Cybersecurity and Connected Cars - Current State and Future Threats

Review Paper

Shivang Gupta, Wai Kin Wong, Kwok Fai Pang
28 November 2016

Introduction

While cars have been fitted with electronic units like ABS and electronic fuel injection since the mid 1980s, 'connected cars' have only emerged in the last decade. To be called 'connected' a car must use some form of electronic communication medium such as radio, internet, cellular, bluetooth or GPS as part of its regular functioning. Forbes estimates that over 152 million vehicles will have an internet connection by 2020. [1]

As connectivity in automobiles becomes more pervasive, cars are now susceptible to a variety of cyber attacks that range from information theft and GPS spoofing to complete remote control. This paper aims to review the current state of cybersecurity measures in automobiles, and to analyse the security implications of cars emerging as a key component of the Internet Of Things.

Background and Existing Literature

With all the electronic units and micro controllers used in modern automobiles, it is tempting to think of a car as a 'computer on wheels', however, it may be more accurate to think of it as '300 computers on wheels' as most of the Electronic Control Units (ECUs) are segregated from each other. For actual functionality, the different parts of the car such as the steering wheel, brakes, fuel system, etc., must be able to communicate with each other. In most vehicles, this is facilitated by the CAN (Controller Area Network) bus, a vehicle bus standard that acts as the central nervous system of the car, connecting all the electronic components.

The aim of most cyber attacks on cars is to gain access to the CAN bus so that the attacker can inject CAN frames, allowing them to take control over the ECUs.

Traditionally, due to their expensive nature, cars have not been researched and targeted by attackers. Car manufacturers have different protocols and systems in place for implementation of the CAN bus and this added complexity makes it hard for attackers to generalise vulnerabilities in cars. Despite this, the rising use of web browsers and other traditional computer technology in cars has given rise to a larger number of vulnerabilities that can be used by hackers.

The cybersecurity community's interest in automobiles first began in 2011 when researchers from the University of Washington and the University of California San Diego, remotely took control of a General Motors car being driven by a television reporter. They did this with the help of an attachment to the OBD-II port, an on-board diagnostics port that provides access to the CAN bus of the car. [2] They were able to access this attachment remotely through GM's OnStar wireless system. While this attack garnered media attention, from a technical point it was not very successful as, it required attackers to gain physical access to the vehicle first.

In 2013, Hak5 featured an interview on a different attack method that does not involve the CAN bus. Jared Boone demonstrated how even simple electronic units like Tire-Pressure Monitoring Systems (TPMS), which are required by regulation in all US cars since 2008, can be used by hackers to gain access to private information about both the car and the driver. These units consist of a simple radio transmitter and pressure sensor, each of which

has a unique ID which could be sniffed by an attacker using a cheap DIY radio apparatus. The attacker could then use this information to trace the car's location and position. [3]

While there have been no known incidents of a connected car being hacked outside of research, the most convincing attack on a car was conducted by Charlie Miller and Chris Valasek in 2015, when they took remote control over an unmodified Jeep Cherokee being driven by a Wired magazine reporter. They were able to exploit the Jeep's cellular Wi-fi service to take control over the car's GPS, radio, transmission, engine and even climate-control. The attack posed such a threat that it forced Chrysler (Jeep's parent company) to recall 1.4 million vehicles to fix the vulnerability. [4]

Both the 2015 Jeep attack and the 2011 attack on the OnStar system, relied on the fact that messages sent on the CANbus are not cryptographically signed. Recently, researchers from the Chinese company Tencent were able to utilise the same fact to remotely attack and take control of a Tesla Model S through a vulnerability in its WebKit browser. Tesla responded to this attack promptly, and in 10 days launched a path to fix the issue which ensures that all messages that travel on the CANbus are cryptographically secured, ensuring that this kind of attack cannot take place in the future. [5]

Related Issues and Security Implications

Remote Attack Surfaces

Connected cars are different from traditional cars as they can be attacked from a distance using the internet, GPS, radio and other technologies. Below we have discussed some of the remote attack surfaces that an attacker could use without being in the car's line-of-sight:

1) Telnet and Telecommunication Services

As shown in Valasek and Miller's attack, cars that use cellular networks to provide in-car Wi-fi are susceptible to remote hacking if the telecom towers are not configured to prohibit two way communication with cars. After their attack Sprint configured all it's US towers to block TCP port 6667, used by the Jeeps internal service, but other manufacturers may use other ports.

2) Software Testing

Automobile companies are not software companies and as such the software used in cars is not put through many layers of testing. As cars are expensive, independent researchers are also reluctant to test the software's limits. This gives attackers the opportunity to find vulnerabilities before they are patched.

3) Internet and Web Browsers

The Tesla attack used a known vulnerability in the open source WebKit browser to access the car. Internet software is reliable only as long as it is updated frequently and due to the hardware-software configuration, this is very difficult to achieve in cars.

4) Radio and Vehicle-to-vehicle (V2V)

Cars pose unique issues as wires cannot be used in moving parts like tires, making radio communication necessary. Radio packets can be easily sniffed by a nearby attacker, but the true threat lies in the implementation of the V2V protocol. This protocol is now being tested, and will allow cars on the road to communicate with each other to better equip drivers. This will a key part of self-driving car technology in the future. While current specifications for this

protocol indicate a Public Key Encryption system for all communication, it will be up to manufacturers to implement their own security protocols to ensure safe communication which cannot be spoofed/intercepted.

5) Software Updates

Car software, like any other software, requires updates. At DEFCON 22, Miller and Valasek demonstrated how an attack could be conducted by hijacking the update mechanism used by Chrysler cars. [6] The update is performed by downloading and burning an ISO file onto a USB disk, and then plugging in the USB stick into the car. By reverse-engineering the update file and creating a fake update, an attacker could potentially upload malicious code into the car. Other similar update methods may also be vulnerable.

Tesla is one of the industry leaders in creating secure connected cars with a well established 'bug bounty' program. Updates in Tesla cars are handled through over-the-air firmware downloads. This is a relatively more secure, approach, however, it involves the use of a central update server, introducing another threat: if the central server is compromised, an attacker could potentially gain access to all Tesla cars.

Security Threats

In the following section we will analyse potential threats based on the CIA triad:

1) Confidentiality

By hacking a connected car, an attacker could gain access to vehicle information such as position, fuel, etc., as well as private information about the car's owner through the cars stored files/browser. In the future, the attacker may also be able to access information about other nearby cars through the V2V protocol.

Wireless sniffing over a cars Wi-fi service, radio packet sniffing and remote access through the internet are the biggest threats to confidentiality in a car.

2) Integrity

Modern cars and autonomous vehicles are dependent on environmental information such as GPS, distance from other cars (sonar), etc. An attacker could tarnish the integrity of the car's service through attacks such as GPS spoofing, blasting IR lights to blind cameras, and producing fake smoke to confuse the gas and sonar sensors.

3) Accessibility

Connected cars are susceptible to remote access through shell injection and denial of service attacks. A possible future threat could be ransomware that would lock up the car and not allow the user to access it unless they pay the attackers money. While accessibility is a relatively lesser concern for websites, if a car is put out of commission, it may lead to an accident and even death. As such threats that diminish the accessibility of cars are the most dangerous.

Future Implications

Automobile companies are pushing for rapid development of connected cars, but not all of them are mandating strict cybersecurity measures as the same time. Companies in developing nations may be tempted to jump on the bandwagon by developing connected cars using open source software and other existing tools, leaving the cars vulnerable to existing threats.

Self driving cars are a big part of the future, with companies like Google and Uber already running trials. However, with a computer being the brains behind the car, they will be susceptible to new types of attacks. These cars will be responsible for the lives of their passengers, and car companies must invest heavily in cybersecurity to ensure that rapid development is not done at the cost of safety.

References

[1] McCarthy, Niall. "Connected Cars By The Numbers." Forbes. Forbes Magazine, 27 Jan. 2015. Web. 27 Nov. 2016.

[2] Checkoway, Stephen, et al. "Comprehensive Experimental Analyses of Automotive Attack Surfaces." *USENIX Security Symposium*. 2011.

[3] Boone, Jared. "Hak5 1511 – Tracking Cars Wirelessly And Intercepting Femtocell Traffic." Hak5 - Technolust since 2005. Hak5, 30 Oct. 2013. Web. 27 Nov. 2016.

[4] Miller, Charlie, and Chris Valasek. "Remote exploitation of an unaltered passenger vehicle." *Black Hat USA* (2015).

[5] "Car Hacking Research: Remote Attack Tesla Motors." Keen Security Lab Blog. Tencent, 19 Sept. 2016. Web. 27 Nov. 2016.

[6] Miller, Charlie. "Remote exploitation of an unaltered passenger vehicle." *DEFCON 22* (2015)

Other Resources

S. Woo, H. J. Jo and D. H. Lee, "A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 993-1006, April 2015.

T. Bécsi, S. Aradi and P. Gáspár, "Security issues and vulnerabilities in connected car systems," 2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS), Budapest, 2015, pp. 477-482.

https://www2.idexpertscorp.com/blog/single/connected-cars-security-risks-on-wheels

http://resources.infosecinstitute.com/the-nightmare-of-car-hacking/

http://resources.infosecinstitute.com/future-now-car-hacking/

http://www.strategyand.pwc.com/reports/connected-car-2016-study