정 보 보 호 학 회 지
제29권 제1호, 2019. 2

차량 통신 및 ITS 보안 국제 표준화 동향

이 상 우*, 정 보 흥*, 나 중 찬*

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 진행되고 있는 표준화 과제 내용과, 지난 2018년 8월 회의에서 신규로 채택된 표준화 과제의 내용을 소개한다.

Ⅰ. 서 론

자율주행 차량의 필수 요소 기술로서 차량통신 기술의 상용화가 진행되고 있으며, 차량 통신 환경에서의 사이버 보안 사고 방지를 위한 연구 개발 및 다양한 표준화 활동이 진행되고 있다.[1,2,3,4]. 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 기술의 중요성이 부각되고 있다.

ITU-T SG17 표준화 그룹은 통신 분야의 표준화를 다루는 국제 기구인 ITU-T 산하의 사이버 보안 기술에 대한 전문 표준화 그룹이다. 현재 4개의 중그룹(Working Party) 산하 14개의 연구반(Question)이 운영되고 있다. 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 ITS 보안 국제 표준화 현황을 소개한다.

Ⅱ. ITS 보안 기술 표준화 현황

본 절에서는 ITS 보안 연구반(Q13)에서 현재 진행 중인 표준화 과제와 지난 2018년 8월 신규 채택된 표준화 과제를 소개한다.

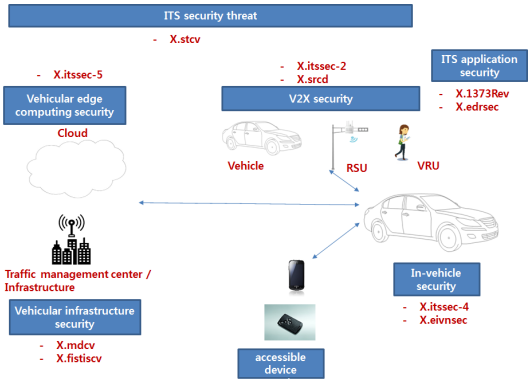
2.1. ITU-T SG17에서의 표준화 활동

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

현재 Q13에서는 2018년 8월 신규과제로 채택된 3건을 포함하여 아래의 11개 표준화 과제가 진행 중이다.

- X.itssec-2: Security guidelines for V2X communication systems
- X.itssec-3: Security requirements for vehicle accessible external devices
- X.itssec-4: Methodologies for intrusion detection system on in-vehicle systems
- 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 based on big data analysis for connected vehicles
- X.stcv: Security threats in connected vehicles

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 (ttomlee@etri.re.kr, bhjung@etri.re.kr, njc@etri.re.kr)



〔그림 1〕 Q13 표준화 현황

- X.eivnsec: Security guidelines for Ethernet-based In-Vehicle networks
- X.edrsec: Security guidelines for Ethernet-based In-Vehicle networks
- X.fstiscv: Framework of security threat information sharing for connected vehicles
- X.1373rev: Software update capability for ITS communication devices

그림 1은 Q13 표준화 과제 현황 및 분야를 나타낸 것이다. V2X 보안 분야에서는 전반적인 보안 가이드라인이 X.itssec-2에서 다루어지고 있으며, 데이터 속성에 따른 보안 등급 분류는 X.srcd에서 다루어 지고 있다. 차량진단포트 및 블루투쓰를 통하여 차량에 접속하는 디바이스에 대한 보안은 X.itssec-3에서 다루어지고 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. 앞서 언급한 표준들의 기반 문서로서 커넥티드 차량 환경에서의 보안 위협은 X.stcv에서 다루어 지고 있다.

X.itssec-2에서는 차량통신시스템에 대한 보안 가이드라인을 표준의 범위로 설정하고 있으며, 한국의 ETRI 및 현대차 주도로 표준화 마무리 작업을 진행 중이다[5]. V2X 통신 시스템은 차량 통신 시스템을 통칭하는 것으로 차량과 차량(V2V), 차량과 인프라(V2I) 및 차량과 노매딕 디바이스(V2ND) 간의 통신 환경을 의미한다. X.itssec-2에서는 V2V, V2I, V2ND 통신 환경에서의 보안 위협 및 보안 요구 사항을 정의하고, 차량 등록 및 인증 서비스 모델 등의 유즈 케이스를 표준화 범위로 지정하고 있다. 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.

지난 8월 회의에서는 한국 주도로 아래의 내용이 표준안에 반영되었다.

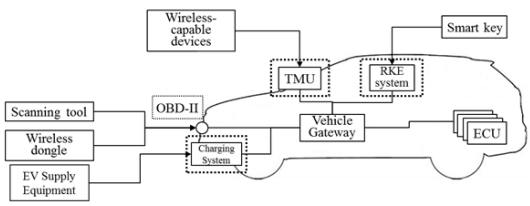
첫째, 차량용 PKI(Public Key Infrastructure)의 참조 예로서, 유럽 ETSI의 예 및 미국의 CAMP(Crash Avoidance Metrics Partnership)의 참조 모델에 대한 설명이 부록에 추가되었다.

둘째, 차량통신에서의 메시지 암호화 방법 및 메시지 서명 방법이 수정 기술되었다. 이는 현재 차량통신 분야에서 많이 사용되고 있는 ECIES(Elliptic Curve Integrated Encryption Scheme) 및 ECDSA(Elliptic Curve Digital Signature Algorithm)의 구현을 위한 알고리즘의 내용을 설명한 것이다.

또한, 지난 11월 인터림 회의를 통하여, V2X 통신 환경에서의 사이버 보안 위협을 기밀성, 무결성, 가용성, 부인 봉쇄 등의 보안 특성을 기준으로 수정 기술한 내용이 반영되었다.

X.itssec-2는 올해 말에 표준화 사전 채택을 목표로 표준화 최종 작업이 진행 중이다. 차기 회의에서 차량용 공개키 기반 구조의 참조 모델 설명 추가 수정 등을 통해 내용을 확정할 예정이다.

X.itssec-3의 목적은 차량에 접속하는 디바이스의 보안요구사항을 정의하는 것으로, 현대차에서 주도적으로 표준화를 진행 중이다[6]. 차량 내부 진단 도구가



〔그림 2〕 차량접속디바이스 환경

많이 활용하고 있는 OBD-II (On-Board-Diagnostic II) 포트 및 블루투쓰 등을 이용하여 차량에 접속하는 디바이스에 대한 보안요구사항을 정의하고 있다. (그림 3)은 본 표준안에서 정의할 OBD-II를 통하여, 차량에 접근하는 환경을 도시한 것이다. 본 표준안에서는 OBD-II, TMU(Telematics Unit), RKE(Remote Keyless Entry) 및 충전 시스템을 이용하여 차량에 접속하는 환경을 도시한 것이다.

지난 8월 회의에서는 전기차를 대상으로 하는 충전 시스템을 위부 접속 디바이스로 포함시켰으며, 충전을 위한 위부 접속 디바이스의 보안 위협 및 요구사항을 정의해 나갈 계획이다.

X.itssec-4의 표준화 범위는 차내망에서의 침입탐지 시스템 구성 방법을 정의하는 것으로, 고려대 및 현대차에서 주도적으로 표준화를 추진 중이다[7]. CAN(Controller Area Network) 환경에 적합한 침입탐지시스템의 기능 및 규격 정의를 진행 중이다. 지난 8월 회의에서는 아래의 내용이 반영되었다.

첫째, CAN 환경에서의 보안 위협을 기밀성, 무결성 및 가용성을 기준으로 수정 기술하였다.

둘째, 침입탐지시스템의 기능 요구사항이 추가되었다. 침입탐지시스템을 오작동 탐지 및 비정상행위 탐지 시스템으로 구분하고, 각각의 기능요구사항이 추가되었다.

X.itssec-5는 차량 에지 컴퓨팅 보안 가이드라인을 정의하는 것으로 ETRI가 주도적으로 표준화를 추진하고 있다[8]. 에지 컴퓨팅은 기존의 클라우드 서비스를 엔드 클라이언트와 물리적으로 가까운 곳으로 옮기는 것을 의미한다. 즉, 기존의 클라우드 컴퓨팅 환경에서의 스토리지 서비스 서버 등은 각 서비스 제공자의 데이터 센터에 존재한다. 이러한 환경에서는 네트워크 지연 시간으로 인하여 사용자에게 실시간 응답 서비스 제공 어렵다. 따라서, 엔드 클라이언트에게 보다 빠른 서비스를 제공하기 위한 에지 컴퓨팅이 활발히 연구되고 있으며, 특히 ETSI에서는 이동통신 기지국을 에지 컴퓨팅 서버로 활용하는 MEC (Mobile Edge Computing)에 대한 표준화가 진행 중이다. 차량 통신 환경에서는 도로기지국(RSU, Road-Side Uinit)이 에지 컴퓨팅 서버로 활용될 수 있으며, 이에 대한 보안 규격을 정의하는 것이 X.itssec-5의 표준화 목표이다.

지난 8월 회의 및 11월 인터림 회의를 통해서 아래의 내용이 반영되었다.

첫째, 차량에지컴퓨팅 환경에서의 보안 위협을 기밀성, 무결성, 가용성 등을 기준으로 수정 기술되었으며, 보안 취약성으로 인한 문제점 등이 추가 기술되었다. 둘째, 차량 에지 컴퓨팅의 사용 예로서, VRU (Vulnerable Road User), 즉 보행자, 자전거 등을 탐지하기 위하여 차량용 에지 컴퓨팅을 활용하는 예가 추가 기술되었다.

2018년 3월에 신규로 채택된 과제는 아래와 같다.

- X.srcd의 표준화 목적은 V2X 통신환경에서 송수신되는 데이터를 분류하고, 분류된 데이터에 따른 보안 레벨을 정의하고, 정의된 보안 강도를 보장하기 위한 보안요구사항을 정의하는 것이다[9].
- X.mdcv의 표준화 목적은 빅데이터 분석에 기반하여 차량의 사이버 보안 관련 비정상행위 탐지 매커니즘을 정의하는 것이다. 본 표준에서는 차량, 도로 기지국 등의 인프라 등으로부터 수집하는 데이터 구조를 정의하고, 비정상행위 탐지 방법을 정의할 계획이다[10].
- X.stcv의 표준화 범위는 커넥티드 차량 및 에코시스템에서의 보안 위협을 정의하는 것이다. UNECE(United Nations Economic Commission for Europe) WP29에서 정의되고 있는 “차량 사이버보안 권고안“의 보안 위협을 기반으로 하여, 커넥티드 차량에 대한 상위 레벨의 위협을 정의하는 것이 표준의 목적이다[11].

2.2. ITS 보안 연구반(Q13) 신규 표준화 과제

지난 2018년 8월 SG17 회의에서는 아래의 3가지 신규 표준 과제가 채택되었다[12,13,14].

- X.eivnsec: Security guidelines for Ethernet-based In-Vehicle networks
- X.edrsec: Security guidelines for Ethernet-based In-Vehicle networks
- X.fstiscv: Framework of security threat information sharing for connected vehicles

X.eivnsec(이더넷기반 차량내부네트워크 보안가이

드라인)의 표준화 목적은 이더넷 기반 차량 내부 네트워크의 보안위협, 보안요구사항 및 Use case를 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 제안하여 신규 과제로 채택되었다.

X.edrsec(차량용 클라우드 기반 사고기록장치 보안 가이드라인)은 한국의 ETRI 및 현대차가 제안한 것으로, 표준화 목적은 클라우드 기반의 차량 사고기록장치 시스템의 보안위협, 보안요구사항 및 Use case를 정의하는 것이다. ITU-T에서는 포커스 그룹 Aviation Applications of Cloud computing for Flight Data Monitoring (FG AC, 2014-2016)를 운영하여, 항공시스템에서의 사고기록장치에 대한 표준화 선행연구를 진행하였으며, 나아가 전반적인 교통시스템에 대한 클라우드 기반 사고기록장치에 대한 표준화를 추진하고 있다. Q13에서는 차량 사고기록장치에 대한 표준화를 시작으로, 철도 및 해상 분야로 표준화 범위를 확장해 나갈 예정이다.

Ⅲ. 결 론

본 논문에서는 SG17 ITS 보안 연구반에서 현재 추진 중인 표준화 내용과 신규로 선정된 표준화 과제에 대하여 기술하였다. ITU-T SG17에서 ITS보안연구반(Q13)이 2017년 3월 생성된 이후로, ITS 보안 표준화가 활발히 진행되고 있다. 특히, 중국의 IT 연구기관 CAICT(China Academy of Information and Communications Technology), 및 안티바이러스 업체 360 Technology, 그리고 침해대응센터인 CN-CERT에서 신규 표준화 과제를 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 등의 표준화기구와의 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 draft Recommendation, X.itssec-2, Security guidelines for V2X communication systems. 2018

[6] ITU-T SG17 draft Recommendation, X.itssec-3, Security requirements for vehicle accessible external devices, 2018.

[7] ITU-T SG17 draft Recommendation, X.itssec-4, Methodologies for intrusion detection system on in-vehicle systems, 2018.

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

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

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

[11] ITU-T SG17 draft Recommendation, X.stcv, Security threats in 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.

〈저 자 소 개〉

이상우 (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 : 인하대학교 컴퓨터공학과 박사
2002년~현재 : 한국전자통신연구원 책임연구원
<관심분야> 정보보호, 네트워크/융합 보안, 자동차보안

나 중 찬 (Jung Chan Na)
종신회원
1986년 2월 : 충남대학교 계산통계학과 학사
1989년 2월 : 숭실대학교 전자계산학과 석사
2004년 2월 : 충남대학교 컴퓨터과학과 박사
1989년2월~현재 : 한국전자통신연구원 정보보호연구본부 시스템보안연구그룹 그룹장/책임연구원
<관심분야> 제어시스템보안, 펌웨어 보안 취약성