



# Automotive Cybersecurity

---

By: Pan, Jimmy, Talha



# What is Automotive Cybersecurity?

- Securing the technology in a vehicle
- Preventing unwanted people access to key features of the vehicle
- Technological advancement in automotive industry makes this extremely important



Scenario: Software attack lets hackers send commands through the car's entertainment system.

Dashboard Functions

Steering

Brakes

Transmission



# Wired Vs. Wireless

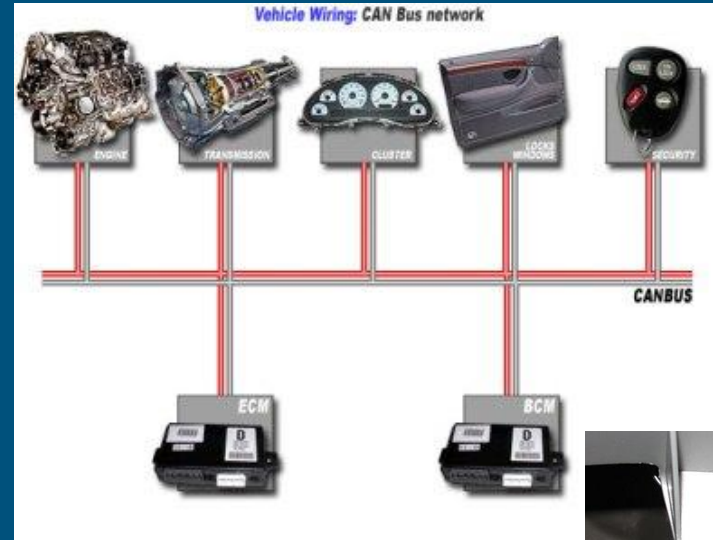
Attacker's PC connect into car's onboard diagnostic port.

Recent two years, carjacking has been through wireless.

# Security Measures Employed in Automotive

## Isolation and Access Control

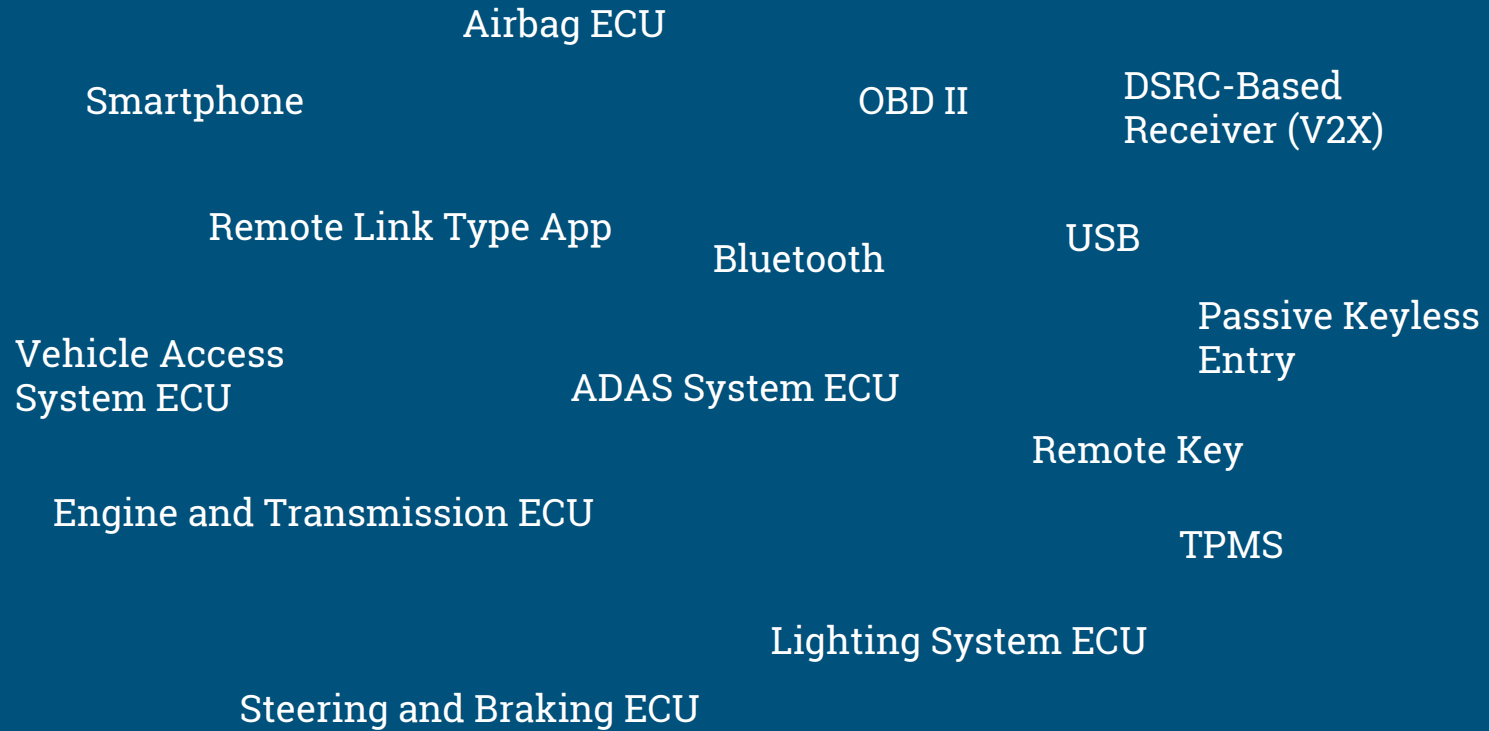
- The driving component should be restricted from communicating with non-driving component
- Attackers only need access to the CAN (Controller Area Network) bus to take control of the car (indirectly or directly)
- The OBD-II port in almost all cars provide an easy access to the CAN bus network
- Communication from outside source should be blocked

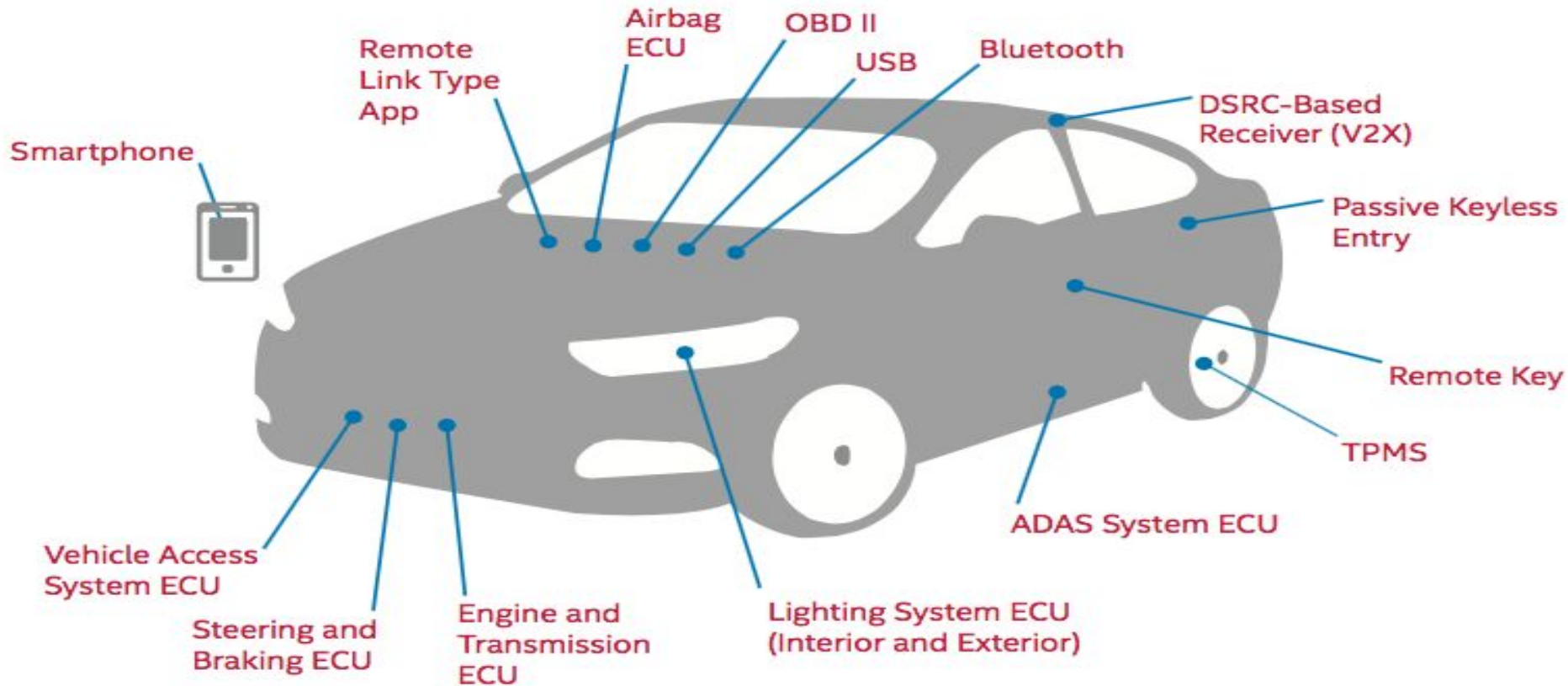


# Hacking a Jeep Through a Cellular Network

- 2015, Chrysler recalled 1.4 million Jeep for this vulnerability
- The jeep are constantly connected to Sprint cellular network
- The researcher broke into the Sprint network to connect to a specific jeep
- Upon gaining access to the the jeep multimedia system, they discovered it can't communicate directly with the CAN bus (due to the isolation between the two system), but it can communicate with another component (V850 controller) connected to the CAN bus
- Took over the V850 controller by changing its firmware through the multimedia system's controller (No authentication done to check if firmware is legit)
- Is now able to remotely control every component of the car







**Figure 2.** Fifteen of the most hackable and exposed attack surfaces on a next-generation car.



# Example

Play music

Climate control system

Turn on/off windshield wipers

Accelerate or Decelerate your car



“Remember to lock your car is no longer sufficient advice to protect your vehicle.”

-- U.S. Senator Edward Markey's Tracking & Hacking report on gaps in automotive security and privacy.

# Importance of Automotive Security?

Driverless car is soon approaching, and they must be secured enough to not be taken as hostage or be used as a weapon.

To protect lives.

5th AUTOMOTIVE CYBER SECURITY SUMMIT

# Security Threats Automotive Faces

---

- Replay Attacks

- DoS attacks

- False/modification of Messages

The three above affect the communication system between cars

- Remote Attacks (bluetooth, Wi-Fi, cellular, radio)

- Direct Attacks (USB port, OBD port)

- Malware (although no reported malware yet)



# Airplane hacked from passenger seat in 2015

- Chris Robert cause the plane to fly sideway by causing a engine to climb
- Accessed the seat electronic box underneath the seat and connected his computer to the in-flight entertainment system
- Accessed the plane's Thrust Management Computer using default ID and password
- Tom Patterson, chief trust officer at Unisys *"One of the key points is to look at weight. In the old days, in-flight avionics were a completely separate system – they were on wires, on controllers, everything was separate. It would have been very difficult for an attacker to jump in there. What's happening now is, to lighten the planes, more systems are sharing common wires and common controllers."*



## The Car Whisperer

---

- 2005, security experts were able to connect the Bluetooth in-car system to their Linux computer.
- can be used to record or inject audio
- take advantage that most handsfree in-car Bluetooth uses the same 4 digit security keys (0000 and 1234 in most cases)
- Normal range of Bluetooth is limited in distance, but can be extended to a mile by Bluesniping

## 100 Cars Remotely Disabled by a Former Employee

- A hacker broke into a car dealership server containing all of its customer car data and remotely shut down by overriding the vehicle-immobilization system on many cars and set many cars alarm to go off
- The hacker was a former employee of the car dealership and was laid off a week before, and still had access to another employee account
- Attacks stopped when the dealership reset all its account passwords, and the IP address of the hacker was traced
- Fortunately, the system is unable to shutdown while a car is running so nothing serious happened

# Nissan Shutdown App that Allowed Potential Hacker to Control part of the Car

-Affected Nissan Leaf cars, through the use of Nissan app that let the car owner know the battery status, record driving info and has climate control functionality

-By just knowing the Vehicle Identification Number, anyone can accessed the driving record of any Leaf car in the world and be able to operate the car climate control

-The vulnerability was that the API didn't verify that the person sending the GET request is indeed the car owner (doesn't do any further authentication after the initial login)

-Doesn't affect driving controls, but the driving records can be used to build a profile, or drain the car battery by turning on climate control



# Security Measures Employed in Automotive

---

## Authentication

- Through car keys, password, or biometrics
- Verify that any communication is coming from approved trusted source
- Protecting communication from being spoofed, recorded and used in replay attacks
- Verify that any update to its firmware is genuine
- Detecting tampering of files by checking digital signature and product key



# Security Measures Employed in Automotive

---

- The ability to update and fix newly discovered vulnerabilities
- Antiviruses
- Encryption
- Recovery mechanism in an event of an attack



# Question 1

---

Which choice is not hackable and exposed on a next-gen car?

- A. Smartphone
- B. USB
- C. Bluetooth
- D. Radio

# Question 1

---

Which choice is not hackable and exposed on a next-gen car?

- A. Smartphone
- B. USB
- C. Bluetooth
- D. Radio**

## Question 2

---

Which one of the following is not an authentication method mentioned earlier?

- A. Passwords
- B. Key
- C. Custom Firmware
- D. Biometrics

## Question 2

---

Which one of the following is not an authentication method mentioned earlier?

- A. Passwords
- B. Key
- C. **Custom Firmware**
- D. Biometrics

## Question 3

---

Why is Automotive Cybersecurity becoming more important?

- A. Aliens
- B. Technological advancement
- C. Hackers
- D. General Safety

## Question 3

---

Why is Automotive Cybersecurity becoming more important?

- A. Aliens
- B. Technological advancement**
- C. Hackers
- D. General Safety

THANK YOU!



# References

---

- <https://www2.deloitte.com/us/en/pages/manufacturing/articles/automotive-cybersecurity-tech-safety-net.html>
- <https://www.mcafee.com/es/resources/white-papers/wp-automotive-security.pdf>
- <http://www.oneminuteinfo.com/2014/02/can-bus-obd-ii-explained-for-dummies.html>
- <https://blog.kaspersky.com/blackhat-jeep-cherokee-hack-explained/9493/>
- <http://www.independent.co.uk/news/world/americas/computer-expert-hacks-into-plane-and-makes-it-fly-sideways-according-to-fbi-10256145.html>
- <http://www.techworld.com/security/is-it-possible-hack-plane-3644970/>-<http://computersecuritypgp.blogspot.ca/2016/02/what-is-car-w-hisperer.html>
- <https://www.wired.com/2010/03/hacker-bricks-cars>
- <http://blog.caranddriver.com/nissan-blocking-leaf-smartphone-app-due-to-security-flaw/>
- <http://ieeexplore.ieee.org.ezproxy.library.yorku.ca/document/7568882/>
- <http://www.gao.gov/assets/680/676064.pdf>