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

Nicola Bates

Technical Report

RHUL–ISG–2020–1

22 June 2020

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Executive Summary

There is much interest from politicians and mainstream press about the driverless vehicle with a host of interested parties fervently researching into this technology. Autonomous Vehicles (AVs) promise mitigation of accidents, reduction in greenhouse gas emissions and more efficient use of infrastructure within the civilian world, as well as opportunities within the military to reduce exposure of troops in warzones. The automotive industry has a lot of work to do to secure these systems, however, if AVs are going to be seen on the road or deployed in a warzone in the not too distant future.

A modern vehicle is an extremely complicated cyber physical system requiring effective operation of between 70 and 100 Electronic Control Units (ECUs) to maintain function and safety governed by around 100 million lines of code [1]. This number is likely to grow by an order of magnitude with AVs with all systems needing to be robust and free from defects. Increased connectivity combined with autonomous functions allow for remote access for malicious hackers posing a considerable counterbalance to the socioeconomic benefits offered.

A major area which needs to be resolved may not be technological, however, but psychological. How civilians will take to this technology once available may be one of the biggest challenges, as negative reactions over the Waymo AVs in Phoenix, Arizona have shown [2]. Back in the 1900's 'self-driving elevators' were invented but widespread adoption was slowed for decades through people refusing to use them [3]. Within a civilian setting there are additional requirements for clear legislation and regulation with insurance liability issues to be resolved.

There are predictions that the army will get AV technology before cities do [4]. A military environment is more flexible in terms of regulations with the arena generally only governed by rules of warfare, which mainly cover humanitarian issues [5]. Added to reduced legislation in the military is the ability to order troops to work with autonomy without having a choice in the matter. In 2016 the US Department of Defence (DoD) stated they will "…exploit all advances in artificial intelligence and autonomy and insert them into DoD's battle networks" with the Pentagon budget released in September 2018 allocating $2 billion over 5 years for artificial intelligence technologies [6].

The purpose of this paper is to describe how AVs work and produce a comprehensive review of both realised and theoretical attacks within the civilian domain. This will give a view as to the types of vulnerabilities which may exist in a military setting, specifically supply line vehicles operating in desert warzone environment. A risk assessment will then be completed which takes as input attacks which would achieve specific enemy objectives. Using the outcomes of this work recommendations will be proposed for how the high and medium level risks identified could be mitigated against.

Analysis highlights the differences between technology requirements for a civilian setting and that which would be needed in a military arena. 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 this has the potential to cost many lives and allow an enemy to capture the AV – and the associated mission data and autonomous technology.

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, with security being included from the design phase. However, with military vehicles having a lifetime of around 20 years and with model changes approximately every 30 years [7] the ability to update security technology is more restrictive.

A key finding from the report is that by linking all vehicle systems through the Controller Area Network (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. Supply line AVs may not carry troops making this system redundant, and even simple changes such as troops having an infotainment system isolated from the safety critical devices would increase system security.

Fortunately for military AVs there exist a series of countermeasures and means of mitigating attacks which do not exist within the normal civilian space. In addition to removal of vulnerable systems frequent service schedules permit software updates through physical, not wireless measures which allow some of the most dangerous attack surfaces to be removed. The benefit of military budgets, during active conflict, 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.

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.