정 보 보 호 학 회 지
제24권 제2호, 2014. 4

V2X 통신을 위한 보안기술

이 유 식*, 심 상 규**, 김 덕 수***

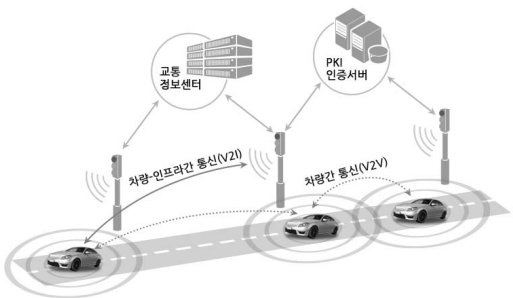
요 약

차량간 소통을 통하여 사고를 미연에 방지하고, 운전자의 편의성을 높일 수 있는 V2X는 차세대 자동차 기술 중 하나로 인식되어, 주요 자동차 생산 업체는 물론 미국이나 유럽의 경우 국가적인 차원에서 관심을 가지고 연구 및 기술개발에 힘쓰고 있는 기술이다. 본 고에서는 IEEE 1609.2를 중심으로 V2X 통신 중 보안부분(Security Service)에 대한 설명과 차량을 위한 PKI 시스템 구축 등을 소개하고, 향후 연구 방향에 대하여 논한다.

Ⅰ. 서 론

과거의 자동차가 전기와 기계 계통으로 조합된 장치였다면, 현대의 또는 미래의 자동차는 하나의 네트워크 장치로 인식될 만큼 많은 정보를 외부와 소통하고 있으며, 차량 내부 또한 대량의 소프트웨어를 탑재하고 있어 컴퓨터 시스템의 집합으로 보아도 무방할 정도이다. 이젠 "무선통신을 통해 차량과 내·외부 네트워크가 상호 연결되어 운전자의 편의성을 높일 수 있는 서비스를 제공"하는 커넥티드 카(connected car)라는 개념이 더 이상 먼 미래가 아니라 우리가 곧바로 도입해야 하는 필수 요소로 자리잡아가고 있다. 특히 V2V(Vehicle to Vehicle, 차량간 통신)는 도로나 선도 차량의 돌발 상황 등을 실시간으로 확인하여 안전하고 편리한 운행환경을 제공할 기술로 주목받고 있다.

지난 2월 미 교통국에서는 V2V 기술의 채용 의무화에 대한 입법을 예고했다. 지난 2012년부터 미시건 주 앤 아버에서 1년여에 걸쳐 3000여대의 차량을 통하여 V2V 기술의 가능성을 시험하였고, 차량 충돌 사고의 80% 정도를 감소시킬 것으로 예상하였다. 미래에는 안전밸트나 에어백과 함께 안전을 위한 필수 요소가 될 것으로 예상하며, 수년 내 새로운 차량에 V2V 기기를 장착하도록 하는 규제안을 만들 예정이라고 한다.



〔그림 1〕 V2X 구성도

또한 유럽에서는 C2C-CC(Car-to-Car Communicatoin Consortium)를 필두로 미국과 유사한 V2V 과제나 시험이 진행중이고, EVITA, OVERSEE, PRECIOSA, PRESERVE 등 V2X 및 차량 보안 관련 연구가 활발하게 이루어지고 있으며, 벤츠는 2013년 말부터 C2X(Car-to-X)를 선언하여 차량간 통신을 도입한 최초의 업체가 되었다.

국내에서는 정부의 주도하에 스마트하이웨이 연구사업을 통하여 V2V 및 ITS 기술 개발을 추진하고 있다. 스마트하이웨이 연구 사업은 국토해양부에서 수립한 건설교통 R&D 혁신 로드맵에서 세계 일류 기술 개발을 위한 10대 중점 추진 R&D 프로젝트로 지정되어 추진되고 있으나, 완성차 업체의 참여도 저하나 통신을

* 펜타시큐리티시스템(주) 보안기술연구소, 고려대학교 정보보호대학원 임베디드 연구실 (yslee@pentasecurity.com)
** 펜타시큐리티시스템(주) 보안기술연구소 (sgsim@pentasecurity.com)
*** 펜타시큐리티시스템(주) 보안기술연구소 (dskim@pentasecurity.com)

위한 주파수 확보 등의 어려움을 겪고 있고[1], 완성차 업체에서는 V2V나 V2I보다는 V2N (Vehicle to Nomadic device, 차량과 모바일 기기간 통신)에 집중하고 있는 상태이다.

이런 세계적인 자동차 업계 및 정책의 흐름으로 미루어보아 우리나라에서도 V2V와 V2I(Vehicle to Infra)에 대한 연구 및 시험이 본격적으로 진행되어야 할 것이고, 이에 발 맞추어 해당 통신의 보안이 매우 중요한 요소로 부각될 것이다. 전술한 바와 같이 차량에서 점차 소프트웨어의 비중이 높아지고, 네트워크와 연결되어 점차 외부와의 통신이 잦아지게 되면서, 일반적인 컴퓨터 환경에서 이루어지던 해킹과 악의적인 공격들이 동일하게 차량 또는 인프라에게 적용될 수 있게 되었다. 전통적인 정보통신산업에서의 취약한 보안은 금전적 손실과 연관되지만, 자동차 산업에서의 취약한 보안은 운전자의 생명과 직결될 수 있는 문제이므로 무엇보다 먼저 선결되어야 할 과제이다.

본 고에서는 V2V와 V2I 통신을 위하여, WAVE (Wireless Access in Vehicular Environments) 관련 국제 표준인 IEEE 1609.2의 규격에 준하여 구축한 시스템을 소개하고, 향후 개선 및 연구되어야 할 방향에 대하여 논하고자 한다.

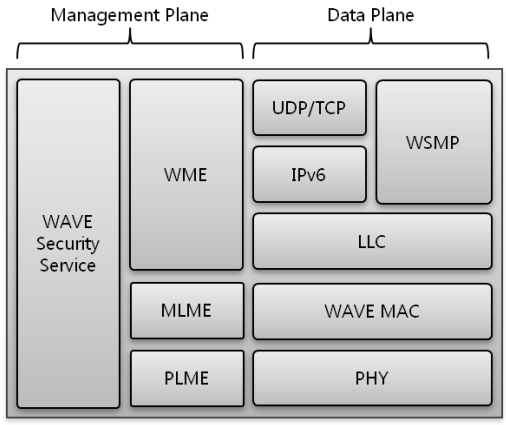
Ⅱ. IEEE 1609.2

IEEE 1609 시리즈는 WAVE 관련 아키텍처와 구현, 보안 서비스 및 인터페이스를 정의한 표준으로 다음의 [표 1]과 같이 구성되어 있다.

〔표 1〕 IEEE 1609 시리즈의 구성

표준	내용
1609.0	Architecture
1609.2	Security Services for Applications and Management Messages
1609.3	Networking Services
1609.4	Multi-channel Operation
1609.11	Over-the-Air Electronic Payment Data Exchange Protocol for Intellitgent Transportation System (ITS)
1609.12	Identifier Allocations

WAVE의 Protocol stack은 다음의 [그림 2]와 같으며, 본 고에서 논하는 부분은 WAVE Security Service ([그림 2]의 왼편)에 국한한다.



〔그림 2〕 WAVE Protocol Stack

WAVE Security Service는 크게 다음의 다음과 같이 구성된다.

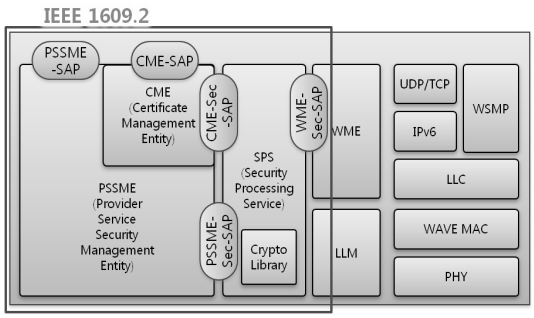
1) Security Processing Services

- 차량 데이터와 WSAs(WAVE Service Advertisements)가 보안 통신을 하기 위한 프로세스 제공

2) Security Management Services

- Certificate Management Service 제공.
  - Certificate Management Service는 CME (Certificate Management Entity)와 모든 인증서의 유효성과 관련된 관리 정보를 제공받는다.
- Security Management Service 제공.
  - Security Management Service는 PSSME (Provider Service Security Management Entity)와 secured WSAs를 전송하는데 사용하는 개인키 및 인증서 관련 정보를 제공받는다.

[그림 3]과 [표 2]는 IEEE 1609.2에서 정의하고 있는 Security Service를 보여준다.



〔그림 3〕 IEEE 1609.2 Component

〔표 2〕 IEEE 1609.2 Component의 역할

항목	역할
Sec-SAP	데이터 통신 시 보안 서비스 제공
PSSME-SAP PSSME-Sec-SAP	Secure WSA 전송 시 사용하는 인증서 및 개인키 정보 관리
CME-SAP CME-Sec-SAP	인증서 및 인증서 폐지 목록에 대한 정보 관리
WME-SAP	WSA 서명 생성 및 검증

Ⅲ. V2X를 위한 PKI

앞서 살펴본 바와 같이 IEEE 1609.2에서는 보안 목표를 달성하기 위해 해시, 대칭키 암호 알고리즘, 공개키 암호 알고리즘을 사용한다. 대칭키 암호알고리즘은 주로 데이터에 대한 기밀성을 제공하기 위해 사용되고, 해시는 데이터의 무결성 체크를 위해, 공개키 알고리즘은 대칭키 교환 및 전자서명에 사용된다. 이 때, 이 공개키가 어떤 개체의 것인지 증명하기 위해 신뢰할 수 있는 기관(CA, Certificate Authority)에서 인증서를 발급하고 검증할 수 있어야 하므로 PKI(Public Key Infrastructure, 공개키 기반 구조)가 필요하다.

일반적으로 사용되는 PKI는 다음과 같은 요소들로 구성된다.

- 인증서를 발급하고 검증하는 인증 기관(CA)
- 인증서 발급 대행기관(RA)
- 인증서들을 보관하는 하나 이상의 디렉토리(LDAP) 및 인증서 관리 서버

전통적으로 인증서가 사용되는 시스템에서는, 인증서의 소유자가 누구인지 확인하는 과정이 반드시 필요하다. 예를 들어, 금융기관에서 인터넷 뱅킹을 이용하기 위하여 공인인증서를 사용할 경우, 금융기관에서는 이용자가 누구인지 확인할 수 있어야 인증 및 권한을 부여하고 서명을 통하여 거래가 수행된다. 하지만, V2V의 경우에는 “어떤 차량으로부터 메시지가 전송되었는가” 보다는 “신뢰할 수 있는 개체로부터 메시지가 전송되었는가”가 중요하다. 즉, 상대차량은 식별의 대상이 아니라 신뢰의 대상이 된다. 게다가 만약 상대방의 차량을 식별하게 된다면 Privacy 문제에 직면하게 된다. 차량을 식별할 수 있으면, 차량의 소유주와 연계하여 위치정보, 운전 습관 등 개인정보를 알게 되므로 법적인 문제를 초래한다.

따라서 신뢰할 수 있는 CA로부터 인증서를 발급받은 정당한 개체인지만을 확인하게 하고, 인증서의 DN(Distinguished Name)을 통하여 차량을 식별할 수 없도록 익명성을 부여하는 것이 필요하다.

차량에서 사용하는 인증서는 다음과 같이 크게 두 가지 종류가 있다.

- CSR(Certificate Signing Request) 인증서
- 익명 인증서(Anonymous Certificate)

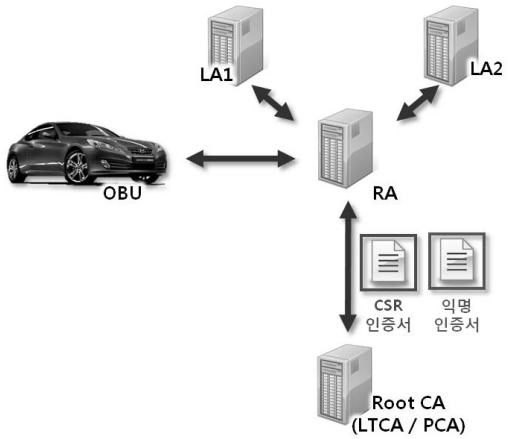
CSR 인증서는 차량을 식별할 수 있는 인증서로써, , Infra와 통신할 때(V2I) 사용되고, 익명 인증서는 차량간 통신 시(V2V) 신뢰성 여부를 확인하기 위하여 서명 및 서명 검증을 위하여 사용된다.

인증서에 익명성을 부여하는 방식은 표준으로 정의된 바 없고, 미국(CAMP VSC3)과 유럽(C2C-CC)이 각각의 방식에 따라 정의하고 있다.

3.1. CAMP VSC3

CAMP(Crash Avoidance Metrics Partnership)는 자동차 메이커들로 구성된 컨서시엄으로 미국의 DOT (Department of Transportation)와 그 산하기관인 NHTSA(National Highway Traffic Safety Administration)과 협력하여 PKI 관련 규격을 제정하고, 이를 반영하여 VII(Vehicle Infrastructure Integration) 프로젝트를 진행하였다. CAMP 규격에서는 익명성을 보장하기 위하

여 전통적인 PKI에 LA(Linkage Authority)를 도입하여 ID를 발급하고, 해당 ID를 기반으로 인증서를 발급하므로 ID를 알고 있는 LA들과 CA 모두가 협력하지 않는 이상 차량과 인증서의 연결고리를 확인할 수 없다.[2]



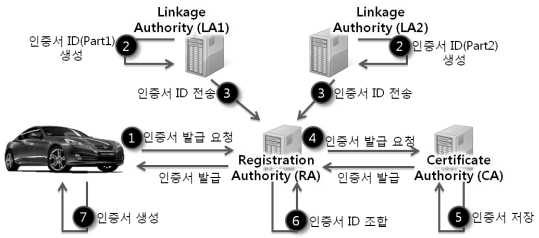
〔그림 4〕 익명성 보장을 위한 PKI 구성(CAMP)

익명 인증서를 발급하는 과정은 다음과 같다.

1) 인증서 발급 요청
① RA로 CSR 인증서를 통하여 익명 인증서 발급 요청(차량)
② 요청 수락

2) 인증서 발급
① CSR 인증서 검증 및 LAn으로 인증서 ID 요청(RA)
② 인증서 ID 발급(LAn)
③ 인증서 ID를 통하여 CA로 인증서 발급 요청(RA)
④ 인증서 발급(CA)
⑤ 인증서 ID 조합 및 암호화(RA)

3) 인증서 전송
① 인증서 전송 요청(차량)
② 인증서 암호화 및 전송(RA)
③ 인증서 복호화키 요청(차량)
④ 인증서 복호화키 전송(RA)
⑤ 인증서 복호화 및 저장(차량)



〔그림 5〕 익명 인증서 발급 과정(CAMP)

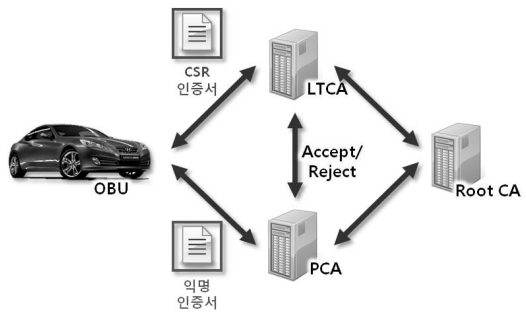
상기의 과정에서 보듯이 각 과정들이 분리되어 있는 이유는, 익명 인증서는 유효기간이 매우 짧고, 한 번 발급받을 때 달, 또는 년 단위로 받기 때문에 대량의 인증서를 발급 및 전송해야 한다. 따라서, 세션을 유지한 채 동기화 방식으로 발급이 진행되면 많은 문제를 야기할 수 있으므로, 차량에서는 발급 요청 후 주기적으로 전송 요청을 하는 것이 일반적이다.

3.2. C2C-CC

CAMP에서는 익명 인증서와 CSR 인증서 모두를 CA에서 발급한 반면, C2C-CC에서는 각각의 인증서를 발급하는 주체가 다르다.[3]

[그림 6]에서 보는 바와 같이 CSR 인증서는 LTCA(Long Term CA)에서, 익명 인증서는 PCA (Pseudonym CA)에서 발급한다.

차량에서 CSR 인증서를 이용하여 PCA로 발급 요청을 하면, PCA에서는 LTCA를 통하여 해당 CSR 인증서의 유효성을 확인하고, 익명 인증서를 발급해 준다.



〔그림 6〕 익명 인증서 발급 과정(C2C-CC)

CAMP의 방식에서는 RA에 접근 가능한 내부자라 하더라도 CSR 인증서와 익명 인증서의 연결고리를 발견할 수 없는 반면, C2C-CC의 방식은 PCA에 접근 가능한 내부자가 CSR 인증서와 익명 인증서의 연결고리를 찾을 수 있으므로 권한 관리 및 교육, 감사 증적 확보 등을 통한 내부자 유출 방지가 무엇보다 중요하다고 할 수 있다.

Ⅳ. 시험 시스템 소개

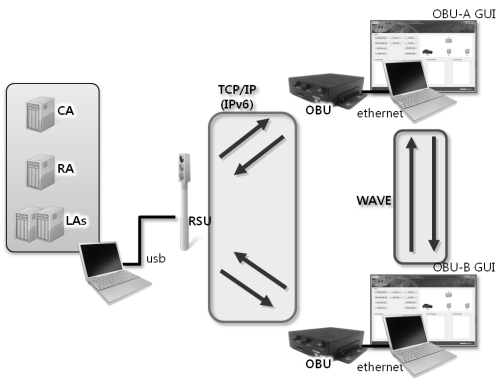
본 장에서는 V2X 통신 보안을 위하여 펜타시큐리티 시스템(주)에서 구축한 시험 시스템에 대하여 설명한다.

시험 시스템은 다음의 요소들로 구성된다.

〔표 3〕 시험 시스템 구성 요소

구분	항목	
	Logical	Physical
Infra	CA	Notebook1
	RA	
	LA1	
	LA2	
	RSU	OBU로 대체
Vehicle	OBU1	Notebook2
	OBU2	Notebook3

즉, PKI 서버 군을 하나의 노트북에서 실행시키고, 차량 역할의 OBU와 해당 OBU를 제어하기 위한 GUI 프로그램이 실행되는 노트북이 각 2개씩 준비되었다.



〔그림 7〕 시험 시스템 구성도

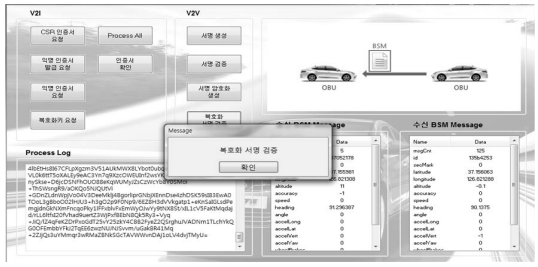
상기 그림에서 보듯이 본 시스템은 CAMP의 방식으로 제작되었다.

시험은 다음의 항목들에 대하여 이루어졌다.

1) V2I
- CSR 인증서 발급 요청
- 익명 인증서 발급 요청
- 익명 인증서 전송 요청
- 복호화키 요청

2) V2V
- 서명생성
- 서명검증
- 서명 및 암호문 생성
- 복호화 및 서명 검증

〔그림 8〕 발급된 익명 인증서



〔그림 9〕 V2V 서명 및 복호화 시험

시험 시스템에서 인증서를 발급하는데 소요되는 시간은 다음과 같다.

〔표 4〕 시험 시스템 사양

CPU	Intel(R) Core(TM) i5 CPU 760 @ 2.80GHz
RAM	2G
OS	Linux devel 2.6.32-45-generic

- 익명 인증서 발급 소요시간 : 54분
- 발급 익명 인증서 개수 : 105,120개
  - 12개(5분 간격) * 24 * 365(1년치)

Ⅴ. 결 론

본 고에서 V2X 통신을 위한 WAVE 표준인 IEEE 1609.2와 V2X를 위한 PKI를 소개하고, 펜타시큐리티 시스템(주)에서 구축한 시험 시스템을 살펴보았다.

시험 시스템의 소개에서 보았듯이 시험은 두 대의 OBU를 통하여 시험이 이루어졌고, V2X에 필요한 필수 항목들에 대하여 대체로 만족할 만한 성능 및 결과를 확인하였다.

하지만 현실에서는 두 대의 차량이 통신하는 것이 아니라 군집된 차량들 간에 통신이 이루어지므로 미국의 경우와 같이 대규모의 차량이 참여하는 실차 환경 시험이 필요하다. Infra와의 통신도 대규모의 차량이 인증서를 요청할 경우, 안정성, 성능 및 Load balancing 등도 고려해야 하며, RA가 관할하는 지역을 넘어설 경우 교차 인증에 대한 부분도 고려해야 한다. 또한 표준이나 규격에서 언급하고 있지 않는 부분들, 즉 Infra의 운영에 대한 부분은 연구 및 대규모 시험을 통해서 우리 환경에 맞게 제정해야 하는 부분이다. 즉, CA나 RA의 Coverage를 정의하고, 적절한 인증서 유효기간을 산정하는 등의 과정은 반드시 필요하다.

상기 문제를 해결하기 위하여 대규모의 실차 시험은 반드시 필요하며, 이런 시험을 추진하는 것은 장소 선택과 다양한 차량의 참여 및 기반 시설(WAVE 통신을 위한 주파수 선정, PKI 시스템 등) 구축이 필요하므로 민간 주도로 이루어지기에는 어려움이 있다. 따라서, 정부가 주도적으로 V2X 도입을 추진하고, 자동차 메이커와 부품 업체, 보안 전문 업체 등이 적극 참여하는 대규모의 시험 및 환경 구축을 통해서 기술을 축적해야 한다.

또한 세계적으로 인증서를 발급하고 운영하는 체계가 표준화가 되지 않는다면, 수출/입 되는 차량의 경우 해당 국가의 V2X 체계에 편입될 수 없으므로, 표준화 작업에 주도적으로 참여해야 한다.

향후, 인증서 발급 소요시간을 단축시키기 위한 새로운 알고리즘과 인증서 및 CRL의 효율적인 배포 방식, 차량 내부에 인증서를 안전하게 저장하는 방법, 차량에 대한 DoS 공격을 막을 수 있는 차량 전용 방화벽 등에 대한 연구가 활발히 이루어져야 한다.

V2X 기술은 교통 사고를 줄이고, 운전 편의성을 향상시키며, 원활한 교통 흐름을 유도하여 에너지 절약에도 일조하는 차세대 기술이다. 자동차 산업분야에서 가장 주목하고 있는 기술 분야의 하나이며, 기계와 SW의 융합을 통하여 산업 전반에 큰 변화를 이끌어 낼 수 있을 것으로 예상된다. 해외의 선진국 및 유명 자동차 메이커들이 그러하듯 우리나라에서도 V2X 기술을 위한 정책과 환경을 조성하고, 다양한 연구로 기술 경쟁력을 확보해야한다.

참 고 문 헌

[1] 김용주, “자동차도 없는 ‘반쪽짜리’ 스마트 하이웨이 사업”, 전자신문, 2013.03.24

[2] Andre Weimerskirch, “Data Security and Privacy in Vehicle-to-Vehicle Communication”, SAE 2011 Intelligent Vehicle Systems Symposium, Novemver 9th, 2011

[3] Elmar Schoch, “Securing Cooperative ITS: C2C-CC’s Pilot PKI”, 6th CAR 2 CAR Forum, November 2012

[4] IEEE, IEEE Std. 1609.2TM-2013 “IEEE Stnadard for Wireless Access in Vehicular Environments -Security Services for Applications and Management Message”, April 2013

[5] http://www5.mercedes-benz.com/en/innovation/car-to-x-communication-dialogue-on-the-road-increases-safety-comfort-efficiency/

[6] http://www.nhtsa.gov/About+NHTSA/Press+Releases/2014/USDOT+to+Move+Forward+with+Vehicle-to-Vehicle+Communication+Technology+for+Light+Vehicles

〈저 자 소 개〉

이 유 식 (Lee You Sik)
정회원

1999년 2월 : 성균관대학교 공과대학 학사
2001년 2월 : 성균관대학교 공과대학 석사
2012년 9월~현재 : 고려대학교 정보보호대학원 박사과정
2009년 9월~현재 : 펜타시큐리티시스템(주) 보안기술연구소
관심분야 : Automotive Security, Mobile Security, Cryptography

김 덕 수 (Kim Duk Soo)
비회원

1997년 2월 : 포항공과대학교 전자공학과 학사
1999년 2월 : 포항공과대학교 전자공학과 석사
1999년 6월~현재 : 펜타시큐리티시스템(주) 보안기술연구소장, CTO

심 상 규 (Sim Sang Gyoo)
비회원

1996년 2월 : 포항공과대학교 전자공학과 학사
1998년 2월 : 포항공과대학교 전자공학과 석사
2004년 2월 : 포항공과대학교 전자공학과 박사
2012년 2월~현재 : 펜타시큐리티시스템(주) 보안기술연구소
2014년 3월~현재 : 순천향대학교 융합서비스보안학과 겸임교수