Abstract

Modern automobiles include more and more electronic control units (ECUs) by the years, with these having ever so increasing coupling via on-board buses between them. This cloud of interconnected units has begun to expand beyond the physical limits of the vehicle. Today's automobiles feature a never before seen range of wireless communication capabilities and advanced driver assistance systems. One major aspect of communication systems has been mostly ignored by the automotive industry, the security of the vehicle networks and components against adversaries. In this present the recently identified attack surfaces and system vulnerabilities, which leads me to create a security model of the on-board and diagnostic communication. I investigate the cryptographic, hardware and software building blocks needed to create a secure ECU communications interface to the on-board networks.

Based on the identified system weaknesses I selected the most vulnerable attack surface of the ECU – the diagnostic communication – for a security application implementation. I constructed the necessary diagnostic hardware-software toolkit that can connect to the ECU, which is composed of a CAN-USB gateway and a PC user application. I have compiled a compact, portable cryptographic C software library, which features all basic cryptographic algorithms with the currently most widespread cryptographic ciphers and hash functions. I have conducted measurements on an embedded platform in order to determine the code size and run time costs of each cryptographic scheme. I created a custom security access protocol which is compliant to the underlying diagnostic standard, which verifies a diagnostic client by a cryptographic signature, and which also produces a shared secret key for the parties. I also added secret key-based cryptographic encryption and authentication capabilities to the security access-protected memory transfer services. This functionality was extended to support the upload of a new main software to the ECU. In the final chapter I make a brief overview of the security improvements provided by a hardware security module supporting ECU.