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

**Date:** 2015
**Model:** Jeep Cherokee
**Details:** The infamous attack. This was the fastest recall in NHTSA history. Researchers remotely deactivated the accelerator pedal of a vehicle while driving.

### 2. Man-in-the-middle Attack

**Date:** 2015
**Model:** OneStar
**Details:** 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.

### 3. Bugs In On-board WiFi

**Date:** 2016
**Model:** Mitsubishi Outlander
**Details:** The Outlander’s car alarm had a weakness: by hacking the vehicle’s WiFi system, an attacker could override the vehicle’s security.

### 4. Protocol Vulnerability

**Date:** 2017
**Model:** Controller Area Network
**Details:** 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.

### 5. Old Protocols & Lack Of Encryption

**Date:** 2018
**Model:** Electric Car Charging Station
**Details:** 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.

### 6. Misconfigured Server

**Date:** 2018
**Model:** Viper SmartStart
**Details:** 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.

### 7. Weak Encryption

**Date:** 2018
**Model:** Tesla Model S
**Details:** Researchers discovered that the Tesla Model S wireless key fobs used to unlock vehicles were equipped with poorly designed encryption standards. This allows criminals to unlock the vehicles in as little as two seconds.

### 8. Remote Start Vulnerabilities

**Date:** 2019
**Model:** MyCar
**Details:** 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.


**Date:** 2020
**Model:** Ford & Volkswagen
**Details:** 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.

### 10. Vulnerabilities In Encryption

**Date:** 2020
**Model:** DST80
**Details:** 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.