정 보 보 호 학 회 지
제24권 제2호, 2014. 4

escar 회의 등을 통한 각국의 자동차 보안 기술 연구 동향

김 광 조*, 이 동 수**

요 약

본 고는 최근 10년간 유럽과 미국에서 개최된 바가 있는 자동차 보안 기술에 관한 국제 학술 대회인 escar (Embedded Security in Cars)에서 발표된 논문을 분석하여 그동안의 기술 추이를 조사한 결과, 본 회의의 참가자 수가 매년 점차 증가하고 있어 국제적으로 자동차 사이버 보안에 대한 관심도가 증가하는 것을 알 수 있었다. 또한, 국내 자동차 보안 기술의 경쟁력 향상을 위하여 최근 2-3년간 미국, 유럽, 일본에서 ICT 기술을 접목한 스마트 자동차의 보안 기술에 관하여 정부 및 민간 차원에서 최신 프로젝트 추진 상황을 조사한다.

Ⅰ. 서 론

본 논문은 저자 등이 일본 큐슈 지역의 남부에 있는 가고시마현에서 2014년 1월 21일에서 1월 24일에 일본의 전자정보통신학회인 IEICE가 주관하여 개최한 제31회 SCIS2014 (Symposium on Cryptography and Information Securty)[1] 에 [그림 1]과 같이 논문 발표차 참석하여,

〔그림 1〕 저자 등의 SCIS2014 참가 사진

자동차 보안에 관한 국제 학술 대회인 escar (Embedded Security in Cars)[2]에 과거 10년간 발표한 내용을 분석한 발표 논문[3]를 참조하여 최근의 자동차 보안 기술에 관한 국제적인 연구 동향에 대하여 조사 분석하고, 일본 IPA(정보처리 추진기구)에서 발표한 "2012년 자동차 보안 기술 동향 보고서"[4] 를 참고하여 미국, 유럽, 일본의 최신의 자동차 보안 연구 동향을 분석하여 제시하고자 한다.

본 논문의 구성은 다음과 같다. 제 2 장에서는 최근 자동차 생산의 경쟁력 향상과 안전 주행의 편리성 향상을 위하여 ICT 기술 도입 동향과 부수되는 자동차 위협 요소 및 사례를 기술하고, 제 3 장에서는 지난 10년간 escar에서 발표현황 및 주요 세션동향을 소개하고 제 4 장에서는 자동차 선진국인 미국, 유럽, 일본의 자동차 보안 관련 최근 프로젝트와 연구 동향을 요약하고 제 5 장에서는 요약 및 국내 자동차 보안 기술 향상을 위한 제언으로 끝을 맺는다.

Ⅱ. 자동차와 ICT 기술의 도입과 위협

2.1. 차량차별화를 위한 ICT 기술의 경쟁적인 도입

종래의 기계적인 메커니즘에만 의지한 자동차 제조 기술은 현재는 치열한 경쟁을 하는 각 자동차 제조자들 간의 능력이 모두 향상되어 기술 격차는 거의 없어지고 있다고 하며, 운전자의 주행 편리성과 자동차의 운행 안전성 및 고급화를 위하여 이미 널리 사용하고 있

* 한국과학기술원 전산학과 (kkj@kaist.ac.kr)
** 한국과학기술원 전산학과 (letrhee@kaist.ac.kr)

는 각종 ICT 기술과 접목하여 connected car 또는 smart car을 생산 보급에 박차를 가하고 있다

“최신의 자동차는 145개 이상의 actuator, 4,000개 이상의 신호 정보, 75개 이상의 각종 센서 (레이더, 수중 음파 탐지기, 카메라, 가속도계, 온도계, 강우 센서 등)가 작동되며 이들은 시간당 25GB 이상의 데이터를 생성하며, 이 데이터는 70개 이상의 OBC (On-board Computer)에 의해 분석 된다.”고 보고하고 있다[5].

또한, 차량 내외부의 통신을 위하여 기존의 IT 분야에 널리 보급된 유무선 통신 시스템인 Bluetooth, Wi-Fi, RFID, DRSC(Dedicated Short Range Communications), NFC (Near Field Communications), GSM(Global System for Mobile Communications), CDMA(Code Division Multiple Access), UMTS(Universal Mobile Telecommunication System) 등이 적용되고 있다.

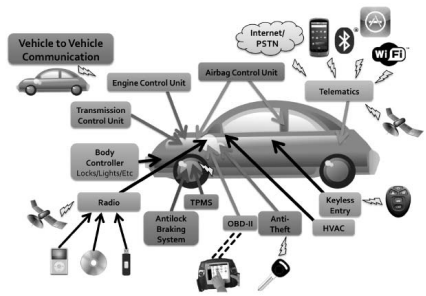
또한 이와 더불어 원격 스마트 키, 텔레메트리 송수신을 포함하여 다수의 기능을 지원하는 장치가 사용되고 있다. 현재의 자동차 기술은 차량 1대 단독으로 동작하는 제어 구조로부터, 다른 자동차도 포함한 다양한 노드에서 공개된 시스템에 의한 자동 제어 구조로 변화하고 있다.

2.2. ICT 기술 도입에 따른 새로운 위협

위와 같이 ICT 기술과 접목을 통하여 운전자에게 운행의 편의성, 자동차의 안전성 등에 크게 개선을 하였으나, 한편으로는 이를 악용하여 안전하지 못한 암호 시스템의 공격, 무선 접속 신호의 정보 변경 등 새로운 공격이 가능하게 된다.

[그림 2]에서 보듯이 최신의 자동차는 새로운 ICT 기술의 접목에 따른 위협 요소는 공존하고 있으며 이에 대한 대비를 자동차 초기 생산 단계에서부터 철저히 고려하여야 한다.

지금까지 알려진 자동차 보안 위협의 성공 사례를 몇 가지 소개한다. 차량 도난을 방지하기 위하여 차량 개폐 장치 또는 엔진 시동을 근거리 무선통신으로 제어할 수 있는 무선 스마트 키는 내부에 안전한 일방향 인증 프로토콜을 위한 KeeLoq[7]라는 비선형 쉬프트 레지스터를 이용한 블록 암호 알고리즘을 이용하고 있으나 재생 공격이나 부채널 공격 등으로 암호해독[8,9]이 쉽게 되



〔그림 2〕 자동차의 보안 위협 요소〔6〕

어 스마트키가 무용지물이 된 사례도 있다.

또한, 자동차의 자체 무선 접속으로는 타이어 공기압 감시 장치 (Tire Pressure Monitoring System, TPMS)가 미국에서는 전 차종에는 의무적으로 사용하도록 되어 있으나, 이 무선 신호를 도청하여 계기판에 표시되는 공기압 신호 정보를 바꾸어 차량 운전자를 혼란시키게 하는 사례도 있다.[10]

이와 같이 차량의 기본적이 주행 정보와 관련하여 제어 기능을 방해하거나 허위 정보를 삽입을 하는 경우 이외에

- 자동차 엔진 이나 구동 기능에 위협
- 에어백에 오동작 유발
- 도난 방지 장치에 대한 무력화
- 냉난방 및 공조 장치(HVAC)에 대한 공격
- 차량 출입 제어 장치 및 시스템에 대한 공격
- V2X 보안 및 인증 기술에 대한 취약점 공격
- CD, DVD, i-Pod 등의 IVI (In-Vehicle Infotainment)에 대한 개인정보 무단 유출

등과 같은 새로운 위협과 방어 기능이 요구된다.

이러한 위협과 공격 방식을 크게 분류하면[11] 물리적인 공격, 시스템 공격, 간접 공격, 부분 기능 공격이 있으며 공격 대상으로는 주행 계통, 제어 계통, 오락 계통, 암호 알고리즘, 인증 프로토콜, S/W 변조 등이 있을 수 있다.

특히, 자동차 보안에 사용되는 각종 보안 기술은 산업 보안 기술에서 필요한 가용성과 안전성을 우선하고 검정된 기술을 사용하여야 하는 특수한 조건이 있다. 즉, 자동차가 제공하는 고유의 안전성, 오락성에 저해되지 아니한 범위에서 새로운 취약점이 발생하면, 각종 S/W에 대한 보안 패칭이 아니 되더라도 장기적인 방어

기술이 적용되어야 하며, 공격자가 자동차에 물리적인 접근이 용이하여 자동차 제어 S/W에 대한 역공학 등이 이루어 진다하여도 보안 대비책을 강구하여야 하며 생산자, 각종 부품 납품자, 운전자, 정비자간 공급망(Supply Chain) 상과 유기적인 보수 측면에서의 보안 기술도 염두에 두어야 하는 특수성이 있다.

Ⅲ. 최근 10년간 escar 논문 내용 분석

이에 유럽 암호학자들은 자동차 보안 기술을 공개적으로 토론하는 학술적인 모임으로 escar[2]라는 국제 학술대회를 2003년에 최초로 escar 2003(처음에는 유럽에서만 개최하여 escar Europe2003으로 명명하지는 아니하였음.)을 개최하였으며, 그 이후 매년 개최하여 2013년 escar Europe을 11번째로 개최하여 왔다.

자동차 보안에 대한 최근 기술을 토의하기 위하여 escar Europe 2013에 공지된 논문 모집 분야를 보면 다음과 같다.

- 보안 공학, 형식 검증, 개발 및 검증 도구
- 보안 표준 및 자동차 보안 경제학
- 자동차 영업, 정비, 서비스에서 보안 기술
- 자동차 개인정보 도난 방지
- 자동차 H/W 보안 모듈
- 자동차 부품 보호 기술
- 자동차 주행 기록 또는 블랙박스 보안 기술
- 자동차 과금, 통제구역 접근 및 자동차 감시
- 자동차 도난 방지 및 대응 기술
- 자동차 권한 제어 및 감사
- 미래 자동차 응용 보안 기술
  (예, ITS, 전기차)
- 도로 및 항공 교통수간을 위한 보안 기술

지금까지 escar는 독일 전역의 주요 도시에서 개최되었으나, 2013년에 처음으로 미국 디트로이트에서 escar USA2013이 개최되었다. [표1]는 현재까지 escar Europe에서 발표한 세션 이름과 발표 논문수를 정리하였다.

〔표 1〕 현재까지 escar에 발표된 세션과 발표 논문 수

escar2013 Europe	
Automotive Security Threats	3
Automotive Security Solutions	4
Secure On-board Communication	3
Car-to-Car Communication Security	2
Automotive Standardization	3
escar2013 USA	
On-board Security	6
Telematic Security	8
escar2012 Europe	
Trends and current developments	4
Secure on-board Communication	3
Anti-theft protection	2
Cryptography in the embedded domain	4
escar2011 Europe	
Automotive Security Protocols	9
Security in V2X	3
Automotive Hardware Security II	2
escar2010 Europe	
Copy Protection	3
Future Topics in Automotive Security	3
Communication Security	3
Hardware Security	3
Dependability, Trust, Privacy	3
escar2009 Europe	
Automotive Security Standards	2
On-Board Security	2
Authentication	1
Security Analysis and Security Architecture	4
Privacy and VANETs	2
New Directions in Hardware Security	4
escar2008 Europe	
Privacy	2
Trusted Hardware and OS Security	2
Inter and Intra-Vehicle Communication Security	2
Location and Telematic	2
Hardware and Security	2
Theft Control	2
Standards and Architectures	2
escar2007 Europe	
On-board Security	2
Telematic Security	9
escar2006 Europe	
Vehicular Communications I	2
Secure Software Architectures	2
Secure Positioning	1
Securing Vehicular Communications II	3
escar2005 Europe	
Trusted Computing in Automotive Applications	3
Car Communication Networks	6
Hardware Security and Attacks	2

System Issues	3
Privacy	1
escar2004 Europe	
Software in Automobile	5
Security in Software Applications	2
V-to-V Communication	2
In-Car Communication	2
Development in Telematic Area	2
escar2003 Europe	
IT-Security in Automobile	4
Telematic Technologies and Applications	3
IT-Security in Automobile Applications	4
Perspective in Telematic and Automobile Data Protection	2

그리고 [표 2]에는 지금까지 독일에서 개최된 escar Europe의 개최 도시를 요약하였다.

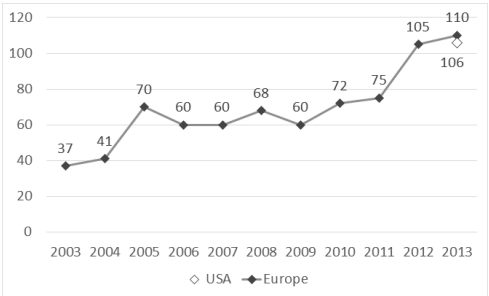
〔표 2〕 escar Europe의 독일 개최 도시

escar Europe	년도	개최 도시
제 1 회	2003	Cologne
제 2 회	2004	Bochum
제 3 회	2005	Cologne
제 4 회	2006	Berlin
제 5 회	2007	Munich
제 6 회	2008	Hamburg
제 7 회	2009	Düsseldorf
제 8 회	2010	Bremen
제 9 회	2011	Dresden
제 10 회	2012	Berlin
제 11 회	2013	Frankfurt

[그림 3]에는 escar에 참가자 수를 표시하였다. 최초 2003년 제1회 escar 에는 40명 내외였으나, 최근 3 회 (escar USA를 포함)는 110 명 내외 로 3 배 가까이 증가하였다. 이것은 자동차 보안에 대한 세계적인 관심이 높아지고 있음을 나타내는 것이다.

지금까지 escar에 발표한 각각의 세션을 크게 분류하면 On-board 보안 기술과 텔레마틱 보안 기술로 나눌 수 있으며 이 주제는 지난 10년간 지속적으로 다루고 있다.

또한, 자동차 보안 프로토콜, 복제 방지 기술, 보안 기술 표준, 보안 S/W, 개인 정보보호 및 인증 등의 문제는 자동차 네트워크의 확장됨에 따라 새롭게 대두하게 되었으며, escar의 명칭인 Embedded Security in Car의 의미대로 처음에는 자동차에 적용되는 제한적인 보안 기술 분야로 한정하였으나, 최근에는 자동차와



〔그림 3〕 escar 참가자 수

ICT 기술의 접목에 따른 자동차에 관한 종합적인 사이버 보안에 관한 국제회의로 성격으로 확장되어 가고 있다.

Ⅳ. 선진국의 자동차 보안 관련 최근 동향

4.1. 미국의 자동차 보안 연구 동향

여기서는 최근 활동이 증가하고 있는 미국의 연방 정부와 각 단체에서 추진하고 있는 자동차 보안 기술에 대한 연구 동향에 대하여 기술한다.

4.1.1 SAE의 자동차 보안 활동

SAE (Society of Automotive Engineers)는 2011년 2월부터 자동차의 보안 관련 그룹을 결성하여, 2012년 11월 현재 “SAE Motor Vehicle Council, Electrical Systems Group (TEVEES18)” 이라는 위원회 명으로 활동하고 있다. 여기에 escar Europe 2012에서 GM (General Motors)이 발표한 SAE 활동에 대한 내용을 소개한다.

TEVEES18에는 자동차의 전장 시스템을 대상으로 시스템 침해를 조기 발견 및 처리하고, 피해를 받았다 하더라도 최소화 방법을 검토하고 있다. 본 위원회에서는 자동차 보안 및 항공기 보안 전문가를 초청하여 발표회를 실시하는 등 각종 정보를 공유하고 있다. 또한 위원회는 자동차, 도로 및 교통 관련 정보 공유 분석 센터 (ISAC : Information Sharing and Analysis Center)[12] 와 공조도 하고 있다. 이 위원회에서는 두 개의 하위 위원회를 설립하였는데, 하나는 자동차의 보안지침 및 위험평가 작업반(TEVEES18A)이고 다른 하나는 자동차 전자제품의 보안작업반 (TEVEES18B)이다.

〔그림 4〕 SAFETY PILOT에서 제공하는 정보 예시

4.1.1.1 SAE의 TEVEES18A - 보안 평가 방법

TEVEES18A는 자동차 시스템에 대한 보안 위험의 평가 기법을 위하여 EVITA 위험 평가 방법[13], NIST (National Institute of Standards and Technology) SP 800-53[14], Microsoft STRIDE 위협 모델 기법 [15]을 검토 대상으로 하고 있다. 최종적으로는 위협 요소를 바탕으로 위협 평가 수법과 보안 요구 사항에 관한 지침을 제정할 예정이다.

4.1.1.2 SAE의 TEVEES18B - ECU 보안

TEVEES18B에서는 특히 보안 상 대단히 중요한 ECU의 하드웨어 보안에 관한 대응 방법을 검토하고 있다. 후보로는 HIS의 SHE, EVITA의 HSM, TCG (Trusted Computing Group)의 TPM (Trusted Platform Module)을 검토되고 있다.

4.1.1.3 SAE 보안 관련 활동 배경

미국에서는 자동차의 보안이 필요하다고 하는 배경으로는 미국 의회에 의해 제정된 법규로 MAP-21 (Moving Ahead for Progress in the 21st Century Act)에 근거를 두고 있다. MAP-21는 NHTSA (National Highway Traffic Safety Administration)에 대해 2014년까지 전자적인 안전 표준의 검토가 요청되고[16], 이것이 사실상 자동차의 정보 보안을 필수로 하고 있다. SAE는 미국 운수부 (USDOT)와 운수부 산하 연구 기관인 RITA(The Research and Innovative Technology Administration)[17], RITA의 한 부분인 Volpe Center[18]도 협력기관으로 참여하고 있으며 매년 1 월에는 미국 자동차 업계와 미국 정부의 정보 교환 회의[19]을 개최 하고 있다. 미국 SAE 와 일본의 JSAE 사이의 활동에 대해 전반적으로 정보 교환을 활발히 실시하고 있다고 한다.

4.1.2 미국 운수부의 Safety Pilot(SAFETY PILOT)

SAFETY PILOT[20]은 미국 운수부가 수행하는 차량간 통신에 관한 현장 운용 시험을 의미한다. 미국 운수부 산하 연구 기관인 RITA[21] 의 연구 프로젝트 중 하나로, 미시간 대학 교통 연구소 (The University of Michigan Transportation Research Institute, Human Factors Division)가 본 프로젝트를 수행하고 있다. 수행 기간은 2011년 8월부터 2014년 2월까지이다. SAFETY PILOT에서는 [그림 4]와 같이 도로와 자동차 간의 통신을 이용하여 운전자에게 주변의 경고 상황이나 교통 표지판 정보를 제공하여 안전 운전의 효과를 검증한다. 현장 운용 시험에 사용되는 자동차, 트럭, 버스는 총 2,800대 이상[22], 자동차 기계 및 계측기는 총 20종을 사용하여 각 제조사와 복수 기종 간의 상호 운용성을 시험하고 있다.[23]

SAFETY PILOT는 보안 및 개인 정보에 대해서도 평가 대상이다. RITA에 따르면 ITS 산업 규격으로 보안을 위한 V2I (Vehicle to Infrastructure, 도로와 자동차 간 통신)는 양방향 통신을 사용하지만, V2V(Vehicle

to Vehicle, 차량 간 통신)에는 단방향 통신 만 사용한다[24]. 또한, 미국 SAE 2012년 발표 자료[25] 등에 따르면 SAFETY PILOT에서는 IEEE1609.2[26]로 표준화된 전자 인증서 기술을 이용하며 CAMP VSC3 의한 전자 인증서 유효성 검사 횟수를 최소화하는 “Verify-On-Demand” 등의 기술[27]을 사용하고 있다고 한다.

4.1.3 CyberAuto Challenge

2012년 8월, 메릴랜드 주에 있는 미 육군 시험장에서 고등학생 및 대학생이 참가하여 자동차에 대한 사이버 공격을 실험하는 워크샵 “CyberAuto Challenge”가 개최되었다[28]. 주최자는 기술 혁신을 지원하는 비영리 단체 Battelle[29]이다. 회의장에서는 주요 지도자로서 미국 국방부, 미국 운수부 담당자 외에도 자동차 3사에서 기술자가 참가했다. 이 이벤트는 앞으로도 계속될 예정이며, 자동차 보안에 대한 전문 인재 육성의 장으로 될 것으로 예측한다.

4.1.4 TCG의 활동

TCG (Trusted Computing Group)[30]는 신뢰할 수 있는 플랫폼 인프라를 구축하기 위하여 하드웨어 및 소프트웨어 업계 표준 규격을 개발하고 보급 활동을 실시하고 있는 국제적인 단체이다. 정보 통신 기기에 소프트웨어나 데이터의 검증 및 인증 기능을 제공하는 TPM(Trusted Platform Module) 규격이 있다. 2012년 3월에는 도요타 자동차가 TCG에 신규 가입하였고 TCG에서 자동차를 포함하여 삽입하는 장비들에 대한 기술 검증을 담당하는 “EmSys WG (Embedded Systems Work Group)”에서 자동차용으로 활용되는 사례집 등을 배포하고 있다.

2012 년 11월 도쿄에서 열린 TCG 일본 지부 주최 제 4 회 TCG 공개 워크샵[31] 에서는 TCG 이사 회사와 EmSysWG의 공동 의장이기도 한 후지쯔에서 자동차 용 TPM의 가능성 등에 대해 강연이 있었다. 이 워크샵은 TPM의 가능성에 대해 “ARM이 Android 장치에서 이용되고 있으므로, 스마트 폰 등에서의 활용이 기대된다”와 “자동차 기기의 소프트웨어 업데이트 (원격 유지 보수) 에서 업데이트 할 소프트웨어 식별 및 코드 검증 및 일련의 작업 로그 기록 저장 및 기록 기능에 TPM을 활용할 수 있다” 로 보고되고 있다. 이러한 기능을 이용한 운용을 자동차에 널리 보급하기 위해 정부 기관 등의 지침 정비도 필요하다고 TCG는 지적하고 있으며, 동시에 TPM이 세계 표준의 하나 인 ISO(International Organization for Standardization) 표준화로 제정이 된다면 그 파급효과는 대단히 클 것으로 전망하고 있다. TPM은 반드시 하드웨어 칩으로 구현 되어야 하는 것이 아니라, 소프트웨어로 안전한 실행 환경에서 실현, 측정 및 검증 기능을 제공 할 수 있고, 가상으로도 실현 될 수 있으므로 다양한 적용 가능성이 있다.

4.2. 유럽의 자동차 보안 연구 동향

본 절에서는 유럽의 자동차 보안 연구 동향을 정리한다.

4.2.1 EVITA 프로젝트 HSM 평가 시험 결과

유럽 EVITA (E-safety Vehicle Intrusion proTeceted Applications) 프로젝트 (이하 “EVITA”로 표기)는 FPGA (Field Programmable Gate Array)로 구현한 HSM (Hardware Security Module)의 평가 시험 결과를 정리하여 2011년 11월에 보고회를 개최하고 그 활동을 종료하였다. 그 후 2012년에 EVITA가 개발 한 HSM 평가 시험 보고가 공개되어 그 일부를 소개한다.

4.2.1.1 HSM과 저수준 드라이버 퍼지 시험

EVITA가 공개 한 “D4.4.2 Test Results”[32]에서는 FPGA로 개발한 HSM에 대한 시험 결과를 정리하였으며, 이 가운데 HSM에 퍼지 시험 (문제가 발생할 가능성 있는 데이터를 대량으로 보내, 응답 및 동작을 감시하여 알려지지 않은 취약점을 검출하는 검사 방법)을 시행한 결과가 있다. EVITA는 FPGA에서 구현한 하드웨어와 이를 이용하기 위한 드라이버 소프트웨어를 동시에 개발하였고, 평가 시험에서는 하드웨어와 드라이버 모두에 대해 퍼지 시험을 실시하였다.

EVITA의 퍼지 시험에서는 하드웨어인 HSM 과 저수준 드라이버의 취약점 테스트를 위해 별도의 퍼징 엔진을 개발하였다. HSM에 대해서는 동일한 FPGA에 탑재 된 PowerPC를 임베디드 Linux (ELDK : Embedded

Linux Development Kit[33])로 구동하여 퍼지를 수행하였다. 저수준 드라이버에 대해서는 Infineon의 멀티코어 형 자동차 마이크로 컴퓨터인 TriCore TC1797/MCAL 을 이용하여 퍼징 데이터를 주입하였다. 마이크로 컴퓨터에 마이크로 컴퓨터로 퍼지하는 방법은 일반적인 소프트웨어 기술에 비하여 대단히 독특한 것이다.

4.2.1.2 EMVY RPC 세션 인증 대책

EVITA 보안 사양을 이용할 때는, BMW 사의 자동차 시스템 개발 프레임 워크인 “EMVY” 를 이용한다. EMVY에서는 RPC (Remote Procedure Call)와 같은 클라이언트 와 서버 간 통신을 이용하고 있지만, EMVY의 RPC가 서비스를 호출하는 클라이언트 세션을 위장하는 취약점이 있다고 한다. 따라서 EVITA는 인증 티켓을 이용하여 세션을 보호하는 기능을 추가하고 있다.

4.2.1.3 시스템 레벨 검증 - 성능 평가

EVITA에서는 시스템 레벨 검증으로 MATLAB Simulink 를 사용하여 CAN 버스의 성능 평가를 실시하고 있다. MATLAB Simulink는 모델링 된 구성 요소를 GUI (Graphical User Interface)에 결합함으로써 시뮬레이션에 의한 평가 및 시험을 쉽게 실시할 수 있는 도구이다[34]. 내부적으로는 하드웨어로 동작하는 CAN 버스 상에서 통신을 하므로 실제 상황과 거의 유사한 평가가 가능하다고 한다.

4.2.1.4 동적 시험 - 침입 탐지

침입 탐지는 알려지지 않은 취약점에 대한 공격을 방어하는 방법의 하나로서 특히 제어계의 침입 경로가 되는 기능을 일시 정지시키는 고장 에 대한 대비책을 위하여 대단히 중요하다. EVITA는 침입 탐지를 위해 여러 EVITA 대응 ECU (Electronic Control Unit)에서 작동 하는 EMVY 클라이언트에서 로그를 수집하고 감시하는 소프트웨어 워치독 (SWD: Software Watchdog)을 개발하였다. SWD는 수집 한 로그 정보에서 비정상적인 이벤트와 동작을 검출하고, 특정 통신이나 기능을 정지 등의 보호 조치를 수행한다. EVITA는 실증 실험으로 프로브 및 필터를 이용하여 매 초당 이벤트의 수집 시험을 수행하였으며. 또한 실증 구현은 UNIX OS에 구현 되어 있으나, HSM과 연동되어 있지 아니하다.

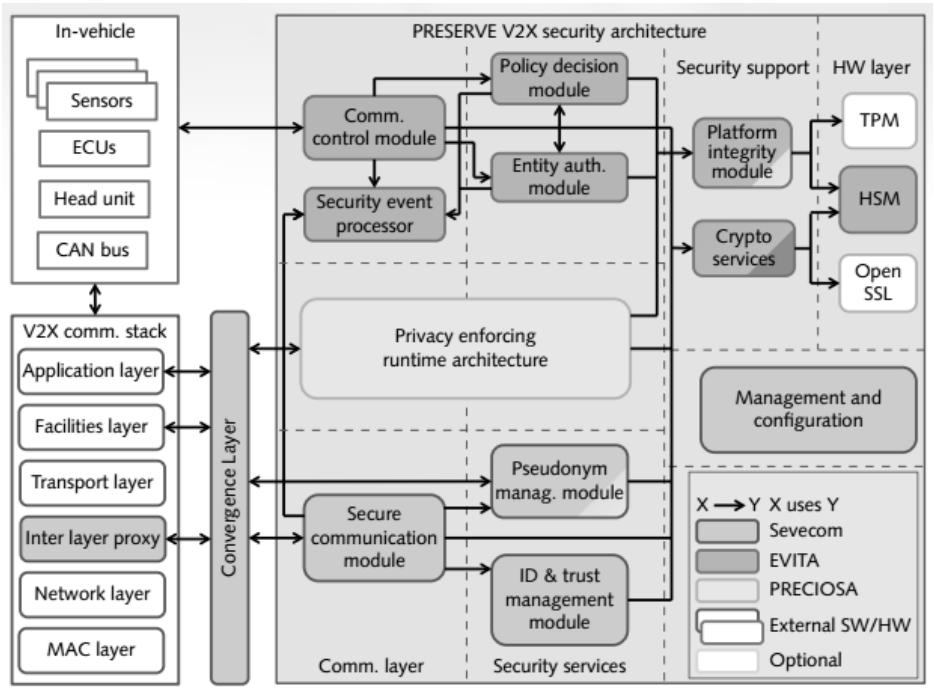
4.2.1.5 EVITA 의 성과와 향후 과제

EVITA는 자동차 LAN 보안 규격인 API (Application Programming Interface)를 제정하고 FPGA에 구현하였으며, EMVY 프레임워크에 의한 시험 환경을 개발하였다. 그 결과, 보호된 메시지 교환 기능 및 성능에 대한 양호한 시험 결과를 얻었다. 상용 제품으로 사용할 수 있는 수준이 아니라, 어디까지나 연구 목적의 성과라고 할 수 있다. 향후에는 특정 통신 버스를 위한 제품화를 위한 공개 시험과 기존 부품과 통신할 때 취약점을 검증할 필요가 있다. 또한, EVITA는 보안 부팅에 필수 기능이 필요하다고 하지만, EVITA 프로젝트에서는 이 시험을 실시하고 있지 아니하여 이것도 향후의 과제로 남아 있다.

4.2.2 PRESERVE 프로젝트의 동향

EVITA에서 개발한 HSM을 ASIC(Application Specific Integrated Circuit)으로 구현하여 저가로 대량 생산하고, PKI (Public Key Infrastructure: 공개 키 기반 구조)와 연계한 실증 시험을 실시하는 것이 PRESERVE 프로젝트 (이하 PRESERVE로 표기)이다.

PRESERVE의 총 예산은 544만 유로, 그 중 385만 유로가 유럽의 연구 개발 예산인 FP7[35]에 의하여 조성되었다. 활동 일정으로는 2011년 1월부터 2014년 12월까지로 실제 작업을 담당하는 프로젝트 팀은 Twente 대학(네델란드), escrypt(독일), 프라운호퍼 연구소(독일), KTH 스톡홀름(스웨덴), 르노 (프랑스), Trialog(프랑스)이다. 자문 기관인 자문위원회에는 아우디(독일), BMW(독일), 다임러(독일), 덴소(일본), 인피니언(독일), 폭스바겐(독일)과 독일의 주요 자동차 제조사가 참가하고 있다. 미국에서도 지원 회원으로 차량간 통신을 이용하여 자동차 안전 기능에 관한 연구 개발을 실시하는 단체 인 CAMP VSC3 (Crash Avoidance Metrics Partner- ship, Vehicle Safety Communications 3) 컨소시엄이 참여하고 있다. CAMP VSC3는 미국 SAFETY PILOT 실험에서 중요한 역할을 하고 있다.



〔그림 5〕 PRESERVE의 V2X 보안 아키텍처

4.2.2.1 V2X 보안 아키텍처 (VSA)

PRESERVE의 첫 번째 성과로는 지금까지 EU's Seventh Framework Programme for Research (FP7)에서의 자동차 관련 보안 연구 개발 활동인 SeVeCom, EVITA PRECIOSA의 성과를 가져온 V2X 보안 아키텍처(VSA : V2X Security Architecture)이다. V2X는 자동차와 무언 인가(Vehicle to X)의 약자로 차량과 도로 간 및 차량 간 통신을 의미한다. 주요 성과 중 하나는 융합 계층(convergence layer)에서 통신 계층과 차량 보안 서브 시스템사이의 통신 API를 제공하는 계층이다. 이것은 [그림 5]에서 왼쪽에서 두 번째에 위치한다. 융합 계층은 프랑스 SCORE@F[36] 등과 같은 V2X 통신 기능으로 타사 제품과 상호 운용성을 위한 정합규격이다. 또한, SCORE@F는 프랑스의 연구 개발 프로젝트로서 도로와 차량 간 및 차량 간 통신으로 자동차의 안전을 향상시키는 것을 목표로 하고 있다.

4.2.2.2 현장 운용 시험

PRESERVE는 소규모 현장 운용시험을 시작으로 대규모 현장 운용시험, 프랑스의 V2X 프로젝트 SCORE@F와 연동 시험 순으로 몇 년 동안 시험을 실시 할 예정이다.

4.2.2.3 PRESERVE의 보급 활동

PRESERVE는 세계 표준 보급 활동의 일환으로 유럽과 미국의 ITS용 보안 표준과 형평성을 맞추는 활동도 실시하고 있으며, 미국 운수부 또는 IEEE 등 EU-US ITS Cooperation HTG Harmoniza- tion Task Group (EU-US HTG)에 참가하고 있다. 유럽 측의 상위 조직으로는 유럽의 C2C-CC (CAR 2 CAR Communication Consortium)[37], 표준화에 대하여는 유럽 ETSI (European Telecommunications Standards Institute)[38]가 있다.

유럽에서는 유럽 위원회의 M/453 지령[39]에 의해 2013년까지 ITS 표준화를 목표로 하고 있다. 유럽과 미국 간 협조 창구인 EU - US HTG 내용은 2012년 11월 15일 워크샵이 개최[40] 된 바가 있으며, 활동 상황이 보고되고 있다[41]. 유럽과 미국 간에는 별도로 정의된 ITS의 보안 표준 간의 상호 연결을 가능하게 하기 위한 조화 활동을 하고 왔지만, 100건 이상의 규격 상 불일치 문제가 있고, 그 중 절반 정도가 중간 이상의 상위

수준에서의 문제가 있다고 보고하고 있다. 예를 들면, 보안 API가 어떤 소프트웨어에서 호출 되는지에 관한 불일치 및 PKI를 이용하다면 5년 이상 장기간 입증 방법에 대한 문제가 지적되고 있다. 따라서, 이 때문에 HTG에서는 미국과 유럽 간의 표준 규격의 통일에는 도달하지 못한 상황이다. 또한, 일본을 비롯한 지역 간의 메시지 비교 및 차이점은 JARI 보고에 많이 보고되고 있으며[42] 또한 EU-US HTG에 대한 추진 동향 및 일본과 한국을 포함한 협력 관계에 대해서는 JSAE 보고서[43]에 기술되어 있다. 향후 PRESERVE에 의한 규격이 전 세계에 통용되는 규격으로 발전될 가능성이 있으므로 지속적인 참여가 필요하다.

4.2.3 DIAMONDS 프로젝트

독일의 Dornier 컨설팅 사[44]에서는 고 비도를 필요로 하는 시스템에서 모델 기반의 보안 시험 방법 및 도구 개발을 위하여 DIAMONDS 프로젝트[45]를 진행 중에 있다[46]. DIAMONDS 프로젝트는 유럽의 연구개발 보조금 프로그램 인 EUREKA[47]의 일부인 정보기술 관련 ITEA2(Information Technology for European Advancement)[48]에 소속한다. DIAMONDS 프로젝트에서는 보안 테스트를 개발 초기 단계에서 자동으로 수행하는 모델 기반의 시험 및 모니터링 하는 방법론을 연구 목표로 하고 있다. 그 결과, 설계 초기 단계에서 취약점을 발견하고 보안에 대응하기 위한 효율적인 시스템 설계가 가능하게 된다.

또한, 본 프로젝트의 대상으로는 산업계, 은행, 교통, 통신 등의 복수 도메인의 보안에 대응하고 있다. DIAMONDS 프로젝트처럼 보안 시험을 자동화 및 기계화함으로 하여 설계 기간의 단축 외에도 정보 누출이나 불일치 문제를 조기에 검증 하는 것이 용이하게 될 것으로 생각된다.

4.2.4 OVERSEE 프로젝트

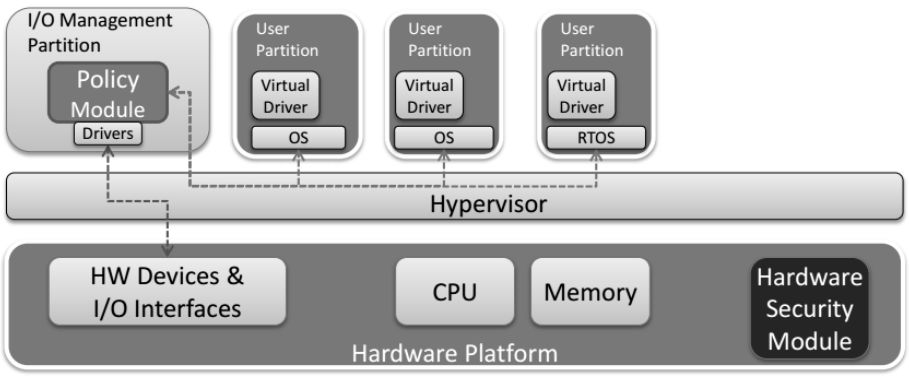
OVERSEE 프로젝트[49]는 FP7의 교통 시스에 관한 보안 프로젝트 중의 하나이다. 자동차 시스템에서 여러 업체로부터 제공되는 복수의 응용 프로그램을 하나의 멀티 코어 보드에서 공존하기 위해 가상 머신을 이용하여 실행 환경을 분할하면서 정책 제어를 통하여 보안 서비스를 제공한다.

[그림 6]은 OVERSEE의 입출력 관리를 나타내는 보안 모델에 관한 그림[50]이다. 그림의 오른쪽 상단에서 여러 응용 프로그램이 동일한 하이퍼바이저의 가상 머신인 “User Partition” 상에 실행되고 있다. 이러한 응용 프로그램이 그림 하단에 있는 하드웨어를 통해 입출력을 할 경우 반드시 그림의 왼쪽 상단에 있는 입출력 관리 정책 모듈(Policy Module)을 통해 허용 또는 차단하는 보안 제어를 실시한다. OVERSEE 프로젝트 는 2012년 12월에 최종 발표를 완료하였다. 이 성과는 PRESERVE로 인계되고 ASIC으로 구현되어 있다.

4.3. 일본의 자동차 보안 연구 동향

4.3.1 IPA의 자동차 보안 연구

IPA는 “2011 년도 자동차 정보 보안 동향에 관한 조



〔그림 6〕 OVERSEE 보안 모델

사"[51], IPA 기술 동향 보고서[52]를 발표하였다. 이 가운데 스마트 폰의 보급과 자동차의 인터넷 연결로 인하여 자동차 기기간의 개방화, 이에 따라 네트워크를 통해 자동차가 외부에서 공격을 받을 가능성이 높아지고 있다고 지적하고 있다. 2012년 10월에 개최 된 ITS 관련 세계적인 학술대회인 「ITS 세계 대회 2012」[53] 는 자동차 보안에 관한 세션[54]이 개설되어 escrypt, IPA 등 5 명이 발표를 하였다. 본 대회의 대부분의 내용이 이용에 관한 전시 및 발표이지만, 향후 보안에 대한 논문도 함께 발표하여야 할 것이다.

4.3.2 JSAE 및 JEITA에 의한 표준화 활동

JSAE(Society of Automotive Engineers of Japan, 일본 자동차공학학회)는 2010 년부터 자동차 보안에 대한 표준화를 목표로 "보안 표준화 기획 분과위원회"에서 중점적으로 연구하고 있다. 2014년 4월 현재, 이 위원회에서는 SAE 내부에서 사용할 수 있는 지침을 제정하고 있다. JSAE는 ITS 관련 국제 표준화 활동에서 일본 업계 대표로 참여하고 있으며, "ITS 표준화 위원회"는 자동차, 도로, 통신, 소비자 등을 대표하는 위원 43명으로 구성되어 있다[55]. 또한, JEITA(Japan Electronics and Information Technology Industries Association: 전자정보기술산업협회)[56]가 담당하고 있는 ISO TC204 는 자동차 본체 의 표준화를 담당하는 ISO TC22와 연계 활동을 하고 있으며, 자동차 본체와 부속 장치간의 정합 표준인 ISO13185 등을 연구하고 있다.[57]

ISO TC204와 WG17 Nomadic Device에서는 자동차 시스템과 스마트 폰 등과의 정합 및 자동차와 외부 연결이나 인터넷 연결을 위한 통신 정합에 관하여 많은 단체가 참여하고 있으며 보안문제도 중요한 표준화 활동이라고 인식하고 있다.

4.3.3 ITS Japan의 보안 가이드라인 제정

일본 ITS Forum[58]는 ITS의 보급 촉진을 위한 연구 개발과 표준화를 진행하는 단체이다. ITS Forum은 2011년 4월에 V2X 운용 시스템과 통신 시스템에 대한 보안 지침을 공개하고 2012년 통신 시스템에 대한 보안 지침 개정안을 공개[59] 하고 있다. ITS Forum의 보안 지침은 V2X 통신 구조와 사용 과정이 자세히 기술되어 있으며 지침 상 내용은 모델의 정의, 서비스의 특정 위협 분석 및 필요한 보안 대책을 제시하고 있다. 보안 대책은 미국의 IEEE 1609.2을 이용한 PKI 방식도 포함되어 있으며, 국제적인 협조까지 망라되어 있다. 또한 V2X 운영 관리의 3 가지 형태에 대한 보안 대책이 제시되고 있으며, 운영 관리까지 포함되어 있다. 2012년 발표 자료 중 「부록」에는 다음 정보가 추가 되어 있다.

- 대칭 키 알고리즘의 적용 시 키 관리 방안
- 재생 공격 대비
- 도로 정보 및 도로간 정보의 공격과 대책
- 보안 정보의 저장 · 갱신 · 설정을 변경할 프리미티브에 관한 사항

단, ITS Forum의 보안 지침 사양으로 규정되어 있지 않은 부분은 보완할 예정이므로 향후 최종 표준 규격은 어떻게 제정될지는 아직 미지수이다.

4.3.4 일본의 현장 운용 시험

도요타 자동차는 ITS 실험장[60]으로 3.5 헥타르의 광대한 부지에 700MHz 대역의 전파를 사용할 수 있는 실험장을 도요타 동 후지 연구소(시즈오카 현 소노시 소재)에 설치하였다. ITS 실험장에서는 일반 도로와 신호등 등 시가지를 설치하여, 안전 운전 지원 시스템과 환경 시스템의 연구 개발을 하고 있다. 앞으로 자동 운전 등을 포함한 ITS를 보다 적극적으로 활용한 새로운 응용기술을 실현하기 위해 중요한 역할을 할 것으로 생각된다.

4.3.5 ISIT의 자동차 보안 워크샵

일본 ISIT[61] 에서 주관하여 자동차 전자 연구회에서 2008년부터 현재까지 워크샵을 개최하여 왔으며 매년 다음과 같은 주제로 발표를 하였다.

- 2008년 : 차세대 차량 마이크로프로세서
- 2009년 : Car Electronic의 기술동향
- 2010년 5월: 21세기 자동차 산업의 기술, 서비스, 경영
- 2010년 9월 : 아시아의 21세기 자동차 도전

- 2011년 5월 : 차량 SW의 개발과 검증
- 2011년 10월 : Car Electronic으로부터 타 산업으로 확장
- 2012년 1월 : Model-based 개발
- 2012년 5월 : Model-based 개발 방법론
- 2012년 9월 : 전기자동차 기술의 최신 동향
- 2013년 5월 : Modeling 방법론의 적용
- 2014년 1월 : 자동차 글로벌 경쟁력을 유지하는 Car Electronic 기술

Ⅵ. 결론

escar 국제회의는 처음에 자동자의 embedded 보안 기술에만 토의 대상이 되었으나, ICT 기술을 접목한 새로운 스마트 카의 출현 등으로 불특정 다수인이 연결되는 사이버 공간으로 유무선으로 연결되어 획기적인 편리성을 제공하나 부수적으로 발생하는 사이버 보안 문제는 반드시 해결을 하여야 할 분야이므로 토의의 대상이 점차 확대일로에 있으며 과거 10년 동안 유럽(독일)에서 주로 개최되어 왔으나 2013년부터 매년 미국에서 개최되며, 2014년 4월에는 최초로 아시아 지역인 일본에서 개최되어 국제 학술대회로의 영역이 점차 확대 일로에 있다.

이미 자동차 선진국에서는 정부 및 민간 단체가 주도적으로 자동차 보안에 관련하여 각종 프로젝트를 다각적으로 추진하고 있으므로 국내에서도 이러한 프로젝트에 적극적인 참여가 필요하며 세계 기술 동향 추이를 지속적인 파악이 요구된다.

또한, 전자화에 따른 주행 편리성, 안전성, 원격 감시, 오락도구 제공, 차량간 통신으로 각종 경보 신호 수신 기능 등으로 차종별 서비스에 차별성이 제공되나, 이에 따른 새로운 위협과 공격에 대하여는 철저히 대비하여 새로운 자동차 개발에 힘써야 한다.

그리고, ICT 분야에서 보안 취약점과 보안 사고가 자동차 산업에도 파급효과가 있을 것이므로 기존의 ICT 분야에서 보안 위협과 대응 기술을 타산지석의 지혜를 모아 자동차 보안 기술을 개발 및 보급하여야 할 것이다.

한국의 세계 최고 수준의 보안 기술과 공개키 인증 기반 구조, ICT 장치 (스마트 폰 등) 의 생산 능력을 최대한 활용하여 win-win 전략을 세워 세계 시장을 선도할 수 있도록 준비하여야 할 것이며 기계적인 자동차 생산은 세계적인 경쟁력을 확보하였다고 하나 향후 자동차 생산은 안전하고 우수한 SW 개발 능력에 좌우하므로 상대적으로 차량 선진국에 비하여 뒤떨어진 SW 기술에 대하여는 부단한 연구 개발과 고급 인재 양성을 하여야 할 것이다.

참 고 문 헌

[1] 31st Symposium on Cryptography and Information Security (SCIS2014), Kagoshima, Japan, Jan. 21-24, 2014. http://www.iwsec.org/scis2014

[2] escar (Embedded Security in Cars Conference) https://www.escar.info/

[3] Hiroaki Anada, Shin-ichi Matsumoto and Kourich Sakurai, “Trend of Car-Information Security: a Report on International Conference ‘escar’”, Proc. of SCIS2014, Session 1B3-4, Kagoshima, Japan, Jan. 21-24, 2014.

[4] IPA (Infomation-technology Promotion Agengy, Japan), “자동차의 정보 보안에 대한 대처 가이드”, 2012-03, http://www.ipa.go.jp/ security/fy24/reports/emb_car/index.html

[5] R. Charette, “This car runs on code”, Feb, 2009, http://www.spectrum.ieee.org/feb09/7649

[6] S. Checkoway, et al. “Comprehensive Experimental Analyses of Automotive Attack Surfaces.” USENIX Security Symposium. 2011.

[7] F. Bruwer, W. Smit and G. Kuhn, “Microchips and remote control devices compromising same”, US patent 5517187, May. 14, 1996

[8] A. Bogdanov, “Cryptanalysis of the KeeLoq block cipher”, IACR ePrint Archive 2007/055

[9] E. Biham, O. Dunkelman, S. Indesteege, N. Keller, and B. Preneel, “How to steal cars- a practical attack on KeeLoq”, Proc. of Eurocrypt2008, LNCS 4965, pp.1-18, Springer, Apr. 13-17, 2008.

[10] I.Rouf, R. Miller, H.Mustafa, T.Taylor, S.Oh, W.Xu, M.Gruteser, W.Trappe, and I. Seskar, “Security and privacy vulnerabilities of in-car wireless networks; A tire pressure monitoring

system case study", USENIX Security 2010, pp.323-338, USENIX Association, Aug., 2010.

[11] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automative attack surfaces", SEC11, pp.1-16, 2011.

[12] National Council of ISAC, http://www.isaccouncil.org/

[13] EVITA Deliverable 2.3, EVITA Project, 2009-12,http://ec.europa.eu/information_society/apps/projects/logos/5/224275/080/deliverables/001_EVITAD423.pdf

[14] NIST SP 800-53 Rev. 4, 2012-02-28, http://csrc.nist.gov/publications/PubsSPs.html

[15] STRIDE : Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege, Microsoft, 2006, http://msdn.microsoft.com/ja-jp/magazine/cc163519.aspx

[16] HR 4348 : MAP - 21, Govtrack.us / Civic Impulse, LLC, 2012-04-16, http://www.govtrack.us/congress/bills/112/hr4348

[17] RITA : The Research and Innovative Technology Administration, http://www.rita.dot.gov/

[18] Volpe Center, http://www.volpe.dot.gov

[19] "SAE 2013 Government / Industry Meeting, Technical & Business Session", SAE, 2012, http://www.sae.org/servlets/techSession?EVT_NAME=GI&GROUP_CD=SPEC&SCHED_NUM=199952&REQUEST_TYPE=SESSION_LIST

[20] "Connected Vehicle Safety Pilot Program", NHTSA, 2012-08-21, http:// www.safercar.gov/ConnectedVehicles/

[21] RITA : The Research and Innovative Technology Administration, http://www.rita.dot.gov/

[22] "SAFETY PILOT MODEL DEPLOY- MENT", UMTRI, 2011, http://www.umtri.umich.edu/ content/SafetyPilot_brochure_v3.pdf

[23] "Safety Pilot", 미국 RITA, 2012-11-21, http://www.its.dot.gov/safety_pilot/

[24] "USDOT ITS Research Program", RITA, 2012-05 - 01, http://www.pcb.its.dot.gov/ t3/s120501/s120501_row.pdf

[25] Presentations from the 2012 Event "Crash Avoidance II", SAE, 2012, http://www.sae.org/events/gim/presentations/2012/

[26] ITS Standards Fact Sheets, IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments (WAVE), RITA, http://www.standards.its.dot.gov/Factsheets/Factsheet/80

[27] 올랜도 ITS 세계 회의 보고, http://www.its-jp.org/wp-content/uploads/2011/11/IS09-Security-for-Cooperative-Mobility.pdf

[28] CyberAutoChallenge Helps Expose Car Security Flaws, TechNewsDaily, 2012-08-17, http://www.technewsdaily.com/6109-cyber-auto-challenge-car-security.html

[29] Battelle, http://www.battelle.org/

[30] TCG : Trusted Computing Group, http://www.trustedcomputinggroup.org/

[31] 제4회 TCG 공개 워크샵, TCG 일본 지부, 2012-11, http://www.trustedcomputinggroup.org/jp/jrfworkshop/pastworkshop4

[32] EVITA - Deliverable D4.4.2: Test Results, 2012-02-15, http://ec.europa.eu/information_ society/apps/projects/logos/5/224275/080/deliverables/001_EVITAD442.pdf

[33] Embedded Linux Development Kit (ELDK), XILINX, http://wiki.xilinx.com/installing-eldk

[34] MATLAB Simulink, http://www.math works.co.jp/products/simulink/

[35] FP7 : EU's Seventh Framework Progra- mme for Research, http://ec.europa.eu/research/fp7/index_en.cfm

[36] SCORE@F, ITS World 2012, http://2012.itsworldcongress.com/zone/ExhibitorList/Exhibitor/8633/SCOREF

[37] C2C-CC : CAR 2 CAR Communication Consortium, http://www.car-to-car.org/

[38] ETSI : European Telecommunications Standards

Institute, http://www.etsi.org

[39] EC M/453 : STANDARDISATION MANDATE ADDRESSED TO CEN, CENELEC AND ETSI IN THE FIELD OF INFORMATION AND COMMUNI- CATION TECHNOLOGIES TO SUPPORT THE INTEROPERABILITY OF CO-OPERATIVE SYSTEMS FOR INTELLIGENT TRANSPORT IN THE EUROPEAN COMMUNITY, EU, 2009-10-06, http://ec.europa.eu/enterprise/sectors/ict/files/standardisation_mandate_en.pdf

[40] "International ITS Harmonization Workshop", EU - US HTG, PRESERVE 공동 , 2012-11-15, http://www.preserve-project.eu/harmonization-workshop

[41] EU-US Standards Harmonization Task Group Report: Overview of Harmonization Task Groups 1&3, 2012-11-15, http://ntl.bts.gov/lib/48000/48500/48524/4487DD4C.pdf

[42] "도로와 자동차 및 차량 간 협조 시스템의 통합 방법" JARI 스즈키 히로요시, 2012-10-06, http://www.jari.or.jp//tabid/259/pdid/53/Default.aspx

[43] ITS Standardization Activities in Japan, JSAE, 2013, https://www.jsae.or.jp/01info/its/2013_bro_e.pdf

[44] Dornier Consulting GmbH, http://www.dornier-consulting.com

[45] DIAMONDS Project, http://www.itea2-diamonds.org/

[46] A case study report on security testing of Bluetooth functionality in an automotive environment, Dornier Consulting, 2012-11-29, https://www.escar.info/fileadmin/Datastore/2012_escar-Vortraege/Dornier_Presentation.pdf

[47] EUREKA, http://www.eurekanetwork.org/

[48] ITEA2 : Information Technology for European Advancement, http://www.itea2.org/

[49] OVERSEE Project (Open Vehicle Secure Platform), https://www.oversee-project.com/

[50] OVERSEE - A Secure and Open In - Vehicle IT Platform, Hakan Cankaya, escrypt, 2012-11-28, https://www.escar.info/fieadmin/Datastore/2012_escar-Vortraege/ESCRYPT_OVERSEE_Presentation.pdf

[51] "2011 년도 자동차 정보 보안 동향에 관한 조사 보고서 의 공개 - 네트워크화 오픈화에 수반되는 자동차 보안", IPA, 2012-05-31, http://www.ipa.go.jp/security/fy23/reports/emb_car/index.html

[52] IPA 기술 동향보고서 "자동차 정보 보안에 관한 보고서", IPA, 2012-05-31, http://www.ipa.go.jp/about/technicalwatch/20120531.html

[53] ITS World Congress 2012, 2012-10-22, http://2012.itsworldcongress.com/

[54] Cybersecurity and the impacts on the Intelligent Transportation System, ITS World Congress, 2012-10-25, http://2012.itsworldcongress.com/zone/Timetable/Event/178

[55] 2012 년도 ITS 표준화 위원회 위원 참가자 명단, JSAE, 2013-08-29, https://www.jsae.or.jp/ 01info/org/its/its_meibo.pdf

[56] JEITA : 일반 사단 법인 전자 정보 기술 산업 협회, http://www.jeita.or.jp/

[57] Nomadic Device "자동차 관련 활용 및 관련 표준화 동향", JARI, 2012-06-27, http://www.jari.or.jp/tabid/76/Default.aspx?itemid=9

[58] ITS 정보 통신 시스템 추진회의, http://www.itsforum.gr.jp/

[59] 운전 지원 시스템 에 대한 보안 지침 ITS FORUM RC009 1.1 판, ITS Forum, 2012-04-25, http://www.itsforum.gr.jp/Public/J7Database/p41/p41.pdf

[60] ITS 기술의 조기 실용화를 위하여, 「ITS 실험장」을 구축 [도요타 자동차], JSAE, 2012-11-12, http://guide.jsae.or.jp/topics/44144/

[61] ISIT 제13회 차량 일렉트로닉스 연구회, http://www.car-electronics.jp/old/13th/

〈저자소개〉

김 광 조 (Kwangjo Kim)
종신회원

1980년 2월: 연세대학교 공과대학 전자공학과 졸업
1983년 8월: 연세대학교 대학원 전자공학과 석사 (M/W 전공)
1991년 3월: 일본 요코하마 국립대 대학원 전자정보공학 박사 (암호학 및 정보보호 전공)
1979년 12월 ~ 1997년 12월: ETRI 부설연구원 부호1실장/책임연구원
1999년 1월 ~ 2004년 12월: 세계암호학회(IACR) 이사
1998년 1월 ~ 2009년 2월: 한국정보통신대학교 정보통신대학원장 및 공학부장
2003년 1월 ~ 2005년 1월: IT 영재교육원 원장
2005년 1월 ~ 2008년 12월: Asiacrypt 조정위원회 의장
2005년 2월 ~ 2005년 5월: MIT 방문학자
2005년 6월 ~ 2005년 11월: UCSD 방문교수
2009년 1월 ~ 2009년 12월: 한국정보보호학회 회장
2012년 1월 ~ 2012년 8월: KUSTAR(UAE) 방문교수
2013년 1월 ~ 2013년 2월: ITB(인도네시아) 방문교수
2013년 7월 ~ 2013년 8월: ITB(인도네시아) 방문교수
2009년 3월 ~ 현재: 한국과학기술원 전산학과 교수
2010년 1월 ~ 현재: 한국정보보호학회 명예회장
2014년 4월 ~ 현재: IFIP TC-11 한국대표
관심분야 : 암호와 정보보호 이론 및 응용

이 동 수 (Dongsoo Lee)
학생회원

2013년 2월 : 한국과학기술원 전산학과 졸업
2013년 3월 ~ 현재 : 한국과학기술원 전산학과 석사과정
관심분야 : 정보보호, SCADA, 네트워크 보안, 인증 프로토콜