Does the Cyber-Security of Driverless Cars Need to U-Turn?

An Overview of Cyber Threats to Driverless Cars, Solutions to these Threats and Issues Driverless Cars Face in the Future

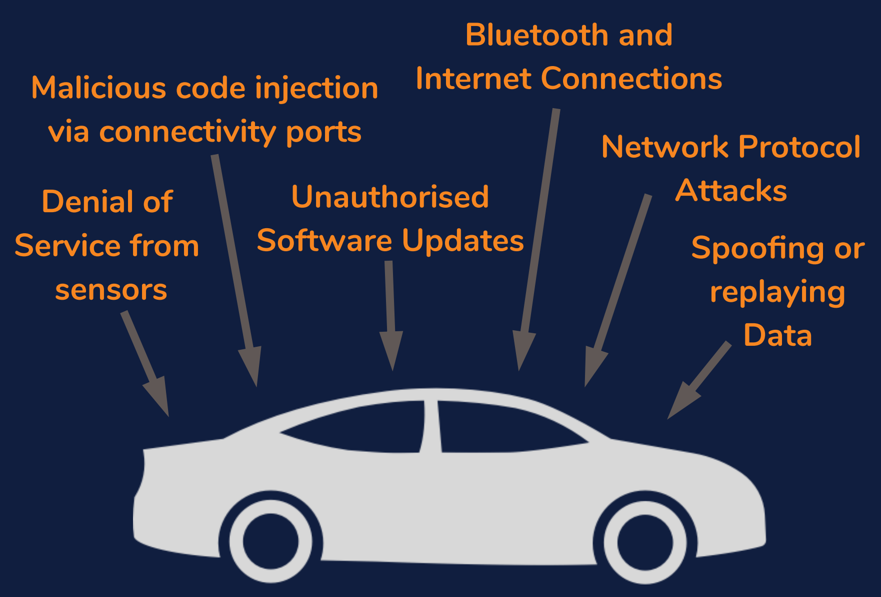
COM6017 - Security of Control and Embedded Systems
David CJ Kennedy

Introduction

Driverless cars are defined as a vehicle that is aware of its surroundings and moves with little or no human input. (Gehrig & Stein, 1999) A concept that once was only possible in films is now being fully utilised on roads all over the world with some driverless cars covering thousands of miles. A race is underway between car makers to develop and deploy more advanced automation systems. With the complexity of these systems and pressure to deliver before competitors, vulnerabilities could be being unknowingly added which Black Hat hackers could exploit.

Major Cyber Threats To Driverless Cars

Both driverless and modern cars share a major similarity; all systems are controlled by electronic control units (ECU's). These ECU's are specialised computers that are programmed to handle specific tasks. Driverless cars contain over 10 times more ECU's than standard modern cars, many of these ECU's are connected to the internet, external sensors or form part of a communication channel to other devices. (Miller & Valasek, 2015) Therefore they possess similar attack vectors to personal computers :



Bluetooth and Internet Connections

Malicious code injection via connectivity ports

Network Protocol Attacks

Denial of Service from sensors

Unauthorised Software Updates

Spoofing or replaying Data

Remote Access

In 2014 a team of researchers released details of a vulnerability in 1.4 million vehicles that contained Fiat/Chryslers UConnect system. The UConnect system was capable of using Sprints 3G network to connect to the internet and so anyone who knew the port and IP that the car was using, would be able to remotely send malicious data packets to the vehicle. The UConnect system is connected to the vehicles Controller Area Network which directly communicates with the ECU's. That manage adaptive cruise control, parking assist and collision warning systems. A hacker then has remote control access to features such as:

- The steering column
- Disable the brakes completely or apply the brakes
- Switch off the engine
- Control Radio and Seat Belt Tensioners

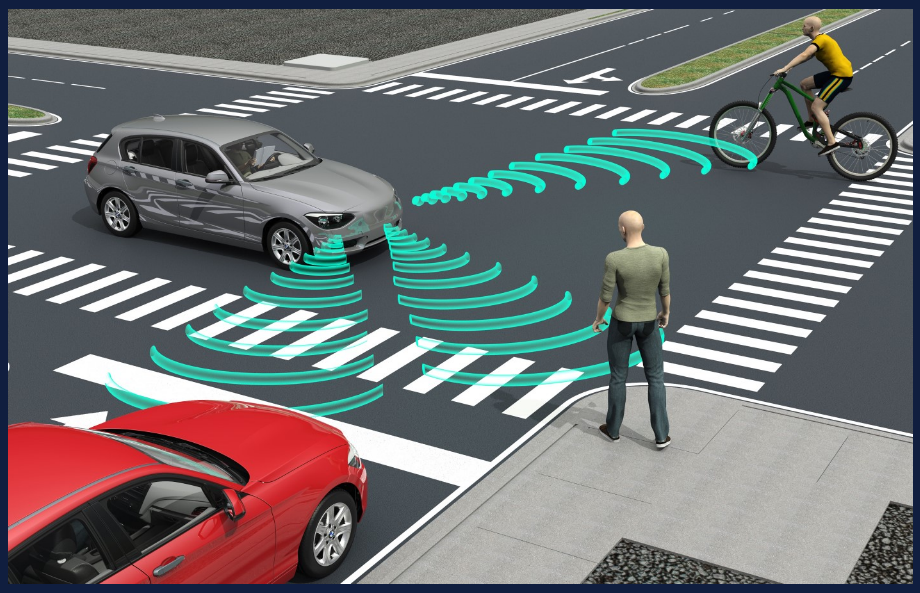
What was the Vulnerability in the Fiat/Chrysler Hack?

The main vulnerability in UConnect was that there was no robust method to determine whether data on the network originated from trusted sources. Network packets are assigned a count that increases by 1 for each packet. Each packet of data could be critical in making correct decisions about the status of the car.

Any delay in data transmission would lead to late arriving signals that are required for example, to stop the car because there is a person in the road. This is the reason why a counter was used as authentication, any complicated and robust authorisation methods could slow the reaction of the vehicle to hazards and obstacles.

Close Proximity Attacks

The Fiat/Chrysler hack is by far the highest profile and most remote attack seen on driverless cars, but there are many more vulnerabilities that can be exploited with physical access to the vehicle or initiated from a close proximity. Driverless cars use numerous sensors such as LiDAR, Ultrasound and RADAR to build a digital picture of the vehicles surroundings. (Petit et al., 2015)



Demonstration of how the sensors on a driverless car recognise obstacles. Pulses are emitted from the vehicle in all directions. If there is an object, the pulse is reflected and received by the car. The car can then determine the distance of the object.

All these sensors work by emitting electromagnetic waves and recording the distance of obstacles from reflections. To send false information to the vehicle these reflections can be spoofed, jammed or muted. In 2016 a Tesla Model S with autopilot engaged crashed into a truck killing the driver, the crash was caused by the autopilot system failing 'to notice the white side of the trailer against the bright blue sky'. (Tesla, 2016) This situation was caused by a rare natural phenomena but it shows that false data arriving from sensors can be deadly. Manual exploits of self driving car sensors have been demonstrated by:

- Replaying recorded LiDAR reflections to mimic objects. (Petit et al., 2015)
- Using IR materials that absorb electromagnetic waves, so objects appear invisible to sensors. (Veil, 2017)
- Generating pulses that cause destructive interference.

All these exploits require some sort of knowledge about how electromagnetic sensors work, driverless cars can simply be exploited via injecting malicious script files through the USB or ODB-IT ports. For this to happen you need access to the car but a rogue mechanic or valet could do this. Especially if financial gain via Ransomware was possible. (Palanca, et al., 2017)

Solutions to Threats

It is far harder to defend from attacks than it is for attackers to compromise systems. In data centres exploits could lead to loss of data in driverless cars it could lead to loss of life. A major solution into stopping would be attackers from exploiting vulnerabilities is to offer 'bug bounties'. Tesla has been doing this for many years with rewards ranging for $25 up to a Tesla Car. (Rapier, 2019) If all driverless car makers used similar schemes, then even if exploits are found they can be patched before being made public.

The major threat to the concept of driverless cars is remote control of the vehicle such as in the Fiat/Chrysler hack. The solution to this hack was to stop all incoming TCP/IP packets and Sprint blocked traffic on the ports used by the vulnerable vehicles. (Miller & Valasek, 2015) This solution limits who can connect to the vehicle but the exploit remains locally as the ECU's remain linked to connectivity ports. A better solution would be to disconnect the driving segment of the vehicle from the internet or localising data like in military systems which ensure unauthorised users cannot send data on the network. (Palanca, et al., 2017) (Kumar & Koti, 2018)

Petit et al, (2015) explains how sensors are the primary input to driverless cars and that bad inputs lead to bad decisions. Multiple methods have been proposed to limit how sensors can be exploited, all these methods attempt to reduce the predictability of electromagnetic waves and receivers:

- Combining multiple wavelengths, restricting the ability to capture all the signals at the same time.
- Use measurements taken from multiple nearby vehicles in decision making.
- Randomly changing the pulse period to stop synchronisation to sensors.

Future Challenges

Future driverless cars may not have any manual controls, for this to be the case the idea of sharing data from nearby vehicles could allow for an almost Block-Chain like system where other vehicles could identify, control and even stop exploited vehicles from causing damage. The morality of hacking vehicles is also questionable, would a hacker really want to cause death or rather create Ransomware that locks you out of your car and demands a fee to get

References

Gehrig, S. K. & Stein, F. J., 1999. *Dead reckoning and cartography using stereo vision for an automated car.*. s.l., s.n., pp. 1507-1512.

Kumar, A. & Koti, C., 2018. *A Brief Survey on Autonomous Vehicle Possible Attacks,Exploits and Vulnerabilities,* s.l.: arXiV.

Miller, C. & Valasek, C., 2015. *Remote Exploitation of an Unaltered Passenger Vehicle.* Las Vegas, s.n.

Palanca, A., Evenchick, E., Maggi, F. & Zanero, S., 2017. A Stealth, Selective, Link-layer Denial-of-Service Attack Against Automotive Networks. *DIMVA*, 4 June, pp. 185-206.

Petit, J., Kargl, F., Stottelaar, B. & Feiri, M., 2015. Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and Lidar, s.l.: Black Hat Europe.

Rapier, G., 2019. Tesla will give you a free Model 3 if you can hack its computer system. [Online] Available at: https://www.businessinsider.com/tesla-model-3-reward-bug-bounty-research-program-2019-1?r=US&IR=T

Tesla, 2016. A Tragic Loss, s.l.: s.n.

Veil, 2017. Anti-Laser Stealth Coating. [Online] Available at: https://www.stealthveil.com/faq [Accessed 23 April 2019].