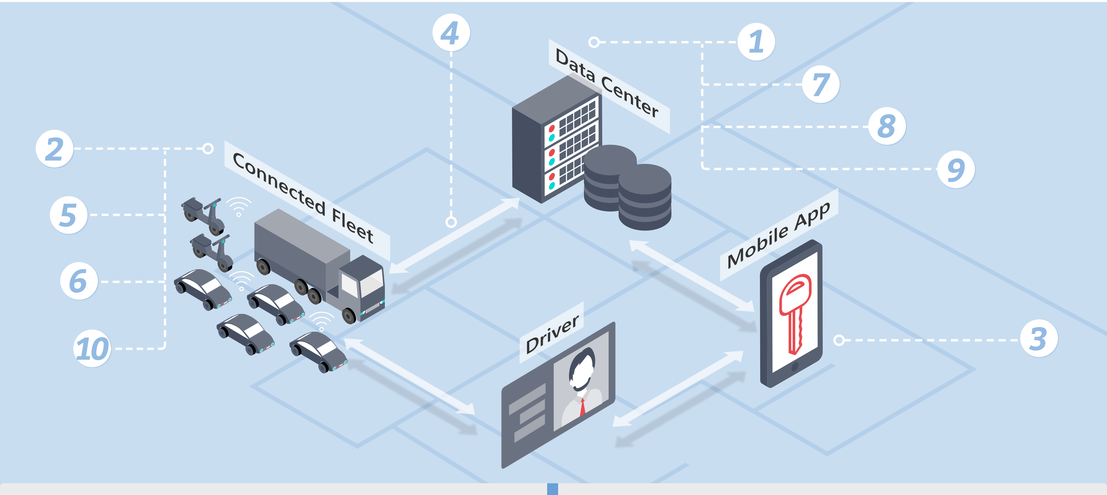
Top Real-World Threats Facing Connected Cars and Fleets

Modern connected cars are a complex amalgamation of powerful on-board computers and connectivity. There is an ever-growing range of cyber security risks facing the connected car industry. The problem is acute for car manufacturers, connectivity service providers and businesses managing car fleets. Automotive cyber threats introduce the potential for mass compromise of vehicles and entire fleets. Here is a snapshot of the top real-world cyber security threats highlighting the diversity of attack vectors already challenging connected car ecosystem players.



1 Command & Control Server

Over 100 cars disabled remotely by a disgruntled employee of a Texas car dealer who hacked Webtech Plus, a web-based vehicle-immobilization system.

Mar 2010

2 OBD II Port

Hackers were able to kill the engine and disable the brakes of a car moving at 65km/h using a laptop and custom-written software plugged into the OBD II port.

May 2010

3 Mobile App

Hackers remotely controlled a car's door locks, headlights, wipers, sunroof, and horn while it was in motion.

Jul 2014

4 Cellular Network

Hackers remotely controlled Jeep's engine while driving along a highway.

Jul 2015

5 Telematics Control Unit

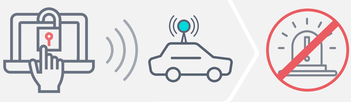
Hackers cut a Corvette's brakes by hacking remotely into a TCU OBD-II device connected to the dashboard.

Aug 2015

6 Wi-Fi

A Mitsubishi car's Wi-Fi was hacked allowing attackers to control its lights, unlock the doors remotely and disable the alarm.

Jun 2016



7 Data Center

Renault and Nissan plants hit by massive ransomware (aka WanaCrypt0r) attack which, as a result, stopped production across several of its European plants.

May 2017

8 Data Center

Hackers accessed Uber's cloud servers and stole 57 million users' private information.

Nov 2017

9 Identity Theft

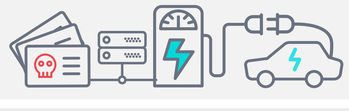
A fraudster hacked a car sharing company's database, using stolen members' personal information to ride vehicles for free.

Jan 2018

10 Electric cars charging station

Electric car charging stations enable hackers to collect ID card numbers, imitate them and use them for transactions, rewire charging request and gain root access to the station.

Jan 2018



What will the next connected fleet cyber-attack be ?

?

Learn about the first centralized, non-intrusive cloud-based automotive cybersecurity solution to identify, monitor and protect connected vehicle fleets from cyber-attacks and fraud.

Upstream
www.upstream.auto

Sources

1. https://www.wired.com/2010/03/hacker-bricks-cars | 2. https://www.newscientist.com/article/dn18901-modern-cars-vulnerable-to-malicious-hacks
3. https://www.techspot.com/news/57455-chinese-security-firm-hacks-tesla-model-s-to-gain-control-of-door-locks-wipers-sunroof-and-more.html
4. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway | 5. https://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget
6. https://arstechnica.com/cars/2016/06/mitsubishi-outlander-hybrid-is-the-latest-connected-car-to-prove-vulnerable-to-hacking
7. https://jalopnik.com/renault-and-nissan-plants-hit-by-massive-ransomware-att-1795190743
8. https://www.wired.com/story/uber-paid-off-hackers-to-hide-a-57-million-user-data-breach
9. https://www.tripwire.com/state-of-security/latest-security-news/man-arrested-allegedly-hacking-car-sharing-service-using-vehicles-free
10. https://www.kaspersky.com/blog/electric-cars-charging-problems/20652