SECURE CAV

Advanced cybersecurity for connected and autonomous vehicles

COPPER HORSE

EFFECTIVELY ADDRESSING THE CHALLENGE OF SECURING CONNECTED AND AUTONOMOUS VEHICLES

David Rogers MBE, Copper Horse

CONTENTS

EXECUTIVE SUMMARY

Vehicles are becoming the most sophisticated connected objects in the 'Internet of Things'. As vehicles integrate functionality that will enable a fully autonomous future, the attack surface grows substantially. Combined with remote connectivity at multiple points, the clock is ticking in a race to improve cybersecurity in all types of vehicles to ensure that all stakeholders, but particularly drivers and passengers, can have full confidence that future Connected and Autonomous Vehicles (CAVs) are both safe and secure.

The automotive industry has a challenge in that legacy technologies are both insecure and take a long time to age-out. Unlike many other connected products, vehicles can have a very long lifespan, which demands an innovative approach when it comes to cybersecurity concerns.

The Innovate UK-sponsored Secure-CAV consortium set out to develop and prove hardware-based security technology that will allow the automotive industry to leap ahead of the threats that it faces currently and in the near-term, putting the industry into a much more tenable cybersecurity posture than it currently holds.

Siemens has developed Intellectual Property (IP) as well as anomaly detection software, which is able to monitor protocols and transactions at the lowest level in hardware. This is backed by unsupervised machine learning algorithms and statistical analysis, with expert input from the University of Southampton. This was integrated into Field-Programmable Gate Array (FPGA) technology and linked to two vehicle demonstrators developed by teams at Coventry University and cybersecurity specialists Copper Horse. A range of selected real-world threats were exercised, including purchasing and analysing hacking equipment for existing vehicles.

Whilst the COVID-19 pandemic presented practical issues for the consortium members, the participants overcame the majority of the issues and were able to prioritise a number of real-world and theoretical attacks. Building these into a demonstrator enabled the consortium to prove the theory that security anomalies can be detected and responded to appropriately, forming the foundation and basis for future developments in this emergent security solution space.

SECURE CAV

Advanced cybersecurity for connected and autonomous vehicles

COPPER HORSE · Coventry University · University of Southampton · SIEMENS