정 보 보 호 학 회 지
제28권 제4호, 2018. 8

ITS 보안 국제 표준화 동향

이 상 우*, 권 혁 찬*, 나 중 찬*

요 약

ITU-T SG17에서는 2017년 9월 회의부터 ITS(Intelligent Transport System) 보안연구반(Question 13)이 신설되어, ITS 보안 표준 개발을 중점적으로 추진하고 있다. 이는 최근 자율주행차량, 차량통신기술 등의 상용화가 임박함에 따라, 대두되는 여러 가지 보안 기술에 대한 국제표준화의 필요성이 강조되고 있기 때문이다. 본 논문에서는 ITS 보안 연구반에서 진행되고 있는 표준화 과제 내용과, 지난 3월 회의에서 신규로 채택된 표준화 과제의 내용을 소개한다.

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[1-4].

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, 2017년 9월 회의에 이어, 2018년 3월에 두 번째 정규회의가 개최되었다. 본 논문에서는 SG17의 ITS 보안 연구반의 활동을 중심으로 ITS 보안 표준화 현황을 소개한다.

Ⅱ. ITS 보안 기술 표준화 현황

ITS 보안 연구반(Q13)의 현재 진행중인 표준화 과제와 지난 3월 신규 채택된 표준화 과제를 소개한다.

2.1. ITU-T SG17에서의 표준화 활동

SG17에서는 2017년 3월 회의에서 ITS 보안 연구반 Q13을 신설(라포쳐:이상우, ETRI, 부라포쳐: 박승욱, 현대자동차)되어 ITS 보안 분야의 표준화를 추진하고 있다. Q13의 표준화 분야는 차량통신보안 분야에 국한되는 것이 아니라, 차내망 통신, 차외망 통신을 포함하고, 안전한 지능형교통시스템 구축을 위한 보안 기술 전 분야를 포함한다.

현재 Q13에서는 아래의 4개 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

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

X.itssec-2, Security guidelines for V2X communication systems에서는 차량통신시스템에 대한 보안 가이드라인을 표준의 범위로 설정하고 있다[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 3월 회의에서는 한국 주도로 아래의 내용이 표준안에 반영되었다.

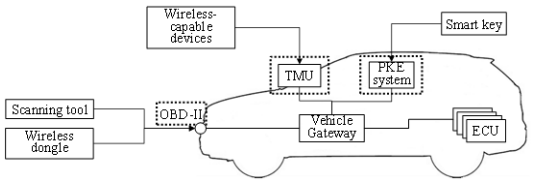
첫째, X.itssec-2의 보안 위협을 UNECE(United Nations Economic Commission for Europe)의 사이버 보안 권고안의 내용을 반영하여 수정하였다. UNECE WP29의 TFCS(Taskforce for Cyber Security)에서는 올해 말까지 차량 사이버 보안 권고안을 확정할 예정이며, X.ittsec-2도 이와 연관되게 수정이 진행될 예정이다.

둘째, 차량통신에서의 메시지 암호화 방법 및 메시지 서명 방법이 기술되었다. 이는 현재 차량통신분야에서 많이 사용되고 있는 ECIES 및 ECDSA에 대한 일반적인 방법론을 기술한 것이다

셋째, 차량통신시스템의 사용 예가 추가되었다. 도로에서의 차량 안전 관련 긴급 경고 메시지를 전파하는 사용 예와, 군집 주행 서비스의 사용 예가 추가되었다.

X.itssec-2는 올해 말 또는 내년 초에 표준화 승인을 목표로 표준화 최종 작업이 진행 중이다. 차기 회의에서 차량용 공개키 기반 구조의 예 및 보안 위협등이 추가 기고서를 통해 반영될 예정이다.

X.itssec-3의 목적은 차량에 접속하는 디바이스의 보안요구사항을 정의하는 것이다[6]. 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 1)은 본 표준안에서 정의할 OBD-II를 통하여, 차량에 접근하는 환경을 도시한 것이다. 본 표준안에서는 OBD-II를 이용하여 차량에 접속하는 외부 장치는 HSM



〔그림 1〕 차량접속디바이스 환경

(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.

지난 3월 회의에서는 한국 주도로 차량외부접속 디바이스의 보안 위협을 UNECE WP29 사이버 보안 권고안의 위협을 기반으로 수정하였다. X.itssec-3의 보안 위협 역시 올해 확정되는 UNECE WP29 사이버 보안 권고안에 따라 내용이 수정될 예정이다. 또한, 지난 6월 인터림 회의를 통하여, 전기차 관련 외부 접속 디바이스도 표준의 범위에 포함하여 표준화가 진행될 예정이다.

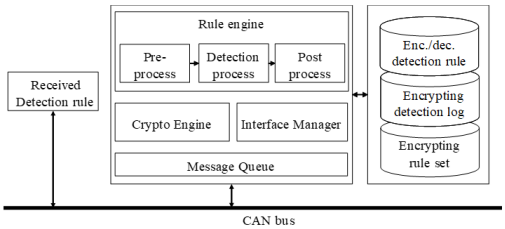
X.itssec-4의 표준화 범위는 차내망에서의 침입탐지 시스템 구성 방법을 정의하는 것이다[7]. 기존의 침입탐지시스템은 이더넷망, TCP/IP망에 대한 악성 코드 탐지를 수행한다. 그러나, 기존의 침임탐지시스템은 CAN (Controller Area Network) 환경에서는 적용이 불가능하므로, 차내망에 적합한 침입탐지시스템의 기능 및 규격 정의가 필요하다. 이러한 요구사항을 부합하기 위하여 지난 3월 회의에서는 아래의 내용이 반영되었다.

첫째, 현재 차내망에서 많이 활용되고 있는 CAN의 프레임에 대한 구체적인 설명이 추가되었다.

둘째, 그림 2와 같이 차내망 IDS의 기본 개념 및 규칙 엔진의 기본적인 절차가 추가되었다.

셋째, 차내망에서 IDS(Intrusion Detection System) 구현 시 IDS의 위치에 따른 구현 및 설치 가이드라인이 추가되었다. IDS가 차내망 중앙게이트웨이의 앱으로 구현되는 경우, 중앙게이트웨이이 뒷 단에 설치되는 경우, 서브게이트웨이 상에 구현되는 경우 및 개별 ECU에 구현되는 경우로 구분하여 각 특징을 기술하였다.

X.itssec-5는 차량 에지 컴퓨팅 보안 가이드라인을 정의하는 것이다[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 제공자



〔그림 2〕 차내망 IDS 개념도

의 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 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. 차량 에지 컴퓨팅 환경에서는 도로기지국이 에지 컴퓨팅 서버 기능을 담당하게 되며, 엔드 클라이언트가 고속 이동 가능한 차량으로 구성되는 것이 특징이다.

지난 3월 회의에서는 아래의 내용이 반영되었다.

첫째, 차량에지컴퓨팅 환경에서의 보안 위협 및 취약성 내용이 추가되었다. 둘째, 차량 에지 컴퓨팅의 사용예가 추가되었다. 실시간 교통환경 전파의 경우, 엔드 클라이언트 차량에서 실시간 정보를 제공하기 위하여, 도로기지국이 에지 컴퓨팅 서버 역할을 할 수 있다. 또한, 후방의 차량이 추월하는 경우, 중앙선 반대편에 진행하는 차량과의 정보 교환이 필요한 경우, 실시간 응답을 위하여, 도로기지국이 에지 컴퓨팅 서버 역할을 할 수 있다.

2.2. ITS 보안 연구반(Q13) 신규 표준화 과제

지난 3월 SG17 회의에서는 아래의 3가지 신규 표준 과제가 채택되었다[9,10,11].

- 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

X.srcd(V2X 통신 환경에서의 데이터보호 요구사항)의 표준화 목적은 V2X 통신환경에서 송수신되는 데이터를 분류하고, 분류된 데이터에 따른 보안 레벨을 정의하고, 정의된 보안 강도를 보장하기 위한 보안요구사항을 정의하는 것이다. 본 신규과제는 중국의 IT 연구기관, CAICT(China Academy of Information and Communications Technology)에서 기존의 클라우드 보안 표준화 내용을 기반으로 ITS 보안 분야의 표준화도 추진하기 위하여 제안하였다.

X.mdcv(커넥티드 차량에서의 빅데이터 기반 비정상행위 탐지 매커니즘)의 표준화 목적은 빅데이터 분석에 기반하여 차량의 사이버 보안 관련 비정상행위 탐지 매커니즘을 정의하는 것이다. 본 표준에서는 차량, 도로기지국 등의 인프라 등으로부터 수집하는 데이터 구조를 정의하고, 비정상행위 탐지 방법을 정의할 계획이다. 본 과제는 중국의 대표적인 안티바이러스 업체인 360 Technology에서 제안한 것으로서, 중국의 보안 업계가 ITS 보안 기술 개발 및 ITS 보안 분야로의 사업 영역 확대, 그리고 국제표준화 추진 등을 적극적으로 추진하고 있음을 알 수 있다.

X.srcv(커넥티드 차량 보안 위협)의 표준화 범위는 커넥티드 차량 및 에코시스템에서의 보안 위협을 정의하는 것이다. UNECE WP29에서 정의되고 있는 차량 사이버보안 권고안의 보안 위협을 기반으로 하여, 커넥티드 차량에 대한 상위 레벨의 위협을 정의하는 것이 표준의 목적으로, 향후 ITS 보안 연구반에서 개발될 표준들의 기초 표준 문서의 성격으로 개발될 계획이다.

Ⅲ. 결 론

본 논문에서는 SG17 ITS 보안 연구반에서 현재 추진 중인 표준화 내용과 신규로 선정된 표준화 아이템에서 대하여 기술하였다. ITU-T SG17에서 ITS보안연구반(Q13)이 2017년 3월 생성된 이후로, ITS 보안 표준

화가 활발히 진행되고 있다. 특히, 중국의 IT 연구기관 CAICT 및 안티바이러스 업체 360 Technology에서 신규 표준화 과제를 제안하는 등 표준화에 박차를 가하고 있다.

한국에서는 현대차, ETRI 등이 주도적으로 표준화에 참여하고 있으나, 중국의 약진 등의 상황을 고려할 때, 지속적인 차량보안 표준화의 주도권 선점을 위하여, ISO TC 204 등의 표준화기구와의 협업을 통한 표준의 실효성 및 파급력을 고취시킬 필요가 있으며, 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.

〈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

권 혁 찬 (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