정 보 보 호 학 회 지
제 33 권 제4호, 2023. 8

ITU-T SG17에서의 차량 통신 보안 국제 표준화 동향

이 상 우*, 전 용 성*

요 약

차량통신기술은 차량 간, 차량과 인프라 간 정보 교환을 가능하게 함으로써, 센서 기반의 자율 주행 차량의 센서로 인한 한계점을 보완할 수 있는 자율주행의 구현 요소 기술이다. 이러한 차량통신기술의 활용성이 증대됨에 따라, 보안 위협에 대응하기 위한 보안 기술도 활발히 연구 개발 추진 중이다. 또한, 이와 연관된 국제표준화의 필요성도 부각되고 있다. ICT 보안 국제표준화 기구인 ITU-T SG17에서는 ITS(Intelligent Transport Systems) 보안 연구반(Q13)에서 지속적으로 차량통신표준화를 추진하고 있다. 본 논문에서는 ITS 보안 연구반의 최근 활동 및 표준화 진행 계획을 소개한다.

Ⅰ. 서 론

차량통신기술은 자율 주행 차량의 센서 기반 주변 인식을 보완하여, 센서의 한계로 인해 수집할 수 없는 주변 정보를 차량과 차량, 차량과 인프라 간 통신을 이용하여 제공할 수 있다. 그러나, 차량 간 통신 기술은 보안 사고 발생 시 탑승자 또는 보행자의 생명에 심각한 문제를 초래할 수 있으므로, 반드시 보안기술이 선행적으로 연구되고, 상용화 시에 필수적으로 보장되어야 한다. 이러한 차량 통신 환경에서의 보안 사고 방지를 위한 연구 개발과 활발한 표준화 활동이 추진 중이다.[1-9].

ITU-T SG17 표준화 그룹은 ICT 분야의 표준화를 다루는 국제 기구인 ITU-T 산하에서 ICT 보안 기술에 대하여 전문적으로 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 연구반의 2023년 2월 회의 및 6월 라포처 그룹 회의(RGM, Rapporteur Group Meeting)에서 진행된 내용을 중심으로 차량 통신 보안 국제표준화 현황을 살펴본다.

Ⅱ. ITU-T SG17에서의 차량통신보안 표준화 현황

본 절에서는 ITS 보안 연구반(Q13)에서 최근 2023년 상반기까지 표준 최종 승인이 완료된 건과 현재 표준화과 진행중인 내용을 소개한다.

2.1. Q13의 2023년 2월 회의 주요 내용

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

지난 2023년 2월 회의에서 아래의 표준이 최종 표준 승인(Approval) 되었다 [12-15].

- X.1380: Security guidelines for cloud-based data recorders in automotive environment
- X.1381: Security guidelines for Ethernet-based in-vehicle networks
- X.1382: Guidelines for sharing security threat information on connected vehicles
- X.1383: Security requirements for categorized data in V2X communication

X.1380(기존 X.edr-sec) “클라우드 기반 차량 데이터 기록 장치 보안가이드라인”은 클라우드 기반의 차량 사고기록장치의 보안 위협, 보안 요구사항 및 사용예를 정의하고 있다. 차량 사고 시 차량 상태를 저장하고 있는 사고기록정보(EDR, Event Data Recorder)를

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2020-0-00913, 무선 은닉채널 위험성 검증 연구)
* 한국전자통신연구원 사이버보안연구본부 (책임연구원, ttomlee@etri.re.kr, ysjeon@etri.re.kr)

안전하게 클라우드로 전송하는 방법을 기술하고 있다. 또한, 자율주행차 운행에 있어서, 사고 당시의 차량운행주체정보의 안전한 전송 및 관리 방법에 대한 보안 요구사항을 정의하고 있다. 이 표준은 한국의 ETRI 및 현대차가 주도적으로 표준화를 추진하였다.

X.1381(기존 X.eivn-sec) “이더넷 기반 차내망 보안 가이드라인”은 이더넷 기반 차량 내부 네트워크의 보안 위협, 보안 요구사항 및 사용 예를 정의하는 것이다. 차량에 탑재된 카메라 및 센서 등의 도입에 따라 차량 내부망에서 송수신되는 데이터 양이 증가하는 상황이며, 이러한 데이터 양의 증가에 대응하기 위하여 현재 완성차 업계에서는 차량용 이더넷의 도입을 추진하고 있다. 이 표준에서는 차량 내부 네트워크가 이더넷 기반으로 구성될 때의 보안 기능 요구사항을 정의하고 있다. 부록에는 차량용 이더넷을 지원하는 AUTOSAR(AUTomotive Open System ARchitecture) 규격과 차량 게이트웨이에 대한 정보를 포함하고 있다. 이 표준은 한국의 ETRI 및 독일의 ETAS에서 주도적으로 표준화를 추진하였다.

X.1382(기존 X.fstiscv) “커넥티드 차량의 보안 위협정보 공유 가이드라인”은 커넥티트 차량 환경에서 자동차 제조업체 및 CERT(Computer network Emergency Response Team) 등이 사이버 보안 위협정보를 공유할 때, 각 이해관계자들의 역할을 정의하는 것이다. 공유되는 정보는 Automotive -ISAC(Information Sharing and Analysis Center)에서 제안한 Indicators, TTP(Tactics, Techniques and Procedures), Security alert, Threat intelligence report를 활용하며, 보안위협정보를 공유하는 단계를 정의하고 각 단계에 따른 요구사항을 기술하고 있다. 이 표준은 중국의 IT 침해대응센터인 CN-CERT가 주도적으로 추진하였다.

X.1383(기존 X.srcd) “V2X 통신 데이터 분류에 따른 보안 요구사항”은 V2X 통신환경에서 송수신되는 데이터를 분류하고, 분류된 데이터의 라이프 사이클을 고려하여 보안 레벨을 3가지 수준으로 정의하고, 정의된 보안 강도를 보장하기 위한 보안 요구사항을 정의하는 것이다. 일반적인 IT 환경에서의 클라우드 보안을 위한 데이터 보안 표준화 내용을 V2X 통신 환경에 적용한 표준이다. 이 표준은 중국의 CAICT(China Academy of Information and Communications Technology)와 일본의 KDDI에 의해 주도적으로 개발되었다.

2023년 2월 회의에서는 아래와 같이 진행 중인 표준화 과제에 대한 신규 TD(Template Document)가 발행되었다[16-20].

- X.1373rev, Secure software update capability for intelligent transportation system communication devices
- X.itssec-5, Security guidelines for vehicular edge computing
- X.idse: Evaluation methodology for in-vehicle intrusion detection systems
- X.evtol-sec: Security guidelines for electric vertical take-off and landing (eVTOL) vehicle in an urban air mobility environment
- X.sup-cv2x-sec: Supplement to X.1813 - Security deployment scenarios for cellular vehicle-to-everything (C-V2X) services supporting ultra-reliable and low latency communication (URLLC)
- X.evpnc-sec: Security guidelines for electric vehicle plug and charge (PnC) services using vehicle identity (VID)

또한, 아래의 아이템이 신규 과제로 채택되었다[21].

- X.ota-sec: Implementation and evaluation of security functions to support over-the-air (OTA) update capability in connected vehicles

X.ota-sec(OTA업데이트 기능을 지원하는 보안 기능의 구현 및 평가)의 표준화 범위는 커넥티드 차량에서 차내의 소프트웨어 또는 펌웨어를 원격에서 OTA(Over-The-Air)를 이용하여 업데이트 하는 경우, 이를 지원하는 보안 기능의 구현 고려사항과 평가방법을 제안하는 것이다. 현재 Q13에서는 X.1373rev(ITS 통신 디바이스의 안전 소프트웨어 업데이트 기능)의 개정 작업이 진행 중이다. 기존의 X.1373rev에서는 차량제조업체의 서버, 차량정비센터를 통하여 원격으로 차량의 소프트웨어를 업데이트하는 절차를 기술하고 있다. 그러나, 기존의 X.1373rev에는 OTA 기능을 이용하기 위한 보안 기능은 정의하고 있지 않고 있다. 이를 해결하기 위하여 X.ota-sec이 23년 2월 회의에서 신규 표준화 과제로 채택되었으며, 한국의 단국대, 이

타스 코리아, ETRI가 에디터쉽을 가지고 표준화를 추진할 계획이다.

2.2. Q13의 2023년 6월 RGM 회의 주요 내용

Q13에서는 2023년 8월 회의에서 1건의 표준화 과제에 대한 사전채택을 추진할 계획이다. 이를 위하여 지난 6월 RGM 회의에서는 사전채택 계획인 X.1373rev의 심도있는 논의가 진행되었다. X.1373rev의 주요 개정 내용은 다음과 같다.

첫째, 기존 X.1373에서 부가사항으로 지정하여, 정의되지 않았던 차내망에서의 소프트웨어 업데이트 절차가 지정되었다. 이를 위하여 차내망에서의 소프트웨어 업데이트 절차를 위한 메시지 형식을 기존의 차외망에서의 메시지 형식과 일관성을 가지도록 설계한 내용이 반영되었다.

둘째, 차내망에서 소프웨어를 업데이트하는 다양한 방법이 제시되었다. 압축된 형태로 업데이트할 소프트웨어를 전송하는 방법, 기존의 소프트웨어 대비 업데이트 될 내용과의 차이를 전송하는 방법, 메모리를 이중화하여, 업데이트된 소프트웨어와 이전 버전의 소프트웨어를 교체하는 방법을 제시하고 있다.

셋째, 기존 X.1373에서 기술하고 있는 위험 평가 내용이 부록에서 삭제되고, 본문과 연관된 위협과 보안요구사항만이 부록 1에 기술되었다.

또한, 지난 RGM에서는 기존에 진행 중이던 X.sup-cv2x-sec에 대한 표준 개발 작업이 추진되었다. X.sup-cv2x-sec (URLLC(Ultra-Reliable and Low Latency Communication)를 지원하는 C-V2X 배치 시나리오)는 초고신뢰·저지연 통신의 셀룰라 V2X 통신 서비스에서의 보안 기능 배치 시나리오를 정의하는 것을 목적으로 한다. 이 표준화 과제에서는 아래의 모듈을 정의한다.

- NMSF(Network Monitoring Server Function): C-V2X 환경에서 보안 체크 패킷을 수신하는 모듈
- NMCF(Network Monitoring Client Function): C-V2X 환경에서 보안 체크 패킷을 송신하는 모듈
- NMRF(Network Monitoring Relay Function): C-V2X 환경에서 보안 체크 패킷을 전달(릴레이)하는 모듈

〔표 1〕 Q13 23년 8월 회의 추진 계획

표준과제	에디터	승인 방식
X.1373rev	이상우(ETRI), 박승욱(Hyundai Motors) Koji Nakao(NICT)	사전 채택

이 표준화 과제에서는 차량의 NMCF가 보안 패킷을 직접적으로 전송하는 경우와, 주변 차량의 NMRF를 경유하여 보안 패킷을 전송하는 경우로 구분하여 배치 시나리오를 정의하고 있다. 또한, NMSF가 네트워크 에지에 있는 경우와, 5G 코어망에 존재하는 경우를 구분하여 배치 시나리오를 정의하고 있다. 그리고, 종단 단말이 차량이 아니라 도로기지국인 경우도 고려하여 배치 시나리오를 정의하고 있다.

또한, X.evtol-sec(전기동력 수직이착륙기 보안 지침)의 표준 개발도 진행되었다. 이 표준화 과제에서는 도심용 항공 모빌리티(UAM, Urban Air Mobility)분야에서의 사용 예를 정의하고 있다. 서비스 관점에서는 고정 항로를 가지는 셔틀 서비스, 항공 화물 운송, 항공 응급 지원 서비스를 사용 예로 제시한다. 또한, 구동환경 관점에서의 사용 예는 조종사가 탑승하는 경우, 원격에서 조종하는 경우 및 자율운행의 경우로 구분한다. 그리고, 이러한 도심용 항공 모빌리티 환경에서의 보안 위협, 보안 요구사항 및 보안 기능 구현 시의 고려사항을 정의하고 있다.

Ⅲ. 결 론

본 논문에서는 SG17 ITS 보안 연구반(Q13)에서 추진되고 있는 표준화 진행 현황을 소개하였다. 특히, 최근 2023년 상반기에서 최종 승인된 표준화 과제와 신규로 채택된 표준화 과제에 대하여 소개하였다. 또한 2023년 하반기 SG17회의에서 사전채택을 계획하고 있는 표준화 과제에 대한 최근 동향을 소개하였다. 2023년 하반기 SG17 회의는 한국의 일산 킨텍스에서 진행될 예정이다. 한국은 지난 2016년부터 의장국으로서 ICT 보안 표준화를 주도적으로 추진하고 있으며, COVID19 이후 스위스가 아닌 국가에서 처음으로 개최하는 회의로서, 중요한 의미를 가진다. 따라서, 예정된 표준화 과제의 승인 및 신규 과제 채택 등의 표준화를 주도적으로 추진해 나갈 필요가 있다.

중국에서는 ITS 보안 표준화의 중요성을 인식하고, 안티바이러스 업체 360 Technology(현재, 베이징

Qihu Keji Co.), 침해대응센터인 CN-CERT 및 차이나 모바일, 그리고 중국의 IT 연구기관 CAICT에서 지속적인 기고서 제안을 통하여 적극적으로 표준화를 추진 중이다. 일본에서도 통신회사인 KDDI, 연구소인 NICT(National Institute of Information and Communications Technology)에서 지속적으로 표준화에 참여하고 있다.

한국에서는 ETRI, 현대차, 고려대, 순천향대, 단국대, TTA, 맥데이타, 현대오토에버 등이 주도적으로 표준화에 참여하고 있으며, 지속적으로 표준의 제정에 기여하고 있다. 차량통신보안 국제표준화의 지속적인 국제 표준화 주도권 선점을 위하여 산업계, 연구기관, 학계 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 Recommendation, X.1377, Guidelines for intrusion prevention systems for connected vehicles 2022.

[11] ITU-T SG17 Recommendation, X.1379, Security requirements for road-side units in intelligent transportation systems, 2022.

[12] ITU-T SG17 Recommendation, X.1380, Security guidelines for cloud-based data recorders in automotive environment, 2023.

[13] ITU-T SG17 Recommendation, X.1381, Security guidelines for Ethernet-based In-Vehicle networks, 2023.

[14] ITU-T SG17 Recommendation, X.1382, Guidelines for sharing security threat information on connected vehicles, 2023.

[15] ITU-T SG17 Recommendation, X.1383, Security requirements for categorized data in V2X communication, 2023.

[16] ITU-T SG17 draft Recommendation, X.1373rev, Software update capability for ITS communications devices, 2023.

[17] ITU-T SG17 draft Recommendation, X.itssec-5, Security guidelins for vehicular edge computing, 2023.

[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, 2023.

[19] ITU-T SG17 draft Recommendation, X.evpnc-sec: Security guidelines for electric vehicle plug and charge (PnC) services using vehicle identity (VID), 2023.

[20] ITU-T SG17 draft Supplement, X.sup-cv2x-sec: Supplement to X.1813 - Security deployment scenarios for cellular vehicle-to-everything (C-V2X) services supporting ultra-reliable and low latency communication (URLLC), 2023.

[21] ITU-T SG17 draft Recommendation, X.ota-sec: Implementation and evaluation of security functions to support over-the-air (OTA) update capability in connected vehicles, 2023.

〈저 자 소 개〉

이 상 우 (Sang-Woo Lee)

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, 무선은닉채널보안

전 용 성 (Yong-Sung Jeon)

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