International Journal of Cyber Warfare and Terrorism
Volume 10 • Issue 2 • April-June 2020

The Security Aspects of Automotive Over-the-Air Updates

James Howden, De Montfort University, Leicester, UK

Leandros Maglaras, De Montfort University, Leicester, UK
https://orcid.org/0000-0001-5360-9782

Mohamed Amine Ferrag, Guelma University, Guelma, Algeria
https://orcid.org/0000-0002-0632-3172

ABSTRACT

Over-the-air (OTA) update is a method for vehicle manufacturers to remotely distribute maintenance updates, performance, and feature enhancements through the vehicle's lifespan. Recalls of vehicles cost the manufactures a lot of money. OTA solves the recall issue, while allowing consumers to pay for services and features via an update. The OTA ecosystem includes the coders who first developed the firmware, the 1st Tier suppliers, the vehicle manufacturers, and the vehicle itself. Currently, manufacturers designed the networks for speed and responsiveness, and not security. This article examines these elements and drills into the security available for each. The slowest and one of the most vulnerable parts of the system is the communications within the vehicle. The vehicle networks must ensure the integrity and authenticity of messages transmitted to guarantee software programmed onto ECUs are authorized and tamper-free. Specialist hardware within the vehicle makes this possible in an operation environment, such as hardware security modules.

KEYWORDS

Electronic Control Units, Automated Cars, Over-The-Air Updates, Connected Vehicles, Security, Cryptography, Hardware Security Module, Trust

1. INTRODUCTION

Modern connected vehicles contain up to 100 Electronic Control Units (ECUs) and up to 100 million of lines of code (Continental, 2019, Riggs et al., 2018, Petri et al., 2016, Holmes, 2018). The increase in functionality, i.e. advanced driving-assist system and autonomous driving, has increased the value of the vehicle's software.

With the introduction of new concepts, i.e. paying for vehicle functionality per feature aka Software-as-a-Service (SaaS), the automobile is evolving into a software-driven mobility service defined by the experience it delivers whilst transporting passengers (Windriver, 2018; Stevic, 2018). The consumer's desire to stream music, receive emails and social media posts has intensified this issue (Petri et al., 2016). The increase in software functionality means more potential for bugs, and so we have seen an increase in after sales software/firmware updates (Teraoka et al., 2016; Windriver, 2017).

Most vehicle software updates have occurred at dealerships either for a recall or an upgrade (Quain, 2018; Chowdhury, 2017; Continental, 2019). This can be inconvenient to the user, expensive for the dealership and affect the brand image (Windriver, 2017).

DOI: 10.4018/IJCWT.2020040104

The software industry has implemented over-the-air (OTA) updates for many years to fix bugs and make enhancements to software on computers, mobile devices, and even televisions (Chowdhury, 2017; Quain, 2018). OTA is wireless delivery of the software update to the vehicle (Rouse, 2018). In the automotive industry it is still rare. OTA on vehicles eliminates the need to take the vehicle to the dealership, protects brand-image and saves the waiting for updates (Riggs et al., 2018; Holmes, 2018).By 2022 the car-parc will contain hundreds of millions of connected vehicles, and consequently VMs would save $35 billion by using OTA rather than vehicle recalling (Neiger, 2016).

Some VMs have implemented software OTA systems but have concentrated on non-essential systems such as updates to the vehicle's infotainment systems, maps, and telematics software. This is known as SOTA. Some VMs, notably Tesla, have ventured into updating the firmware on individual ECUs including safety-critical systems, such as the brakes. This is known as FOTA (Quain, 2018; Kim & Park, 2018).

Even though OTA updates seem like a panacea, new vulnerabilities still occur. An attacker could take control if they introduced a malicious update to a vehicle, either at the back-end or in transit (Pedroza, 2011; Verma, 2018). History has shown software systems are most at risk to lapses in safety and security when undergoing change (Chowdhury et al., 2017). An OTA update is a substantial change; therefore, it is essential security is paramount. This paper explores OTA concept with an emphasis on security. Proceeding sections dive deeper into the OTA ecosystem, into the back-end systems, and the vehicle internals. Although many of the concepts discussed are in relation to software and firmware, this paper concentrates on the less trivial FOTA.

2. RELATED WORK

Recently several scholars have researched the area of security issues of smart cars (Maglaras, 2015) and especially those related to OTA. An OTA update system must be resilient to spoofing, tampering, repudiation, information-leakage, denial-of-service, and escalation-of-privileges attacks among others (Vasenev, 2019). Several security and privacy issues may arise from different parts of the ecosystem, like cloud, Service station, car or OEM backend and several security methods must be combined in order to counter those threats. The freshness of the update information also needs to be preserved in order to prevent replay attacks (Halder, 2019). Moreover, software distribution during OTA updates must be arranged in such a way that high security; low latency and continuous data protection are guaranteed.

Hash algorithms and digital signatures are some common methods that can be used in order to ensure authenticity and integrity of software updates, but more sophisticated methods were recently proposed (Zhou, 2019). Another promising idea is to use fog computing in smart vehicles (Fizza, 2019). Fog nodes are distributed in an ad-hoc fashion, and hence lead to a more reliable and robust system, without a single point of failure.

Having in mind to present a holistic model of a smart car that includes all different technologies that make the car 'smart' ENISA issued a report last year where relevant threats and cybersecurity risks pertaining to smart cars are analyzed and several security measures are proposed (Enisa, 2019). The report takes into account the particularities of this highly complex, heterogeneous and volatile environment and the fact that no modern system can be analyzed in isolation. In this report the interconnection of sensors, AI, machine learning algorithms, cloud computing and connectivity is presented and threats that come from all these components of smart car are analyzed. In one of the scenarios presented in the report a large-scale deployment of a rogue firmware after hacking OEM back-end servers affects OTA and consequently the proper behaviour of the vehicle. In this article we focus mainly on the OTA rather than the Wi-Fi and within a V2V/V2I ecosystem.