Chapter 7
Services in Connected Vehicles:
Security Risks and Countermeasures

Marcus Bertilsson
Chalmers University of Technology, Sweden

Michel Folkemark
Chalmers University of Technology, Sweden

Qingyun Gu
Chalmers University of Technology, Sweden

Viktor Rydberg
Chalmers University of Technology, Sweden

Abdullah Yazar
Marmara University, Turkey

ABSTRACT

Smart vehicles have introduced many services which can be categorized by their functionality (infotainment, comfort, ADAS, OEM services). Introducing new services increases the risk of compromising security. A mobile app used by drivers to connect the vehicle could be infected with malware and spread to the vehicle. Forging remote starting signals enables an attacker to start the vehicle without a key. Security implications of these services should be investigated and addressed thoroughly. This chapter investigates such problems and provides an overview of vulnerabilities, attacks, and mitigations related to these services along with findings including software bugs and insecure protocols. The mitigations for these attacks

DOI: 10.4018/978-1-7998-7468-3.ch007

include strengthening the security protocol of the vehicle CAN bus and incorporating security protocols such as TLS and IPsec. It is hard to say that all connected vehicles are secured. In conclusion, security cannot be neglected, and best practices like sufficient logging (e.g., IDS), reviewing, security testing, and updating of software and hardware should be used.

INTRODUCTION

Nowadays, vehicles are deeply rooted in our daily lives integrating with social and economic factors. Vehicles were invented as a purely mechanical machine, but it is now becoming more and more complex as computers and electronics are embedded into every component of newly designed vehicles. Today, connected vehicles not just provide basic transportation service but also can provide services like information, entertainment, communication, etc. Basically, a vehicle is a set of networks and electrical control units (ECUs) that are connected to the Internet, with the purpose of providing different functions and services that fits the users' needs (Stoltzfus, 2020). Some of these functions are relatively simple such as controlling lights or seats, others are more advanced e.g. collision detection and automatic parking. Figure 1 illustrates the use of radar and collision detection systems in action. A smart vehicle is usually connected to an external network in order to provide information services, get updates or diagnostics to the vehicle which exposes the internal systems to external threats. There is also an increase in security problems with the increasing complexity of smart vehicles and their software needs. In 2019, the number of reported cyber-attacks on connected vehicles was seven times higher compared to 2016 (Upstream, 2020). According to Ponemon Institute's (2018) survey in the automotive industry, 84% of the respondents believed that security practices taken Today are not keeping up with the evolution of technology. This indicates that the security implications of smart vehicles are highly concerned by the consumers and should be addressed accordingly.

This chapter aims to investigate the security of connected smart vehicles with respect to services provided. A comprehensive overview of previous attacks, weaknesses that were exploited to achieve a successful attack, and possible countermeasures against identified attack vectors are provided. Although a broad perspective of the overview of smart connected vehicles is provided, this chapter does not deep dive into technical details.

Methodology to Support the Triage of Suspected COVID-19 Patients in Resource-Limited Circumstances

Alexandre Ramalho Alberti, Eduarda Asfora Frej, Lucia Reis Peixoto Roselli, Murilo Amorim Britto, Evônio Campelo, Adiel Teixeira de Almeidaand Rodrigo José Pires Ferreira (2022). *International Journal of Decision Support System Technology (pp. 1-21).*

www.irma-international.org/article/methodology-to-support-the-triage-of-suspected-covid-19-patients-in-resource-limited-circumstances/309993