정 보 보 호 학 회 지
제34권 제4호, 2024. 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 차량 통신 보안 표준화를 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[1-14].

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 2024년 2월 회의 및 6월 라포처 그룹 회의(Rapporteur Group Meeting, RGM)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 2024년 상반기까지 표준 최종 승인이 완료된 건과 현재 표준화가 진행중인 내용을 소개한다.

2.1. Q13의 2024년 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 2024년 2월 회의에서 아래의 표준이 최종 표준 승인(Approval) 되었다 [15].

- X.1373: Software update capability for ITS communications devices

  X.1373(ITS 통신장비의 소프트웨어 업데이트)는 안전한 차량의 소프트웨어 업데이트 절차를 정의한다. 차량에서는 다수의 ECU(Electronic Control Unit)를 활용하고 있고, 리콜이 요구되는 차량의 약 30%가 ECU 소프트웨어의 업데이트로 인한 문제라고 보고되고 있는 현상을 반영하여, SG17의 ITS 보안 표준화 아이템 중에서 가장 먼저 2018년에 표준으로 승인되었다. 그러나, 2018년 표준안 최종 승인 과정에서 차내망과 연관된 메시지는 부가적인 메시지로 지정되었으나, 완성차 업계에서의 차내망 연관 규격을 포함하여야 한다는 의견이 반영되어 2024년 2월 회의에서 개정안이 최종 승인되었다. X.1373에서는 차

이 논문은 2024년도 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)

량의 원거리 소프트웨어 업데이트 개요, 위협 요소 및 위협 분석, 기능 요구사항, 안전한 소프트웨어 업데이트 구조를 정의한다. 이 표준에서는 차량 소프트웨어 업데이트 세부 절차의 메시지 포맷과 XML(Extensible Markup Language) 예제도 포함하여 기술하고 있다. 특히, 개정본에는 UDS(Unified Diagnostic Service) 프로토콜을 포함한 차내망 메시지 규격을 정의하는 것이 특징이다. 또한, 소프트웨어 업데이트 시 소프트웨어의 압축된 파일 전송, 기존 대비 차분 파일 전송, 메모리 복제 방식을 통한 업데이트 등의 구체적인 업데이트 방법을 정의하고 있다.

또한, 2024년 2월 회의에서는 아래의 표준이 사전 채택(Determination) 되었다.[16].

- X.1384(X.itssec-5), Security requirements and guidelines for vehicular edge computing

X.1384(X.itssec-5)는 차량 에지 컴퓨팅 보안 가이드라인을 정의하고 있다. 에지 컴퓨팅은 기존의 클라우드에서 수행되는 기능 또는 서비스를 수요자와 물리적으로 가까운 곳에서 수행하여 사용자에게 보다 빠른 응답 서비스를 제공하기 위하여 활발히 연구되고 있다. 이 표준에서는 차량 통신 환경에서 도로기지국이 에지 컴퓨팅 서버로 활용되는 것을 고려하여, 보안 위협 및 보안요구사항을 정의하고 있다.

또한, 아래의 아이템이 신규 과제로 채택되었다[21].

- X.aamd-sec: Security guidelines for categorized data in advanced air mobility (AAM)

X.aamd-sec(AAM 환경에서의 분류된 데이터에 대한 보안 가이드라인)의 표준화 범위는 미래 항공 모빌리티(Advanced Air Mobility, AAM)에서 통신 개체 간에 송수신되는 메시지의 종류를 보안 등급별로 구분하고, 이의 보안 처리 지침을 제공하는 것이다.

AAM은 도심형 항공 모빌리티(Urban Air Mobility, UAM)에서 운항 영역을 도심으로 한정하지 않고, 외곽지역에서 운행되는 항공 모빌리티를 모두 고려하는 개념이다. Q13에서는 기존의 X.evtol-sec에서 도심형 항공 모빌리티에 대한 보안 표준화를 다루고 있으며,

〔표 1〕 Q13 24년 2월 회의 주요 결과

표준과제번호	에디터	상태
X.1373	이상우(ETRI), 박승욱(현대차), Koji Nakao(NICT)	최종승인
X.1384 (X.itssec-5)	이상우(ETRI),	사전채택
X.aamd-sec	박승욱, 정창훈(현대차), 이상우(ETRI), 이유식(순천향대)	신규과제 채택

모빌리티의 기술 발전에 따라 미래 항공 모빌리티 분야에서 데이터 보안 표준을 선도적으로 추진하기 위하여, 24년 2월 회의에서 신규 아이템으로 채택되었다. 한국의 현대차, ETRI, 순천향대에서 에디터쉽을 가지고, 주도적으로 표준화를 추진할 계획이다.

2024년 2월 회의에서는 아래와 같이 진행 중인 표준화 과제에 대한 신규 TD(Template Document)가 발행되었다[17-21].

- X.idse: Evaluation methodology for in-vehicle intrusion detection systems
- X.evtol-sec: Security requirements and guidelines for telecommunications in an urban air mobility (UAM) 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)
- X.ota-sec: Implementation and evaluation of security functions to support over-the-air (OTA) update capability in connected vehicles
- X.af-sec: Evaluation methodologies for anonymization techniques using face images in autonomous vehicles
- X.fod-sec: Security guidelines for a feature on demand (FoD) service in a connected vehicle environment

2.2. Q13의 2024년 6월 RGM 회의 주요 내용

Q13에서는 2024년 8월 회의에서 표준최종승인(Approval) 1건, 사전채택(Determination) 1건, 동의(Agreement) 1건을 추진할 계획이다. 이를 위하여 지난 6월 RGM 회의에서는 사전채택을 계획하고 있는 X.evtol-sec 및 동의를 추진할 X.sup-cv2x-sec의 마무리 작업이 진행되었다.

X.evtol-sec의 주요 개정 내용은 다음과 같다.

첫째, 표준의 제목을 “Security requirements and guidelines for telecommunications in an urban air mobility (UAM) environment” 로 변경하였다. 이것은 지난 2월 회의에서, eVTOL(Electric Vertical Take-Off and Landing) 기체에 대한 보안이 아닌, 도심형 항공 모빌리티 환경에서의 통신 보안을 다루는 표준임을 강조하기 위하여, 표준의 제목에 telecommunications를 반영하고 eVTOL을 삭제하였다.

둘째, 용어 정의에 있어서, 원격 조종사(remote pilot)의 정의를 ICAO(International Civil Aviation Organization)의 정의를 준용하는 것으로 변경했으며, 의미가 불명확했던 보안관리자(safety manager)를 ICAO에 정의된 승무원(cabin crew member)으로 변경하여 표준안에 반영하였다. 이러한 수정 작업은 도심형 항공 모빌리티가 항공 체계 표준과 연관성이 높으므로, 가능한 ICAO에 정의된 용어를 활용하기 위하여 수행되었다.

셋째, 본 표준은 도심형 항공 모빌리티에서의 통신 보안을 다루는 것이 주요 목적이므로, 모빌리티 기체에 대한 내용을 부록으로 이동하여 작성하였다.

X.sup-cv2x-sec(URLLC(Ultra-Reliable and Low Latency Communication)를 지원하는 C-V2X(Cellular Vehicle-to-Everything) 배치 시나리오)의 표준화 범위는 초고신뢰·저지연 통신의 셀룰라 V2X 통신 서비스에서의 보안 기능 배치 시나리오를 정의하는 것을 목적으로 한다. C-V2X 서비스 환경에서 URLLC의 특성을 저해하는 상황인 보안 이벤트를 정의하고, 보안 이벤트를 감지하기 위하여 최대 종단간 지연시간 및 무선신호의 품질, 전력값 등을 측정하고 이 값들을 NMSF로 전달하는 메시지 규격을 정의하고 있다. 이러한 보안 이벤트를 탐지하기 위한 정보를 담고 있는 메시지를 보안 패킷으로 정의한다. 이 표준화 과제에서는 차량의 NMCF(Network Monitoring Client Function)가 보안 패킷을 직접적으로 전송하는 경우와, 주변 차량의 NMRF(Network Monitoring Relay Function)를 경유하여 보안 패킷을 전송하는 경우로 구분하여 배치 시나리오를 정의하고 있다. 또한, NMSF(Network Monitoring Server Function)가 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. 이번 회의에서의 주요 개정 내용은 다음과 같다.

첫째, 수집한 최대 종단 간 지연시간 및 무선신호정보(품질 및 전력 등)들을 이용하여 보안 이벤트로 판단하는 기준은 배치 시나리오 및 구현 상황에 따라 달라짐을 본문에 추가하였다.

둘째, 특정 배치 시나리오에서의 패킷 전달 지연 시간 및 무선신호 수신 전력 실험 데이터를 부록에 추가하였다.

또한, 지난 RGM에서는 기존에 진행 중이던 X.fod-sec(커넥티드 차량의 FoD 서비스 보안 지침)에 대한 표준 개발 작업이 추진되었다. 차량의 주문형기능(Feature on Demand, FoD)은 소비자의 필요에 따라 차량의 소프트웨어 기능을 선택적으로 구매할 수 있는 기능을 의미한다. 즉, 차량의 특정 기능이 제조사가 차량을 사용자에게 제공하는 시점에 차량에 장착되어 차량을 판매하는 것이 아니라, 사용자가 차량을 구매한 이후, 필요한 기능을 선택적으로 요청하여 차량의 기능을 탑재하는 것을 의미한다. 이것은 일종의 SDV(Software-Defined Vehicle)의 개념으로 생각할 수 있다. 이를 위하여, FoD 서버를 도입하고, 커넥티드 차량과의 통신을 통한 차량 기능의 설치 개념을 소개하고 있으며, 차량 FoD 서비스에서의 보안 위협, 보안요구사항, 구현고려사항을 표준화할 계획이다.

Ⅲ. 결 론

본 논문에서는 SG17 ITS 보안 연구반(Q13)에서 추진되고 있는 표준화 진행 현황을 소개하였다. 특히, 최근 2024년 상반기에서 최종 승인된 표준화 과제와 신규로 채택된 표준화 과제에 대하여 소개하였다. 또한 2024년 9월 SG17회의에서 사전채택 및 동의를 계획하고 있는 표준화 과제에 대한 최근 동향을 소개하였다. 2024년 9월 SG17 회의는 지난 2022년부터 시작된 연구회기의 마지막 회의이다. 한국은 지난 2017년

부터 의장국으로서 ICT 보안 표준화를 주도적으로 추진해 왔다. 이번 회의를 통하여, 그간의 표준화 성과들을 정리하고, 차기 연구회기에도 한국이 주도적으로 표준화를 추진하기 위한 준비 작업이 필요한 시기이다. 또한, 이번 회기에서 한국이 주도적으로 추진했던 표준화 과제들을 계획대로 최종승인, 사전채택 및 동의를 추진할 필요가 있다.

중국에서는 ITS 보안 표준화의 중요성을 인식하고, 안티바이러스 업체 360 Technology(현재, 베이징 Qihu Keji Co.), 침해대응센터인 CN-CERT(China Computer Network Emergency Response Team) 및 차이나 모바일, 그리고 중국의 IT 연구기관 CAICT(China Academy of Information and Communications Technology)에서 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 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.1372, Security guidelines for Vehicle-to-Everything(V2X) communication. 2020.

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

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

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

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

[9] ITU-T SG17 Recommendation, X.1377, Guidelines for intrusion prevention systems for connected vehicles 2022.

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

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

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

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

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

[15] ITU-T SG17 Recommendation, X.1373, Software update capability for ITS communications devices, 2024.

[16] ITU-T SG17 draft Recommendation, X.1384 (X.itssec-5), Security guidelins for vehicular edge computing, 2024.

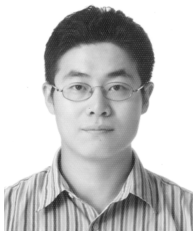
[17] ITU-T SG17 draft Recommendation, X.evtol-sec, Security guidelines for electric vertical take-off and landing (eVTOL) vehicle in an urban air mobility, 2024.

[18] ITU-T SG17 draft Recommendation, X.evpnc-sec: Security guidelines for electric vehicle plug and charge (PnC) services using vehicle identity (VID), 2024.

[19] 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), 2024.
[20] 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, 2024.
[21] ITU-T SG17 draft Recommendation, X.af-sec: Evaluation methodologies for anonymization techniques using face images in autonomous vehicles, 2024.
[22] ITU-T SG17 draft Recommendation, X.fod-sec: Security guidelines for a feature on demand (FoD) service in a connected vehicle environment, 2024.

〈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