정 보 보 호 학 회 지
제26권 제4호, 2016. 8

ITS 보안 기술 표준화 동향

이 상 우*, 나 재 훈*

요 약

오늘날 차량 교통 시스템은 지능형 교통 시스템(ITS, Information Transportation System) 으로 진화하고 있다. 특히 차량 간 통신 및 차량과 인프라 간 통신을 활용하여 차량 주행의 안전성을 높이고 교통 체계의 운영 및 관리를 과학화하고자 하는 연구가 활발히 진행 중이며, 특히 운전자의 안전을 확보하기 위한 보안 기술에 대한 연구 또한 활발히 진행되어야 한다. 본 고에서는 ITS 보안 기술에 대한 표준화가 활발히 진행 중인 ITU-T SG17 에서의 표준화 동향을 살펴 본다.

Ⅰ. 서 론

최근 들어, 자율 주행 차량의 상용화가 가시화 되고 있다. 자율 주행 차량은 차량의 주변 정보를 인식하는 레이더, 카메라 등의 센서 기술, 차량과 차량, 차량과 도로기지국 간의 통신 기술, 그리고, 주변 인식 정보와 통신 정보를 바탕으로 차량을 실시간 제어하는 기술로 구성된다. 특히, 레이더 등의 가시 거리 한계, 야간에서의 시각적 한계 상황을 보완하기 위하여 차량 간 통신 기술은 필수적인 기술이다. 그러나, 차량 간 통신 기술을 활용하기 위해서는 반드시 보안 기술의 확보가 선행되어야 한다[1]. 차량 네트워크 환경은 기존의 인터넷 등의 네트워크 환경과 달리 네트워크의 보안성 확보 여부가 운전자 의 생명과 직결되는 위험 상황을 유발할 수 있기 때문이다. 이러한 상황을 반영하여, 현재 ITS 보안 표준화가 활발히 진행 중에 있다. 본 고에서는 ITS 보안 기술 중 차량 통신 보안 기술의 표준화 동향을 소개한다.

Ⅱ. ITS 보안 기술 표준화 현황

ITS 보안 표준화는 IEEE, ETSI, ITU-T 등에서 추진 중이다. IEEE와 ETSI에서는 이미 1차 버전이 제정되어 개정이 추진 중인 상태이고, ITU-T에서는 새로이 표준화를 추진 중이다[2-5]. 특히 본 절에서는 IEEE 및 SG17에서 진행 중인 표준화 활동을 살펴본다.

2.1. IEEE WAVE (Wireless Access in Vehicular Environment) 보안 표준화 현황

IEEE 1609.2 에서는 WAVE 기술을 위한 보안 서비스를 정의한다[4]. WAVE 메시지에 대한 인증 메커니즘 메시지 규격을 제공한다. 특히, 2016년 1월 2016년 개정 버전이 표준으로 제정되었다. IEEE 1609.2 에서는 WAVE 기술을 위한 보안 서비스를 정의한다[4]. WAVE 메시지에 대한 인증 메커니즘 및 사용자에 대한 인증 메커니즘을 제공한다. 특히, 2013년 버전에서는 포함하지 않았던 익명/가명 인증서에 대하여 기술하고 있고, 기존의 보안 기능을 상위계층 보안 서비스와 내부 보안 서비스로 구분하고, 상위계층 보안 서비스에서는 인증서폐지목록검증 기능 및 P2P 인증서 배포 기능을 포함한 것이 특징이다.

2.2. ITU-T SG17에서의 표준화 활동

SG17에서는 2014년부터 ITS 보안 분야의 표준화가 진행되었다. 기존의 차량통신보안 표준화는 차량 통신을 표준화하는 단체에서 전체 표준의 일부 항목으로 표준화가 진행되었다. 따라서, SG17같은 보안 분야를 담당하는 전문 표준화 기구에서 차량 통신 보안 분야에

본 연구는 산어통상자원부 및 한국산업기술진흥원의 국제공동기술개발사업의 일환으로 수행되었음.[N0001710. 자율(협력)주행 차량 간 및 주변환경과 안전한 신뢰 연동을 위한 고속상호인증 및 해킹대응보안플랫폼 기술 개발]
* 한국전자통신연구원(ttomlee@etri.re.kr, jhnah@etri.re.kr)

대한 표준화를 진행하고 있다는 것이 그 의의가 크다고 할 수 있다.

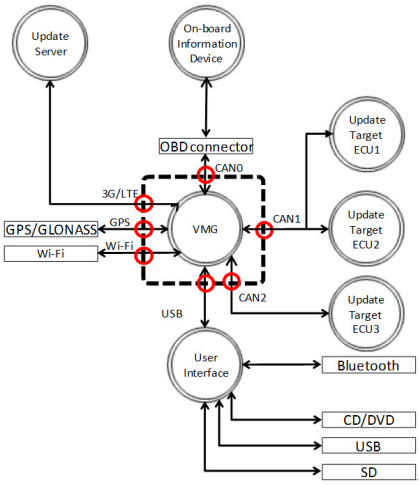
ITU-T SG17에서는 차량 통신 보안 및 ITS 보안을 주제로 2개의 신규 워크 아이템을 선정하고 이에 대한 표준화가 진행 중이다. 한 건은 ITS 보안을 포괄적으로 접근하는 표준안(X.itssec-2)[7]이고, 또 다른 한 건은 ITS 보안 분야 중 특정 분야에 대한 표준(X.itssec-1)[6]을 제정하는 것이다.

X.itssec-1, Software update capability for ITS communications devices의 표준화 범위는 에서는 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 반영하고, 안전한 소프트웨어 업데이트 절차를 표준화하고자 하는 것이 X.itssec-1의 목적이다.

X.itssec-1에서는 차량의 원거리 소프트웨어 업데이트 개요, 위협 요소 및 위협 분석, 기능 요구사항, 안전한 소프트웨어 업데이트 구조를 정의한다.

[그림 1]은 본 표준의 차량 SW 업데이트 절차의 동작 환경을 나타낸 것이다. 본 표준에서는 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 받아서, 차내망의 SW 업데이트가 요구되는 ECU에게 제공하는 역할을 수행한다.

[그림 2]는 본 표준의 범위를 나타낸 것이다. 차량게이트웨이를 기준으로 차량 SW 업데이트 시 발생할 수 있는 보안위협을 분석하고, 해당 위협에 대응할 수 있는

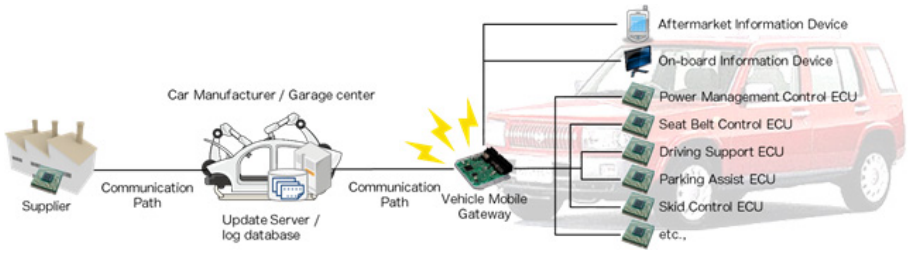


〔그림 2〕 X.itssec-1의 표준화 범위

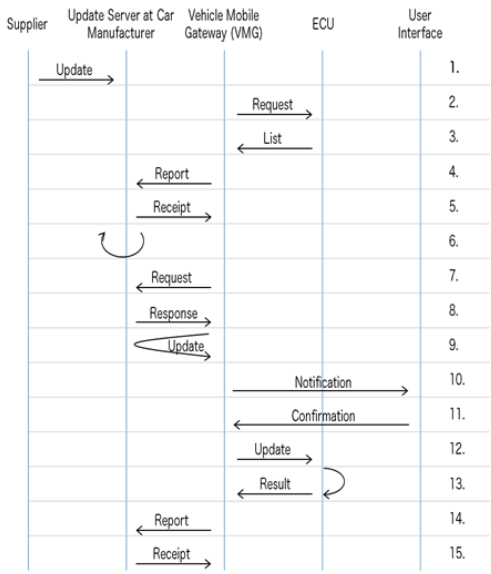
보안요구사항을 도출하는 것을 표준의 범위에 포함하고 있다.

또한, 본 표준에서는 차량 SW 업데이트 절차를 15단계로 기술하고 있다. [그림 XX]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



〔그림 1〕 X.itssec-1의 차량 SW 업데이트 환경



〔그림 3〕 X.itssec-1의 차량 SW 업데이트 절차

VMG에게 전송한다.

9. VMG는 SW 업데이트 모듈을 다운로드 한다.
10. VMG 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.

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

[그림 4]는 진단 요청 메시지의 메시지 포맷 및 XML예제를 나타낸 것이다.

지난 3월 SG17 회의 및 6월 인터림 회의에서 제안된 내용과 반영 내용은 다음과 같다. 미국은 차량 SW 업데이트 절차 15단계에서 재시도의 횟수 제한이 필요함을 제안하였으며, 차량 게이트웨이의 자원제약성을 언급하고, 이에 대한 표준의 수정을 제안하였다. 한국의 현대차 그룹은 ECU SW 업데이트 절차 단계에서 ECU의 하드웨어 버전에 따른 업데이트 SW의 차이점이 있

Element	Attribute in element	Description
Message	-	Container of the message.
	protocol	Always "1.0".
	version	The version number of the message sender.
	type	Message type (always "diagnose").
	subtype	Message subtype (always "request").
	sessionid	Session ID is a random global user ID (GUID) associated with the diagnose session. An identical session ID is applied to a set of diagnose request, report, submit and receipt messages.
	trustlevel	Trustlevel is determined based on the security capability and safety requirement of the device that generated this message.
	messageid	Message ID is a random GUID associated with an individual message.
IssuedTime	-	Time of generation of this message.
ExpirationTime	-	Expiration time of this message.

```
<Message protocol="1.0" version="1.0.2" type="diagnose" subtype="request"
sessionid="{7316A97D-8C04-4288-B498-0F51087A1093}" messageid="{2E255A59-B875-4347-
90CA-92326BF45BEF}" trustlevel="3">
  <IssuedTime>1903-07-01T00:00:00Z</IssuedTime>
  <ExpirationTime>1903-07-01T00:00:00Z</ExpirationTime>
</message>
```

〔그림 4〕 진단요청메시지의 규격 및 XML 예제

음을 언급하고, 이에 대한 표준의 표준을 제안하였다. 상기한 의견을 반영하여 현재 표준안에는 6장에서 재시도 횟수 및 차량게이트웨이의 자원제약성 내용이 반영되었으며, 메시지 규격에 하드웨어 버전이 포함되도록 수정되었다. 지난 6월 인터림에서는 일본에서 차내망 규격을 본 표준의 범위에서 제외시킬 것을 건의하였고, 이에 대하여 차기 9월 SG17회의에서 추가 논의 후, 반영될 예정이다.

X.itssec-2, Security Guidelines for V2X communication Systems에서는 차량통신시스템에 대한 보안 가이드라인을 표준의 범위로 설정하고 있다. V2X 통신 시스템은 차량 통신 시스템을 통칭하는 것으로 차량과 차량(V2V), 차량과 인프라(V2I) 및 차량과 노매딕 디바이스(V2N) 간의 통신 환경을 의미한다. X.itssec-2에서는 V2V, V2I, V2N 통신 환경에서의 보안 위협 및 보안 요구 사항을 정의하고, 차량 등록 및 인증 서비스 모델 등의 유즈 케이스를 표준화 범위로 지정하고 있다.

차량 통신 환경에서의 보안 위협에 따른 구체적인 공격의 형태는 다음과 같다.

- 차량 및 RSU 인증에 대한 공격

라우팅 테이블, LDM의 변조 공격은 차량의 위치 정보를 거짓으로 조작하여 전송하거나, GPS 위치 정보를 스푸핑(spoofing)하거나, GPS의 신호 정보를 조작하는 공격을 의미한다. 위장(Impersonation) 공격은 공격자가 네트워크 상의 다른 노드로 위장할 수 있음을 의미한다. 이것은 공격자가 위장하고자 하는 노드의 비밀 정보를 획득함으로써 가능하다. 위장 공격에 의해 특정 노

드에 전달될 정보가 공격자에 의해 수신되거나, 특정 노드가 전송해야만 하는 정보를 공격자가 거짓으로 전송하는 것이 가능하다. 예를 들어, 공격자는 응급 차량 ID를 도용하여 전방 차량으로 하여금 응급 차량이 접근한다는 거짓 정보를 전송할 수 있다.

Sybil 공격은 임의의 공격자가 다수의 ID를 가지고 네트워크를 공격하는 방법을 의미한다. 차량 통신 환경에서는 하나의 차량이 다수의 차량 ID를 이용하는 것을 의미한다. 예를 들면, 공격자(하나의 차량)가 다수의 차량 ID를 도용하여 도로가 병목 상태에 있다는 거짓 정보를 전파할 수 있다. 서비스 인프라에 대한 공격은 PKI 인증 센터에게 OBU의 거짓 침해 정보를 전달하여, 잘못된 인증서 취소 목록을 생성하게 하는 공격을 의미한다.

- 메시지 무결성에 대한 공격

라우팅 메시지의 위/변조 공격은 중간 노드가 자신이 전달하게 되는 메시지를 위/변조함으로써 다른 차량으로 하여금 거짓 정보를 수신하게 하는 공격이다.
센서 정보 위/변조 공격은 차량 내 통신망에서 물리적인 주소를 위/변조 하거나, ECU의 센서 제어 정보를 위/변조하는 공격이다. 차량 비밀 정보 위/변조 공격은차량의 개인 키 및 고유 정보(예 : 차량 ID)에 대한 위/변조 및 비인가된 사용을 의미한다.

- 기밀성에 대한 공격

차량 통신 메시지의 도청 공격은 차량 통신 메시지의 도청은 차량 간 통신 메시지 및 차량과 인프라 간의 통신 메시지에 대한 도청을 의미한다. OBU 또는 RSU의 비밀 소프트웨어의 도청 공격은 OBU 또는 RSU의 원거리 업데이트 중에 소프트웨어를 가로채거나, 가로챈 소프트웨어로부터 차량의 비밀 정보를 유출하는 공격을 의미한다.

- 프라이버시에 대한 공격

개인정보의 수집 공격은 차량 통신 메시지를 수집 및 분석하여 차량의 소유자를 분석하고, 그 차량의 출발지, 경유지 및 목적지 등의 위치 정보를 수집하는 공격을 의미한다. 가명(Pseudonym) 분석 공격은 가명 분배 과정의 메시지를 획득하여 차량의 고유 ID와 가명의 연결 관계를 획득하거나 서로 다른 가명들이 동일한 차량임을 분석하는 공격을 의미한다.

- 부인 봉쇄에 대한 공격

차량 통신에서 부인 봉쇄를 제공하는 보안 메커니즘은 디지털 서명이다. 따라서, 부인 봉쇄에 대한 공격은 디지털 서명에 연관된 공격 행위가 된다. 인증서 DB 공격은 CA에 저장된 가명 DB를 위조하거나, 장기 인증서(long term certificate)와 가명 인증서(short term pseudonym certificate) 간의 관계를 조작하는 형태의 공격을 의미한다. 디지털 서명 생성을 위한 개인 키 및 인증서에 대한 비인가된 접근도 부인 봉쇄 요구 사항을 위배하는 공격이 된다.

- 가용성에 대한 공격

가용성에 대한 공격은 통신 채널을 점유하여 정상적인 메시지 송수신이 불가능하게 하는 것을 의미한다. 이것은 다수의 OBU 또는 RSU를 해킹하거나, 하나의 차량으로 하여금 무한대의 메시지를 전송하게 함으로써 가능하다. 또한, 메시지를 라우팅 하는 차량이 라우팅을 하지 않거나, 특정 메시지만 라우팅 하는 것도 가용성에 대한 공격의 일종이다.

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.

X.itxec-2는 현재 표준화가 활발히 진행 중인 초기 단계로서, 아직 논의가 진행 중인 V2N 환경에서의 보안 위협 및 보안요구사항 정의, 그리고, 다양한 형태의 차량 통신 보안 시스템에 대한 Use Case에 대한 표준화가 진행될 예정이다.

X.itssec-1과 X.itssec-2에 대하여 미국과 일본이 적극적으로 표준화를 추진 중이므로, 이에 대응하여 한국 또한 국내 기술을 반영하여 적극적으로 표준화를 추진할 필요가 있다.

Ⅲ. 결 론

본 논문에서는 ITS 보안 기술 표준화가 활발히 진행 중인 ITU-T SG17의 표준화 현황에 대하여 살펴보았다. ITU-T SG17에서는 차량 소프트웨어 업데이트라는 특정 응용으로부터 접근을 취하는 표준안(X.itssec-1)과

포괄적인 접근을 취하는 표준안(X.itssec-2)에 대한 표준화가 진행 중이다.

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 SG16 draft Recommendation, H.VGP-ARCH, Architecture of Vehicle Gateway Platform.

[6] ITU-T SG17 draft Recommendation, X.itssec-1, Software update capability for ITS communications devices.

[7] ITU-T SG17 draft Recommendation, X.itssec-2, Security Guidelines for V2X communication Systemsoftware update capability for ITS communications devices.

〈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 사이버보안연구본부 선임연구원
2014년~현재 : ITU-T SG17 editor
<관심분야> 임베디드 보안, 차량통신보안, 융합보안

나 재 훈 (Jae Hoon Nah)
종신회원

1985년 2월 : 중앙대학교 컴퓨터공학과 졸업
1987년 2월 : 중앙대학교 컴퓨터공학과 석사
2005년 2월 : 한국외국어대학교 전자정보공학과 박사
1987년~현재 : 한국전자통신연구원 사이버보안연구본부 전문위원/책임연구원
2009년~현재 : ITU-T SG17 Q7 Rapporteur
2011년~2012년 : 한국정보보호학회 학회지 편집위원장
<관심분야> IPv6/MIPv6, P2P, IPTV, 웹메시업 보안