Hacking Safety: Providing Security for Connected Vehicles in Australia

Sean McQueen

Transport Certification Australia

Abstract

Connected vehicles are being deployed to make our roads safer and smarter. The benefits of this technology are widely discussed; less so the risks. These risks are familiar to the ICT/cybersecurity sphere; but they are safety threats for the connected transport network. A Cooperative Credential Management System provides security for the 'internet of cars' and is being deployed in the US and Europe. Australia has co-led CCMS development, and is proposing to implement its own CCMS. Combining Australian and international perspectives, this paper provides an update on this work, and gives insights into new methods of safety and security management.

Background.

Connected and automated vehicles (vehicle-to-vehicle [V2V], vehicle-to-infrastructure [V2I] and vehicle-to-elsewhere [V2X]) will see the progressive introduction of connected systems that will change the way transport networks function and how they are managed. Widespread adoption will progressively link vehicles and infrastructure to build real-time situational awareness, increasing the safety and productivity of the transport network. These technologies are a critical part of the disruptive transformation occurring to our vehicles, roads and cities – including automated vehicles, smart cities and smart infrastructure, and the Internet of Things.

Providing security for this new environment has emerged as one of the key deployment challenges (and it will be a permanently ongoing challenge). The paradox is that by introducing technologies intended to boost safety, we introduce an entirely new set of safety threats and challenges. This is not simply because these are new types of technologies – many are commonplace in other spheres of our lives. But this type of technology – and the scale of its proposed deployment – is new for the automotive industry, and will be new for drivers, road managers, and all transportation users. As the barriers between being on the road and being 'online' become indistinct, it is becoming apparent that *(physical) safety and (digital) security are one and the same*.

Moreover, the safety benefits of cooperative vehicle technology can only be realised with substantial user uptake, and this uptake will be driven by non-safety 'pull factors' (such as infotainment, mobility etc.) that do not prioritise so much as assume that safety and security risks have been managed (by industry and by government) – not to mention secure communications and interoperability requirements. For these reasons, a commercially sustainable global market for connected vehicles will not be possible without security, and neither will safety nor true connectivity.

Cooperative Credential Management System (CCMS)

While not the only solution to these challenges, a cryptosystem system that enrols new vehicles into the connected environment, and provides lifecycle security services through the creation, management, distribution and revocation of digital certificates ('electronic passports') for vehicles has been internationally co-developed by technical and policy experts across the United States, Europe and Australia (the lead agencies are United States Department of Transportation, the European Commission and Transport Certfication Australia, respectively).

The system, called a Cooperative/Security Credential Management System (CCMS/SCMS), builds on widespread implementations and experiences with Public Key Infrastructure (PKI) (frameworks that consist of cryptographic technologies, standards, organisational and policy controls and procedures to provide security for exchanges of data e.g. in e-commerce) and adds some entirely novel concepts and functions that are designed to provide security infrastructure and services for what can be rightly described as the 'internet of cars.'

Australia has been a key player in developing the CCMS (which is currently being deployed in the United States and across Europe) and is now proposing to implement a CCMS of its own. The design, implementation and operation of a CCMS in Australia will require new and existing parties across government and industry to rethink the nature of their role in providing safety for end-users. This paper lays out the safety challenges posed by connected vehicle technology, those involved in effectively overhauling what safety means for the sector, and highlights how safety and security can be achieved through the provision of such a distributed cryptosystem whose design and deployment is imminent in Australia.

References

European Commission. 2016. C-ITS Platform WG5: Security and Certification. Final Report. ANNEX 1: Trust models for Cooperative-Intelligent Transport Systems (C-ITS). An analysis of the possible options of the design of the C-ITS trust model based on Public Key Infrastructure (PKI). Available at https://ec.europa.eu/transport/themes/its/c-its

European Commission, United States Department of Transportation, Transport Certification Australia. 2015a. Public Key Infrastructure (PKI) Architecture Analysis and Recommendations for Harmonization. EU-US ITS Task Force. Standards Harmonization Working Group. Available at https://ec.europa.eu/digital-agenda/en/news/harmonized-security-policies-cooperative-intelligent-transport-systems-create-international.

European Commission, United States Department of Transportation, Transport Certification Australia. 2015b. Cooperative-ITS Credential Management System Functional Analysis and Recommendations for Harmonization.. EU-US ITS Task Force. Standards Harmonization Working Group. Available at https://ec.europa.eu/digital-agenda/en/news/harmonized-security-policies-cooperative-intelligent-transport-systems-create-international.

United States Department Of Transportation. 2016a.Connected Vehicle Pilot Deployment Program Phase 1, Security Management Operational Concept – ICF/Wyoming. Available at http://ntl.bts.gov/lib/59000/59200/59237/FHWA-JPO-16-288.

United States Department of Transportation. 2016b. Federal Motor Vehicle Safety Standards; V2V Communications. Available at https://www.transportation.gov/briefing-room/us-dot-advances-deployment-connected-vehicle-technology-prevent-hundreds-thousands

Whyte, W., Weimerskirchy, A., Kumar, V., Hehn, T. 2013. A security credential management system for V2V communications. Conference paper. Available from William White, Security Innovation, Inc.