Cyber security of connected autonomous vehicles trialled

September 16 2019

Credit: CC0 Public Domain

The privacy and security of data in CAVs has been improved thanks to WMG, University of Warwick who tested four innovations that were results of the PETRAS project. CAVs can now connect to each other, roadside infrastructure, and roadside infrastructure to each other more securely.

In the near future Connected and Autonomous Vehicles are expected to become widely used across the UK. To ensure a smooth deployment, researchers from WMG, University of Warwick undertook real-world testing of four academic innovations in the IoT-enabled Transport and Mobility Demonstrator project funded by Lloyd's Register Foundation.

The testing looked at how the vehicles will connect to each other, as well as to roadside infrastructure, and the roadside infrastructures to each other.

The four innovations tested were developed within the PETRAS Internet of Things Research Hub and aimed to improve the security, privacy and safety of future connected vehicles.

The four new innovations included:

1. Group Signatures:

For a vehicle to communicate it is important that the messages it sends contain a proof that the vehicle is who they claim to be (via a digital signature). However, by revealing and proving the vehicle's identity it allows that vehicle to be tracked over a long time. In order to provide privacy a group signature can be used, which only indicates that the

vehicle is a member of a group.

The group signature scheme can be extended to use a timestamp that updates every 10 minutes as a component of the signature. Therefore, if the vehicle was to send the exact same message at 10:00am and 10:10am the group signature would differ and an eavesdropper would not be able link that the vehicle sent both messages. This scheme would be useful in vehicle platooning where vehicles want to demonstrate they are part of the platoon group.

2. Authentication Prioritisation:

It is an expensive task for a vehicle to verify another's identity. Vehicles will have limited computing resources and so will only be able to verify a specific number of identities included in messages per second. For example, if a vehicle is on a busy motorway in traffic there may already be more vehicles sending messages that can be verified in a timely manner. An adversary may also try to send many messages with incorrect signatures in order to prevent vehicles from verifying the identity of actual vehicles. Therefore the order in which the identity of messages are verified is decided based on assigning a priority to the messages. A higher priority means that those messages have the identity of the sender verified first.

3. Decentralised PKI:

When a vehicle is travelling down a road it may meet multiple vehicles in a short space of time. In order to check the identity of these vehicles, the public key of the other vehicle needs to be downloaded from a keyserver. However, hosting this keyserver in the cloud has limitations due to additional communication hops increasing the time before the vehicle receives the necessary keys. Instead, vehicles can receive these keys faster if the keysever is distributed over Edge infrastructure that

sits next to the road.

4. Decentralised PKI with Pseudonyms:

This innovation extended the previous innovation to support periodically issuing new identities to vehicles on the road to provide privacy. Both this innovation and group signatures may be required, as they are useful in different scenarios.

Each of the techniques above were demonstrated in the real world on the campuses of the Universities of Warwick and Surrey, as well as Millbrook Proving Ground.

A follow up executive summary, informed through feedback when the work was presented at the House of Lords, is now available. The summary makes a number of recommendations, including more communication infrastructure should be deployed, and that researchers should have an ability test different types of cyberattacks on CAVs and roadside infrastructure. 5G should also be used to perform the testing, as 5G is being rolled out across the UK in the future.

Lead of the project Professor Carsten Maple of WMG, University of Warwick comments:

"The cyber-security of CAVs is key to make sure that when the vehicles are on the roads, the data is trustworthy and that vehicle communications do not compromise privacy. We tested four innovations developed in the PETRAS Project, and being able to apply them to the real world is the first major step in testing security of CAV systems.

"The units being investigated to be used in cars and on the roadside were taken to Parliament in February to demonstrate how they work; now we can focus on further testing in the real world. Future work include will

include testing on 5G systems, and with different types of attacks"

Provided by University of Warwick