정 보 보 호 학 회 지
제 30 권 제4호, 2020. 8

ITU-T SG17에서의 차량 통신 및 ITS 보안 국제 표준화 동향

이 상 우*, 정 보 흥*

요 약

최근 자율주행차량, 차량통신기술 등의 상용화가 임박함에 따라, 대두되는 여러 가지 사이버 보안 위협에 대응하기 위한 보안 기술이 활발히 연구 개발 추진 중이며, 국제표준화의 필요성도 부각되어 활발히 추진 중이다. 본 논문에서는 ITU-T SG17 정보보호 표준화 기구의 ITS(Intelligent Transport System) 보안 연구반에서 최근 회의에서 신규로 채택된 표준화 과제의 내용과 향후 표준화 진행 계획을 소개한다.

Ⅰ. 서 론

차량통신기술은 자율주행차량의 필수 요소 기술로서 상용화가 진행 중이며, 차량 통신 환경에서의 사이버 보안 사고 방지를 위한 연구 개발 및 다양한 표준화 활동이 진행되고 있다.[1-4]. 특히, 자율주행차량에서 다양한 센서를 통해 수집되는 정보의 한계를 극복하기 위한 차량 간 통신, 증가되는 차량 내부 데이터 처리를 위한 차량 이더넷 도입 시 발생할 수 있는 보안 취약점에 대한 대응 기술 및 차량과 클라우드와의 연계를 통한 차량 사이버 보안성 강화 등의 중요성이 부각되고 있다.

ITU-T SG17 표준화 그룹은 통신 분야의 표준화를 다루는 국제 기구인 ITU-T 산하의 사이버 보안 기술에 대한 전문 표준화 그룹이다. 특히, ITS 보안 연구반이 2017년 3월 신규 연구반으로 승인되었고, 차량 내외부 통신망 보안 및 ITS 응용 보안 분야에 활발한 표준화가 진행 중이다. 본 논문에서는 SG17의 ITS 보안 연구반의 활동을 중심으로 2020년 최종 승인된 표준을 통하여 ITS 보안 국제 표준화 최신 현황을 살펴보고, 현재 진행 중인 표준화 과제 및 20년 말을 목표로 사전 승인을 계획 중인 표준화 과제 및 향후 진행 계획을 소개한다.

Ⅱ. ITU-T SG17에서의 ITS 보안 표준화 현황

본 절에서는 ITS 보안 연구반(Q13)에서 최근 표준 최종 승인이 완료된 건과 현재 진행중인 표준화 과제를 소개한다.

2.1. Q13의 최종 표준 승인 현황

Q13의 표준화 분야는 차량통신보안 분야에 국한되는 것이 아니라, 차내망 통신, 차외망 통신을 포함하고, 안전한 지능형교통시스템 구축을 위한 보안 기술 전 분야를 포함한다.

현재 Q13에서는 2020년 3월 및 5월 회의를 통해 아래의 2건의 표준이 최종 승인되었다.

- X.1371: Security threats to connected vehicles
- X.1372: Security guidelines for Vehicle-to-Everything(V2X) communication

2020년 3월에 X.1372(기존 X.itssec-2)가 최종 승인되었다. X.1372는 차량통신시스템에 대한 보안 가이드라인을 정의하는 것으로, 한국의 ETRI, 현대차 및 카카오모빌리티 주도로 표준화가 진행되었다[5]. V2X 통신 시스템은 차량 통신 시스템을 통칭하는 것으로 차량과

본 연구는 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2018-0-00312, 오토모티브 이더넷 기반 차량 보안위협 예측,탐지,대응 및 보안성 자동진단기술개발)
* 한국전자통신연구원 (책임연구원, ttomlee@etri.re.kr; 책임연구원, bhjung@etri.re.kr)

차량(Vehicle-to-Vehicle, V2V), 차량과 인프라(Vehicle-to-Infrastructure, V2I) 및 차량과 노매딕 디바이스(Vehicle-to-Nomadic Device, V2D) 간의 통신 환경을 의미한다. 노매딕 디바이스는 스마트폰, 네비게이터 등 차량과 통신하는 사용자 단말을 의미한다. 본 표준에서는 차량과 보행자 간의 통신(Vehicle-to-Pedestrian, V2P)은 보행자의 노매딕 디바이스와 차량과의 통신으로 정의하고, V2D의 일종으로 간주한다. X.1372에서는 V2V, V2I, V2D 통신 환경에서의 보안 위협 및 보안 요구 사항을 정의하고, 차량 등록 및 인증 서비스 등 보안 기능을 구현하기 위한 가이드라인을 제공한다. 특히, 본 표준에서는 V2V/V2I 통신 환경을 차량간 경고 전파, 차량 그룹 통신, 차량 경계, 차량과 인프라간 경고 전파 형태로 구분하고, 상기 형태에 따른 보안 요구사항을 정의하고 있다. 또한, 차량용 PKI(Public Key Infrastructure)의 참조 예로서, 유럽 ETSI의 예 및 미국의 CAMP(Crash Avoidance Metrics Partnership)의 참조 모델에 대한 설명이 부록에 기술되어 있으며, 차량 통신에서의 메시지 암호화 방법 및 메시지 서명 방법으로서 ECIES(Elliptic Curve Integrated Encryption Scheme) 및 ECDSA(Elliptic Cureve Digital Signature Algorithm)를 소개한다. 특히, 군집주행서비스를 위하여 차량의 인증 절차를 정의하고 있다. 2020년 3월 회의에서는 X.1372를 표준으로 최종 승인하고, 이에 관하여 3GPP SA3 워킹 그룹에 표준의 승인 사실을 알리고, 향후 차량통신보안 표준화에 협력을 추진할 예정이다. 또한 지난 3월회의에서는 ITU-R에서 셀룰러 V2X(C-V2X)에 대한 기술보고서 발간에 대한 협조 문서를 수신하여, 향후 C-V2X에 대한 보안 표준화 개발에 협조해 나갈 계획이다.

2020년 5월에 X.1371(기존 X.stcv)가 최종 승인되었다. X.1371의 표준화 범위는 커넥티드 차량 및 에코시스템에서의 보안 위협을 정의하는 것이다[6]. UNECE(United Nations Economic Commission for Europe) WP29에서 정의한 “차량 사이버보안 권고안“의 보안 위협을 기반으로 하여, 커넥티드 차량에 대한 상위 레벨의 위협을 정의하는 것이 표준의 목적이다. UNECE WP29은 각국의 차량 제조업체 및 차량 규제 기관으로부터 차량 및 에코시스템의 보안 위협을 식별하였으며, SG17은 표준화 기구로서, 식별된 위협을 표준으로 작성한 것이 X.1371이다. X.1371에서는 보안 위협을 5가지 형태로 구분하여 정의한다.

- 백엔드 서버에서의 보안 위협
- 통신 채널의 보안 위협
- SW 업데이트에서의 보안 위협
- 비의도적인 사용자의 행위에 의한 보안 위협
- 외부 접속 환경에서의 보안 위협

또한, 보안 취약점으로서, 사이버 공격의 잠재적인 목표와 잠재적인 취약점을 기술하고 있다. 향후 SG17에서는 X.1371에서 정의한 보안 취약점을 차량통신 및 ITS 분야에서 대처할 수 있는 보안요구사항 및 보안 구현 가이드라인에 대한 표준화를 진행해 나갈 예정이다.

2.2. Q13의 표준화 진행 과제 현황

2019년 8월 신규과제로 채택된 2건을 포함하여 아래의 11개 표준화 과제가 진행 중이다[7-15].

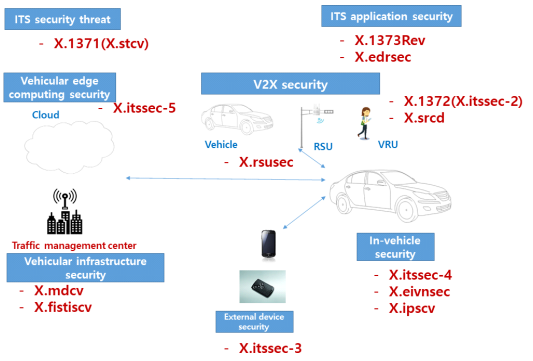
- X.itssec-3: Security requirements for external interfaces and devices with vehicle access capability
- X.itssec-4: Methodologies for intrusion detection system on in-vehicle networks
- X.itssec-5: Security guidelines for vehicular edge computing
- X.srcd: Security requirements for categorized data in V2X communication
- X.mdcv: Security-related misbehaviour detection mechanism for connected vehicles
- X.eivnsec: Security guidelines for Ethernet-based In-Vehicle networks
- X.edrsec: Security guidelines for cloud-based event 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 2020년 8월 현재 Q13 표준화 과제 현황 및 분야를 나타낸 것이다. V2X 통신환경에서 데이터 속성에 따른 보안 등급 분류는 X.srcd에서 다루어 지고 있다. 차량진단포트 및 블루투쓰를 통하여 차량에 접속하는 디바이스에 대한 보안은 X.itssec-3에서 다루어 지고 있으며, 보안관리서버, 교통관제서버 등의 인프라 및 클라우드에 연관된 보안 표준화는 X.mdcv, X.fstiscv 및 X.itssec-5에서 다루어 지고 있다. 특히, 차량내부망 보안을 위해서는 X.itssec-4에서 일반적인 차량용 침입탐지시스템 방법론이 개발되고 있으며, 현재 이슈가 되고 있는 차량용 이더넷 보안 분야는 별도의 표준화 과제인 X.eivnsec에서 심도있게 다루어 지고 있다. 또한, ITS 응용분야로서, 차량용 소프트웨어 업데이트 보안은 X.1373rev에서, 차량용 사고기록장치 보안은 X.edrsec에서 다루어지고 있다.

특히, X.itssec-3 및 X.itssec-4는 20년 8월 회의에서 사전 승인(consent)를 목표로 표준화가 추진 중이다.

X.itssec-3의 목적은 차량에 접속하는 디바이스의 보안요구사항을 정의하는 것으로, 현대차 및 ETRI에서 주도적으로 표준화를 진행 중이다[7]. 차량 내부 진단 도구가 많이 활용하고 있는 OBD-II (On-Board-Diagnostic II) 포트 및 블루투쓰 등을 이용하여 차량에 접속하는 디바이스에 대한 보안요구사항을 정의하고 있다. 지난 6월 인터림 회의에서는 20년 8월 사전 승인을 위하여, 표준안의 마무리 작업을 진행하고 아래의 내용이 반영되었다.

첫째, 차량외부접속 장치는 하드웨어 지원 보안 모듈을 구비하고, 상기 하드웨어 지원 모듈은 Root of Trust로서 암호 연산 기능 및 암호화 키를 저장하는 기능을 보유할 것을 명시하였다.



〔그림 1〕 Q13 표준화 현황

둘째, 차량외부접속장치로서, 스마트 키, 전기차충전 시스템, Wi-Fi 또는 블루투쓰를 이용하는 접속장치에 적용될 수 있는 보안 제어 방법을 유즈 케이스로 추가하였다.

셋째, 차량에 접속하는 장치가 사용하는 무선 통신 기술 중 블루투쓰 및 이동통신망에 대한 기술 규격을 부록에 추가하였다.

X.itssec-4의 표준화 범위는 차내망에서의 침입탐지 시스템 구성 방법을 정의하는 것으로, 고려대, 현대차 및 ETRI에서 주도적으로 표준화를 추진 중이다[8]. CAN(Controller Area Network) 환경에 적합한 침입탐지시스템의 기능 및 규격을 정의하고 있다. 지난 6월 인터림 회의에서는 20년 8월 사전 승인을 위하여, 표준안의 마무리 작업을 진행하고, 아래의 내용이 반영되었다.

첫째, 차내망에서의 침입탐지시스템의 기본 구조와 각 구성요소의 설명이 추가되었다.

둘째, 침입탐지시스템을 정적탐지(Static detection), 오용탐지(Misuse detection) 및 비정상탐지(Anomaly detection)으로 구분하고, 탐지 보고 시의 룰셋의 내용이 추가되었다.

2.3. ITS 보안 연구반(Q13) 신규 표준화 과제

2019년 8월에 아래의 과제가 신규로 채택되었다.

- 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[17]. 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.itssec-4와 연계하여, 탐지 기능을 이용하여, 침입 방지 할 수 있는 방법론을 정의해 나갈 계획으로, 한국의 고려대, 현대차,

ETRI가 주도적으로 추진하고 있다.

Ⅲ. 결 론

본 논문에서는 SG17 ITS 보안 연구반(Q13)에서 추진되고 있는 표준화 진행 현황을 소개하였다. 특히, 최근 2020년에 최종 승인된 표준안 2건과 2020년 8월 사전 승인을 예정하고 있는 표준안 2건의 현황에 대하여 기술하였다. SG17은 올해 말 4년간의 연구 회기를 종료하고, 내년부터 차기 연구 회기를 시작한다. 현재까지는 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.

한국에서는 현대차, ETRI, 고려대 등이 주도적으로 표준화에 참여하고 있으나, 중국의 약진 등의 상황을 고려할 때, 지속적인 차량보안 표준화의 주도권 선점이 필요하며, 표준의 실효성 및 파급력을 고취시키기 위하여 ISO TC 204, UNECE WP29 등과의 구체적인 협업을 통한 표준화 개발이 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 draft Recommendation, X.itssec-3, Security requirements for vehicle accessible external devices, 2020.

[8] ITU-T SG17 draft Recommendation, X.itssec-4, Methodologies for intrusion detection system on in-vehicle systems, 2020.

[9] ITU-T SG17 draft Recommendation, X.itssec-5, Security guidelines for vehicular edge computing, 2018.

[10] ITU-T SG17 draft Recommendation, X.srcd, Security requirements for categorized data in V2X communication, 2018

[11] ITU-T SG17 draft Recommendation, X.mdcv, Security-related misbehaviour detection mechanism based on big data analysis for connected vehicles, 2018.

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

[13] ITU-T SG17 draft Recommendation, X.edrsec, Security guidelines for Ethernet-based In-Vehicle networks, 2018.

[14] ITU-T SG17 draft Recommendation, X.fstiscv, Framework of security threat information sharing for connected vehicles, 2018.

[15] ITU-T SG17 draft Recommendation, X.1373rev: Software update capability for ITS communications devices, 2018.

[16] ITU-T SG17 draft Recommendation, X.rsu-sec: Security requirements for road-side units in intelligent transportation systems, 2019.

[17] ITU-T SG17 draft Recommentation, X.ipscv: Methodogies for intrusion prevention system in connected vehicles.

〈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 PL/책임연구원

2014년~현재 : ITU-T SG17 editor

2017년~현재 : ITU-T SG17 Q13 Rapporteur

<관심분야> 임베디드 보안, 차량통신보안, 융합보안

정 보 흥 (Chung Bo-Heung)

정회원

1996년 2월 : 인하대학교 컴퓨터공학과 졸업

1998년 2월 : 인하대학교 컴퓨터공학과 석사

2002년 2월 : 한국대학교 컴퓨터공학과 박사

2002년~현재 : 한국전자통신연구원 책임연구원

<관심분야> 정보보호, 네트워크/융합 보안, 자동차보안