Ethernet Security

AUTHORS

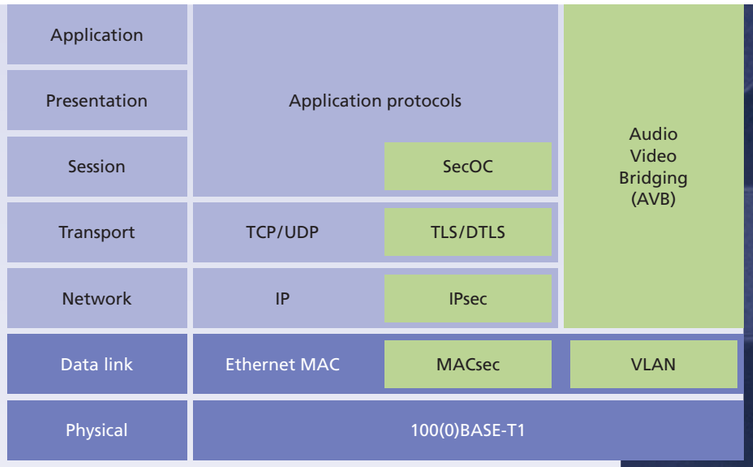
Norbert Fabritius and **Ramona Jung** are Security Engineers at **ESCRYPT GmbH**.

Dr. Jan Holle is Security Engineer and Product Manager at **ESCRYPT GmbH**.

ESCRYPT is a 100-percent subsidiary of ETAS GmbH and offers security solutions for embedded systems.

Secure Ethernet – an opportunity for vehicle IT

For over 40 years, the Ethernet has been an established IT standard widely used in data centers and in the consumer sector. Now it is conquering the world of modern vehicles. Following initial applications in systems without cross-domain communication, the E/E architecture is now expanding across domain boundaries. This raises questions about security, safety, and reliable time response behavior. Practical Ethernet solutions are required.



Classification of various safety-relevant protocols (in green).

The data rates in automobiles are increasing rapidly. To manage them, there is a new sheriff in town to help traditional bus systems such as CAN and FlexRay: the Ethernet. A technology that started out in the infotainment sector is now being used in cross-domain vehicle systems.

To make sure that data buses can work securely, independently, and with each other, there is a need for robust solutions that have been well thought through. The solutions shall support communication between Ethernet components as well as smooth, seamless data exchange with conventional buses. It is very important to adapt Ethernet standards – where necessary – to the specific requirements in vehicles. In some cases, traditional IT solutions can be used as it is or implemented after minor modifications. In other cases, new developments are necessary. This decision hinges on the question of how to achieve maximum security, safety, and reliable time response behavior, even when dealing with large data volumes such as video signals.

Classic IT problems and solutions

In the Ethernet's decentralized structure, it is possible to avoid having a central control entity – and therefore a single point of failure – by using in-built redundancies and dynamic network paths. However, this distributed structure is itself a source of doubt: if all members of Ethernet networks have equal privileges, how do we detect and ban members trying to gain unauthorized network access? How do we identify and prevent network manipulation?

To do this, there are established solutions out there, such as virtual networks – VLANs – for partitioning the network traffic. Originally, the network ports were assigned to the switches on various VLANs. Now it is also possible to mark ("tag") Ethernet frames and port-independent VLANs. This tagging is regulated in the IEEE 802.1Q standard. However, the logical separation of network traffic alone does not prevent the participation of unwanted devices. Equally, it shields the traffic only conditionally from manipulation and spying. To achieve this, we need cryptographic authentication or encryption. Classic IT solutions also exist for this problem: initial solutions focused on the upper protocol layers with data formats and standards such as Transport Layer Security (TLS); later solutions offered additional security mechanisms for the deeper layers. This includes the encryption of IP packets (Layer 3) with IPsec and of Ethernet frames (Layer 2) with MACsec (IEEE 802.1AE). These solutions are likewise regulated by industry standards.

In addition, there are security components: using filter rules, classic firewalls control which packets are allowed to move between different networks or end points. Modern variants are able to analyze and evaluate the traffic right down to the packets' payloads by means of deep packet inspection. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) build on this foundation and expand the control options available to administrators.

Security requirements of modern vehicle networks

There are many parallels between the network architectures of modern vehicles and those used in classic IT. However, the technical criteria and protection objectives differ substantially. In vehicles, safety of passenger and property is the top priority. This shifts the spotlight to system availability and the authenticity of network traffic. Moreover, this is where the real-time critical requirements in vehicle operation come into play, requiring network components to behave in a virtually delay-free, deterministic manner.

These requirements stand in apparent contradiction to the Ethernet's nature as a packet-based best-effort medium that does not require guarantees for the delivery time of data packets. In addition, the fulfillment of safety goals and real-time requirements is difficult to achieve due to the fact that vehicle ECUs have limited computing power.

For these reasons, established security technologies often make their way into vehicle networks only in modified form – for example, when VLANs are used to enhance their fail-safe properties. To this end, the network is divided into virtual zones with different protection needs, via which the network traffic of safety-relevant components can be identified in real time. If required, it can then be prioritized or isolated. If a Denial-of-Service (DoS) attack or faulty component floods the network with packets, they can be stopped at the next switch by means of rate limiting to give precedence to the communication in the prioritized VLAN.

Using firewalls or more powerful IDS/IPS systems, it is possible to separate adjacent IP networks with different protection requirements more strictly from each other and monitor them more precisely. By contrast, traditional automotive bus systems, by virtue of being broadcast media, cannot be separated logically – unless, that is, an additional physical bus is installed.

Existing and new security solutions

With the TLS IT security protocol, caution was required. Because it threatened to cause conflicts with the real-time requirements in the vehicle, it could only be considered for time-uncritical communication with backend systems or test devices. The TLS 1.3 specification offers substantial innovations: thanks to optimizations in how connections are established (zero-RTT handshakes), TLS-secured data can be accommodated in the first packet during the handshake. Additional round-trip times (RTTs) are no longer required when using TLS. As the use of pre-shared keys (TLS-PSK) could mean that asymmetrical processes are no longer needed, the overhead cost of TLS can also be reduced dramatically. For the present, however, the focus is on carefully evaluating the possibilities with regard to possible weakness of the TLS security guarantees.

The real-time requirements in vehicles are an obstacle to the use of cryptographic signatures based on asymmetric processes. To protect the authenticity of data packets, the Secure On-Board Communication (SecOC) module specification was released in 2014 as part of AUTOSAR 4.2. The specification is so flexible that SecOC is also suitable for Ethernet/IP-based traffic.

The same goes for various Time-Sensitive Networking (TSN) standards, including Audio Video Bridging (AVB), which was originally developed for transmitting time-critical video data. It runs over the Ethernet and defines its own mechanisms, which govern the reservation of network resources, the synchronization of time signals, and the prioritization of data streams. In addition, AVB permits the transmission of conventional bus data. This takes into account the requirements in environments with real-time specifications without having to renounce the Ethernet as the basic technology. The latest version of the AVB transport protocol (late 2016) can also support the encryption of transmitted payload data, if required – with relatively low hardware requirements.

Ethernet security in vehicles – development and integration

Integration of Ethernet-based solutions into vehicle networks is in full swing. The standard enables implementation of the functions expected for future vehicles. At the same time, this development is not in any way at variance with the security requirements in vehicles. With in-depth support from security experts and custom-fit security solutions, it is possible to successfully implement secure Ethernet architectures in spite of the extreme complexity. To this end, ESCRYPT can draw on many years of experience in the Ethernet security and automotive sectors. With this know-how, we support customers in all phases of Ethernet integration: from developing viable security concepts and analyses through to implementing customized software and hardware solutions from our broad portfolio tailored exactly to the needs of the automotive industry.

Safeguarded by intelligent security solutions and products, the Ethernet standard will write the next exciting chapters in its success story, which stretches back over 40 years. And these new chapters will feature the automotive industry more than ever before.