Preparing the automotive industry: Investigating the security vulnerabilities and solutions for connected and autonomous vehicle technologies and legislation

William Booth

Technical Report

RHUL–ISG–2022–3

11 April 2022

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

Executive Summary

Connected and autonomous vehicles (CAVs) aim to present solutions for the social, economic and environmental complications caused by traditional vehicles. The way in which vehicles are viewed in society is set to change dramatically, with vehicular mobility being both autonomous and connected. Although the technological development that has brought forward the emergence of CAVs has been significant, the technologies that enable driverless transportation face new and existing cybersecurity threats. Furthermore, the preexisting legislation and principles that apply to traditional vehicles are not suitable for CAVs, with new dangers to security, privacy and personal data being expected. Therefore, a comprehensive assessment of the security vulnerabilities that concerns the underlying technologies, personal data and privacy protection mechanisms, and applicable legislation is required, where recommendations can be made to protect the future of autonomous automotive transportation.

This report will consider the technological developments that have lead to the emergence of connected and autonomous vehicles, looking towards the underlying sensing, perceiving and communication technologies that are used in high level CAVs. With this, applicable security attacks on the technologies and systems will be discussed, with appropriate countermeasures being proposed. Additionally, the implications on personal data and user privacy will be briefly discussed, emphasising the requirement for compatible data protection legislation. Furthermore, relevant and applicable legislation and principles that govern autonomous driving, user data, privacy and cybersecurity will be critically assessed, revealing areas in which governance is failing. Utilising the findings from the aforementioned, recommendations will be made that can be used by the automotive industry to protect the future of CAVs against security threats.