming more and more like Internet of Things (IoT) devices. An attacker who is able to compromise a vehicle can send arbitrary data to other, connected systems, affecting their ability to function as intended.

One example that shows how vulnerable vehicular networks are was presented at the Black Hat USA 2015 security conference by the researchers Charlie Miller and Chris Valasek (Drozhzhin, 2019). The researchers showed that a vehicle that was produced by a major car corporation could easily be hacked. The demonstration started by showing the ease of taking control of a Jeep vehicle's multimedia system by finding out its password. How to access it remotely over a cellular network was also presented. Furthermore, the researchers were able to control every component of the car through the Controller Area Network (CAN) bus, which is extremely vulnerable from a cybersecurity perspective. The demonstration delivered a clear message showing how insecure vehicular communication systems currently are and the severity of attacks where a remote attacker can be in full control of all functions in a moving vehicle.

Therefore, understanding automotive security vulnerabilities in vehicular communications are very important, not only to experts in the field but also to people in related fields of research. Thus, this chapter aims to provide readers with a comprehensive understanding of automotive security vulnerabilities, specifically inside the in-vehicle communication systems.

The methodology behind this chapter is a study of recent research related to the topic which is categorized and summarized. The scope is restricted to in-vehicle communication, meaning it excludes communication between the vehicle and its surroundings. Within in-vehicle communication, the authors focus on currently existing technologies such as the CAN bus and Local Interconnect Network (LIN) bus,

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/security-of-in-vehicle-communication-systems/282432

Related Content

Towards the Realization of an Integrated Decision Support Environment for Organizational Decision Making

Shaofeng Liu, Alex H.B. Duffy, Robert Ian Whitfield, Iain M. Boyleand Iain McKenna (2009). *International Journal of Decision Support System Technology (pp. 38-58).*

www.irma-international.org/article/towards-realization-integrated-decision-support/37432

Systematic Model for Decision Support System

Ramgopal Kashyap (2021). *Research Anthology on Decision Support Systems and Decision Management in Healthcare, Business, and Engineering (pp. 78-106).*

www.irma-international.org/chapter/systematic-model-for-decision-support-system/282581

DSS-CMM: A Capability Maturity Model for DSS Development Processes

Omar F. El-Gayar, Amit V. Deokarand Jie Tao (2011). *International Journal of Decision Support System Technology (pp. 14-34).*

www.irma-international.org/article/dss-cmm-capability-maturity-model/62640

Examining the Implications of Process and Choice for Strategic Decision Making Effectiveness

Paul L. Drnevich, Thomas H. Brushand Alok Chaturvedi (2012). *Integrated and Strategic Advancements in Decision Making Support Systems (pp. 147-162).*

www.irma-international.org/chapter/examining-implications-process-choice-strategic/66732

Integration of BI in Healthcare: From Data and Information to Decisions

Xue Ning (2021). *Research Anthology on Decision Support Systems and Decision Management in Healthcare, Business, and Engineering (pp. 969-982).*

www.irma-international.org/chapter/integration-of-bi-in-healthcare/282626