The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 16, No. 5, pp.39-48, Oct. 31, 2016. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2016.16.5.39
JIIBC 2016-5-7

차량 전자/전기 아키텍쳐에 이더넷 적용을 위한 보안 기술에 대한 연구

Security of Ethernet in Automotive Electric/Electronic Architectures

이호용*, 이동훈**

Ho-Yong Lee*, Dong-Hoon Lee**

요 약 차량 네트워킹 아키텍처의 주요 트렌드 중 하나는 차량 이더넷의 도입이다. 이더넷은 이미 차량 어플리케이션에서 이용되고 있으며 (예를 들어, 비디오 카메라와 같은 고속 데이터 전송 소스의 연결), IEEE에서 진행중인 표준화 (IEEE802.3bw - 100BASE-T1, IEEE P802.3bp - 1000BASE-T1)로 인해 나중에 훨씬 광범위하게 채택될 것으로 예상된다. 이러한 어플리케이션은 단순히 지점 간 연결에 한정되지 않지만, 전체적인 전기/전자 아키텍처에 영향을 미칠 수 있다. 이더넷을 통해 IP 기반의 트래픽은 추가적인 구성요소(차량용 방화벽 또는 IDS)와 함께 현재까지 잘 확립된 IP 보안 프로토콜(예를 들어, IPSec, TLS)을 통해 보안을 구현할 수 있을 것으로 보고있다. 리소스 제한이 있는 디바이스 상에서 안전 및 실시간 어플리케이션의 경우에, 복잡하고 높은 성능이 요구되는 TLS 또는 IPsec을 사용하는 IP 기반 통신은 선호하는 기술은 아니다. 예를 들어, 이 어플리케이션은 IEEE와 같이 현재 표준화되어[13] 있는 Layer 2 기반 통신 프로토콜로 사용될 수 있을 것이다. 본 논문은 보안에 대한 최신 통신 개념을 반영하고 향후 이더넷 스위치 기반 EE-아키텍처에 대한 구조적인 도전과 잠재적인 솔루션을 식별한다. 또한 차량 이더넷에 관한 지속적인 보안 관련 표준화 활동에 대한 개요와 통찰력을 제공한다. 또한, 예를 들어 IEEE 802.1AE MACsec 또는 802.1X 포트 기반 네트워크 액세스 제어와 같이 기존에 적용되지 않은 차량 이더넷 보안 메커니즘을 적용 가능성을 고려하고, 차량 어플리케이션에 대한 적합성을 평가한다.

Abstract One of the major trends of automotive networking architecture is the introduction of automotive Ethernet. Ethernet is already used in single automotive applications (e.g. to connect high-data-rate sources as video cameras), it is expected that the ongoing standardization at IEEE (IEEE802.3bw - 100BASE-T1, respectively IEEE P802.3bp - 1000BASE-T1) will lead to a much broader adoption in future. Those applications will not be limited to simple point-to-point connections, but may affect Electric/Electronic(EE) Architectures as a whole. It is agreed that IP based traffic via Ethernet could be secured by application of well-established IP security protocols (e.g., IPSec, TLS) combined with additional components like, e.g., automotive firewall or IDS. In the case of safety and real-time related applications on resource constraint devices, the IP based communication is not the favorite option to be used with complicated and performance demanding TLS or IPSec. Those applications will be foreseeable incorporate Layer-2 based communication protocols as, e.g., currently standardized at IEEE[13]. The present paper reflects the state-of-the-art communication concepts with respect to security and identifies architectural challenges and potential solutions for future Ethernet Switch-based EE-Architectures. It also gives an overview and provide insights into the ongoing security relevant standardization activities concerning automotive Ethernet. Furthermore, the properties of non-automotive Ethernet security mechanisms as, e.g., IEEE 802.1AE aka. MACsec or 802.1X Port-based Network Access Control, will be evaluated and the applicability for automotive applications will be assessed.

Key Words : Security, Automotive, ECU, Ethernet

*정회원, 고려대학교 정보보호대학원 석사과정
**정회원, 고려대학교 정보보호대학원 교수 (교신저자)
접수일자 : 2016년 8월 19일, 수정완료 : 2016년 9월 19일
게재확정일자 : 2016년 10월 7일

Received: 19 August, 2016 / Revised: 19 September, 2016 / Accepted: 7 October, 2016
**Corresponding Author: donghlee@korea.ac.kr
Dept. of Information Security, Korea University, Korea

Ⅰ. Introduction and Motivation

The first security related recall campaign hit the automotive industry in July 2015[4]. While typical automotive attack vectors[5],[6] and the underlying challenges for automotive security have been discussed for years[7], security was still sometimes considered to be an academic, respectively long-term topic and additional cost factor until those moments. But the recall of up to 1.4 Mio cars in the US demonstrated that unaddressed security weakness may not only damage OEM reputation, but is a today issue which may also have a significant monetary effect. The publication, which revealed the security deficiencies in the affected vehicles[8], provides a detailed description on how the security researchers chained together several vulnerability exploits to demonstrate a long-range attack (i.e. virtually only limited by the ability to register within the same mobile phone provider network) on an exemplary selected 2014 model year vehicle. Based on the security issues, necessary countermeasures are required to effectively mitigate those kind of attacks. For preventing long-range attacks (i.e. easily scalable attacks via the backend/infrastructure and the end-point of communication in the car), the security of the automotive EE-Architectures and especially the in-vehicle communication needs to be improved. Positively, efforts in this field are also suitable to mitigate local attacks, e.g., via an infotainment unit compromised by a manipulated media file[6] or the OBD port[9].

Security concepts for enhancing classical automotive EE-Architectures, i.e., based on CAN/FlexRay/LIN and sometimes MOST, have been already discussed in the past and some of the proposed mechanisms already made their way to standardization. The current paper will be focused on the security of future automotive EE-Architectures based on Ethernet. The Ethernet and its related upper layer protocols will be not only a simple but replace the legacy automotive bus systems. However, it will change fundamental concepts of current automotive EE-Architectures.

The introduction of Ethernet would be a great chance to improve in-vehicle security, because many of the security issues in automotive domain have been already addressed for Ethernet in classical IT. But huge challenges would be expected due to the constraints of automotive/embedded systems and assure at least the same security as currently envisaged for classical IT.

Ⅱ. Security Requirements of Automotive EE-Architecture

In this section, a brief overview is provided on the security of current automotive EE-Architectures as well as an idea how EE-Architectures Ethernet might look like and what kind of security challenges could be placed in the recent future.

1. State-of-the-Art Security in Current Automotive EE-Architectures

Though several in-vehicle networking technologies (e.g., FlexRay, MOST, LIN) have been introduced, CAN is still predominant as an in-vehicle network protocol. In terms of security, it can be distinguished into two kind of current (mainly CAN based) automotive EE-Architectures: Those with and those without a called central gateway (CGW). The CGWs have been designed to reduce the bus load in CAN based on specific forwarding rules i.e., only forward CAN messages from one CAN bus to another in case they are relevant for the other domain. Furthermore the existence of a Gateway reduces the vulnerability, e.g., a separation between buses which connect ECUs with “cyber physical features” has been assessed[8] and ECUs with remote interfaces can be determined as the “most hackable” car[10].

An additional security feature, which will be introduced, can provide an authentic in-vehicle communication[2],[3]; the detail mechanism will be described as standards in AUTOSAR in Sec. 3.1. While this security mechanism is not common yet, a Ethernet-based automotive EE-Architecture is

expected to provide comparable assurances in terms of security. Please note that a comprehensive in-vehicle security concept will also be required to incorporate security mechanisms to harden the ECUs, e.g., software authentication, secured diagnosis interfaces, and integration of hardware security features as well as key management aspects, which are not addressed in the present paper.

2. Upcoming Automotive EE-Architectures

Tomorrow's automotive EE-Architectures are shaped by a few key technologies, which enable new functionalities such as highly automated driving and high definition infotainment systems.

Some of the new key technologies can be summarized: Advanced gateways, connected vehicles, domain ECUs, new in-vehicle communication networks and new software approaches, cf. Figure 1.

The automotive Ethernet fulfill the requirements for higher bandwidth that provide the chance to introduce better security and safety measures at the same time.

The advanced gateways will provide low latencies and high throughput through hardware-based cryptographic acceleration with new routing mechanisms. Furthermore, the hardware-based acceleration mechanisms for crypto graphic operation are also required to reduce CPU load, which will be generated by the introduction of automotive Ethernet.

The multi-core ECUs will enable the integration of application software with availability of higher performance. This can be achieved through virtualization of the hardware by employing hypervisors. It will be required due to upcoming automotive use cases requiring communication with the external world as, e.g., over the air software updates of vehicle ECUs. Moreover, it can be used for utilizing the full benefits of the connected vehicle with keeping the vehicle secure and safe from malicious attacks.

In addition, vehicle domains (e.g., infotainment, chassis systems, body electronics and powertrain)are to be handled by domain controllers or integration platforms (e.g. engine control unit or ESP) that provide high computing power and work as domain masters by controlling and handling the higher level domain computations for the vehicle. Since domain ECUs will perform the bulk of the high-level computation, current component blocks will handle only the basic component computations for enabling standardized component blocks.

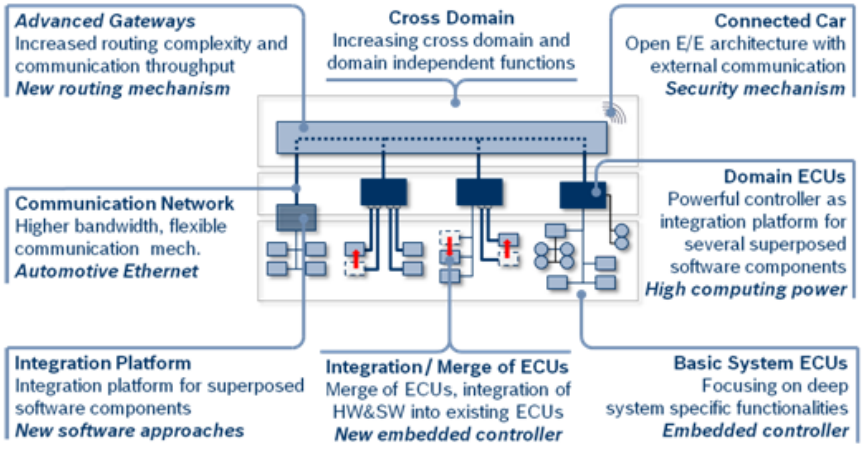

Fig. 1. Key Player in EE Architectures 2020
그림 1. 2020년 EE 아키텍쳐상에서의 주요 역할

3. Theoretical Security Requirements of Upcoming Automotive EE-Architectures

As shown in Figure 1, the Ethernet is expected to be the central component of a future automotive EE-Architecture as the higher bandwidth network for cross domain connectivity. With respect to the security characteristics of today's CGW based automotive EE-Architectures, the network and its security characteristics will be the security hot spot of future EE-Architectures. As a result, if a robust domain separation of network access control and secure communication cannot be achieved, the Ethernet is to become the weak point of future automotive EE-Architectures. Furthermore, the additional efforts are required in a switched Ethernet because it does not provide those security properties.

Ⅲ. Analysis of applicable Security Technologies/Protocols/Standards

Several security issues have been already identified and addressed since the Ethernet and its upper layer protocols are the predominant network technology in a classical IT world. This section provides an overview on the available and existing countermeasures for Ethernet, as well as a secure on board communication as standardized in AUTOSAR 4.2.1.

1. AUTOSAR Secure Communication

As agreed on the importance of protecting the internal communication of vehicle, the AUTOSAR consortium founded a Concept Group for Secure Onboard Communication (SecOC) in July 2013 that focused on the authenticity and integrity of messages transmitted over internal communication systems of vehicle. The concept should support both signal-based communication over classical automotive bus systems (e.g., CAN) and other bus systems as well, furthermore future communication approaches using new communication architecture like automotive Ethernet.

The concept was released as a standard as part of AUTOSAR 4.2.1 in 2014 . It supports a wide range of mechanisms based on both symmetric and asymmetric cryptography and various communication paradigms. As following the recommendation in this standard, a per-message authentication mechanism using symmetric truncated Message Authentication Codes (MACs) and anti-replay counter is specified in the documents. Figure 2 shows the data flow and process of security operation between a sender and a receiver.

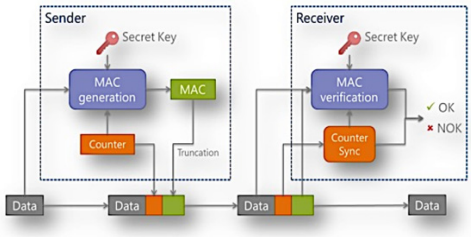

Fig. 2. Secure Onboard Communication (SecOC) according to AUTOSAR 4.2.1
그림 2. AUTOASAR 4.2.1 상의 Secure Onboard Communication (SecOC)

This mechanism assumes exchanging a pre-shared secret key between a sender and receiver(s). The initialization of these pre-shared keys is an important issue but not covered by the AUTOSAR standard since it is not necessary for interoperability. In addition, a monotonic counter should be included to protect this communication against replay attacks, which has to be synchronized between the communication parties. Furthermore, details of re-synchronizing the counters in case of synchronization loss is left to the respective implementation.

Assuming both are available, the sender creates a MAC based on the message, i.e. Protocol Data Units (I-PDU), payload, the current counter value and the secret key, truncates it to a parameterizable length and attaches it as authentication tag to the payload. Then the receiver generates a MAC based on the received data, its own key and current counter and compares it to the MAC received together with the message. Assuming the security of the mechanisms and secrecy of the key is to be satisfied, the MACs coincide if and

only if the message was not changed.

An architecture integration on PDU router level was chosen to allow flexibility for different communication paradigms (especially AUTOSAR COM and the newly discussed Efficient COM approach), and to enable PDU-based routing. Figure 3 shows a schematic view of the processing on a side of sender. The application of SecOC can be completely transparent for the upper layers with using this integration. In addition, the PDU-based routing can be done without interfering with upper layers in both point-to-point and end-to-end security approaches. But, this approach also implies that the upper layers of the stack have to be trusted in terms of security since they are not covered by the protection mechanism.

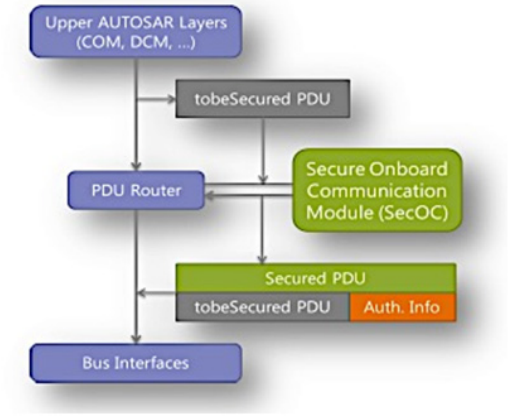

Fig. 3. Secure Onboard Communication (SecOC) processing on sender site
그림 3. 보내는 측에서 처리하는 Secure Onboard Communication (SecOC)

The recommended symmetric approach is based on standardized ciphers like Advanced Encryption Standard (AES) or hashes like SHA2, which enables efficient implementation both in hardware and software. The compromises between transmission bandwidth and security can be found for different use cases with using different truncation lengths. Confidentiality of communication is not covered by the AUTOSAR standard so far but can be easily added on top of the authentication[3].

2. Existing Security Mechanisms for Ethernet and typical upper Layer Protocols

As introduced above, AUTOSAR SecOC is a perfect choice to protect PDUs routed via the AUTOSAR PDU router, but additional and different security means are required to address automotive security use-cases and requirements as, e.g., i) separation within switched Ethernet networks, ii) network access and rate control or iii) secure communication via protocols which do not rely on the AUTOSAR PDU routing mechanism. The current section provides an overview on selected, existing or proposed security protocols and mechanisms which can be considered as candidates to address these use-cases and requirements. The well-established organization of the OSI-model will be used for a structured description.

2.1 Layer 2 (Data Link) Protocols and Mechanisms

The following protocols and mechanism can be associated with the Ethernet data link layer:

A. Virtual Local Area Network

Virtual Local Area Network (VLAN), i.e. IEEE 802.1Q[14] is a well-established mechanism to subdivide a physical network (within a switch or across multiple switches) into separate, isolated logical networks at OSI layer 2. An additional header between Source MAC Address and EtherType and Size field carries the necessary VLAN identifier. VLAN aware network components ensure that packets only flow between nodes which are assigned to the same VLAN, consequently virtual networks are established and communication across the virtual networks shall be only feasible via routing in upper layers, e.g., IP. While there are conceivable attacks to break VLAN isolation, cf. VLAN hopping, e.g., via switch spoofing and double tagging[11], current switch implementations with a well-crafted configuration, especially with respect to dynamic tagging mechanisms and inter-switch communication via trunk ports, are considered to provide a robust isolation mechanism. However,

flooding attacks which might lead to Denial of Service scenarios with respect to safety related communications is still an issue. Thus switches that support at least ingress rate-limiting are required for automotive use-cases.

Based on the robustness of the VLAN mechanism and the widespread support in Commercial of the Shelf (COTS) network components, the application of VLANs can be considered as the basic mechanism to establish different logical Ethernet networks in the vehicle. Please note that communication between different VLANs needs a routing mechanism (might be part of a Layer 3 Switch) on upper layer protocols. This routing mechanism of upper layers might look similar to forwarding rules defined in a CAN communication matrix, but one should be considered that an IP route is somewhat different, because it allows any kind of IP communication between network segments and stations covered by that route. A CAN communication matrix enforced by a CGW would be more comparable with a firewall component comprising a packet filter and deep packet inspection mechanisms.

B. Port-based Network Access Control

Port-based Network Access Control (PNAC), i.e. 802.1X[16] is a well-known mechanism from wireless LANs (IEEE 802.11), but was initially specified to encapsulate the Extensible Authentication Protocol (EAP) specified in RFC5247 over LAN (EAPOL). 802.1X provides a mechanism to authenticate nodes wishing to connect to a LAN, respectively WLAN. The communication via a port of a switch that supports 802.1X is only feasible after the node proved its identity performing EAPOL via the switch to the authentication server. The EAP only defines message formats, respectively the authentication framework. Therefore, the concrete implementation is highly flexible, i.e., the protocol only needs to be supported by supplicant and authentication server. A huge amount of methods are existed to implement EAP, e.g., ranging from Public-Key-Cryptography based systems to Pre-Shared-Key based approaches, which might fit better to automotive constraints. 802.1X is not yet intensively used in automotive Ethernet networks, but there is a high possibility to apply Port-based Network Access Control according to 802.1X in future automotive EE-Architectures.

C. Media Access Control (MAC) Security

Media Access Control (MAC) Security (aka. MACsec), i.e. 802.1AE[12] is a standard which can be used to provide secured (confidentiality as well as integrity) point-to-point communication between trusted entities in a LAN. Each MACsec protected frames starts with a Security Tag (SecTAG), which is an extension of the EtherType field and includes, e.g., the Packet Number (PN), used for replay protection(cf. Figure 4). Then the secured data comprising the VLAN tag and user data is transmitted before the Integrity Check Value (ICV)is appended. The ICV ensures the integrity of the MAC Destination Address, MAC Source Address, SecTAG and User Data.

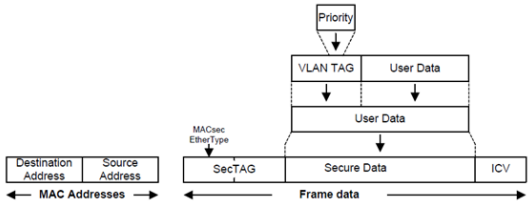

Fig. 4. MACsec Frame including VLAN TAG and QoS[12]
그림 4. VLAN TAG와 QoS를 포함하는 MACsec 프레임[12]

GCM-AES-128/256 (Galois/Counter Mode of Advanced Encryption Standard, 256bit length supported since 2011) and GCM-AES-XPN-128/256 (since 2013) have been specified to be used as the cryptographic algorithms. Please note that key management aspects as well as the establishment of the Security Associations, i.e., the security relationships between the nodes, are not part of 802.1AE. It is assumed that the mechanism relies on the MACsec Key Agreement (MKA) Protocol defined in the 2010 revision of 802.1X.

MACsec protects frames on a hop-by-hop basis. This implies that switches need to support MACsec.

But currently no automotive and embedded switch exists which supports 802.1AE and MKA. Network components which support this mechanism are quite expensive and are today only used in environments with extraordinary security needs. Furthermore, this means that MACsec does not fulfill the typical requirement of end-to-end secured communication.

D. Transport Protocol for Time-Sensitive Applications

Transport Protocol for Time-Sensitive Applications in Bridged Local Area Networks (AVTP), AES/ECC Encrypted Format and ECC Signed Control Format, IEEE 1722 (Draft, April 2015)[13]: The Audio/Video Transport Protocol (AVTP) specifies a protocol to transport time-sensitive audio, video, and control data directly on an underlying MAC layer, such as in this case Ethernet. Because AVTP was originally developed to transport audio/video data, the legacy name AVTP was kept, although the current draft, especially addresses the use case to transport control data[13]. Among others, the control data transport mechanism of AVTP provides support to transport CAN, FlexRay, LIN, MOST and General Purpose Messages in AVTP Control Format (ACF) messages. The current AVTP draft[13] and the current version of the standard also describes three different mechanisms to protect AVTP payload:

- AES Encrypted Format: The payload encapsulated in an AES encrypted AVTP frame is a complete AVTP data unit encrypted with AES-SIV (Synthetic Initialization Vector (SIV) Authenticated Encryption using the Advanced Encryption Standard and a key size of 128/256 bits), shared between the talker and the intended listener.
- ECC Signed Control Format: In ECC signed format, the AVTPDU is cryptographically signed with an Elliptic Curve Cryptography (ECC) algorithm. More concrete, ECSSA_DSA_EMSA1_SHA256 shall be used, cf. IEEE Std. 1363a-2004.
- ECC Encrypted Control Format: The format is used to protect AVTPDUs by application of elliptic curve public key cryptography. More concrete, the Discrete Logarithm and Elliptic Curve Integrated Encryption Scheme (DL/ECIES) as specified in IEEE 1363a-2004 Section 11.3.2 shall be applied.

The draft refers to the specification of the key management which is already included in IEEE 1722.1 and defines the establishment of a chain of trust based on ECC cryptography. However, the ECC parameters (e.g., selected curve) are not addressed in IEEE 1722.

It is important to understand that no security mechanisms of upper layer, e.g., firewalls or IPSec/TLS, can be used to secure IEEE 1722 network traffic since the messages are directly exchanged on the Data Link Layer. Due to the fact that the IEEE 1722 standard already provides a huge selection of security mechanisms, there would be a good chance to use IEEE 1722 with its security features in future vehicles. AES Encrypted Format can be used because the necessary hardware crypto accelerators are often available in typical automotive μCs/μPs.

E. Standard for Local and Metropolitan Area Networks

Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks - Amendment: Per-Stream Filtering and Policing, IEEE P802.1Qci/D0.0[15](Draft): This standard, which is currently under specification, will cover the feature to apply a per-stream filtering and policing for IEEE 1722. Such a kind of mechanism is required, cf. VLAN section, to avoid flooding attacks. However, as the standard is still far from being finalized, no assessment can be provided yet. Furthermore, it is necessary that a misuse of the traffic shaping mechanism, which might lead to Denial of Service attacks, is prevented.

2.2 Layer 3 (Network) and Layer 4 (Transport)

It is assumed that other protocols beside IEEE 1722will be used on top of Ethernet in future automotive EE-Architectures. This means that well

established security protocols as Transport Layer Security (TLS) and IPSec can be reused in automotive systems, as discussed[1]. As those mechanisms are well known, further details are not mentioned. Please note that application of TLS/IPSec might be challenging in the vehicle due to i) key management aspects and ii) missing hardware accelerators for public key cryptography. Assuming the key management aspects need to be solved (cf. Section 3.1 on SecOC), TLS with Pre-Shared-Keys would be an interesting concept for some in-vehicle communication use-cases.

In addition to the protocols, it is important to establish firewalls between the networks to enforce the communication policy for layer 3 and above. Additional information on this topic is not provided since most of the mechanisms (static as well as stateful packet-filtering etc.) are well known from classical IT security.

2.3 Upper OSI Layers

For layers above transport layer, it is hard to provide general recommendations; because suitable security mechanisms are often use-case dependent and

Table 1. Summary of automotive Ethernet security
표 1. 차량 이더넷 보안 요약

OSI Layer	Technologies/ Protocols/ Standards	General IT Environment	Automotive Ethernet
Layer 2	Virtual Local Area Network (VLAN)	A well-established mechanism to subdivide a physical network (within a switch or across multiple switches) into separate, isolated logical networks at OSI layer 2	Can be considered as the basic mechanism to establish different logical Ethernet networks in the vehicle. Communication between different VLANs needs a routing mechanism on upper layer protocols.
	Port-based Network Access Control (PNAC)	A mechanism well known from wireless LANs (IEEE 802.11), but it was initially specified to encapsulate the Extensible Authentication Protocol (EAP) specified in RFC5247 over LAN (EAPOL).	802.1X is required by most of OEMs, but is not yet intensively used in automotive Ethernet networks due to lack of specification.
	Media Access Control (MAC) Security	A standard which can be used to provide secured (confidentiality as well as integrity) point-to-point communication between trusted entities in a LAN.	No automotive/embedded switch exists which supports 802.1AE and MKA. Typically, network components that support this mechanism are quite expensive and are only used in environments with extraordinary security needs.
	Audio/Video Transport Protocol (AVTP)	A protocol to transport time-sensitive audio, video, and control data directly on an underlying MAC layer,	Due to the fact that the IEEE 1722 standard already provides security mechanisms, good chance to use IEEE 1722 with its security features in future vehicles
	Per-Stream Filtering and Policing	The feature to apply a per-stream filtering and policing for IEEE 1722. Such kind of mechanism is needed; cf. VLAN section, to avoid flooding attacks.	No assessment can be provided yet
Layer 3 & 4	IPSec	The ability to encrypt any higher layer protocol, including arbitrary TCP and UDP sessions, so it offers the greatest flexibility of all the existing TCP/IP cryptosystems.	Be challenging in the vehicle due to i) key management aspects and ii) missing hardware accelerators for public key cryptography it is important to establish firewalls between the (virtual) networks to enforce the communication policy for layer 3 and above.
	Transport Layer Security (TLS)	Privacy and data integrity between two communicating computer applications. In addition to the properties of privacy and data integrity, careful configuration of TLS can provide additional privacy-related properties such as forward secrecy.	
Upper Layers	Hard to be defined	Security implementation in the level of application.	Hard to provide general recommendations; because suitable security mechanisms are often use-case dependent and some applications already provide their own end-to-end security mechanism.

some applications already provide their own end-to-end security mechanism. However, one should consider implementing an Application Layer Filter (transparent or proxy).In addition, it is important (while not directly related to layer 7) to carefully review the communication stack and verify that no communications break the security policy, e.g., check integration of diagnosis protocols as XCP.

3. Summary

In this section, the described security features of AUTOSAR and automotive Ethernet are summarized.

To apply secure communication in AUTOSAR, the concept of SecOC supports both signal-based communication over classical automotive bus systems (e.g., CAN) and other, also future communication approaches using new communication systems like automotive Ethernet. The concept was released as a standard as part of AUTOSAR 4.2.1 in 2014. It supports a wide range of mechanisms based on both symmetric and asymmetric cryptography and various communication paradigms.

Furthermore, the security features of automotive Ethernet are summarized with OSI layers in Table 1.

Ⅳ. Conclusion & Outlook

Automotive Ethernet will be an important enabler for future automotive EE- Architectures, e.g., needed for use-cases like automated driving. It provides a huge range of advantages compared to legacy automotive networks, e.g., regarding performance and architectural flexibility. However, as presented in this paper, automotive integration of Ethernet introduces new security challenges. On the other hand, Ethernet provides the chance to reuse well-established classical IT security mechanisms and to define new automotive specific ones. This paper presented a selection of that kind of mechanisms and evaluated their suitability for automotive use. It is concluded that a smart combination of the available mechanisms, all through the whole OSI stack, should provide a sufficiently robust security concept for the future Ethernet-based EE-Architecture.

However, there are a lot of urgent challenges to be solved, e.g., i) implementation of the necessary SW components for the basic software stacks, ii) integration of the necessary hardware security means (crypto accelerators and trusted environments) into typical automotive controllers and iii) concepts for key management. Finally, it is convinced that a highly networked vehicle deserves a customized overall security concept, among others backed by a security concept per ECU.

References

[1] S. Bayer, M. Lange, M. Wolf: Automotive Ethernet Security. In Hanser Automotive Networks Special, Carl HanserVerlag, Issue 2013, November 2013.

[2] B. Glas “Towards Harmonization of ECU Protection and Secure OnBoard Communication in AUTOSAR” ESCAR Asia 2014, Tokyo

[3] B. Glas et al “Towards Authentic In-Car Communication on Automotive Bus Systems”, 29. VDI/VW Gemeinschaftstagung Automotive Security, Kassel, 2013

[4] NHTSA: Part 573 Safety Recall Report - Recall No. 15V-461. 2015-07-23 http://www-odi.nhtsa.dot.gov/acms/cs/jaxrs/download/doc/UCM483036/RCLRPT-15V461-9407.pdf

[5] K. Koscher, et al.: Experimental security analysis of a modern automobile. IEEE Symposiumon Securityand Privacy, Oakland, CA, May16 - 19, 2010.

[6] S. Checkoway, et al:Comprehensive Experimental Analyses of Automotive Attack Surfaces. USENIX Security, August 10 - 12, 2011

[7] M. Wolf, A. Weimerskirch and C. Paar: Security in automotive bus systems. In Proceedings of the Workshop on Embedded Security in Cars (escar)'04

[8] C. Miller and C. Valasek: Remote Exploitation of an Unaltered Passenger Vehicle. 2015-08-10 http://illmatics.com/Remote%20Car%20Hacking.pdf

[9] I. Foster, A. Prudhomme, K. Koscher and S. Savage: Fast and Vulnerable: A Story of Telematic Failures. 9zh USENIX Workshop on Offensive Technologies, Washington D.C., 2015-08-10 http://cseweb.ucsd.edu/~ savage/papers/WOOT15.pdf

[10] C. Miller and C. Valasek: A Survey of Remote Automotive Attack Surfaces 2014-08-06 http://illmatics.com/remote%20attack%20surfaces.pdf

[11] Sean Convery (Cisco Systems): Hacking Layer 2: Fun with Ethernet Switches. 2002-08-01 http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf

[12] IEEE: 802.1AETM-2006 Standard for Local and metropolitan area networks - Media Access Control (MAC) Security. 2006-08-18

[13] IEEE: P1722-rev1TM/D13 - Draft Standard for a Transport Protocol for Time-Sensitive Applications in Bridged Local Area Networks. April 2015

[14] IEEE: 802.1Q-2014Standard for Local and metropolitan area networks--Bridges and Bridged NetworksIEEE 802.1Q

[15] IEEE: P802.1Qci/D0.0 Draft Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks -Amendment: Per-Stream Filtering and Policing. 2015-05-18

[16] IEEE: 802.1X-2010 - IEEE Standard for Local and metropolitan area networks-Port-Based Network Access Control. 2010-02-05

[17] M. Lee: Design of In and Outdoor communication hub in Vehicular networks: The Journal of The Institute of Internet, Broadcasting and Communication (JIIBC), VOL.12 No.3, pp.187-194, June 2012

[18] K. Cho and J. Chung: Development of Auto-Parking Algorithm for Driving in Urban: Journal of the Korea Academia-Industrial cooperation Society(JKAIS), Vol. 12, No. 5 pp. 2360-2366, 2011

저자 소개

이 호 용(정회원)

- 2002년 : 고려대학교 컴퓨터학사
- 2003년 ~ 2013년 : 삼성SDS 보안/네트웍 엔지니어/컨설턴트
- 2013년 ~ 현재 : escrypt GmbH in Korea, Embedded Security consultant
- 2015년 ~ 현재 : 고려대학교 정보보호대학원 석사과정

<주관심분야 : 암호프로토콜, 암호이론, 차량보안, 임베디드 보안>

이 동 훈(정회원)

- 1983년 : 고려대학교 경제학사
- 1987년 : Oklahoma University 전산학과 석사
- 1992년 : Oklahoma University 전산학과 박사
- 1993년 ~ 1997년 : 고려대학교 전삭학과 조교수
- 1997년 ~ 현재 : 고려대학교 정보보호대학원 교수

<주관심분야 : 암호프로토콜, 암호이론, USN이론, 키교환, 익명성 연구, PET 기술>