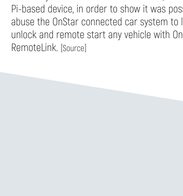
10 MOST SPECTACULAR HACKS OF CONNECTED CARS

Modern cars are connected, and they are getting smarter by the minute. As the automotive industry becomes increasingly connected, it is confronted with a constantly growing range of security risks. As a result, passenger safety is no longer limited to influences from road traffic. The following threats from third parties confront players in the connected car ecosystem with previously unknown challenges.



1. Remote Car Hack Through Cellular Network

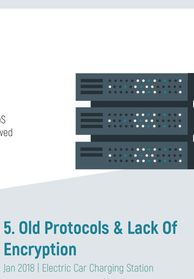
July 2015 | Jeep Cherokee

The infamous attack. This was the fastest recall in NHTSA history. Researchers remotely deactivated the accelerator pedal of a vehicle while driving. [Source 1, Source 2]

2. Man-in-the-middle Attack

July 2015 | OneStar

A security researcher created OwnStar, a Raspberry Pi-based device, in order to show it was possible to abuse the OnStar connected car system to locate, unlock and remote start any vehicle with OnStar RemoteLink. [Source]



3. Bugs In On-board WiFi

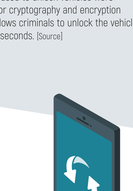
June 2016 | Mitsubishi Outlander

The Outlander's car alarm had a weakness: by hacking the vehicle's WiFi system, an attacker could override the vehicle's security. [Source]

4. Protocol Vulnerability

August 2017 | Controller Area Network

A fundamental issue in the functioning of CAN (Controller Area Network) protocols allowed a DoS attack that disrupted vehicle functions. This allowed airbags to be deactivated, locking systems to be manipulated and vehicles to be stolen. [Source]



5. Old Protocols & Lack Of Encryption

Jan 2018 | Electric Car Charging Station

Lack of encryption and easy access allow criminals to: collect, imitate, and use ID numbers for transactions; rewire charging requests with the charging station basically disabling the charging station; gain root access to the station. [Source]

6. Misconfigured Server

May 2018 | Viper SmartStart

A misconfigured CalAmp server allowed researchers access to back-end systems of Viper SmartStart vehicle management systems. This made it possible to locate vehicles, reset passwords, unlock side doors, deactivate alarms and start engines. [Source]

7. Weak Encryption

September 2018 | Tesla Model S

Researchers discovered that the Tesla Model-S wireless key fobs used to unlock vehicles were equipped with poor cryptography and encryption standards. This allows criminals to unlock the vehicles in as little as two seconds. [Source]

8. Remote Start Vulnerabilities

October 2019 | MyCar

MyCar and other versions of the software had three massive different security vulnerabilities. These allowed access to the MyCar database backend, so that any car connected to the MyCar application could have been located anywhere in the world and stolen. [Source]

9. Vulnerabilities & Lack Of Security Standards

April 2020 | Ford & Volkswagen

The consumer group "Which?" exposes security flaws that range from remotely exposing private, customer information (e.g. location history, contact info) to disabling the traction control system. [Source]

10. Vulnerabilities In Encryption

May 2020 | DST80

Vulnerabilities in Texas Instruments encryption system called DST80 discovered. Proxmark RFID reader/transmitter can determine the secret cryptographic value of the system. This in turn would allow the attacker to unlock the car, disable the immobilizer and start the engine. [Source]

WOULD YOU LIKE TO DISCOVER MORE?

Get in-depth guidance that will lead you into the world of application security!

Download Ressources

code intelligence

CODE INTELLIGENCE
Rheinwerkallee 6
D-53227 Bonn

CONTACT US
+49 228 2869 5830
sales@code-intelligence.com