Homogenous security for hybrid V2X communication

Standard solution enables versatile data transfer during connected driving

Connected driving is one of the most promising concepts in the future of mobility. Achieving it requires a Cooperative Intelligent Transport System (C-ITS) – a solution that enables the real-time exchange of data in both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. In the future, experts expect this vehicle-to-everything communication to work on the basis of multiple technological standards simultaneously. Yet maintaining security will still be paramount.

Up to now, direct V2X communication has been based primarily on ITS-G5, a dedicated short-range communication (DSRC) standard. That means the vehicles and roadside equipment essentially exchange data through direct wireless LAN communication. But this situation is set to change. Efforts are already underway to implement parallel use of another standard for V2X data exchange, namely the LTE-V standard for high-speed wireless communication (currently 4G, soon to be 5G). With new kinds of wireless chips installed in devices, that will make it possible to include other road users (e. g., pedestrians or cyclists) in the communication process in the form of direct, ad hoc data exchange between devices (C-V2X autonomous). A number of other standardized concepts will also be added to the mix, including mobile edge computing (MEC), which distributes messages via a cellular network at close range (e. g., for tailback warnings), and traditional wireless communication via cell towers for communication with cloud and backend services (see Figure 1).

Protocol stacks with a consistent, intelligent structure

The likelihood is that we will see various types of V2X communication designed to serve different channels and standards depending on the particular use case and entity. That raises the question of how to secure this kind of hybrid V2X communication in the most efficient manner. It would be entirely wrong to think that each of the different transmission channels should have its own security solution. Instead, what is called for is a security concept that is effective across the full spectrum of V2X communication with all its different use cases.

> That raises the question of how to secure this kind of hybrid V2X communication in the most efficient manner.

The solution lies in ensuring the protocol stacks used for V2X communication between all V2X devices and entities have a consistent, intelligent structure (see Figure 2). V2X messages are generated on the application or device level and relayed to the transport and transmission level. This is where the security header is added to each V2X message via the security components interface. The header includes the message signature and the associated certificate; if necessary, the message can be symmetrically encrypted in a second step. Information relating to the symmetric key is included in the header to enable recipients to decrypt the V2X message. To ensure data protection for the entities communicating via the V2X network, each V2X message receives a signature before it is encrypted. Even within a hybrid communication network, this method fulfills all the security requirements for V2X data exchange: data integrity, sender authenticity, sender authorization, replay detection, confidentiality, privacy protection, reliability, and revocation of trust.

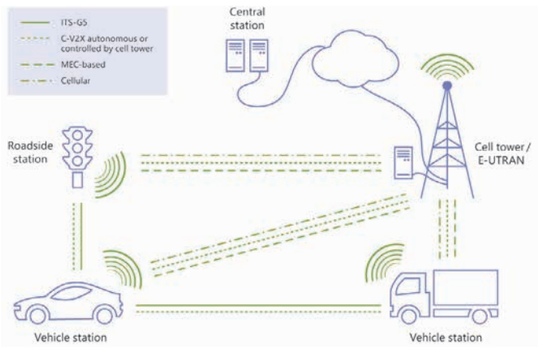

Figure 1: Hybrid V2X communication architecture

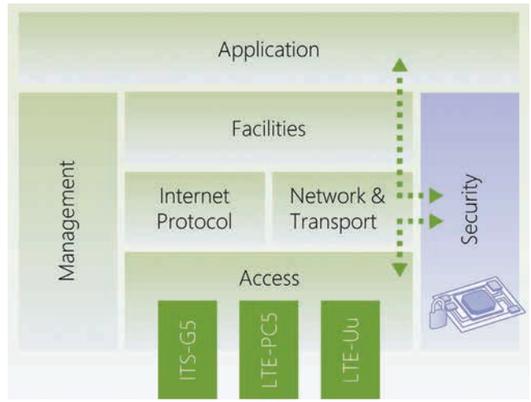

Figure 2: Software stack for consistent V2X security in hybrid communication

Road testing with the CONCORDA project

Hybrid communication for vehicles is a sensible and useful development for connected driving. It paves the way for integrating more systems, road users, and services into V2X data exchange. At the same time, IT security is and will remain a necessary and fundamental condition for V2X. Establishing an intelligent concept means providing consistent, homogeneous, and efficient IT security across the various V2X communication channels and standards.

A trial run is currently underway on test routes in the Netherlands, Belgium, Germany, France, and Spain in the shape of the CONCORDA (Connected Corridor for Driving Automation) project, which is funded in part by the European Union and carried out in collaboration with companies including ESCRYPT, Deutsche Telekom, Nokia, Bosch, and Volkswagen. By mid-2020, CONCORDA will have shown how a hybrid V2X communication system with ITS-G5, LTE connectivity, and a consistent IT security architecture performs in practice. ■

Authors

Dr. Norbert Bißmeyer is Project Manager at **ESCRYPT**.
Jan-Felix van Dam is Security Engineer at **ESCRYPT**.