Autonomous Cars – Evaluation of Security Countermeasures

Aislinn Limbird - Supervised by: Konstantinos Markantonakis and Raja Naeem Akram
Information Security Group, Smart Card and IoT Security Centre

The Smart Card and Internet of Things Security Centre

Objectives

Autonomous and connected vehicles will be a part of reality in the near future. These vehicles are a collection of complex and sophisticated computational architectures. Cybersecurity is among many challenges that an autonomous and connected vehicles face.

- More research into the field
- A thorough study and evaluation of their security mechanism need to be carried out. For evaluation, pen testing of the protection mechanisms is vital.
- The aim is to evaluate the security and privacy measures of the given subsystem.

Introduction

Autonomous cars is a rapidly expanding technology it has moved from the science fiction world onto the road. Autonomous and connected vehicles will be operating in close proximity to the general public. This requires strong assurances regarding the safety and reliable operations of such vehicles. The consequences of getting it wrong can be life and death.

Cars have a varying degree of autonomy. But even within systems as simple as a keyless starts and cars, the Fobs have proven to be vulnerable to hacking.

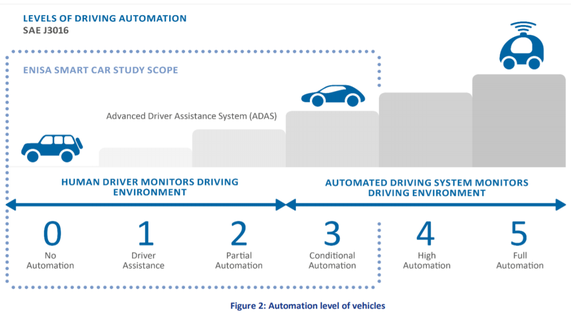
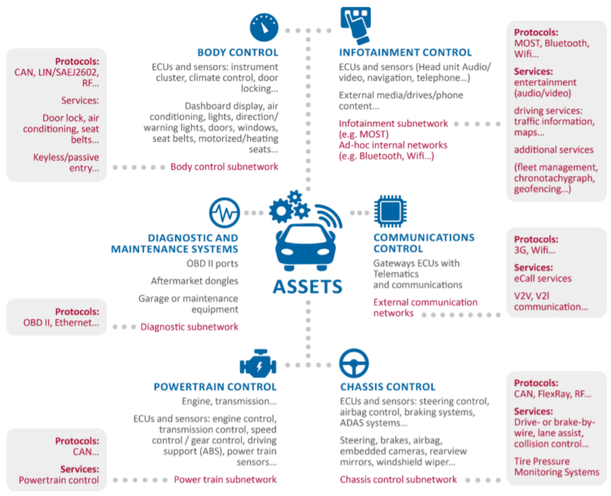


Figure 2: Automation level of vehicles

Attack Vectors of AVs



Vunerabilities of Infotainment

Remote Attacks
Exploit vulnerabilities in the system to gain access to vehicle system. In Bluetooth, WiFi or even multimedia files

Safety Attacks
Infotainment ECUs and networks may also cause safety issues: incorrect navigation data may lead the car to unsafe areas, and a disturbance of the audio in the entertainment system

Surveillance
All wireless emissions: Wi-Fi, Bluetooth and GSM/3G/4G signals can be used to uniquely identify a vehicle e.g. Most TPMS systems, when they are active, broadcast a unique RFID identifier or when the WiFi hotspot function is active it broadcasts its own SSID.

Testing Lab Setup

Specific hardware & software was configured to create a testing lab required for the practical research.

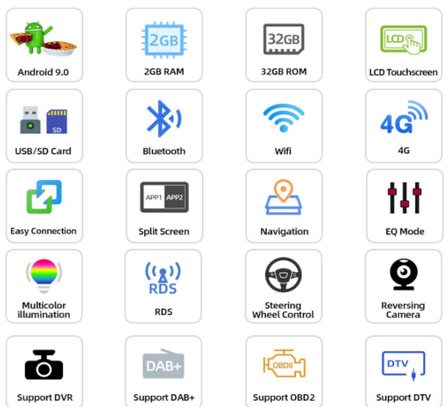
Lab environment:

- Infotainment System running on Android 9 one of the big players in infotainment system operating systems

Pen Testing my System

I have begun to test my system for vunerabilities. The first i am going to look at is bluetooth. Then GPS attacks mainly spoofing. I am also going to research the current attack opportunities in Android 9.

If i can i hope to utilise the vehicle steering part of the infotainment system to cause a vunerabiliy that would be a real safety concern.



Further Research

The next attack vector in AV I hope to target is the CANBUS system. This will prove to be a little harder to set up in a lab environment.

References

- SAE International Surface Vehicle Recommended Practice – Cyber Security Guidebook for cyber physical systems
- ENISA Cyber Security and Resilience of smart cars: Good practices and recommendations
- Kevin Brimshaw Autonomous cars: Past, present and future a review of the developments in the last century, the present scenario and the expected future of autonomous vehicle technology.
- Autonomous vehicle safety: An interdisciplinary challenge. Philip Koopman; Michael Wagner
- Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. Simon Parkinson ; Paul Ward ; Kyle Wilson ; Jonathan Miller
- Autonomous Vehicle Security: A Taxonomy of Attacks and Defences. Vrizlynn L.L. Thing ; Jiaxi Wu
- Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. Taeihagh, Araz, Lim, Hazel Si Min
- Potential Cyberattacks on Automated Vehicles. Jonathan Petit ; Steven E. Shladover
- CyberSecurity considerations for an interconnected self-driving car system of systems. Jeremy Straub ; John McMillan ; Brett Yaniero ; Mitchell Schumacher ; Abdullah Almosalami ; Kelvin Boatey ; Jordan Hartman

Acknowledgements

Konstantinos Markantonakis @ RHUL
Raja Naeem Akram @ RHUL

Contact Information

- Email: zeac005@live.rhul.ac.uk
- Phone: 07879738829
- LinkedIn: www.linkedin.com/in/ashlimbird/