More Secure Security

AUTHORS

Dr. Jan Pelzl is Managing Director of **ESCRYPT GmbH**.

Dr. Thomas Wollinger is Managing Director of **ESCRYPT GmbH**.

Protecting Car-2-Car communication against defects and misuse

Car-2-Car communication is the next major evolutionary stage for road travel. Once vehicles are able to exchange messages and warnings, it will be possible to recognize hazards in advance and better manage traffic flow. But the open communication interfaces they will use must be safeguarded against unauthorized access. Manufacturers, research projects, and pilot projects are working hard to develop protective measures, utilizing well-established security approaches from information technology – and ESCRYPT is at the forefront.

Car-2-Car (C2C) and Car-2-X (C2X) communication offer manufacturers and OEMs a way to support drivers with smart technology and thus prevent accidents. In the future, road users will automatically and directly exchange warnings and messages. The Institute for Transport & Economics at Technische Universität Dresden is convinced that travel delays caused by traffic jams could be reduced by more than half if just ten percent of vehicles supported C2C communication*.

For an application that would potentially intervene in the driving dynamics, having the trust of the user is an absolute must. The integrity and confidentiality of exchanged messages must be guaranteed at all times. This stands in contrast to C2C communication's open, wireless interfaces. If messages are transmitted and received via short-range wireless communications, it is generally possible for anyone to set up a corresponding transmitter-receiver unit and engage in the communication.

The pivotal point is the Certificate Authority (CA), an element of every Public-Key Infrastructure (PKI). This is where ESCRYPT offers attractive solutions that use the necessary state-of-the-art cryptographic keys. ESCRYPT's "Key Management Solution" can be put to use wherever electronic embedded systems need to authenticate, release, or communicate securely. It can be operated either by customers themselves or as a fully managed service by ESCRYPT.

Challenges

Since users are extremely mobile, connection times have to be short. There can be no guarantee of communication with infrastructure. That is why digital signatures – an important part of the C2C protection concept – must be implemented differently than is the case with conventional IT applications. Certificates must have a very long validity, as there is no way to ensure connections to a system that would be able to issue and verify certificates and declare them valid or invalid. In order to prevent the compiling of movement profiles of vehicle and driver, certificates must be pseudonymized.

On-board units are IT systems

C2C communication uses TCP/IP protocols in at least some capacity. This represents a way in for aggressors, who can exploit the well-documented packet formats and use numerous tools. Research projects such as PRESERVE or SEVECOM are attempting to formulate a defensive approach that is as universal as possible. They are analyzing individual systems, data, communications connections, and functions to assess their defensibility based on the protection objectives of integrity, availability, and authenticity. The result is a set of protection requirement categories that also take into account potential aggressors' motives and capabilities. This thorough categorization allows protective measures to be deployed in a very focused manner according to their cost and effectiveness.

Manufacturers, research projects, and organizations such as the Car-2-Car Communication Consortium (C2C-CC) have been working on this array of tasks for many years. In February 2014, fundamental communication standards for networked vehicles in Europe were announced by the European Telecommunications Standards Institute (ETSI) and the European Committee for Standardization (CEN). Working together with their counterparts in the United States and Japan, the organizations reached agreement on a number of issues including wireless frequencies and data formats.

*) Source: www.berliner-zeitung.de