정 보 보 호 학 회 지
제27권 제5호, 2017. 10

ITU-T SG17에서의 ITS 보안 기술 표준화 동향

이 상 우*, 권 혁 찬*, 나 중 찬*

요 약

최근 자율주행차량 기술의 상용화가 임박함에 따라, 차량통신보안 기술의 중요성도 부각되고 있다. 이와 더불어 차량통신보안 표준화의 중요성도 대두되고 있으며, 그 일환으로 ITU-T SG17에서는 2017년 ITS 보안 연구반을 신설하여 표준화를 활발히 추진하고 있다. 특히, 최근 차량 소프트웨어 업데이트 규격이 표준 승인되었으며, V2X 통신 보안 가이드라인의 표준화가 활발히 진행되고 있다. 또한, 최근 회의에서 차내망 침입탐지시스템, 차량 접속 디바이스 보안 요구사항, 차량 에지 컴퓨팅 보안 가이드라인 등이 신규 표준화 과제로 선정되었다. 본 논문에서는 SG17에서 신설된 ITS 보안 연구반에서의 표준화 동향을 살펴 본다.

Ⅰ. 서 론

현재, 차량통신 기술을 이용하여, 도로의 교통 효율을 높이고, 운전자의 안전 및 주행 편리성을 높이기 위한 다양한 실증 연구들이 수행 중에 있다. 특히, 자율주행 차량의 필수 요소 기술로서 차량통신 기술의 중요성이 강조되고 있다. 그러나, 차량 간 통신 기술을 활용하기 위해서는 반드시 보안 기술의 확보가 선행되어야 한다. 차량 네트워크 환경은 기존의 인터넷 등의 네트워크 환경과 달리 네트워크의 보안성 확보 여부가 운전자의 생명과 직결되는 위험 상황을 유발할 수 있기 때문이다. 이러한 상황을 반영하여, 현재 ITS 보안 표준화가 활발히 진행 중에 있다[1,2,3,4].

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, 9월 회의에서 첫 정규 회의를 가졌다. 본 논문에서는 SG17의 ITS 보안 연구반의 활동을 중심으로 ITS 보안 표준화 현황을 소개한다.

Ⅱ. ITS 보안 기술 표준화 현황

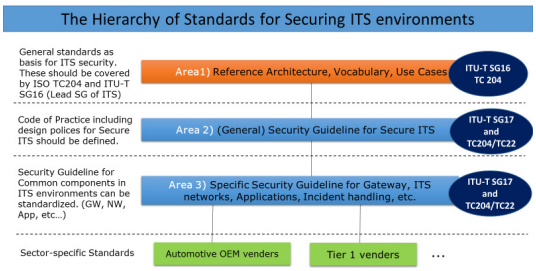
ITS 보안 연구반(Q13)의 표준화 범위 및 향후 계획, 그리고, 표준화 추진 중인 내용을 소개한다.

2.1. ITU-T SG17에서의 표준화 활동

SG17에서는 2017년 3월 회의에서 ITS 보안 연구반 Q13을 신설(라포쳐:이상우, ETRI, 부라포쳐: 박승욱, 현대자동차)하였고, 9월 회의에 첫 정규 회의가 진행되었다. Q13의 표준화 분야는 차량통신보안 분야에 국한되는 것이 아니라, 차내망 통신, 차외망 통신을 포함하고, 안전한 지능형교통시스템 구축을 위한 보안 기술 전 분야를 포함한다. 그림 1은 Q13 표준화 로드맵을 나타낸 것으로, SG17은 보안 가이드라인을 위주로 표준화를 추진할 계획이며, ITS의 참조 모델은 SG16 및 ISO TC204의 표준 내용을 참조로 개발할 계획이다. 또한, ISO TC204와의 협력을 통한 표준 개발을 추진할 계획이다. ITS 보안 연구반(Q13)에서는 기존의 텔레커뮤니케이션/네트워크/IoT 보안 연구반(Q6)에서 추진 중이던 2건의 ITS 보안 표준(X.itssec-1 및 X.itssec-2)을 이관받아서 표준화를 진행한다. X.itssec-1, Software update capability for ITS communications devices은 지난 회

본 연구는 산업통상자원부 및 한국산업기술진흥원의 국제공동기술개발사업의 일환으로 수행되었음.[N0001710. 자율(협력)주행 차량 간 및 주변환경과 안전한 신뢰 연동을 위한 고속상호인증 및 해킹대응보안플랫폼 기술 개발]

* 한국전자통신연구원



〔그림 1〕 Q13(ITS 보안 연구반) 표준화 범위

의에서 X.1373으로 승인되었다[5].

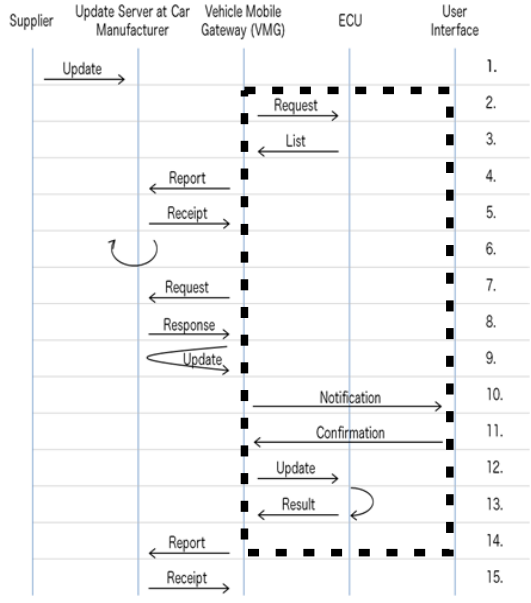
X.1373, Software update capability for ITS communications devices의 표준화 범위는 안전한 차량의 소프트웨어 업데이트 절차를 정의하는 것이다. 오늘날 차량에서는 다수의 ECU(Electronic Control Unit)를 적용하고 있고, 리콜이 요구되는 차량의 약 30%가 ECU 소프트웨어의 업데이트로 인한 문제라고 보고되고 있는 현상을 반영하여, SG17의 ITS 보안 표준안 중 가장 먼저 표준으로 승인되었다. 구체적으로, X.1373에서는 차량의 원거리 소프트웨어 업데이트 개요, 위협 요소 및 위협 분석, 기능 요구사항, 안전한 소프트웨어 업데이트 구조를 정의한다.

본 표준에서 업데이트 서버는 차량 제조업체로부터 SW 업데이트 데이터를 제공받아서 차량의 ECU 원격 업데이트를 수행하는 서버를 의미한다. 차량게이트웨이(Vehicle Mobile Gateway)는 차내망과 차외망을 연결하는 인터페이스를 담당하는 모듈로서, 본 표준에서는 업데이트 서버로부터 SW를 다운 받아, 차내망의 SW 업데이트가 요구되는 ECU에게 제공하는 역할을 수행한다.

또한, 본 표준에서는 차량 SW 업데이트 절차를 15단계로 기술하고 있다. (그림 2)는 차량 SW 업데이트 절차를 나타낸 것이며, 각 단계의 구체적인 수행 절차는 다음과 같다.

1. 공급자가 업데이트 서버를 업데이트 한다.
2. VMG는 ECU에게 SW 리스트를 요청 한다.
3. ECU는 SW 상태를 점검하고, SW 리스트를 생성하여 VMG에게 전송 한다.
4. VMG는 수신한 SW리스트를 업데이트 서버에게 전송한다.
5. 업데이트 서버는 ACK를 VMG에게 전송한다.
6. 업데이트 서버는 수신한 SW리스트를 통해 업데이트 해야할 SW가 있는 지 확인한다.
7. VMG는 주기적으로 업데이트 필요 여부를 업데이트 서버에게 요청한다.
8. 업데이트가 필요하다면, 업데이트 서버는 URL을 VMG에게 전송한다.
9. VMG는 SW 업데이트 모듈을 다운로드 한다.
10. VMG는 운전자에게 업데이트가 필요함을 알린다.
11. 운전자는 업데이트를 승인한다.
12. VMG는 업데이트 모듈을 ECU에게 전송한다.
13. 각각의 ECU는 업데이트를 실시하고 결과를 VMG에게 보고한다.
14. VMG는 ECU 업데이트 실시 결과를 업데이트 서버에게 보고한다.
15. 업데이트 서버는 ACK를 VMG에게 송신한다. 만약 업데이트가 실패되거나, 일부만 업데이트 되었다면, 6 ~ 14 단계를 반복한다.

특히, 최종 표준안 승인 과정에서 [그림 2]의 점선으로 도시한 차내망과 연관된 메시지는 optional 메시지로 지정되었다. 이는 차내망과 연관된 규격은 표준화 범위에서 제외해야한다는 완성차 업체의 의견을 반영한



〔그림 2〕 X.1373 소프트웨어 업데이트 절차

것이다. 본 표준에서는 각 단계에서의 메시지 포맷과 XML 예제도 포함하여 기술하고 있다.

X.itssec-2, Security guidelines for V2X communication systems에서는 차량통신시스템에 대한 보안 가이드라인을 표준의 범위로 설정하고 있다[6]. 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 9월 회의에서는 한국, 일본, 중국, 싱가폴 등 다양한 회원국의 의견이 개진되어 아래와 같은 내용이 표준안에 반영 되었다.

첫째, V2V와 V2I의 절을 구분하고, 보안 위협 및 보안 요구사항을 별도로 기술하기로 하였다. 이는 V2V와 V2I의 통신 환경에 특화된 위협과 보안 요구사항을 반영하기 위함이다.

둘째, V2P(Vehicle-to-Pedestrian)을 표준화 범위에 포함하여, 이에 대한 보안 위협 및 보안 요구사항을 정의하기로 하였다. 그러나, 실제 보행자와 차량의 통신에 있어서, 보행자의 통신 수단으로서 대표적으로 노매딕 디바이스가 사용됨을 고려하여, V2P를 V2ND의 한 형태로 구분하고 이에 대한 내용을 기술할 계획이다.

셋째, 차량과 이통통신네트워크(Vehicle-to-Network)에 대한 보안 위협 및 보안 요구사항 도출의 필요성이 제기되었다. 특히, 현재 LTE-V등 이동통신 진영에서도 차량 통신 분야를 주된 응용 분야로 간주하고, 이에 대한 표준화가 진행되고 있음을 고려하여, 기존의 V2I와 달리 이동통신네트워크 환경에 특화된 보안 위협과 보안요구사항을 정의할 수 있는 지 분석 후 차기 회의에서 이에 대한 내용을 표준안에 포함시킬 지를 결정할 계획이다.

넷째, UNECE의 WP29의 TFCS(Taskforce for Cyber Security)에서 올해 말까지 차량 사이버 보안 위협을 정의할 예정이다. 이와 관련하여, WP29에서 도출된 보안 위협을 X.itssec-2에 반영하여 표준화를 추진할 계획이다.

특히, UNECE WP29와의 협력을 위하여, Correspondence Group을 신설하였으며, 본 그룹을 통하여 UNECE WP29와의 협력을 강화할 계획이다.

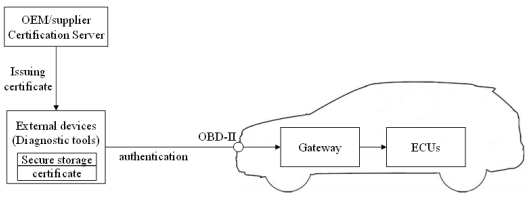
2.2. ITS 보안 연구반(Q13) 신규 표준화 과제

지난 9월에서는 한국 주도로 아래의 3가지 신규 표준 아이템을 제안하여, 신규 과제로 선정되었다.

- 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.itssec-3의 목적은 차량에 접속하는 디바이스의 보안요구사항을 정의하는 것이다[7]. 차량 내부 진단 도구가 많이 활용하고 있는 OBD-II 포트를 이용하는 디바이스 뿐만 아니라, 블루투쓰 등 무선 네트워크를 이용하여 차량에 접속하는 디바이스에 대한 보안요구사항의 정의도 본 표준안에서 다루어질 계획이다. (그림 3)은 본 표준안에서 정의할 OBD-II를 통하여, 차량에 접근하는 환경을 도시한 것이다. 본 표준안에서는 OBD-II를 이용하여 차량에 접속하는 외부 장치는 HSM(Hardware Security Module)을 구비하고,해당 디바이스의 펌웨어를 업데이트하기 위해서는 보안 알고리즘을 이용한 안전한 펌웨어/소프트웨어 업데이트 기능을 구비하여야 하며, 또한, 부팅과정에서 SW의 무결성을 검증하는 기능을 보유할 것을 권고하고 있다.

특히, 최근의 차량 해킹 사례에서, 차내망으로의 접근은 주로 OBD-II를 이용하여 수행되었다. 따라서, 본 표준안은 실제적인 차량 해킹 사고 방지 관점에서 그

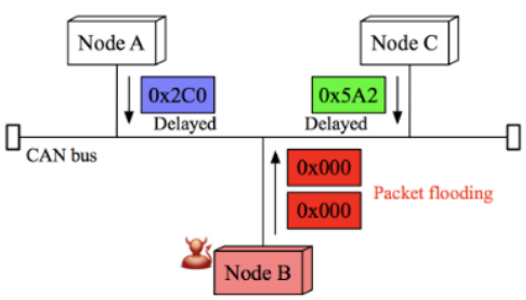


〔그림 3〕 차량접속디바이스 환경

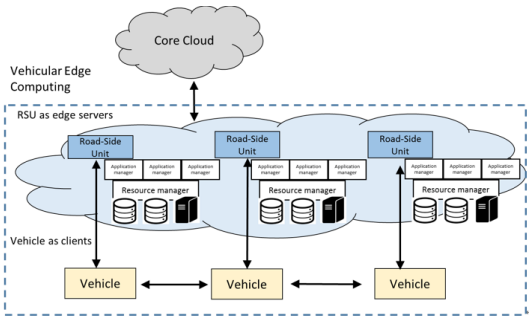
중요성이 매우 높다고 할 수 있다.

X.itssec-4의 표준화 범위는 차내망에서의 침입탐지 시스템 구성 방법을 정의하는 것이다[8]. 기존의 침입탐지시스템은 이더넷망, TCP/IP망에 대한 악성 코드 탐지를 수행한다. 그러나, 기존의 침임탐지시스템은 CAN(Controller Area Network) 환경에서는 적용이 불가능하므로, 차내망에 적합한 침입탐지시스템의 기능 및 규격 정의가 필요하다. 아래 (그림 4)는 CAN에서의 DoS공격의 예를 나타낸 것이다. CAN ID를 0x000으로 지정한 메시지를 짧은 시간에 다량 전송하게 되면, CAN으로 연결된 노드 즉, ECU(Electronoc Control Unit)의 통신 기능 장애를 유발하게 된다. X.itssec-3에서는 이러한 차내망에 특화된 침입탐지시스템의 다양한 구현 방법 및 고려사항에 대하여 표준화를 진행할 계획이다.

X.itssec-5는 차량 에지 컴퓨팅 보안 가이드라인을 정의하는 것이다[9]. 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 사용자에게 실시간 응답 서비스 제공이 필요한 경우에는 네트워크 지연 시간으로 인하여, 서비스 제공이 어렵다. 상기한 문제점을 해결하기 위하여, 기존의 클라우드 서비스 서버를 네트워크의 에지 영역에 구현함으로써, 엔드 클라이언트에게 보다 빠른 서비스를 제공할 수 있다. 유럽의 표준화기구 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 있다. 그러나, 도로기지국은



〔그림 4〕 차내망에 대한 DoS 공격 예



〔그림 5〕 차량 에지 컴퓨팅 개념도

클라우드 서버에 비하여 물리적인 사이버 보안 환경 구축이 취약하며,다양한 인증 및 인가 방식이 적용될 수 있는 네트워크 환경으로 인해 특화된 보안 규격을 정의할 필요가 있다. (그림 5)는 차량 에지 컴퓨팅의 기본 구조를 나타낸 것이다. 도로기지국이 에지 컴퓨팅 서버 기능을 담당하게 되며, 엔드 클라이언트가 고속 이동 가능한 차량으로 구성되는 것이 특징이다.

특히, X.itssec-5는 클라우트 컴퓨팅 보안과의 유사점을 고려하여, SG17의 클라우드 보안 연구반(Q8)과 협력 표준화 과제로 선정되었으며, ITS 보안 연구반(Q13)이 책임 연구반으로서, 클라우드 보안 연구반과 공동으로 표준화를 추진하게 된다.

Ⅲ. 결 론

본 논문에서는 SG17 ITS 보안 연구반에서 현재 추진 중인 표준화 내용과 신규로 선정된 표준화 아이템에 대하여 기술하였다. 현재 대두되고 있는 IoT 보안의 실제적인 적용 사례라고 할 수 있는 ITS 보안 국제표준화가 국제적으로 활발히 진행되고 있는 만큼, 정부, 학계, 연구기관의 적극적인 참여를 통한 국제 표준화의 주도권 선점이 필요한 시점이다.

참 고 문 헌

[1] 이상우 외, “차량 통신 보안 기술 동향,” 주간기술동향, vol. 1556, 2012.

[2] ITU-T Y.2281, Framework of networked vehicle services and applications using NGN, 2011.

[3] ETSI EN 302 665, Intelligent Transport Systems (ITS); Communications Architecture, 2010.

[4] IEEE Std 1609.2, IEEE Standard for Wireless

Access in Vehicular Environments (WAVE) Security Services for Applications and Management Messages, 2016.
[5] ITU-T SG17 Recommendation, X.1373, Secure software update capability for ITS communications devices. 2017
[6] ITU-T SG17 draft Recommendation, X.itssec-2, Security guidelines for V2X communication systems. 2017
[7] ITU-T SG17 draft Recommendation, X.itssec-3, Security requirements for vehicle accessible external devices, 2017.
[8] ITU-T SG17 draft Recommendation, X.itssec-4, Methodologies for intrusion detection system on in-vehicle systems, 2017.
[9] ITU-T SG17 draft Recommendation, X.itssec-5, Security guidelines for vehicular edge computing, 2017.

〈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

권혁찬(Hyeok-Chan Kwon)
정회원

2001년 2월 : 충남대학교 컴퓨터과학과 박사
2001년 1월~현재 : 한국전자통신연구원 정보보호연구본부 PL/책임연구원
관심분야 : 자동차융합보안, IoT 보안, 의료융합보안, 무선 보안

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