Independent Vehicle Authentication Using Non-fixed Attributes

Researchers

Prof. Shlomi Dolev
dolev@cs.bgu.ac.il

Nisha Panwar
panwar@cs.bgu.ac.il

Prof. Michael Segal
segal@cse.bgu.ac.il

Results

All major automotive giants such as BMW, Toyota, GM, Nissan, Bosch, Delphi are customizing their vehicles for these real-world applications. For example, GM has OnStar service in their vehicles which utilizes the cellular infrastructure for driver assistance, road navigation, vehicle repair, theft detection, etc.

Goals

We present a vehicle authentication approach that utilizes the out-of-band verification of dynamic and sense-able attributes of the vehicle.

Authentication is an important issue regarding vehicle network security. Vehicles communicate through wireless channels and need to verify the peer vehicle identity, before exchanging sensitive information. If a vehicle assumes a fake identity and transmits bogus messages to peer vehicles, it could turn into a life-threatening situation.

Description

Vehicles can authenticate peer vehicles using a certificate from a trusted certificate authority. However, besides the certificate verification, an online authenticity proof is also required. In our previous work, we suggested out-of-band fixed attribute verification of a vehicle against the certified attributes from a trusted certificate authority. The coupling between the certified public key and the sense-able static attributes confirms the vehicle's authenticity. There is a scenario in which an impersonation attack is successful, in spite of the out-of-band fixed sense-able attribute verification. Therefore, we suggest coupling the non-fixed sense-able attributes and the session secret of the vehicle. It ensures a unique identity for every vehicle and resolves the active impersonation attack, i.e. man-in-the-middle attack.

Modern vehicles are equipped with Global Positioning System (GPS), sensors, actuators, electronic control and processing units. Moreover, a camera, laser beam source and autocollimator mounted on the vehicle can observe the static as well as dynamic attributes of the peer vehicle. Therefore, it is feasible to implement the proposed approach without any roadside infrastructure available, and only vehicle customization is required.