정 보 보 호 학 회 지
제29권 제1호, 2019. 2

자동차 보안 위협에 대한 표준 개발 동향 연구

김 창 오*

요 약

자율자동차의 시대가 현실로 다가오는 지금, 자동차의 보안 통제는 사람의 생명과 연결된 문제로 인식전환이 이루어져 가고 있다. 이러한 변화는 자동차 산업 기술에 대한 국제 사회의 공통된 관심사가 되었으며, 자동차 보안을 주제로 하는 국제 표준 개발로 이어지고 있다. 이에 본 연구에서는 보안 분야에 있어 대표적인 공적표준기구인 ITU-T SG17에서 진행되고 있는 자동차 보안 표준 연구에서 정의하고 있는 보안 위협에 대한 분석을 통해 자동차 보안의 현주소를 살펴보고, 안전한 자동차의 운행을 보장하기 위한 향후 연구 방향에 대해 제언하고자 한다.

Ⅰ. 서 론

5G 시대가 도래하고 자동차 산업의 성장에 따라 자율주행 자동차가 우리의 생활 환경 속으로 점점 가까이 다가오고 있다. 외부와의 연결 없이 독립적으로 운행하던 자동차는 자율주행이라는 목적을 달성하기 위해서는 더 많은 정보의 수집과 이를 처리하고 스스로 판단할 수 있는 능력이 요구되고 있다. V2X 통신을 기본으로 하는 커넥티드카(Connected Vehicle)는 정보 전달의 기회가 증가하는 만큼 보안 위협도 증가하게 되었다. 미래 자동차 산업은 글로벌 주요 성장 산업으로 국제 사회에서도 공통된 관심사를 가지고 있으며, 이러한 요구로 인해 UNECE WP29/TFCS를 비롯하여 많은 국제 협력기구와 표준단체에서 안전한 자동차 운행 환경을 보장하기 위한 기준을 마련하기 위한 연구를 진행하고 있다. 이에 본 연구에서는 대표적인 공적 국제 표준화 기구인 ITU-T에서 진행되고 있는 자동차 보안 위협 연구에 대한 진행 상황을 살펴보고 향후 연구 방향에 대해 제안하고자 한다.

Ⅱ. 자동차 보안 연구 동향

미국 자동차 공학회 SAE(Society of Automotive Engineers) International에서는 도로주행 자동차의 자율주행 시스템에 대한 규제 체계 및 안전 설계를 안내하는 모범사례를 담은 SAE J3016〔1〕의 발표를 통해 자동차의 운행 자동화 수준을 0~5레벨로, 미국도로교통 NHTSA(National Highway Traffic Safety Administration)[2]에서는 자동차 운행 형태를 0~4레벨로 정의하고 사용자의 안전 기준에 대해 가이드를 제공하고 있다. 자율주행 수준이 높을수록 보안 위협의 가능성이 커지게 되어 생명의 안전 또한 더욱 위협받게 된다. 이에 차량 통신에 대한 안전성을 확보하는 방안에 관한 연구와 함께 SAE에서는 사이버보안 가이드북(Cybersecurity Guidebook for Cyber-Physical Vehicle Systems)[3]을 2016년에 개발 시작하여 공개하였으며, NHTSA에서는 V2X 통신에 대한 가이드라인을 포함하는 Automated Vehicle 3.0[4]을 준비하고 있다.

자동차 산업에 있어 대표적인 표준 개발 단체인 ISO TC22 SC32에서는 자동차에 탑재되는 전기전자 시스템의 오류로 인한 사고 방지를 위해 자동차 기능 안전성(프로세스 모델과 함께 요구되는 활동, 유무형의 증거물, 그리고 개발과 생산에 사용되는 방식을 정의)을 위한 국제 표준으로 ISO26262[5]를 개발하였다.

Ⅲ. ITU-T에서의 자동차 보안 위협 개발

국제전기통신 연합의 하나로 통신 분야의 표준을 개발하는 ITU-T(International Telecommuni -cation Union Telecommunication Standardi -zation Sector)의 SG17(Study Group 17; 보안연구반)에서는 2017년 9월 총회에서 자동차 보안 워크숍을 열고 Q(Question)13의

* 카카오모빌리티 (ispiadviser@gmail.com)

ITS(Intelligent Transport System) 보안연구반을 신설함으로써 본격적으로 자동차 보안에 관한 연구를 시작하였다. ITU-T SG17에서의 자동차 보안에 대한 연구는 2014년 9월 차량 소프트웨어 업데이트 절차를 정의하는 X.itssec-1과 V2X통신 가이드라인을 정의하는 X.itssec-2에서부터 시작이 되었다. 특히, 차량 소프트웨어 안전 업데이트 절차인 X.itssec-1는 2017년 ITU-T SG17에서 자동차 관련 첫 번째 표준 문서인 X.1373로 승인된 이후 현재는 X.1373rev[6]개정이 진행되고 있다.

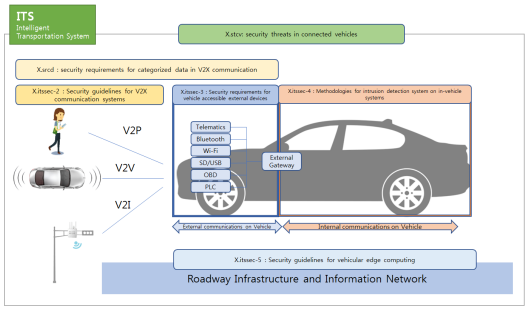
2019년 1월 총회를 마친 지금 자동차 보안연구반에서는 [표 1]에서 보는 바와 같이 X.1373의 개정을 포함한 11개의 표준이 연구 개발되고 있으며, 현재 연구 개발 중인 표준 중 8개의 표준(X.itssec-2[7], X.itssec-3[8], X.itssec-4[9], X.itssec-5[10], X.srcd[11], X.stcv[12], X.edrsec[13], X.eivnsec[14])에서 보안 위협에 대해 각각 정의하고 있다.

〔표 1〕 ITU-T SG17 Q13의 Work Programs

Work item	Subject / Title
X.1373rev (X.itssec-1)	차량 소프트웨어 안전 업데이트 절차 정의 표준으로, 업데이트 개요, 위협 분석, 기능 요구사항 및 업데이트 절차를 정의함
X.itssec-2	차량 V2X 통신을 위한 보안 가이드라인 정의 표준으로, V2X 통신에 대한 보안 위협을 식별하고 보안 요구사항을 정의함
X.itssec-3	외부장치를 통한 차량 내부 기능 접근 보안 요건 정의 표준으로, OBD-II 및 근거리 무선 보안 요구사항을 정의함
X.itssec-4	차량 내부네트워크에서의 위협을 탐지하는 기술 정의 표준으로, 차량 내부 네트워크 위협 및 특성을 정의하고 위협 탐지 기술에 대해 정의함
X.itssec-5	차량 엣지컴퓨팅 환경의 보안 요구사항 정의 표준으로, ITS의 엣지 영역에서 서비스를 제공하는 구조에 대해 정의하고 RSU를 안전한 엣지컴퓨팅 서버로 활용할 수 있는 가이드를 정의함
X.mdcv	차량의 통신 데이터의 빅데이터 기반 비정상행위 탐지 기술 정의 표준으로, 대용량 데이터 분석을 통한 보안 위협 식별 및 탐지 기술을 정의함
X.srcd	V2X 통신 데이터 보안 요구사항 정의 표준으로, V2X 통신에서 사용되는 데이터를 객체 속성, 차량 상태 등의 유형으로 분류하고 보안 요구사항을 정의함
X.stcv	차량에 대한 보안 위협을 정의하기 위한 표준으로, IT분야의 개발 중이거나 개발될 표준으로부터 참조 및 활용할 수 있도록 차량 중심의 보안위협을 식별하고 정의함
X.edrsec	클라우드 기반 차량용 EDR(사고 기록장치) 보안 요구사항 정의 표준으로, EDR 소개 및 관련 표준을 포함함
X.eivnsec	차량용 이더넷 보안가이드라인으로 차량 내부망에서의 차량용 이더넷 보안 우협 분석 및 식별, 유즈케이스를 정의하는 표준임
X.fstiscv	연결 차량의 위협 정보를 공유하기 위한 절차를 정의하기 위한 표준임

Ⅳ. 연구 표준별 위협 분석

이장에서는 [그림 1]에 표시된 ITU-T SG17 Q13에서 1년이상 연구 개발된 표준문서 중 위협에 대한 정의를 포함하는 6가지 표준에서 정의하고 있는 위협의 기준 및 정의에 대해 상세히 알아보고자 한다.



〔그림 1〕 보안 위협 정의 연구 표준 과제

4.1. 차량 V2X 통신을 위한 보안가이드라인

X.itssec-2로 불리는 안전한 차량 V2X 통신을 위한 보안가이드라인은 2014년 개발을 시작하여 2019년 개발을 완료하고 승인을 요청할 예정에 있는 표준이다. 본 표준 연구에서는 V2X 통신 환경에서 발생할 수 있는 22가지의 위협들에 대한 식별하고 각각의 위협들에 대한 설명과 위협의 성격 분류를 통해 [표 2]에서와 같이 7가지 속성으로 위협을 분류하고 있다.

〔표 2〕 X.itssec-2의 위협 식별 및 분류

Classification	Threats
Confidentiality	- Eavesdropping - Leakage of PII
Integrity	- Manipulation of routing/ sensor/credential information - Manipulated application on Nomadic device - Replay attack
Availability	- Jamming and DDoS on V2X communication - DDoS attack on OBU - Timing attack - Hacking of sensors
Non-repudiation	- Manipulation of certification database - Unauthorized access to credentials
Authenticity	- Routing table and LDM modification attack - Impersonation attack - Sybil attack - Pseudonym analysis attack
Accountability	- Unauthorized duplication of a nomadic device - Unauthorized duplication of a vehicle and RSU
Authorization	- Unauthorized access to safety-sensitive information/ certain functions

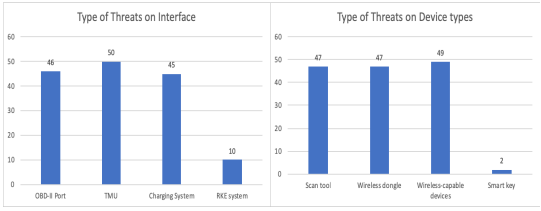
4.2. 차량 외부 접속장치를 위한 보안요구사항 권고

X.itssec-3로 불리는 차량 외부 접속장치들의 보안 위협과 이를 방지하기 위한 보안요구사항을 정의하는 표준으로 2017년 9월 개발이 승인되었으며 2020년 3월까지 개발을 완료하기 위해 연구를 진행하고 있다. 자동차의 내부시스템에 접근할 수 있는 외부장치 사용으로 인한 보안 위협에 대해 50가지의 공격방법에 따른 위협을 식별하고 식별된 위협을 23가지로 특성으로 분류하고 있으며, 외부 접근 접점별 위협과 장치 종류별 위협에 대해 정의하고 있다.

[그림 2]에서 보는 바와 같이 외부 접근 접점별 위협과 접근 장치별 보안 위협의 수로 보았을 때, TMU(Telematics Management Unit)는 가장 많은 위협의 종류에 노출되고 있으며, Wireless-capable device가 가장 많은 위협에 노출되는 장치임을 알 수 있다.

〔표 3〕 X.itssec-3의 위협 식별 및 분류

	High Level description of Threats
1	communication permits tampering with vehicle held code/dada
2	Attack on Integrity / Data Trust
3	Information Disclosure (Including eavesdropping)
4	Denial of Service
5	Elevation of privileges
6	Virus infection
7	Message Injection / tampering
8	Misuse of updates
9	Misconfiguration
10	Vehicle functions using connectivity
11	Hosted 3rd party software e.g. entertainment apps
12	External interfaces
13	Extract Data/Code
14	Manipulate Vehicle Data
15	Erase Data/Code
16	Introduce malware
17	Introduce new software or overwrite existing software
18	Manipulate Vehicle Parameters
19	Encryption
20	Early stage attack
21	Software and hardware development
22	Network design
23	Physical manipulation of systems to enable an attack



〔그림 2〕 외부 접근 접점별 위협과 접근 장치별 보안 위협

4.3. 차량 내부 침입탐지시스템 구현 권고

X.itssec-4로 불리는 차량 내부 위협을 탐지하는 침입탐지시스템 구현 방법에 대한 표준은 2017년 9월 개발을 승인이 되었으며, 2020년 3월까지 개발완료 예정

〔표 4〕 X.itssec-3의 위협 식별 및 분류

Impact on	Threats
Confidentiality	- Sniffing - Wire-Tapping
Integrity	- Impersonation Attack - Fuzzy Attack - Replay Attack
Availability	- DoS Attack - Frame-drop Attack

에 있다. X.itssec-4는 CAN과 같은 특수한 차량 내부의 통신 네트워크 환경에서 발생할 수 있는 보안 위협들에 대한 식별을 포함하고 있다. 식별된 보안 위협에 대해서는 영향을 미치는 속성에 따라 [표 4]와 같이 분류하고 있으며, 식별된 위협을 더 잘 탐지할 탐지 할 수 있는 기술적 방법을 포함하고 있다.

4.4. 차량 에지 컴퓨팅 이용 보안 가이드라인 권고

X.itssec-5로 불리는 차량 에지 컴퓨팅(VEC; Vehicular edge computing)을 위한 보안가이드라인에 대한 표준은 2017년 9월 개발을 승인받았으며, 2021년 9월까지 개발을 완료하고 표준에 대한 승인을 요청할 예정에 있다. X.itssec-5는 차량이 네트워크를 통해 원격의 RSU(Road Side Unit)의 자원을 이용하는 만큼 위협의 식별에 있어 X.itssec-2와 높은 연관성을 가지고 위협을 식별하고 있다.

〔표 5〕 X.itssec-5의 위협 식별 및 분류

Classification	Threats (on/of)
Confidentiality	- Privilege escalation - PII/Data Loss/Leakage - Service traffic hijacking
Integrity	- Traffic sign - Machine vision/perception sensors(camera/sensor) - Addressable channels in long-range wireless - Man-in-the-middle attack - Injection of Information
Availability	- Denial of Service(DoS)
Non-repudiation	- Rogue gateway - Rogue data center
Authenticity	- Insecure interface and API - Service manipulation
Accountability	- None
Authorization	- Browser Security / APT - Cloud malware injection attack

[표 5]에서는 24가지 종류의 보안 위협들에 대해 7가지의 속성으로 분류하고 있으며 있다. 11가지의 Integrity에 영향을 주는 위협과, 5가지의 Confidentiality에 영향을 주는 위협 정의는 차량 에지 컴퓨팅의 보안 위협이 주로 무결성와 기밀성에 영향을 주는 공격들이 주를 이루고 있음을 알 수 있다. 현재까지는 X.itssec-5에서의 위협 분류는 진행 중인 상태로 아직 개발 기간이 2년가량 남아 있는 만큼 좀 더 상세한 위협 정의가 될 것으로 예상 된다.

4.5. V2X 통신 데이터 보안 요구사항 정의 권고

X.srcd로 불리우는 V2X 통신 데이터 보안요구사항을 정의하기 위한 본 권고는 2018년 3월 개발이 승인되었으며 2020년 12월까지 개발을 완료할 계획에 있는 표준이다. 본 표준에서는 데이터의 객체 속성과 차량 상태, 환경, 응용프로그램 서비스, 차량 통제, 기밀 그리고 3단계 보안 레벨로 분류된 데이터 타입들에 대해 정의하고 있다.

[표 6]은 데이터의 라이프사이클을 기준으로 위협을 분류 한 것으로, 전반부에서는 접근 권한 제어에 대한 위협이 존재하며, 중반부에서는 데이터에 대한 유실 위협 그리고 후반부에서는 시스템의 취약점에 의한 위협

〔표 6〕 X.srcd의 위협 식별 및 분류

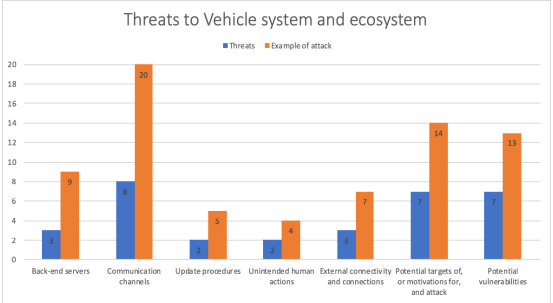
Threats	Data lifecycle
Authorization	(1) Data collection (3) Data transmission
spoofing	(1) Data collection (6) Data destruction
Eavesdropping	(3) Data transmission (4) Data usage
Denial of service	(3) Data Transmission (5) Data migration
Data misuse	(4) Data usage (5) Data migration
System Vulnerabilities	(4) Data usage (5) Data migration (6) Data destruction (7) Data backup and recovery
Data loss and leakage	(2) Data storage (3) Data transmission

이 존재함을 정의하고 있다. 또한, 본 권고에서는 V2X 통신데이터를 3가지 레벨(General, Important, Critical or Sensitive)로 분류하고 important와 Critical or Sensitive 데이터에 대해서는 강화된 보안을 적용하도록 정의하고 있다.

4.6. 차량 보안 위협 정의 권고

X.stcv로 불리는 차량 보안 위협 정의 권고는 2018년 3월 개발이 승인되어 2019년 9월까지 개발을 완료할 계획에 있는 표준이다. 본 표준은 보안 위협에 대한 기준을 마련함으로써, ITU-T SG17을 포함한 여러 기관과 단체에서 자동차에 대한 보안 요구사항을 정의하고 개발을 진행할 때 참조 모델로 사용할 수 있도록 개발 되고 있다. V2X통신을 포함한 차량의 내부와 외부의 통신 환경에서 발생하는 보안위협 및 차량을 중심으로 발생할 수 있는 위협들에 대해 종합적으로 정의하고 있다.

[그림 3]에서는 자동차 환경에서의 위협 대상을 7가지로 분류하고, 각 분류별로 위협의 예의 수를 나타내고 있다. 통신 채널의 경우는 20가지의 위협의 예와 함께 8가지 종류의 위협으로 분류됨으로써 가장 많은 위협이 존재하는 것으로 정의하고 있고, 업데이트 절차와 사용자 행동과 관련해서는 각각 2가지의 종류의 위협으로 정의함으로써 상대적으로 위협 노출이 높지 않은 것을 알 수 있다. 그러나 잠재적인 공격 목표와 취약점에 대해서는 각각 14가지, 13가지 종류의 위협 예가 정의될 만큼 높은 수위의 위협에 노출되고 있음으로 정의하고 있다.



〔그림 3〕 X.stcv의 자동차 보안 위협 분류와 예

Ⅴ. 결 론

자율자동차의 시대를 준비하는 지금 독립적으로 움직이던 자동차는 더 많은 정보를 수집하기 위해 외부와의 연결이 일반화되고 확장되고 있다. 자동차와의 통신 환경에 대한 보안을 다루는 X.itssec-2에서는 22가지, 차량 외부 접속장치 부분의 보안 요구사항을 다루는 X.itssec-3에서는 50가지, 차량 내부의 위협에 대한 탐지 기술을 다루는 X.itssec-4에서는 7가지, 자동차 엣지 컴퓨팅 보안을 다루는 X.itssec-5에서는 25가지, V2X 통신 데이터 보안 요구사항을 다루는 X.srcd에서는 24가지 그리고 차량 보안 위협 정의 권고인 X.stcv에서는 72가지의 보안 위협에 대해 정의하고 있다.

2019년 1월 현재 연구 개발이 진행 중인 자동차 보안 표준 문서에 포함된 보안 위협에 대한 분석을 통해, 기존 IT 환경과 동일하거나 유사한 형태의 보안위협도 존재하지만 자동차만이 가지는 특수한 환경에서 발생할 수 있는 보안 위협에 대해서도 확인할 수가 있었다. 그러나, 이번 연구에서는 표준 개발의 초기 단계에 있는 클라우드 기반 차량용 EDR(사고 기록장치) 보안 요구사항을 정의하는 X.edrsec과 차량용 이더넷 보안가이드라인 권고인 X.eivnsec에 대해서는 포함하지 않았다. 따라서 향후 1~2년 동안 진행될 자동차 보안 표준 연구에서는 더욱 완성된 모습의 자동차 위협 지도가 만들어질 수 있을 것으로 예상한다. 이러한 자동차 보안 위협 지도의 제작을 통한 보안 위협의 식별은 향후 안전한 자동차의 운행 환경을 보장할 수 있는 보안 요구사항을 도출하기 위한 기반 자료가 될 것이며, 더 나아나가 자율자동차의 안전 프레임워크를 구현하는 기준 자료로 활용될 수 있을 것이다.

참 고 문 헌

[1] https://www.sae.org/standards/content/j3016_201806/
[2] https://www.nhtsa.gov/vehicle-manufacturers/automated-driving-systems
[3] https://www.sae.org/standards/content/j3061_201601/
[4] https://www.nhtsa.gov/vehicle-manufacturers/automated-driving-systems#automated-driving-syste

ms-av-30
[5] https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:ed-2:v1:en
[6] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14820
[7] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=13549
[8] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14394
[9] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14395
[10] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14396
[11] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14588
[12] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14587
[13] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14818
[14] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14819

〈저자소개〉

김 창 오 (ChangOh Kim)
정회원

1999년 2월 : 동의대학교 전산통계학 이학사
2001년 2월 : 동의대학교 대학원 전산통계학과 이학석사
2013년 2월 : 고려대학교 정보보호대학원 정보보호학과 박사수료
2019년 1월~현재 : 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증심사원
2018년 4월~현재 : ㈜카카오모빌리티 정보보안팀
2015년 1월~현재 : ITU-T SG17 전문위원/에디터
2015년 4월~현재 : ICT 국제표준전문가
2017년 7월~현재 : ITU-T FG-DLT/DFC 전문위원
2017년 8월~현재 : ISO/TC 307 전문위원
관심분야 : 정보보호관리체계, 개인정보보호, 스팸보안, 자동차보안, 분산원장기술보안