

ITU-T SG17에서의 차량 통신 보안 국제 표준화 동향

이상우*, 전용성*

요약

최근 자율주행차량등의 활발한 기술 개발 및 상용화가 추진되고 있다. 자율주행차량에서는 기존의 센서로부터 수집되는 주변 환경 정보의 한계를 극복하기 위하여 차량통신기술을 활용하여 주변 환경을 보다 정확하고 상세하게 인지하는 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. 최근 IT 보안 국제표준화 기구인 ITU-T SG17에서는 연구반 구조 조정을 진행했으며, ITS(Intelligent Transport Systems) 보안 연구반(Q13)은 지속적으로 차량통신표준화를 추진한다. 본 논문에서는 ITS 보안 연구반의 최근 활동 및 진행 계획을 소개한다.

I. 서론

차량통신기술은 자율주행차량의 센서 기반 주변 인식 판단에 추가적으로 정확성을 제공할 수 있는 기술로서 상용화가 진행 중이며, 이러한 차량 통신 환경에서의 보안 사고 방지를 위한 연구 개발과 활발한 표준화 활동이 추진 중이다.[1-9]. 특히, 현재 상용화에 박차를 가하고 있는 자율주행차량에서는 센서를 통해 수집되는 차량 주변 환경 정보의 한계를 극복하기 위한 기술의 하나로 차량 간 통신 기술의 필요성이 증가하고 있다. 또한, 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 SG17 표준화 그룹은 통신 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 2022년 5월 회의 및 6월 라포치 그룹 회의(RGM, Rapporteur Group Meeting)에서 진행된 내용을 중심으로 차량 통신 보안 국제표준화 현황을 살펴

본다.

II. ITU-T SG17에서의 차량통신보안 표준화 현황

본 절에서는 ITS 보안 연구반(Q13)에서 최근 2022년 상반기까지 표준 최종 승인이 완료된 것과 현재 표준화와 진행중인 내용을 소개한다.

2.1. Q13의 2022년 5월 회의 주요 내용

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

지난 5월 회의에서는 이번 회기(2022~2024) 동안의 라포치 및 부라포치가 확정되었다. 지난 회기(2017~2021)에서부터 라포치로서 이상우(ETRI, 한국)가 선임되어 활동 중이며, 부라포치로서 박승욱(현대차, 한국), Yi Zhang(Beijing Qihu Keji Co., Ltd., 중국)이 계속해서 선임되어 활동 중이다. 이번 회기에서는 Takamasa Isohara(KDDI, 일본)이 신규 부라포치로 선임되었다. 이와 같이, Q13의 연구반은 연구기관, 차량 제조업체, 사이버보안업체, 통신업체 등 다양한 분야의 전문가가 의장단으로 활동하게 되어, 이번 회기에서도

이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2020-0-00913, 무선은닉채널 위협성 검증 연구)

* 한국전자통신연구원 정보보호연구본부 (책임연구원, ttomlee@etri.re.kr, ysjeon@etri.re.kr)

[표 1] Q13 의장단 현황

역할	이름	소속	국가
라포처	이상우	ETRI	한국
부라포처	박승욱	Hyundai Motors	한국
부라포처	Yi Zhang	Beijing Qihu Keji Co., Ltd.	중국
부라포처	Takamasa Isohara	KDDI	일본

상호 간 협력을 통한 차량통신보안 표준화 개발을 적극적으로 추진할 계획이다.

지난 2022년 5월 회의에서 아래의 1건이 표준이 사전 승인(Consent)되었다.[10].

- X.1379: Security requirements for road-side units in intelligent transportation systems

X.1379 (기존 X.rsu-sec)는 중국의 차이나 모바일에서 주도적으로 추진한 표준으로서 ITS 환경에서 도로 기지국(Road-Side Unit)이 만족해야할 보안요구사항을 기술한 표준이다. 도로기지국은 도로의 주변에 설치되어, 도로의 교통상황정보를 차량에 전파하고, 차량과 백엔드 서버 인프라 간의 데이터 중계 역할을 담당한다. X.1379에서는 도로기지국의 하드웨어, 펌웨어, 어플리케이션 및 데이터 레벨에서의 위협을 식별하고, 식별된 위협에 대응할 수 있는 보안요구사항을 정의하고 있다. 부록에서는 도로기지국에 대한 간단한 소개를 포함하고 있다. 2022년 8월 현재 AAP(Alternative Approval Process)의 의견 수렴 과정에 있다.

2022년 5월 회의에서는 아래의 진행 중인 표준화 과제에 대한 신규 TD(Template Document)가 발행되었다[11-17].

- X.srcd: Security requirements for categorized data in V2X communication
- X.eivn-sec: Security guidelines for Ethernet-based in-vehicle networks
- X.edr-sec: Security guidelines for cloud-based data recorders in automotive environment
- X.fstiscv: Guidelines for sharing security threat information on connected vehicles
- X.1373rev: Software update capability for ITS

communication devices

- X.ipscv: Guidelines for intrusion prevention systems for connected vehicles
- X.evtol-sec: Security guidelines for electric vertical take-off and landing (eVTOL) vehicle in an urban air mobility environment

2.2. Q13의 2022년 6월 RGM 회의 주요 내용

Q13에서는 2022년 8월 회의에서 5건의 표준화 과제에 대한 사전승인 및 사전채택을 추진할 계획이다. 이를 위하여 지난 6월 RGM 회의에서는 5건의 표준화 과제의 마무리를 위한 심도있는 논의가 진행되었다.

X.eivn-sec(이더넷 기반 차내망 보안가이드라인)은 이더넷 기반 차량 내부 네트워크의 보안 위협, 보안요구사항 및 보안기능구현 고려사항 및 사용 예를 정의하는 것이다. 차량에 탑재된 카메라 및 센서 등으로 인하여 차량 내부망에서 송수신되는 데이터 양이 증가함에 따라 이를 처리하기 위하여 차량용 이더넷이 상용화를 추진 중이며, 이 때 보안고려사항을 정의하고 있다. 한국의 ETRI 및 차량보안업체 ETAS Korea(구 Escrypt)가 주도적으로 표준화를 추진하고 있으며, 최근 독일의 차량부품업체 Bosch에서 관심을 가지고 적극적으로 표준화를 추진 중이다. 6월 RGM 회의에서는, 그동안 독일에서 제기해왔던 표준의 버전 관리, 차량내부구조에 대한 참조 모델, 그리고 차내망에서의 MAC(Media

[표 2] Q13 22년 8월 회의 추진 계획

표준과제	에디터	승인방식
X.eivn-sec	이상우(ETRI), 이유식(ETAS)	사전채택
X.edr-sec	이상우(ETRI), 박승욱(Hyundai Motors)	사전채택
X.srcd	Yaping Sun(CAICT), Huirong Tian(CAICT), Nan Meng(CAICT), Takamasa Isohara(KDDI)	사전채택
X.fstiscv	Min Shu(CNCERT), Wenlei Wang(CNCERT), Yunwei Zhao(CNCERT), Xiaochun Yun(CNCERT)	사전채택
X.ipscv	정성훈, 김휘강(고려대) 박승욱(Hyundai Motors), 이상우(ETRI)	사전승인

Access Control) 주소의 동적 할당 제약에 대한 보안요구사항에 대한 합의를 도출하고 차기 SG17회의에서 사전 채택을 위한 초안을 마련하였다.

X.cedr-sec(클라우드 기반 차량 데이터 기록 장치 보안가이드라인)은 클라우드 기반의 차량 사고기록장치 시스템의 보안위협, 보안요구사항 및 사용 예를 정의하는 것이다. 이 표준은 한국의 ETRI 및 현대차가 주도적으로 표준화를 추진 중이다. 자율주행차 운행에 있어서, 사고 당시의 차량운행주체정보의 안전한 전송 및 관리 방법에 대한 보안요구사항도 정의하고 있으며 또한, 차량운행주체정보를 클라우드로 안전하게 전송하고, 프라이버시 침해 없이 차량운행주체정보를 관리하는 방법도 기술하고 있다. 6월 RGM 회의에서는 지난 5월 회의에서 일본의 NICT에서 제기한 차량의 클라우드 등록 해제에 대한 필요성 의견을 수용하여, 클라우드 기반 차량 데이터 기록 장치의 등록 해제 절차에 대한 설명이 추가되었다. 이는 렌트카 또는 중고차 거래를 고려하여, 기존에 설정되어 있던 차량 데이터의 클라우드 전송 서비스 해제를 고려한 것이다.

X.ipscv(커넥티드 차량 침입방지시스템 가이드라인)은 차량의 침입방지시스템의 구현방법론을 정의하는 것이다. 차내망 침입탐지시스템은 X.1375로 표준화 되었다. X.ipscv는 차내망 침입탐지시스템과 연계하여 차량 침입방지시스템의 구현 가이드라인을 제공하는 것이다. 차량 내부망에는 최소한의 침입탐지기능만 탑재하고, 수집된 침입 탐지 결과를 활용하여, 차량 외부의 서버에서 탐지 결과를 분석하여, 최종적으로 차량이 외부의 비정상적인 공격에 대응할 수 있도록 하는 침입탐지대응방법을 제공하고 있다. 6월 RGM 회의에서는 차량 침입방지시스템의 핵심 모듈인 프로그래머블 스위치에 대한 정의에 대하여 합의하였고, 커넥티드 차량의 보안 위협에 대한 공격 표면 및 악의적인 이상행위의 예를 분석하여 보안 위협을 도출하였다. 차량 침입방지시스템에서는 특정 ECU(Electric Control Unit)의 ID를 식별하고자 하는 행위, TCP/UDP 포트 스캐닝, 차내망의 DoS 공격, 차내망의 명령어에 대한 스푸핑 공격 등을 위협으로 정의하였다.

X.srvc(V2X(Vehicle-to-Everything) 통신에서의 데이터 분류에 따른 보안요구사항)은 V2X 통신환경에서 송수신되는 데이터를 분류하고, 분류된 데이터에 따른 보안 레벨을 정의하고, 정의된 보안 강도를 보장하기 위

한 보안 요구사항을 정의하는 것이다. 중국의 IT 연구기관, CAICT(China Academy of Information and Communications Technology)와 일본의 통신 서비스 회사 KDDI에서 기존의 클라우드 보안 분야에서의 데이터 보안 표준화 내용을 V2X 통신 환경에 적용한 표준이다. 지난 6월 RGM회의에서는 V2X 데이터의 라이프사이클을 정의하고, V2V(Vehicle-to-vehicle), V2I(Vehicle-to-infrastructure), V2D (Vehicle-to-nomadic device) 환경에 따른 데이터를 분류하였다. 또한, 해당 라이프사이클 및 데이터 분류에 따라 보안 강도를 3단계로 지정하고, 그에 따른 보안요구사항에 대한 최종 합의된 내용을 작성하였다.

X.fstiscv(커넥티드 차량의 보안위협정보 공유 가이드라인)은 커넥티드 차량 환경에서 자동차 제조업체 및 CERT(Computer Emergency Response Team)등이 사이버 보안 위협 정보를 공유할 때, 각 이해관계자들의 역할을 정의하는 것이다. 중국의 IT 침해대응센터인 CN-CERT에서 주도적으로 추진하고 있다. 공유되는 정보는 Automotive-ISAC(Information Sharing and Analysis Center)에서 제안한 Indicators, TTP(Tactics, Techniques and Procedures), Security alert, Threat intelligence report를 활용한다. 지난 6월 RGM회의에서는 보안위협정보를 공유하는 단계에 따른 요구사항에 대하여 합의하고, 차기 회의에서 사전채택을 하기 위한 초안을 마련하였다.

III. 결 론

본 논문에서는 SG17 ITS 보안 연구반(Q13)에서 추진되고 있는 표준화 진행 현황을 소개하였다. 특히, 최근 2022년 상반기에서 사전승인된 표준화 과제와 22년 하반기 SG17회의에서 사전채택 또는 사전 승인을 계획하고 있는 표준화 과제에 대한 최근 동향을 소개하였다. 22년 하반기 SG17 회의는 대면회의로 진행될 예정이다. 따라서, 지난 2년 6개월간 원격으로 회의가 진행됨에 따라 연기되었던 다수의 표준화 과제에 대한 사전채택 및 사전승인이 진행될 계획이다.

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 중이

다. 특히 최근 독일의 Bosch에서도 차량통신보안의 중요성을 인지하고, 적극적으로 표준화에 참여하고 있는 상황이다.

한국에서는 ETRI, 현대차, 고려대 등이 주도적으로 표준화에 참여하고 있으며, 지속적으로 표준의 제정에 기여하고 있다. 차량통신보안 국제표준화의 지속적인 표준화 주도권 선점을 위하여 산업계, 연구기관, 학계 등의 적극적인 표준화 참여가 필요하다.

참 고 문 헌

- [1] 이상우 외, “차량 통신 보안 기술 동향,” 주간기술 동향, 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.1379, Security requirements for road-side units in intelligent transportation systems, 2022.
- [11] ITU-T SG17 draft Recommendation, X.srcd, Security requirements for categorized data in V2X communication, 2022.
- [12] ITU-T SG17 draft Recommendation, X.eivn-sec, Security guidelines for Ethernet-based In-Vehicle networks, 2022.
- [13] ITU-T SG17 draft Recommendation, X.edr-sec, Security guidelines for cloud-based data recorders in automotive environment, 2022.
- [14] ITU-T SG17 draft Recommendation, X.fstiscv, Guidelines for sharing security threat information on connected vehicles, 2022.
- [15] ITU-T SG17 draft Recommendation, X.1373rev, Software update capability for ITS communications devices, 2022.
- [16] ITU-T SG17 draft Recommendation, X.ipscv, Guidelines for intrusion prevention systems for connected vehicles 2022.
- [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, 2022.

< 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

구원 정보보호연구본부 /책임연구원

2014년~현재 : ITU-T SG17 editor

2016년~2017년 : WMG in University of Warwick, UK, 방문 연구원

2017년~현재 : ITU-T SG17 Q13 Rapporteur

<관심분야> 임베디드 보안, 차량통신보안, 융합보안, 무선은닉체널보안



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