정 보 보 호 학 회 지
제 31 권 제4호, 2021. 8

ITU-T SG17에서의 차량 통신 보안 국제 표준화 동향

이 상 우*, 전 용 성*

요 약

최근 자율주행차량등의 활발한 기술 개발 및 상용화가 추진되고 있다. 차량통신기술은 자율주행차량이 주변 환경을 보다 정확하고 상세하게 인지하기 위하여 그 필요성이 강조되고 있는 실정이다. 이러한 차량통신기술의 활용성이 증대됨에 따라, 보안 위협에 대응하기 위한 보안 기술도 활발히 연구 개발 추진 중이며, 이와 연관된 국제표준화의 필요성도 부각되고 있다. IT 보안 국제표준화 기구인 ITU-T SG17에서는 최근 연구반 구조 조정을 진행했으며, ITS(Intelligent Transport System) 보안 연구반(Q13)은 지속적으로 차량통신표준화를 추진한다. 본 논문에서는 ITS 보안 연구반의 최근 활동 및 진행 계획을 소개한다.

Ⅰ. 서 론

차량통신기술은 자율주행차량의 필수 요소 기술로서 상용화가 진행 중이며, 차량 통신 환경에서의 사이버 보안사고 방지를 위한 연구 개발 및 다양한 표준화 활동이 진행되고 있다[1-4]. 특히, 현재 상용화에 박차를 가하고 있는 자율주행차량에서는 센서를 통해 수집되는 차량 주변 환경 정보의 한계를 극복하기 위한 기술의 하나로 차량 간 통신의 활용 필요성이 증가하고 있다. 또한, 다수의 센서의 증가로 인해 증가되고 있는 차량 내부 데이터 처리를 위하여 도입이 추진되고 있는 차량 이더넷 환경에서의 보안 취약점에 대한 대응 기술 및 차량과 클라우드와의 연계를 통한 차량 사이버 보안성 강화 등의 중요성이 부각되고 있다.

ITU-T SG17은 ITU-T 산하에서 ICT 보안 기술에 대하여 표준화를 추진하는 그룹이다. ITS 보안 연구반은 2017년 3월에 설립되어, 차량내부망 보안, 차량외부망 보안 및 ITS 응용 보안 분야에서 표준화가 활발히 진행 중이다. 본 논문에서는 SG17의 ITS 보안 연구반에서 2021년 4월 회의에서 논의된 내용을 중심으로 국제 표준화 최근 동향을 살펴보고, 현재 진행 중인 내용 및 앞으로의 추진 계획을 소개한다.

Ⅱ. ITU-T SG17에서의 차량통신보안 표준화 현황

본 절에서는 ITS 보안 연구반(Q13)에서 최근 2021년 상반기까지 표준 최종 승인이 완료된 건과 현재 표준화과 진행 중인 내용을 소개한다.

2.1. Q13의 최종 표준 승인 현황

Q13의 표준화 분야는 차량통신보안 분야에 대한 전반적인 기술을 포함하고 있으며, 특히, 차내망 통신 보안, 차외망 통신 보안, 안전한 지능형교통시스템 구축을 위한 보안 기술 등을 포함한다.

현재 Q13에서는 2020년 8월 회의 이후 아래의 3건의 표준이 최종 승인되었다[7-9].

- X.1374: Security requirements for external interfaces and devices with vehicle access capability
- X.1375: Guidelines for an intrusion detection system for in- vehicle networks
- X.1376: Security-related misbehaviour detection mechanism for connected vehicles

2020년 8월 회의에서 X.1374(기존 X.itssec-3)가 사전 승인 되고, 회람 후 2020년 10월에 최종 승인되

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2020-0-00913, 무선 은닉채널 위험성 검증 연구)
* 한국전자통신연구원 (책임연구원, ttomlee@etri.re.kr, 책임연구원, ysjeon@etri.re.kr)

었다. X.1374는 차량에 접속하는 디바이스가 만족시켜야 할 보안요구사항을 정의하는 것으로, 현대차 및 ETRI가 주도적으로 표준화를 추진하였다[7]. X.1374는 특히 차량 내부 진단 도구의 접속 인터페이스로 활용되고 있는 OBD-II (On-Board-Diagnostic II) 포트 및 차량에 사용자가 소유하고 다니는 모바일 디바이스의 인터페이스로 활용되는 블루투쓰 등을 이용하여 차량에 접속하는 디바이스에 대한 보안요구사항을 정의하고 있다. 차량에 접속하는 디바이스의 일반적인 보안요구사항으로 하드웨어가 지원하는 보안 기능을 구비할 것을 명시하고 있으며, 세부적인 요구사항으로는 보안 CPU, 보안 저장장치, 하드웨어 암호 가속 기능을 제시하고 있다. 차량 외부 접속 장치의 통신 기능 보안요구사항으로는 블루투쓰, 이동통신, Wi-Fi 사용 시에 준수해야 하는 보안요구사항을 기술하고 있다. 스마트 키의 경우에는 키 추출방지 기능 및 one time programmable 기능 등의 역공학방지요구사항, 상호인증, 재생공격방지 및 무선신호전력제어 등의 통신보안 요구사항과 안전한 키 등록 기능 요구사항을 제시하고 있다. 또한, 외부접속장치로서, 스마트 키, Wi-Fi 또는 블루투쓰를 이용하는 접속장치에 적용될 수 있는 보안 제어 방법을 유즈 케이스로 제시하고 있으며, 특히, 전기차충전시스템 보안요구사항도 기술하고 있다. 부록에는 블루투쓰 및 이동통신망에 대한 세부 기술 규격을 기술하고 있다. 본 표준은 차량 완성차 업계의 요구사항을 반영하여 진행된 표준으로서, 향후 차량에 접속하는 디바이스 제작 및 관련 서비스 업계에서 참고할 필요가 있다.

2020년 8월 회의에서 X.1375(기존 X.itssec-4)가 사전 승인 되고, 회람 후 2020년 10월에 최종 승인되었다. X.1375는 차내망에서의 침입탐지시스템 구성 방법을 정의하는 것으로, 고려대, 현대차 및 ETRI가 주도적으로 표준화를 추진하였다[8]. X.1375는 차내망에서 주로 활용되고 있는CAN(Controller Area Network)에 적용될 수 있는 침입탐지시스템의 기능 및 규격을 정의하고 있다. 본 표준에서는 차내망에서의 침입탐지시스템의 기본 구조와 각 구성요소의 기능을 소개한다. 그리고, CAN 중심의 차내망에서의 보안 위협을 정의한다. 그리고, 차내망 침입탐지시스템 구현을 위한 탐지 방법을 정적탐지(Static detection), 오용탐지(Misuse detection) 및 비정상탐지(Anomaly detection)으로 구분하고, 탐지 보고 시의 룰셋의 내용을 정의한다. 부록에는 차내망 침입탐지시스템의 기본적인 구조와 차내망 트래픽의 특징을 기술하고 있다.

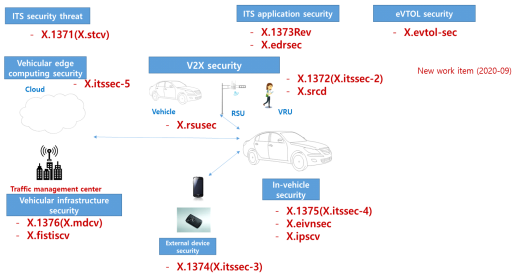
2020년 8월 회의에서 X,1376(기존 X.mdcv)이 사전 채택되고, 2021년 1월 회의에서 최종 승인되었다[9]. X.1376에서는 차량의 사이버 보안 관련 비정상행위 탐지 메커니즘을 정의하고 있으며, 비정상행위 수집 및 탐지 방법을 제공한다. 특히 비정상행위 탐지의 다양한 방법을 제공하고, 해당 방법에 대한 사용 예를 부록에 담고 있다. 이 표준은 중국의 보안 업체 Qihoo 360 Technology에서 주도한 표준으로서, 차량용 안티바이러스 제품에 활용될 가능성이 높다.

2.2. Q13의 표준화 진행 과제 현황

ITU-T SG17 Q13에서는 2021년 8월 현재 아래의 9개 표준화 과제가 진행 중이다[10-17].

- X.itssec-5: Security guidelines for vehicular edge computing
- X.srcd: Security requirements for categorized data in V2X communication
- X.eivnsec: Security guidelines for Ethernet-based in-vehicle networks
- X.edrsec: Security guidelines for cloud-based data recorders in automotive environment
- X.fstiscv: Framework of security threat information sharing for connected vehicles
- X.1373rev: Software update capability for ITS communication devices
- X.rsu-sec: Security requirements for road-side units in intelligent transportation systems
- X.ipscv: Methodologies for intrusion prevention systems for connected vehicles

그림 1은 2021년 8월 현재 Q13 표준화 과제 현황 및 분야를 나타낸 것이다. V2X 통신환경에서 데이터 속성에 따른 보안 등급 분류는 X.srcd에서 다루어지고 있다. 보안관리서버, 교통관제서버 등의 인프라 및 클라우드에 연관된 보안 표준화는 X.fstiscv 및 X.itssec-5에서 다루어 지고 있다. 특히, 차량내부망 보안을 위해서는 X.1375에서 CAN 중심의 일반적인 차량용 침입탐지시스템 방법론이 표준화 진행되었으며, 현재 이슈가 되고 있는 차량용 이더넷 보안 분야는 별



〔그림 1〕 Q13 표준화 현황

도의 표준화 과제인 X.eivnsec에서 심도 있게 다루어지고 있다. 또한, ITS 응용분야로서, 차량용 소프트웨어 업데이트 보안은 X.1373rev에서, 차량용 사고기록장치 보안은 X.edrsec에서 다루어지고 있다. X.rsu-sec의 표준화 목적은 차량통신환경에서 인프라 및 차량과의 통신을 담당하는 노변기지국(RSU, Road-side unit)의 보안요구사항을 정의하는 것이다[16]. 본 표준은 중국의 차이나 모바일이 주도적으로 추진하고 있으며, 향후 셀룰러 V2X 환경을 고려한 보안요구사항도 정의해 나갈 계획이다.

X.ipscv의 표준화의 목적은 차량의 침입방지시스템의 구현방법론을 정의하는 것이다. 차내 침입탐지시스템은 자원 제약으로 인해, 최소한의 탐지기능만 탑재하고, 수집된 침입 탐지 결과를 활용하여, 차량 외부의 서버 단에서 탐지 결과를 분석하여, 최종적으로 차량이 외부의 비정상적인 공격에 대하여 안전할 수 있도록 하는 프레임워크를 제공하는 것이 목적이다. 즉, 차량 침입탐지시스템의 보안 기능을 정의하는 X.1375와 연계하여, 차내망 침입탐지기능을 이용하여, 차량 보안 위협을 방지 할 수 있는 구현 지침을 개발해 나갈 계획으로, 한국의 고려대, 현대차, ETRI가 주도적으로 추진하고 있다.

X.eivnsec의 표준화 목적은 이더넷 기반 차량 내부 네트워크의 보안위협, 보안요구사항 및 사용 예를 정의하는 것이다. 차량에 탑재된 카메라 및 센서 등으로 인하여 차량 내부망에서 송수신되는 데이터 양이 증가함에 따라 현재 완성차 업계에서는 차량용 이더넷의 도입을 추진하고 있으며, 이러한 업계의 현황을 반영하여 한국의 ETRI 및 차량보안업체 Escrypt가 주도적으로 표준화를 추진하고 있다. 또한, 독일의 차량부품 업체 Bosch에서 관심을 가지고 적극적으로 표준화를 추진 중이다. 특히, 지난 4월 회의에서는 이더넷기반 차내망의 보안 위협 및 보안요구사항에 대하여 전반적인 내용을 완성하고, 차내망 이더넷 보안게이트웨이의 기능요구사항을 정의하고 있다. 부록에는 차량용 이더넷을 지원하는 AUTOSAR(AUTomotive Open System ARchitecture) 규격과 차량 게이트웨이에 대한 정보를 포함하고 있다.

X.edrsec은 클라우드 기반의 차량 사고기록장치 시스템의 보안위협, 보안요구사항 및 사용 예를 정의하는 것이다. 특히, 자율주행차 운행에 있어서, 사고 당시의 차량운행주체정보의 안전한 전송 및 관리 방법에 대한 보안요구사항도 정의해 나가고 있다. Q13에서는 차량 사고기록장치에 대한 표준화를 시작으로, 철도 및 해상 분야로 표준화 범위를 확장해나갈 예정이며, 한국의 ETRI 및 현대차가 주도적으로 표준화를 추진 중이다.

X.itssec-5는 차량 에지 컴퓨팅 보안 가이드라인을 정의하는 것으로 ETRI가 주도적으로 표준화를 추진하고 있다. 에지 컴퓨팅은 기존의 클라우드 서비스를 엔드 클라이언트와 물리적으로 가까운 곳에서 수행하는 것을 의미하는 것으로, 기존의 클라우드 컴퓨팅 환경에서의 네트워크 지연 시간으로 인하여 사용자에게 실시간 응답 서비스를 제공하기 어려운 단점을 극복하고 엔드 클라이언트에게 보다 빠른 서비스를 제공하기 위한 에지 컴퓨팅이 활발히 연구되고 있다. 특히 ETSI에서는 이동통신 기지국을 에지 컴퓨팅 서버로 활용하는 MEC (Multi-access Edge Computing)에 대한 표준화가 진행 중이다. 차량 통신 환경에서는 도로기지국이 에지 컴퓨팅 서버로 활용될 수 있으며, X.itssec-5에서는 이에 대한 보안 요구사항 정의를 목표로 한다.

2.3. ITS 보안 연구반(Q13) 신규 표준화 과제

2020년 8월에 도심항공모빌리티 보안 관련 과제가 신규로 채택되었다[18].

- X.evtol-sec: Security guidelines for electric vertical take-off and landing (eVTOL) vehicle in an urban air mobility environment

eVTOL은 전기동력 수직 이착륙 항공기를 의미하는 것으로 도심용 항공 모빌리티(UAM, Urban Air Mobility)의 대표적인 교통 수단이다. eVTOL은 활주로가 필요 없는 교통수단으로서 에어 택시라고도 불린

다. eVTOL과 드론과의 가장 큰 차이점은 eVTOL은 사람을 탑승객으로 하는 교통수단이라는 점이다. 따라서, Q13에서는 차량의 보안 표준화 역량을 기반으로 도심형 항공 모빌리티 보안 표준화를 추진하기 위하여, 20년 8월 회의에서 X.evtol-sec을 신규 표준화 과제로 채택하고, 한국의 현대차 및 ETRI가 표준화를 주도적으로 추진할 계획이다.

Ⅲ. 결 론

본 논문에서는 SG17 ITS 보안 연구반(Q13)에서 추진되고 있는 표준화 진행 현황을 소개하였다. 특히, 최근 2020년 하반기 및 2021년 상반기에 최종 승인된 표준안 3건과 현재 진행 중인 표준화 과제에 대하여 기술하였다. SG17은 올해 상반기에 4년간의 연구회기를 종료하고, 차기 연구회기를 시작하여야 하나, 코로나-19로 인하여 현재 회기가 연장되어 내년 상반기까지 현재 회기의 표준화 연구 체계를 유지한다. 이에 앞서, 지난 4월에 일부 구조 조정을 하여, 4개의 중분류 그룹(Working Party)이 5개로 확장되었으며, 일부 연구반이 통합되었다. 현재까지 ITS 보안 연구반은 차기 연구 회기에도 지속적으로 표준화를 추진해 나갈 것으로 예상되고 있다.

중국에서는 ITS 보안 표준화의 중요성을 인식하고, 중국의 IT 연구기관 CAICT(China Academy of Information and Communications Technology), 및 안티바이러스 업체 360 Technology(현재, 베이징 Qihu Keji Co.), 그리고 침해대응센터인 CN-CERT 및 차이나 모바일에서 신규 표준화 과제를 지속적으로 제안하는 등 표준화에 박차를 가하고 있다. 또한, 독일의 Bosch에서도 차량통신보안의 중요성을 인지하고, 적극적으로 표준화에 참여하고 있는 상황이다.

한국에서는 현대차, ETRI, 고려대 등이 주도적으로 표준화에 참여하고 있으나, 중국의 약진 등의 상황을 고려할 때, 지속적인 차량보안 표준화의 주도권 선점이 필요하며, 이를 위한 학계, 산업계, 연구기관 등의 적극적인 표준화 참여가 필요하다.

참 고 문 헌

[1] 이상우 외, “차량 통신 보안 기술 동향,” 주간기술동향, vol. 1556, 2012.

[2] ETSI EN 302 665, Intelligent Transport Systems (ITS); Communications Architecture, 2010.

[3] IEEE Std 1609.2, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) Security Services for Applications and Management Messages, 2016.

[4] ITU-T SG17 Recommendation, X.1373, Secure software update capability for ITS communications devices. 2018

[5] ITU-T SG17 Recommendation, X.1372, Security guidelines for Vehicle-to-Everything(V2X) communication. 2020.

[6] ITU-T SG17 Recommendation, X.1371, Security threats to connected vehicles, 2020 .

[7] ITU-T SG17 Recommendation, X.1374, Security requirements for external interfaces and devices with vehicle access capability, 2020.

[8] ITU-T SG17 Recommendation, X.1375, Guidelines for an intrusion detection system for in- vehicle networks, 2020.

[9] ITU-T SG17 Recommendation, X.1376, Security-related misbehaviour detection mechanism based on big data analysis for connected vehicles, 2020.

[10] ITU-T SG17 draft Recommendation, X.itssec-5, Security guidelines for vehicular edge computing, 2021.

[11] ITU-T SG17 draft Recommendation, X.srcd, Security requirements for categorized data in V2X communication, 2021.

[12] ITU-T SG17 draft Recommendation, X.eivnsec, Security guidelines for Ethernet-based In-Vehicle networks, 2021.

[13] ITU-T SG17 draft Recommendation, X.edrsec, Security guidelines for cloud-based data recorders in automotive environment, 2021.

[14] ITU-T SG17 draft Recommendation, X.fstiscv, Framework of security threat information sharing for connected vehicles, 2021.

[15] ITU-T SG17 draft Recommendation, X.1373rev, Software update capability for ITS communications devices, 2021.

[16] ITU-T SG17 draft Recommendation, X.rsu-sec,

Security requirements for road-side units in intelligent transportation systems, 2021.
[17] ITU-T SG17 draft Recommendation, X.ipscv, Methodologies for intrusion detection system on in-vehicle systems, 2020.
[18] ITU-T SG17 draft Recommendation, X.evtol-sec, Security guidelines for electric vertical take-off and landing (eVTOL) vehicle in an urban air mobility, 2021.

〈저 자 소 개〉

이 상 우 (Sang-Woo Lee)
정회원
1999년 2월 : 경북대학교 전자공학과 학사
2001년 2월 : 경북대학교 전자공학과 석사
2009년 2월 : 경북대학교 전자공학과 박사
2001년 1월~현재 : 한국전자통신연구원 정보보호연구본부 / 책임연구원
2014년~현재 : ITU-T SG17 editor
2016년~2017년 : WMG in University of Warwick, UK, 방문연구원
2017년~현재 : ITU-T SG17 Q13 Rapporteur
<관심분야> 임베디드 보안, 차량통신보안, 융합보안, 무선 은닉채널보안

전 용 성 (Yong-Sung Jeon)
정회원
1990년 2월 : 경북대학교 전자공학과 학사
1992년 2월 : 경북대학교 전자공학과 석사
2010년 8월 : 경북대학교 전자공학과 박사
1992년 3월~1999년 10월 : 국방과학연구소 선임연구원
1999년 11월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원
<관심분야> 은닉채널, 임베디드 보안, 암호