ROYAL HOLLOWAY UNIVERSITY OF LONDON

Driverless Vehicle Security: Considering Potential Attacks and Countermeasures for Military Applications

Nicola Bates - Supervised by: Raja Naeem Akram
Information Security Group, Smart Card and IoT Security Centre

The Smart Card and Internet of Things Security Centre

Objectives

To gain an overview of the civilian Autonomous Vehicle (AV) environment and apply this to a military setting. Specifically:

- To complete a review of attack techniques that have been attempted or which are theorised
- Investigate potential countermeasures to the attacks identified
- Apply knowledge from civilian sources to complete a risk assessment in a military scenario

Introduction

A modern vehicle requires effective operation of 70-100 Electronic Control Units (ECUs) to maintain function and safety and is governed by around 100 million lines of code [1]. This number is likely to grow by an order of magnitude in AVs with all systems needing to be robust and free from defects.

Vehicles which are fully autonomous are not yet available for the public to purchase, although the Tesla Model S can be bought with all the hardware needed to become so. Waymo operating in Phoenix, Arizona cannot be considered at a level 5 autonomy either, with taxis still required to have a safety driver behind the wheel, a 'human in the loop' if and when required.

There are predictions that the army will get fully AV technology before civilians. This report focuses on a desert supply-line setting in a warzone to analyse risks and countermeasures using civilian data available.

Security Assessment

Security Level (SL)		Impact Level (IL)				
		0	1	2	3	4
Threat Level (TL)	0	QM	QM	QM	QM	Low
	1	QM	Low	Low	Low	Medium
	2	QM	Low	Medium	Medium	High
	3	QM	Low	Medium	High	High
	4	Low	Medium	High	High	Critical

Securtiy level assessment table [2]
TL: Estimation of the 'liklihood' of a risk being realised
IL: The 'effect' if a risk is realised

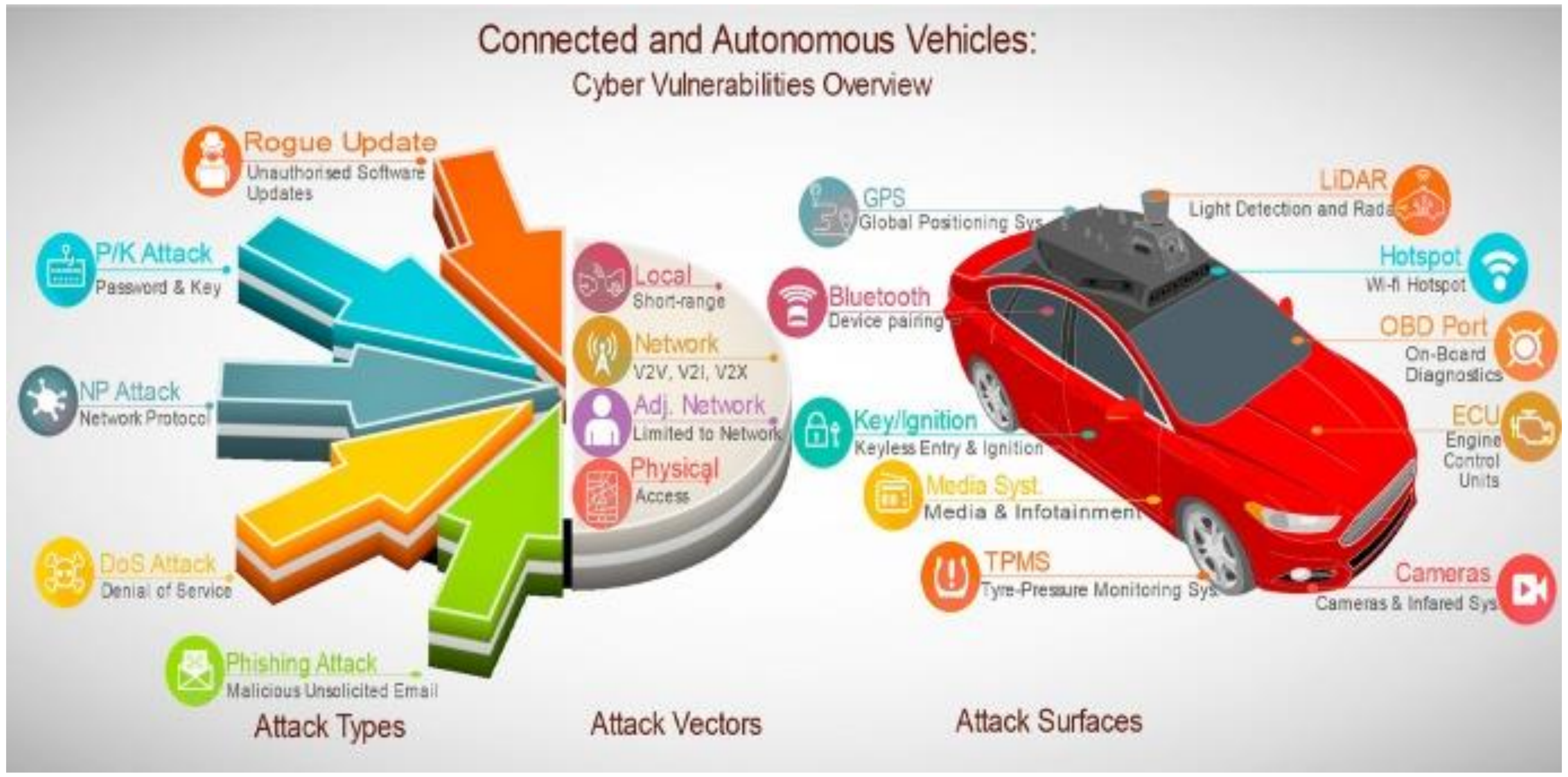

Figure 1: An overview of types of attacks, attack vectors and attack surfaces [3]

Risk assessment based on attack objectives with countermeasures

Attack objective	How the attack is achieved	Threat Level	Impact Level	Security Level	Countermeasures to the attack
Capture a vehicle	Person walks in front of the AV	4	2	High	Algorithm tailored to a warfare situation so AV does not stop in warzone for people or stops if signs of surrender given. Problems exist with both options.
Capture a vehicle	Flat tyre spoofed to force the AV to stop or slow down	2	2	Medium	Use Bluetooth instead of radio which has shorter range and physical wires for redundancy. Data fusion is a challenge, extra sensors used if conflicting data.
Poison other units	Return a captured AV to base containing malware to poison other units when plugged into the OBD port	1	4	Medium	Malware check on OBD port. Technicians check AV movement history before plugging into the central system. Have fleet separation between garages.
Cause confusion and break command	Mission data altered	2	3	Medium	Have W-Fi, mobile and radio communication making spoofing attacks harder to achieve if multiple, independent data sources providing information.
Surveillance	In vehicle discussions of troops obtained	4	2	High	Remove infotainment system. Have isolated system if troops being moved but without microphones or recording data to stop information leaks from troops.
Surveillance	A history of the AVs recorded movements obtained	4	2	High	Wipe history of vehicle movements from GPS after every mission. Add permanent random data to act as noise to hide current mission locations.
Disable or destroy an AV	Force a stop by jamming or spoofing visual sensors to detect and object in front of the AV	2	2	Medium	Additional visual sensors of different type (cameras, radar, sonar, LiDAR). Use of platooning, swarming and /or aerial drones to give further redundancy.
Disable or destroy an AV	Jamming primary sensor to force the AV into a 'safety stop'	2	2	Medium	Remove infotainment unit. Have a separate CAN bus network to reduce attack surface available to access safety critical devices.

Results

Attacks rated as 'high' are: bringing the vehicle to a standstill by walking in front of it, turning microphones on to listen to troop discussions and extracting movement history from the vehicle.

Civilian versus Military AVs

Similarities between civilian and military AVs:

- Interoperability between AVs and countries vital
- Conventional physical attacks are still possible
- Privacy of data collected by the AV required

Differences in military AVs from civilian AVs:

- Environment is extreme, hostile and unmapped
- Specialised equipment with more niche designs
- Deliberate attack is a focus of the enemy
- Cost per vehicle higher and total number less
- Vehicle life higher and models change less often

Conclusion

The highest rated attacks were surprisingly simple.

Many attacks can be prevented by having redundancy in the system with multiple sensors covering the same data point. If conflict exists in sensor readings, the best action to take maybe difficult to determine, however.

To reduce attack surfaces, the infotainment system was removed with safety critical ECUs separated from non-critical ECUs using a separate CAN bus.

The decision to add or remove sensors and security is a constant dilemma. Cryptographic authorisation and authentication mechanisms come at the expense of functionality and speed for example.

How an AV reacts if a person steps in front of it requires further research as does how advanced technology can be destroyed if captured by an enemy.

References

[1] R. Charette, (2009, February 1). "This Car Runs on Code," IEEE Spectrum
[2] (2016, January). "Surface vehicle recommended practice: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems," SAE International..
[3] B. Sheehan, F. Murphy, M. Mullins and C. Ryan, (2019, June). "Connected and Autonomous Vehicles: A Cyber-Risk Classification Framework," Science Direct, vol. 124, pp523-536.

Contact Information

email: nicola.bates.2018@live.rhul.ac.uk