Driverless Vehicle Security for Military Applications

Authors
Nicola Bates, MSc (Royal Holloway, 2019)
Raja Naeem Akram, ISG, Royal Holloway

Abstract

Existing attacks and risk assessment frameworks within civilian Autonomous Vehicles (AVs) can be used to review security of military AVs deployed for logistics purposes in a desert warzone environment. This article examines how suitable these frameworks are for the military logistics AVs. Furthermore, we examine the threats considered from the point of view of what an enemy would like to achieve as opposed to a device-based attack strategy so as to identify critical weaknesses and countermeasures to these. [a]

[a] This article is published online by Computer Weekly as part of the 2020 Royal Holloway information security thesis series `https://www.computerweekly.com/ehandbook/Royal-Holloway-Driverless-vehicle-security-for-military-applications`. It is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full thesis is published on the ISG's website at `https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/`.

Introduction

Since 1975 the development of integrated circuits and microprocessors made it possible to mass produce driver assist Electronic Control Units (ECUs). Modern cars can have up to one hundred of these ECUs which provide capabilities such as cruise control, power steering, engine management, stability control and tyre pressure sensors. In the majority of cars these ECUs are linked with a Controller Area Network (CAN) bus design allowing communication between all parts of the system which paved the way for autonomy.

Such autonomous technology promises fewer road traffic accidents, a reduction in greenhouse gas emissions and a more efficient use of busy civilian road networks as well as opportunities within the military to reduce exposure of troops in warzones. However, interconnectivity combined with complicated autonomous functions requiring hundreds of millions of lines of code poses a considerable counterbalance to the socioeconomic benefits envisioned.

Levels of Driver Autonomy

To assist in classifying the levels of autonomy a formal scale has been designed by SAE International. Level 0-2 describe driver support features which require a human driver to monitor the environment with levels 3-4 consisting of an automated system to monitor the driving environment. Level 5 is considered to be fully autonomous with the system taking on all driving modes.

0	1	2	3	4	5
No Automation	Driver Assist	Partial Autonomy	Conditional Autonomy	High Autonomy	Full Autonomy
All driving operations are performed by a human, e.g., braking, speed, steering etc.	Vehicle has one automated area, e.g., cruise control to monitor speed.	Vehicle able to take over steering and speed but a human can take control and monitors.	Vehicle can complete most driving areas but human override is still needed.	Vehicle can complete all driving tasks under certain conditions but has a human override option.	Vehicle does all driving tasks in all conditions with no human interaction needed.
Human Monitors Driving Environment			Automation Monitors Driving Environment		

Focus of Study

Our study focussed on supply line AVs in a warzone responsible for getting food, troop and other equipment to the front line. It will be assumed supplies will be through desert terrain so will have uneven ground but fewer physical obstructions which represents the terrain most suited to early adoption. These vehicles are likely to be in less hostile territory than other areas of use, so the opportunities for level 5 autonomy - as considered in this work - are higher and likely to be deployed sooner than other more complex and hostile environments. The amount of activity from civilian automotive players such as Google, Apple and Tesla as well as university researchers will also give attack information needed to map to a military setting.

Key Similarities and Differences in Civilian and Military AVs

When assessing AV security we also need to consider the similarities and differences in environments between civilian and military applications. This allows a more informed risk assessment to be completed using the information from civilian sources and also helps to identify countermeasures which could be implemented to mitigate against these risks.

Similarities:

- **Interoperability**: Interoperability is required in both civilian and military applications, to enable seamless travel between states or countries in the civilian case, and in the military for coordinating coalition forces.
- **Attack resistance**: There will still be the ability to attack AVs in conventional physical ways in addition to cyberattacks.
- **Privacy**: With level 5 autonomy requiring a wealth of information to operate the need to protect confidential data will be required.

Differences:

- **Environment**: In civilian settings manoeuvres through cities with narrow lanes, signals, pedestrians and various road markings are commonplace. Within the military terrain maybe unmapped, uneven with changing routes due to artillery damage.
- **Specialised**: The basic structure of civilian vehicle models will be quite similar whereas military equipment could be highly specialised and require complete redesign due to niche operations.
- **Attack threat**: Deliberate attacks on military vehicles are a major focus of an enemy combatant which is also likely to be the case for cyberattacks. This is not seen in a civilian environment with driver error currently the cause of most fatalities.
- **Costs**: There are currently over a billion civilian vehicles globally on the road, while military units only number in the tens of thousands. This results in costs borne by fewer units which, in addition to niche uses, increases cost per unit for military AVs.

- **Life expectancy**: A higher life expectancy and timescales for model changes seen in the military has implications for technology updates.

Risk Assessment

To assess risk, we used a rating for threats and impacts which together are used to give a final security level score. The threat level corresponds to an estimate of how likely it is a threat will be realised with expertise, system knowledge, opportunity window, equipment needed, and cost of attack feeding into this rating. For the impact level safety, financial, operational, political and, privacy and legislation impact are assessed.

A sample of attacks analysed is shown in the table with all low and some medium rated attacks removed to aid clarity. The three key areas to attack, which were rated as 'high' are:

- Bringing the vehicle to a standstill by walking in front of it.
- Turning microphones on to listen to troop discussions.
- Extracting movement history from the vehicle.

Attack objective	**How the attack is achieved**	**Security level**	**Countermeasures to the attack**
AV Capture.	Person walks in front of the AV.	High	Algorithm tailored to a warfare environment so AV does not stop in particular zone of operation for people or stops if signs of surrender given. Problems exist with both options however.
AV Capture.	Flat tyre spoofed to force the AV to stop or slow down.	Medium	Use Bluetooth instead of radio which has shorter range and physical wires for redundancy. Data fusion is a challenge if the extra sensors used give conflicting data.
AV used to poison other units.	Return a captured AV to base containing malware to poison other units when plugged into the diagnostic port.	Medium	Malware check on diagnostic port. Technicians check AV movement history before plugging into the central system. Have fleet separation between garages.
Confusion and break command.	Mission data altered.	Medium	Have Wi-Fi, mobile and radio communication making spoofing attacks harder to achieve if multiple, independent data sources are providing the information.
Surveillance.	In vehicle discussion of troops obtained.	High	Remove the infotainment system. Have an isolated system if troops are being moved but without microphones or recording data to stop information leaks.
Surveillance.	A history of the AVs recorded movements are obtained.	High	Wipe the history of vehicle movements from the GPS after every mission. Add permanent random data to act as noise to hide current mission locations.
Disable or destroy AV.	Force a stop by jamming or spoofing visual sensors to detect an object in front of the AV.	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 AV.	Jam primary sensor to force the AV into a 'safety stop'.	Medium	Remove infotainment unit. Have a separate CAN bus network to reduce attack surface available to access safety critical devices.

As with any risk assessment it should be noted that this shouldn't be seen as static. Threat landscapes can change, for example, through technology becoming more widely available or devices needed to

perform an attack becoming cheaper. Not only that, but the impact of an attack could change, for example, if AVs were operating in a particularly financially or politically constrained environment.

Countermeasures to Attacks

Despite all resource and complexity levels available to an enemy in a potential attack it was noted that the most feasible and impactful attacks were surprisingly simple and low tech. For the majority of vehicle outings considered, only cargo is transported which means certain systems that pose intrinsic risk in civilian use, such as the infotainment system, could be removed, decreasing the attack vectors and making the AV more secure.

In terms of an AV stopping for people within a battlefield, the algorithms required for a military setting will need to be adjusted from those used in a civilian environment. All that is needed to stop a military AV would be for a person to step in front of it causing it to become a 'sitting duck' ready for capture. How the artificial intelligence will deal with this situation is crucial in military AV deployment given it has the potential to cause 'friendly' casualties as well as undermining faith in the technology.

Military AVs will need extra means of protecting the technology in case they are captured by the enemy. The possibility of an enemy reverse engineering technology and using this against allies later is obviously not desirable. Information on the devices would also need to be carefully protected so allied locations or mission critical data could not be determined from the vehicle.

The subject of redundancy is evident in countermeasures to sensor attack from jamming and spoofing. Cameras, radar, sonar, ultrasonic and LiDAR all benefit from having redundancy not only within their own technology but also by using overlapping technologies from different wavelengths. Using other sources of data increases costs but is worthwhile as it significantly improves the decision making and thus safety of an AV. This option is likely to be more available to military vehicles where cost per unit is less of a hindrance. One challenge, however, is how the fusion of all these data sources can be done in order to converge to the most appropriate action.

In the military, regular servicing, especially in a harsh desert environment, would allow for most updates to be done by a technician at a garage. That is not to say that over the air update facility could be disabled, since redundancy is desirable in situations where vehicles could be away for long periods, unable to connect to a physical update source.

The dilemma between removing and adding systems and sensors is a constant juggling act. So too is the decision to add extra security, such as cryptographic authorisation and authentication mechanisms at the expense of technology functioning and speed. A downside of these countermeasures is the increase in computation overhead in time and power.

Before countermeasures are employed the knock-on effect of other parts of the system also need to be considered. These may not always have the desired effect of reducing risks everywhere and could even cause risk to increase by taking away a level of redundancy. Sometimes countermeasures would improve security but the amount of cost and time this would require to be baked into the design from the start would be restrictively high, a situation seen in CAN bus separation options.

Conclusion

When reviewing published attacks on civilian AVs it was noted that they are very similar in sophistication to those which have been performed on computer systems before. In some ways this is not surprising, with AVs being an emerging technology, add-ons have been made to existing vehicle designs which themselves are not particularly secure. Vehicles are experiencing a revolution in connectivity and the lessons learnt from similar advances in everyday computing can be applied by having security integral to the design.

One of the highest rated attacks simply involved a person walking in front of a military AV to make it stop and allow its capture. In a civilian setting this would be an essential feature and would save many

lives. However, in a military scenario it has the potential to cost many lives and allow an enemy to capture the AV which would include the associated mission data and autonomous technology.

A key finding from the dissertation is that by linking all vehicle systems through the CAN bus gives the opportunity for a minor component to enable compromise of safety critical devices. The infotainment system can not only be used to leak troop discussions and vehicle movements but also connect to any ECU which is also connected to the CAN bus.

Simply refining the CAN design and security is difficult with initial design of a vehicle to scrappage being many years, and even more in a military setting. With AV capability being added to existing designs, this does not give the time window to rapidly respond to attacks and add more secure architectures. For the military a way of upgrading encryption and other systems mid-way through a lifecycle would therefore be highly desirable.

AVs will need the highest level of security with a 'secure by design' mindset being adopted, rather than adding on features to an existing vehicle. However, with military vehicles having a lifetime of around 20 years and with model changes approximately every 30 years security by design isn't always feasible with the ability to update security technology being more restrictive.

Fortunately for military AVs there exist a series of ways to mitigating attacks which do not easily exist within the normal civilian space. Supply line AVs may not carry troops making some systems redundant, and even simple changes such as troops having an infotainment system isolated from the safety critical devices would increase system security.

In addition to removal of vulnerable systems frequent service schedules permit software updates through physical, not wireless, methods which allow some of the most dangerous attack surfaces to be removed. The benefit of military budgets during active coonflict permits a luxury civilian AVs will not be able to afford in terms of duplication of sensors and systems creating levels of redundancy which can prevent all but the most sophisticated spoofing attacks. There is also military access to encrypted satellite networks for GPS communications.

Finally, whilst not recommended in this review, the nature of a military setting would permit an AV to be destroyed to defend against its capture. Should there be clear signs it was operating outside of critical parameters or capture was known, self-destruction would be a viable option, with commanders preferring the AV be destroyed than giving the enemy valuable information.

Further Considerations

Single-point of failure: Some militaries have multiple suppliers for various different types of vehicles, which ensures a level of redundancy if technical faults were found with any of the products. This could also be true in the suppliers of the technology so if an exploit is found in a particular algorithm, variety in systems would ensure not all vehicles have to be removed whilst the vulnerability is fixed. There would need to be a balance however between redundancy and the ability to keep technology secret across additional organisations.

Supply chains: Modern vehicles have parts manufactured by many different suppliers so how the security of every component within this supply chain can be assured poses difficult challenges.

Self-destruct mechanism: To prevent the enemy using software or hardware if captured a way of destroying AVs may be desirable. However, issues of having a single point of failure which the enemy could exploit or which could be used in error would need to be critically analysed first.

Swarming: This technology would rely on vehicle to vehicle communication and algorithms for 'intelligent' behaviour. This provides collective redundancy across sensors as well as added cooperation to be more effective than single units.

Interoperability: As cyberspace dependence increases so does the coordination this allows within the other domains of war, namely land, sea, air and space. Interconnection of these different domains of war as well as multiple coalition forces would need detailed risk assessment and secure by design practices.

Failure modes: In a military supply chain the ability to not fail catastrophically is an essential feature. If the AVs 'safe setting' is to return to base or not to move until fully functional this can be exploited. Research is therefore needed into 'fail safe' modes within a hostile environment.

Lethal uses of AVs: There has been a shift in research and technology towards use of lethal AVs, without a human in the loop. A risk profile for this type of technology would be significantly different from a supply chain scenario.

Final Thoughts

In a military setting there is the motivation to attack an enemy using cyber technologies, with increased cyber skills in many countries. Many articles and books point to the importance of cyberspace in future wars with cyber threats high on national security agendas.

The benefits of AVs could be revolutionary, but they need to be designed with security in mind from the outset. The current situation is summarised by Peter Davies of Thales who recognises that with all the complexities of AVs there is never going to be complete safety and we need to make sure when AVs do fail, they will be safe, and the system can recover.

> "[As] It is expected that AV will be compromised it is ensuring the failures aren't catastrophic and knowing how to recover from this when it occurs. The AV will only be safe if we have justifiable and enduring confidence they will do what is expected and when we want this."

Biographies

Nicola Bates received her MSc in information security from Royal Holloway, University of London in 2019 and is continuing her studies within the Centre for Doctoral Training. Prior to her MSc she read Physics at the University of Cambridge before becoming a member of the inaugural intake of the Teach First programme and then working for PwC predominantly within their Transaction Services division.

Raja Naeem Akram is currently a research assistant at the ISG Smart Card and IoT Security Centre, Royal Holloway, University of London. He is currently involved with research projects involving avionics and the banking sector. Previously, he has worked as a Research Fellow at the Cyber Security Lab, University of Waikato, and a Senior Research Fellow at Edinburgh Napier University.

Series editor: S.- L. Ng