Automotive System Security

CONNOR PATCHEN AND JADYN MOORE

History

- In the early 1900s, the removable steering wheel was introduced
- In the early 1920s, we see the first instance of locks on doors. While they were easy to pick, this would be a vital invention for the future of cars
- Electronic ignitions were introduced in the 1940s, offering a more reliable driving experience
- Moving into the late 60s, Volkswagen released the first car with an engine computer
- In 1968, the cassette player developed by Philips was added to vehicles
- Connected cars, introduced in 1996 by GM used the owner's cell phone to call 911 in an accident
- Tesla autopilot was introduced in 2014 consequently launching a widespread development of self-driving technologies

Innovations

Early 1970s

While the airbag was introduced in the early 1970s, there was no monitor to know when the seats were empty, or if a child was occupying the space. Mercedes developed a sensor to detect both in 1997.

1992

Headlights were improved greatly in 1992, with the introduction of High-Intensity Discharge Lamps

1996

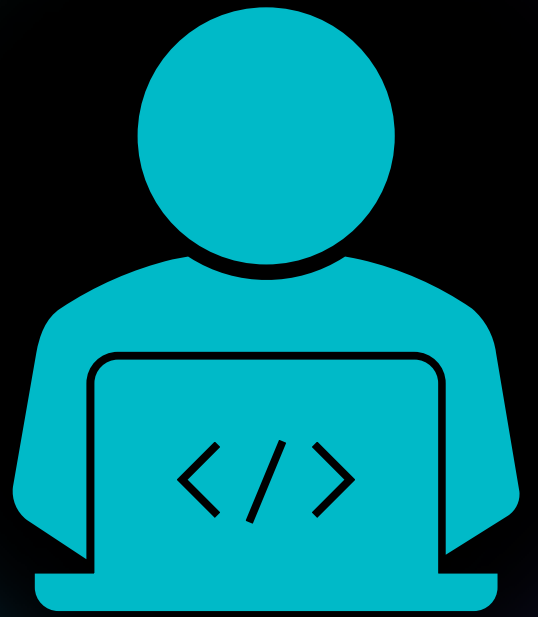
OBD II was a massive improvement between the car and the owner. Introduced in 1996, this second iteration of onboard diagnostics gave clearer instructions pointing to the direct issue within an engine

The Jeep Breach

- In 2015, two men named Charlie Miller and Chris Valasek breached a Jeep Cherokee
- Through an independent software development, they were able to remotely access the entire car
- While a simulated exercise, the probability raised some questions

10 Million U.S. Vehicle Owners' Personal Data Exposed

- Security researchers at Kromtech Security stated the leaked PII included customer names, addresses, dates of birth, and gender
- Researcher Bob Diachenko noted "sophisticated criminals have now created a way to combine traditional offline crimes like stealing cars and technology"
- This gives us a look into the rapid rise of car copying, a crime that has become increasingly popular in the past few years



David Bombal Interview

- Interviewee Sam Curry and his friends had an incredible independent study regarding the vulnerabilities of cars through mobile apps
- They began with hacking scooters at a college campus and were able to make hundreds of them go off at once, prompting their further digging
- For their breach of Mercedes-Benz, they created an account and could view internal dealer portals
- Through a GPS tracking service named Spireon, they were able to affect an estimated 15.5 million semi trucks using administrative privileges
- Land Rover owners in the United Kingdom are having increased issues with their ability to get insurance. This has forced owners to get greatly increased insurance rates due to insurance providers fearing allocating resources to such a commonly breached car

Pwn2Own Hacking Event

- There was one million dollars on the line to any team that was able to gain access to a Tesla's network.
- This is the most difficult car company to breach, but team Synacktiv was able to gain access twice.
- A total of $1,323,750 was awarded to multiple different teams who were able to create an astounding forty-nine zero-day attacks.
- Some of the devices that fell victim to the most hacks at the event included the JuiceBox 40 Smart EV charger, ChargePoint Home Flex, Ubiquiti Connect EV Station, Sony XAV-AX5500 infotainment system, and even Automotive Grade Linux.

Modern Standards

- ISO/SAE 21434 was created by the International Organization for Standardization in connection with the Society of Automotive Engineers.
- The National Highway Traffic Safety Administration (NHTSA) has laid out an extensive plan that they hope will be adopted across the country in order to better adapt to more autonomously driving vehicles on the road.
- Encouraged to be created by the NHTSA was the Auto-ISAC. Created in 2015, the Auto-ISAC allows the different motor vehicle companies to put aside their differences and share crucial security information.

Future Innovations

Car manufacturers and Governments are going to have to continue to innovate in order to keep up with malicious actors and newly created zero-day attacks.

Electric components of vehicles are susceptible to hackers using Bluetooth features or connecting a device via USB connection.

Companies like Tesla, GM, and Ford have begun to introduce hands-free highway driving.

A recent innovation that could become more commonplace in autonomous vehicles soon is a feature where someone calls their car to pick them up directly from their cellphone.

Future Innovations Cont.

- Secure updates are and will be necessary in order for cars and trucks to receive the correct software needed to operate and stay safe.
- Secure boot allows cars to scan their systems upon activation to make sure no malicious content has been installed in the car without the owners notice.
- Constant monitoring of the vehicles network is needed due to features such as the infotainment system. Some network connections include MACsec, IPsec, and TLS.
- The United Nations has created UNECE 155 and UNECE 156 that set recommended guidelines to follow in regards to automotive security.