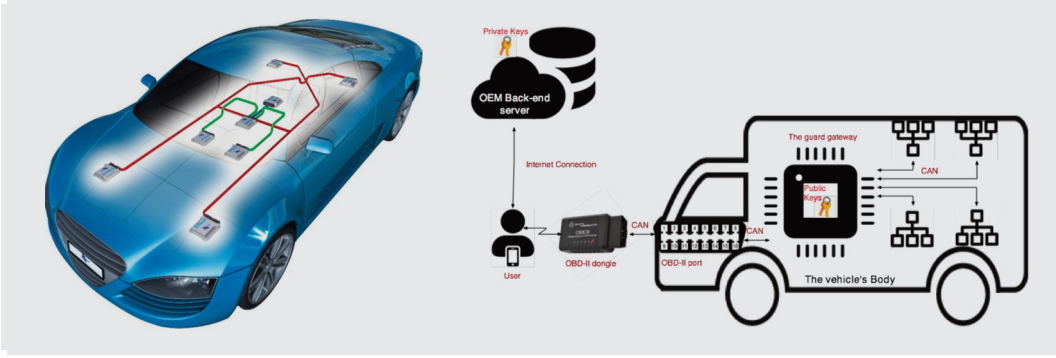
Mahmoud Ammar
KU Leuven

Category: **Road** Country: **Belgium**

Research Area 2: **Digitalisation, Digital Safety and Security** Idea Number: **37**

Securing the OBD-II port in vehicles

Modern vehicles integrate Internet-of-Things components to bring value-added services to drivers and passengers. These components communicate with the external world through different types of interfaces including the on-board diagnostics port (OBD-II), a mandatory interface in all vehicles in the U.S. and Europe. In the current standard, the OBD-II port allows direct access to the vehicle internal network and also software installation on the Electronic Control Units (ECUs). While this historically required physical access to the port using a dedicated tool, today many vehicles support remote access. Because connectivity and security are not pivotal in the design of vehicles, the OBD-II port opens the door to a wide variety of cyber-attacks. We propose a novel, scalable, and lightweight solution to the lack of security in OBD-II ports. Our solution consists in an end-to-end, role-based access-control mechanism based on public-key cryptography able to prevent unauthorized access to any of the vehicle functionality. This solution is AUTOSAR-compliant and architecture-independent, and guarantees a high level of reliability and trustworthiness. Also, because it is purely software-based, it does not require hardware modifications and thus is directly applicable to currently on-road vehicles. Furthermore, any physical attack to a vehicle implementing our solution is not scalable and only limited to that vehicle. We provide a proof-of-concept implementation and evaluation of the proposed solution, showing its robustness and efficiency.



Key Characteristics

On-board diagnostics port • Electronic Control Units • Cryptography