Vehicle Right-to-Repair:
Cyberattack Risks for Massachusetts Residents

Reported and Potential Cyberattack Scenarios

Contents

September 28, 2020

Introduction

The Massachusetts "Right to Repair" Initiative[1], which was introduced as a proposed state statute in 2012, was to require any vehicle owners and independent repair facilities in Massachusetts to have access to vehicle diagnostic information, made available to the manufacturers' authorized repair facilities. The initiative passed with overwhelming voter support (86%) on November 6, 2012. Motivation was clear: to enable vehicle owners to repair their cars and light trucks anywhere they'd like, hence reducing repair costs.

Technological advancements in the automotive sector since this law was put into place have enhanced vehicles with a range of connectivity options, including built-in cellular connectivity, Wi-Fi, Bluetooth and RF access into and/or out of the vehicle.

In 2020, a new ballot question, Question 1, backed by $15 million in funding from national retail chains, would alter the original law and expand access to vehicle wireless technology and 'telematics' information. The Massachusetts Coalition for Right to Repair has resumed its activity promoting the new legislation.

We at Karamba Security believe that sharing OEMs' telematics and wireless protocols and communication credentials with any interested party in the state may, unfortunately, be used by hackers to exploit the open protocols in order to infiltrate vehicles' telematics units, to gain access to customers' personal data, which is stored in the car, and risk consumers' lives.

Cars are Under Risks of Cyberattacks

Vehicles are becoming increasingly connected. Driven by consumer convenience and safety motivations, vehicle manufacturers are adding connectivity features to their vehicles. This includes infotainment systems using Wi-Fi and Bluetooth connectivity, telematics units that connect cars to cellular networks for navigation and safety purposes, and newly added Advanced Driver Assistance Systems (ADAS) that ensure that the car is driven safely by correcting unexpected lane changes and stopping the car before it hits an obstacle.

However, with connectivity comes risk. Almost any system that became connected to the internet has become a target for hackers.

The stakes for hacking vehicles are high. Today's cars can store the driver's personal information (contact list, navigation history, and now even credit card data for remote payments). But beyond that, hacking into the vehicle's infotainment system, telematics unit or ADAS controller enables hackers to take control of the car and confiscate speed and direction from the driver's hands, risking the driver's, passengers' and others' lives.

[1] https://en.wikipedia.org/wiki/Massachusetts_Right_to_Repair_Initiative

In 2016 the United States Assistant Attorney General for National Safety said[2] that connected cars are the next battleground for national safety. "If you were able to do something that could affect a large scale of an industry—like 100,000 cars—you could see that being in the arsenal of a nation-state's tool kit is a new form of warfare. We've seen rogue nation states try to assassinate those that do not share their beliefs. If they were able to do it remotely through a car, I don't see why they consider that a safe zone."

In this paper we share known cyberattacks on vehicles. Those attacks were performed by researchers but could have been conducted by ill-intent hackers.

Automotive Cyberattacks

The attacks reported herein show how hackers gain access to the vehicle by infiltrating one of its externally connected ECUs (electronic control units). After gaining access to that ECU, hackers succeed to expand their presence in the vehicle, in order to retrieve personal data, or take control of the car, i.e. stop the car and/or change its direction.

It is important to emphasize the first step in hackers' journey is to gain access to the ECU firmware, in order to reverse engineer, it and find vulnerabilities in it. Such vulnerabilities will be exploited by the hackers to gain access to their target systems.

Recent security research projects aimed at automotive Infotainment systems or OBD-II connections demonstrate that after hackers gained access to those ECUs' firmware, they succeeded to analyze them, find the anticipated vulnerabilities and exploit them.

Once exploited, hackers gained code-execution privileges within a process. This effectively enables the attacker to control the device, with complete freedom to decide how to proceed. At the minimum the hacker can research the hacked device to retrieve all data stored on it. At the maximum, the device can be used as an entry to the entire car, in order to manipulate the car's safety systems.

This situation is intolerable in automotive ECUs, where cybersecurity is critical for driver and passenger safety.

[2] https://www.infosecurity-magazine.com/news/attorney-general-connected-cars/

Jeep Cherokee

The vulnerability: Incorrect Configuration (an open port on the infotainment system)

The attack vector: Dropper attack via the cellular network

In 2015 security researchers exploited the car's infotainment system that was connected to the mobile data network, and they were able to move laterally into other electronic parts of the vehicle (air conditioning, transmission, and even the car's steering controls).[3]

In 2016[4] they showed the same attack in principal; this time, however, they were also able to bypass the software update guards and control the powertrain and steering.

In their experiments, researchers managed to gain local access to the system via the device's USB port, and remote access via the cellular data interface that provides Internet connectivity and via an SMS interface. The researchers were able to activate the wipers, engage the brakes, and disable the brakes at low speed.

Tesla

The vulnerability: In-Memory vulnerability in the infotainment web browser

The attack vector: Wi-Fi Hotspot, man-in-the-browser, and full control of the infotainment [5] [6], Tesla's brakes and door locks were hacked remotely.

Researchers from Keen Security Lab exploited multiple flaws in two models (Model S and Model X).

The attack was perpetrated by connecting through a Wi-Fi hotspot and executing malicious code on Tesla infotainment after exploiting a number of in-memory vulnerabilities.

After achieving control, the researchers realized a full attack chain to implement arbitrary CAN-bus and ECU remote controls, taking control of the brakes.

BMW

The vulnerabilities: In-Memory (Bluetooth stack, USB-Ethernet stack, Cellular interface); Improper configuration (Stored passwords and keys)

The attack vectors: Infotainment, Telematics, OBD-II Ethernet diagnostics service

The report shows that the readily available attack surface into the vehicle are the infotainment, the telematics (TCU) and the OBD-II port. It also shows that placing a gateway between these units and the safety-critical side of the vehicle is not sufficient, as attackers have found ways to bypass the gateway: either by sending legitimate messages, or by exploiting vulnerabilities in the gateway ECU itself.

[3] https://thehackernews.com/2015/07/car-hacking-jeep.html

[4] https://www.forbes.com/sites/thomasbrewster/2016/08/02/charlie-miller-chris-valasek-jeep-hackers-steering-brake

[5] https://thehackernews.com/2016/09/hack-tesla-autopilot.html

[6] http://keenlab.tencent.com/en/2017/07/27/New-Car-Hacking-Research-2017-Remote-Attack-Tesla-Motors-Again/

The researchers from Keen Lab identified and exploited zero-day in-memory vulnerabilities in 3rd-party software stacks such as Bluetooth, USB and Ethernet.[7]

Annual Attack Landscape

A summary prepared by Upstream[8] of the 2019 attacks, and incident history since 2010, illustrates the rapid and consistent growth of cyber threats:

> *Over the past 10 years, the number of automotive cybersecurity incidents has increased dramatically. **In the past year alone, the number has doubled.** As more connected vehicles hit the road, the potential damage of each incident rises exponentially, placing companies and consumers at risk.*

Among the top 2019 cybersecurity incidents cited in the report (approximately one per month) were the following findings:

- ADAC tested 237 cars by 33 brands, and 99% of them contained vulnerabilities that enabled criminals to easily hack them in minutes to unlock the vehicles and drive away.
- Smart car alarm systems had major security flaws that affected 3 million cars. Hackers were able to remotely take over accounts and track and control vehicles.
- Security vulnerabilities found in smart trackers allow hackers to take over accounts, track cars in real-time, extract personal data, and more.
- A mobile app used by car owners to remotely locate and start cars displayed account and vehicle information of other users.

The correlation between connectivity and vulnerability was pointed out, where *“each new service and capability introduces additional risks, points of entry for hackers, and opportunities for potential privacy breaches. As the use of connected vehicles and smart mobility services increases, there is a growing number of … incidents, threatening both companies and consumers.”*

The motivation of black-hat hackers is clear, and these players are quick to craft attacks utilizing publicized vulnerabilities as well as acting on their own capabilities and findings. Online resources (including YouTube tutorials) are readily available and can enable even amateur hackers.

The concerning conclusion in the Upstream report is that there has been a shift of interest towards criminal activity, and that a majority *(57%)* of the 2019 incidents originated from black-hat activity.

[7] https://www.computest.nl/wp-content/uploads/2018/04/connected-car-rapport.pdf
[8] https://www.upstream.auto

Undermining Tremendous Cybersecurity Efforts Already Done

During 2020, the automotive industry has adopted strict cybersecurity measures, and new standards were ratified, such as the UN ECE WP.29[9] or were voted on, prior to formal ratification, such as ISO 21434[10] . Those standards mandate car manufacturers to protect their electronic control units (ECUs) against cyberattacks, and to protect and authenticate wireless and cellular traffic into the telematics unit. The proposed changes to Right-to-Repair are in direct conflict with measures such as these. The new standards mandate protecting drivers and passengers by creating a controlled and carefully audited vehicle environment, whereas the new bill suggests giving access to whomever desires such access thus creating an uncontrolled risk.

Moreover, the United Nation's initiative and the global ISO initiative have emerged after years of diligence, which resulted in guidelines to vehicle manufacturers to protect their consumers' data privacy and safety by encrypting vehicle communication credentials. Massachusetts' proposed legislation neutralizes those measures and may defeat the purpose of mitigating increased connectivity risks to cyberattacks.

The standardization efforts are just the tip of the iceberg of the inherit changes that OEM are going through with respect to cyber security in the recent decade or so. OEMs have invested tremendous efforts, billions of dollars, and are already doing a lot to strengthen their cyber defenses in light of the expected attacks, such as the ones mentioned above. OEMs have been proactively adopting available guidance and best practices for security controls, including guidance published by the National Highway Traffic and Safety Administration (NHTSA)[11] and the National Institute of Standards and Technology (NIST)[12][13].Accepting the new right to repair language will undermine the strong defenses automakers already have in place to prevent cyber criminals from accessing their vehicles.

Proposed Changes to the Right to Repair

The proposed legislation updates the law to include:

> *"Access to vehicle on-board diagnostic systems shall be standardized and not require any authorization by the manufacturer"*

[9] https://www.unece.org/trans/main/welcwp29.html

[10] https://www.iso.org/standard/70918.html

[11] https://one.nhtsa.gov/Laws-&-Regulations/Recommended-Best-Practices-for-Importers-of-Motor-Vehicles-and-Motor-Vehicle-Equipment

[12] https://www.nist.gov/cyberframework

[13] https://nvd.nist.gov/800-53/Rev4/impact/HIGH

> *"Access shall include the ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair."*

These changes will put vehicles at risk for cyber-attack , as:

- Allowing the sending of any command, which can be used by hackers to control cars (as shown in the exploits described above)
- Allowing reading of diagnostics data and commands will enable hackers to:
  - Gather information regarding encryption keys and specific protocols, which will allow hackers to infiltrate the vehicles by using those communication keys.
  - Obtain private information such as location and driving habits, and then sell it on the dark web (as done today, with credit-card information and medical records).
  - Use such access to escalate their privilege on the hacked device, lock it, and require the driver to pay ransom in order to release the device to be able to drive the car again.

Opening OEMs' telematics, wireless protocols and communication credentials will make it possible for malicious actors to exploit the open protocols, take over vehicles' telematics and other units and, as outlined above, cause damage ranging from information theft to road accidents.

Moreover, as the bill requires a standardized access across all vehicle makes and models, any vulnerability that is identified by a hacker in one model, inherently puts all other cars at the similar safety risk. In other words, the suggested wordings significantly multiplies the potential victims of cyberattacks.

Worst of all, as shown in the Jeep, BMW and Tesla attacks, entering the vehicle through the telematics unit (by using the communication credentials) could enable hackers to access brakes and safety systems, carrying out widespread attacks that could yield major fatalities and collateral damage.

Conclusion

In light of the reported automotive exploits we recommend voting against changes to the Right to Repair, as these changes will open the doors to increased malicious activities. The recently-established ISO 21434 and UNECE WP.29 standards mandate car manufacturers to protect their electronic units and the incoming wireless and cellular traffic. It will be ironic if – during the very year in which rigid security enforcements were placed on OEMs – the State of Massachusetts will require automotive OEMs to give those authentication keys to any interested party, which can easily be a hacker aimed at sacrificing car owners' privacy and safety.