Securing connected cars from cyberthreats

2024

ZIMPERIUM®

Your new car may be safer and smarter, but is it cyber-secure?

The auto industry reached an important milestone in 2020: over half of the cars sold globally included internet connectivity as a standard feature.

Modern vehicles have started to resemble mobile supercomputers, each containing millions of lines of code and able to process vast amounts of data. They've also begun integrating with mobile devices and apps. Ford is the latest automaker to announce that it will use Google Android to drive its connected systems.

The automotive industry is doubling down on data to improve the driving experience and monetize the insights. But this hyperconnectivity comes with significant risks. Earlier this year, two researchers showed how a Tesla — and possibly other cars — can be hacked remotely, without any user interaction, with a drone.The biggest implied security threats for the automotive industry are:

- Car Theft
- Supply Chain Risks
- Data Breaches
- Remote Manipulation or Control

With that in mind, we wanted to explore some of the biggest security challenges facing automotive manufacturers in the foreseeable future.

Supply Chain Risk

Hackers are turning their attention to connected cars, as they have multiple entry points and several ways to profit from attacks. As of 2016, cyberattacks on connected vehicles have risen by nearly 100% annually, revealing significant issues in securing the supply chain of the components and apps.

Theft of Connected Cars

One goal of incorporating better technology into cars is to make them more convenient and secure against theft. An example is the move from physical keys to key fobs that use a short-range radio transmitter. Yet today, all it takes is a pair of $11 radio gadgets to hack key fobs and steal the car. Remote start is another feature that has become increasingly abused by car thieves.

As a result, automotive thefts in the UK have increased 50% in the last six years, and major cities across the US saw significant spikes in 2020, despite falls in most other crime categories.

The hacking of connected car security systems and the availability of cheap theft devices, even ones made using old Nintendo Game Boys, means thieves can access nearly any connected car they want.

Data Breaches

With large processors and multiple data receptors, connected vehicles have the potential to collect more personal information about their users than nearly any other connected device. Former Intel CEO Brian Krzanich predicted that vehicle connectivity would create a flood of data, with each car creating 40 terabytes of data for every eight hours spent driving.

Unfortunately, with seven different modes of connectivity and information stored in unsecured repositories, this data is highly vulnerable to theft. A Washington Post investigation, for example, revealed how much personal data could be extracted from a second-hand Chevy infotainment computer. With more and more models shipped with 4G or 5G connectivity, hackers don't even require physical access to a vehicle to infiltrate it and extract private information.

Cars Performing Unwanted Actions

Action movies depict dystopian scenarios where bad actors gain access to a vehicle and take control away from the driver. Researchers made history by hacking into and taking out the transmission of a Jeep Cherokee while it was going 70 mph. This ultimately led to Chrysler recalling 1.4 million vehicles.

The remote takeover of system functions is a prominent worry for autonomous vehicles. Researchers have shown how the advanced driving assistance systems (ADAS) on a Tesla Model X could be fooled into swerving towards incoming traffic. Other research has shown how autonomous vehicles could shut down New York if they were hacked and turned off in mid-traffic. Automakers need to convince regulators and customers that they are truly safe and secure for connected vehicles to reach their full potential.

Connected Car Apps

Mobile apps replacing key fobs is the next significant advancement we are starting to witness. Today, these apps can carry out simple functions like unlocking the car to advanced actions like self-parking or summoning that car. All of these features require sensitive information to be stored and communicated from within the app. So, securing data at rest and in motion becomes critical to earning customer trust.

For this to happen, application developers need to make connected car cybersecurity a top priority. But that isn't as easy as it sounds. Maintaining a large enough in-house security team to keep application security at the required level might not always be a viable option for automotive manufacturers. Applications are already the third most popular attack vector used to infiltrate connected cars. With thefts growing, car apps are likely to become even bigger and more lucrative targets.

How are we helping the automotive sector today?

1

Vetting The Supply Chain

Enable a large enterprise mobility team evaluate and approve every release of in-house developed and third-party supply chain apps before deploying them to managed devices.

2

Secure In-Car Services

The protection of code used for in-vehicle security, emergency services, theft deterrence, turn-by-turn navigation, and remote diagnostics.

3

Prevent Car Theft

Secure critical code in apps that allow consumers to control their cars remotely and create, manage, and share digital keys.

The Road Ahead: Better Security for Modern, Connected Cars

Bolstering connected car cybersecurity and keeping associated automotive applications safe from hacking requires multiple techniques to block and frustrate hackers' efforts. Here is a simple recommendation for where to start:

- Use advanced code obfuscation and anti-tampering capabilities. These together shield the application from hackers performing static and dynamic analysis once they have the app.
- Add capabilities such as run-time self-protection (RASP) and anti-malware protection that allow apps to defend themselves when running on end-user devices whose health is unknown.
- Use white-box cryptography to protect all the cryptographic keys used to secure storage, communication, and access.

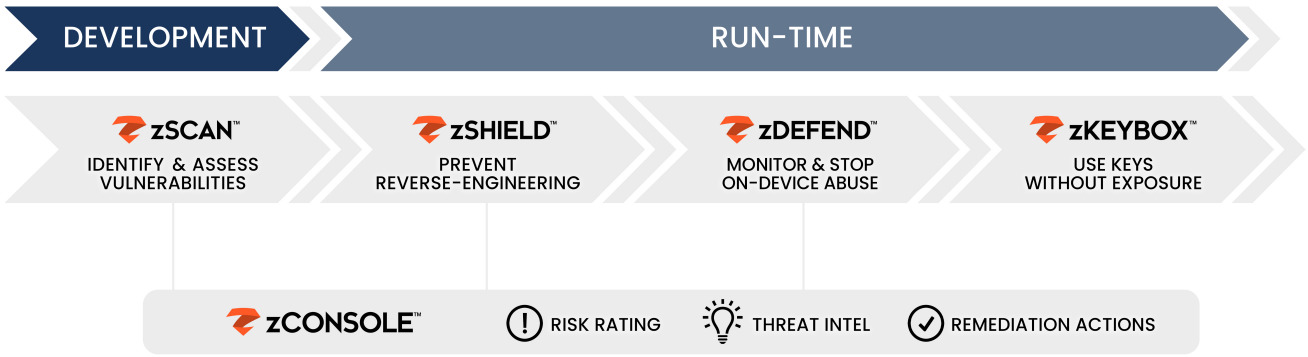
Zimperium's Mobile Application Protection Suite (MAPS) helps automobile manufacturers keep data safe and their vehicles secure, allowing them to fully capitalize on advanced technologies and build differentiated products. MAPS is comprised of four capabilities, each of which addresses a specific need when it comes to securing the entire application lifecycle:

zShield | Application Shielding
Protects the source code, intellectual property (IP), and data from potential attacks like reverse engineering and code tampering

zKeyBox | White-box Crypto Protection
Protects your secrets and keys so they cannot be discovered, extracted, or manipulated

zScan | Application Security Testing (AST)
Helps your mobile app development organization discover and fix compliance, privacy, and security issues within the development process before you publicly release your apps

zDefend | Runtime Application Self-Protection (RASP)
Helps detect and defend against run-time exploitation and abuse from device, network, phishing, and malware
Learn more about our Mobile Application Protection Suite here.



About Zimperium

Zimperium, the global leader in mobile security, offers the only real-time, on-device, machine learning-based protection against Android, iOS, and Chromebook threats. Powered by z9, Zimperium provides protection against device, network, phishing, and malicious app attacks. For more information or to schedule a demo, contact us today.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244