한국ITS학회논문지
J. Korea Inst. Intell. Transp. Syst.
14(6): 133~140 (2015)

pISSN 1738-0774, eISSN 2384-1729
DOI http://dx.doi.org/10.12815/kits.2015.14.6.133

C-ITS 공격 시나리오와 예방 및 대응 방안 연구

A Study on Cooperative-Intelligent Transport System Attack Scenarios and their Prevention and Response Mechanisms

장 윤 서* (Yoonsuh Jang) (Seoul Women's Univ.)
이 동 섭** (Dong-Seob Lee) (Pusan National Univ.)
임 동 호*** (Dong-Ho Lim) (Kangnam Univ.)
안 소 희**** (So-Hee Ahn) (Tongmyuong Univ.)
신 정 훈***** (Jeonghoon Shin) (Sejong Univ.)

· Corresponding author : Jeonghoon Shin (Sejong University), E-mail sjh21a@gmail.com

요 약

차세대지능형교통시스템(C-ITS)는 차량과 차량, 차량과 인프라 간의 양방향 통신으로 교통 정보를 공유하여 더욱 편리하고 안전하게 교통을 제어하는 시스템이다. C-ITS의 보안에 대한 준비가 제대로 갖춰지지 않을 경우 일시적인 교통 마비 및 대형 교통사고를 유발할 수 있고, 이에 따라 운전자의 생명에도 직접적인 영향을 미칠 수 있다. 본 논문에서는 C-ITS에서 발생할 수 있는 사이버 공격들을 시나리오를 통해 연구하여 그 예방 및 대응 방안을 제시한다.

핵심어 : 차세대지능형교통시스템, 교통신호제어체계, 망분리, 사이버 공격 시나리오, 디버그 메시지

ABSTRACT

C-ITS is a system that uses bidirectional communication between two vehicles or infrastructures to control traffic more conveniently, and safely. If C-ITS security is not properly prepared, it can cause traffic congestions and fatal traffic accidents, and therefore can affect greatly on the driver's life. This paper proposes the prevention and response mechanisms based on the cyber attack scenarios that can be used to attack C-ITS.

Key words : C-ITS, Traffic Signal Control System, Network Separation System, Cyber Attack Scenarios, Debug Message

† 본 연구는 한국정보기술연구원 KITRI의 2015년도 차세대보안리더양성프로그램 Best of the Best 4기 소속 Team KLAJY 프로젝트의 일환으로 수행하였습니다.
† 본 논문은 한국ITS학회의 2015년도 추계학술대회에서 발표되었던 논문을 수정·보완하여 작성하였습니다.
* 주저자 장윤서 : 서울여자대학교 정보보호학과 학사 재학
** 공저자 이동섭 : 부산대학교 정보컴퓨터공학과 학사 재학
*** 공저자 임동호 : 강남대학교 컴퓨터공학과 학사 재학
**** 공저자 안소희 : 동명대학교 정보보호학과 학사 재학
***** 교신저자 신정훈 : 세종대학교 컴퓨터공학과 학사 수료
† Received 20 November 2015; reviewed 22 December 2015; Accepted 25 December 2015

Ⅰ. 서 론

21세기 유비쿼터스 사회에 들어서며 도로, 차량, 운전자 간의 관계가 유기적인 협력 관계로 발전하고 있다. 차량은 센터로부터 정보를 수신하거나 CCTV로 교통 상황을 확인할 수 있고, 운전자는 스마트해진 내비게이션 시스템을 통해 보다 편안하고 안전한 경로로 운전자를 안내하고 있다. 통신기술이 조금 더 발전하면 응급사고 발생 시 환자의 차량을 무인으로 제어하여 원하는 목적지나 병원으로 주행시키는 등의 다양한 협력형 서비스가 등장할 것으로 예상된다.[1]

위와 같은 서비스를 제공하기 위한 기반 기술로 차세대 지능형교통시스템(Cooperative Intelligent Transport System, 이하 C-ITS)의 기술개발 및 표준화가 활발하게 이루어지고 있다. 특히 유럽을 비롯한 여러 선진국에서는 안전 문제를 교통 분야의 최우선 과제로 판단하고 이를 해결하기 위해 C-ITS 기술의 연구 개발 및 현장 적용에 박차를 가하고 있으며[2], 이에 따라 우리나라에서도 C-ITS에 대한 연구와 표준화에 대한 추진이 이루어지고 있다. 국토 교통부는 '교통안전혁신과 신시장 창출을 위한 차세대 ITS 활성화 방안' 보고에서 국내에 C-ITS가 도입될 경우 교통사고의 약 46%를 예방하고 연간 3조6000억 원의 교통사고 비용을 절감하는 효과를 거둘 것으로 전망했다.[3]

하지만, 차량 및 도로와 연계된 C-ITS의 경우 한 번의 해킹으로 소규모 인명 피해에서부터 국가 차원의 대규모 피해를 입힐 수 있어 해킹 사고를 방지하기 위한 다양한 기술 개발 및 이에 대한 표준화 연구가 시급하다.

본 연구에서는 C-ITS를 제어하는 ITS센터의 취약성, V2X 통신 중에 주파수 간섭이 발생할 가능성과 물리적인 취약점들을 사용하여 사이버 공격 시나리오를 구상한 후에 C-ITS에서 보안해야할 요소들을 식별하고, 이에 대한 예방 및 대응 방안을 구상하여 보다 효율적이고 안전한 C-ITS를 구축하는 데 도움이 되고자 한다.

Ⅱ. 공격 시나리오 및 대응 방법

1. ITS센터 해킹

1) 공격 시나리오

국내 ITS센터는 현재 일반 운전 환경을 관리하기 위해 교통 정보 제공, 제한 속도 및 교통류 처리, 사고 데이터 기록 등의 서비스를 하고 있다. 향후 C-ITS로 확장 시, ITS센터는 더 많은 양과 다양한

〈표 1〉 2016년 이후부터 제공 예정인 국내 C-ITS의 주요 15개 서비스, 통신방식과 적용 지역[4]
〈Table 1〉 Main 15 services, communication modes and their locations of Korean C-ITS from 2016[4]

Service			Communication mode			Location		
			V2I	V2V	V2P	Motor way	Route	Street
Basic info. collection and supply	1	Location based vehicle data collection	○	○	-	○	○	○
	2	Location based traffic information supply	○	○	-	○	-	-
	3	Toll collection using WAVE communication technology	○	-	-	○	○	○
Safety (caution) driving support	4	Hazardous road driving support	○	○	-	○	○	○
	5	Road condition / Weather information supply	○	-	-	○	○	○
	6	Roadwork section driving support	○	○	-	○	○	○
Inter-section safe passage support	7	Intersection traffic signal violation hazard warning	○	○	-	-	○	○
	8	Right-turn safety driving support	○	○	-	-	○	○
Public transportation safety support	9	Bus operation management	○			○	○	○
	10	Yellow bus (child protection vehicle) operation guide	○	○	-	-	○	○
Pedestrian Care	11	School / Silver zone warning	○	-	-	-	○	○
	12	Pedestrian collision detection warning	○	-	○	-	○	○
Car accident prevention	13	Vehicle collision detection support	○	○	-	○	○	○
	14	Emergency vehicle approach warning	○	○	-	○	○	○
	15	Vehicle emergency circumstances warning	○	○	-	○	○	○

종류의 정보를 수집, 관리 및 제공하게 되며, 이는 해킹 사고 발생시 더 많은 권한과 정보가 공격자의 손에 들어갈 수 있음을 의미한다.

센터에서 교차로에 있는 제어기 및 ITS 장비들을 원격 제어를 할 수 있게 되므로 가장 치명적인 공격 시나리오는 ITS센터 해킹이라 할 수 있다.

교통 시스템은 보통 지역 ITS센터 또는 시의회 내 ITS 부서가 담당하는데, 그 부서를 제외한 다른 부서 또한 상당히 많으므로, 내부에서 효과적인 일처리를 위해 소수의 AP를 두어 네트워크를 형성한다. 만약 해당 네트워크가 C-ITS 조작 네트워크와도 연결되어 있고, 외부에서 내부에 존재하는 무선 AP에 연결할 수 있다면 공격 벡터로 발전될 가능성이 크다.

무선랜(LAN) 환경의 취약점은 다음과 같다.[5]

① Rogue AP : Rogue AP를 통해 공격자는 AP에 대해 인증 없이 네트워크 접근할 수 있게 되며, 내부 AP가 암호화 기능을 사용하지 않거나 WEP 등과 같은 약한 수준의 보안설정일 경우 해당 AP는 내부 네트워크에 접속할 수 있는 출입구 역할을 하게 된다.

② IP 스푸핑(Spoofing) : 기밀성에대한 위협으로, TCP/IP 프로토콜의 설계상 문제로 인하여 허가되지 않은 사용자가 내부망에서 외부망으로 전송되는 패킷으로부터 발신처를 도용하여 허가된 사용자인 것처럼 위장하여 시스템을 공격하는 방법이다.

③ 데이터 변조(Injection and Modification of Data) : 전송 중인 데이터에 변형을 가하여 수신자로 하여금 잘못된 데이터를 수신하게 하는 공격 방법이다. 송수신채널을 마비시킬 수 있으며, 특히 DoS(Denial of Service) 공격에 사용될 수 있다.

④ 통신 방해(Communication Jamming) : 전파 특성을 고려한 통신 방해를 일컫는 재밍은 무선랜 환경에서도 주요한 위협요인이 될 수 있다.

또한, C-ITS 조작 네트워크가 폐쇄망일지라도 노후한 내부시스템을 최신 버전으로 업데이트하기 위해서는 인터넷망에 연결하거나 USB 등으로 패치를 해야 하므로 이 과정에서 내부망으로 접근할 수 있는 통로가 마련되어 해킹에 완전히 안전한 폐쇄망은 존재할 수 없다.

지난 2014년에 발생한 한국수력원자력 SCADA망 공격 사례와 비슷한 시나리오를 구상할 수 있다. 먼저 공격자는 무선랜 취약점을 사용하거나 이메일 등을 통해 외부망에 연결된 내부 PC를 악성코드에 감염시킨다. 그 후 내부 사원이 감염된 PC에 USB나 외장하드와 같은 저장매체를 연결하여 해당 저장매체 또한 악성코드에 감염된다면, 이 저장매체를 내부자가 C-ITS 네트워크 내부 PC에 연결시킨 순간 결국 내부에 있는 PC까지도 악성코드에 감염이 된다. 이때 해당 저장매체에 내부 PC의 자료를 옮긴 뒤 내부자가 이를 모르고 다시 외부망의 PC에 연결시킨다면 내부에서 공격자에게 정보를 보내는 형식으로 해킹 및 자료 유출 등이 가능하다. 이외에도 공격자가 외부망 컴퓨터를 장악한 뒤 같은 네트워크에 있는 업데이트 서버를 통해 업데이트 파일을 악성파일로 변조하고, 내부 PC가 업데이트 서버의 악성코드를 내려받아 실행하면 악성코드에 감염되는 방벙, 네트워크 관리자에게 접근하여 키로깅을 통해 업데이트 서버 또는 자료 서버를 감염시켜 내부로 침투하는 방법 등이 있으며, 내부망과 외부망이 분리되어 있을지라도 네트워크 관리자의 실수 등의 이유로도 해킹 가능성은 충분히 존재한다. [6]

외부로부터 내부의 C-ITS에 접근 가능해진다면 공격자가 C-ITS가 수집한 중요 정보들을 탈취할 수 있음과 동시에 최악의 경우 원격시스템까지도 조작될 수 있음을 의미한다. 공격자는 교통 신호 제어시스템을 통하여 교통 혼잡을 발생시킬 수 있고, V2C 네트워킹을 변조하여 센터에서 차량 및 장비들에 보내는 정보를 악의적으로 변경할 수도 있다. 인프라에 대한 정보나 기능에 조작이 가해진다면 차량간 사고 예방 서비스가 오작동하여 버스 운행 관리와 어린이 보호차량 운행 서비스와 같은 대중교통 안전 지원에 위협이 되며, 이는 막대한 인명 피해로까지 이어질 수 있다.

2) 예방 및 대응 방안

외부 비인가자가 무선 AP망을 통해 C-ITS 제어망까지 침투가 가능할 수 있으므로 최선의 방법으

로는 ITS센터 내 무선 AP를 모두 제거해야한다. 하지만 업무의 효율을 위해 부득이하게 사용해야 하는 경우가 많다. 이 경우 무선 AP 보안을 강화해두어야 한다. WEP 방식은 보안 취약점이 존재하기 때문에 AES (Advanced Encryption Standard) 암호화 기술로 보안을 강화한 WPA-PSK 이상의 강한 암호화 방식을 적용해야한다. WIPS와 같은 무선침입방지시스템 또한 함께 적용해야한다. WIPS는 무선침입방지 시스템으로서 무선AP의 범위 내에서 불법 AP나 사용자단말기를 이용한 침입시도, Ad-Hoc연결, AP의 MAC변조, 서비스 거부(DoS)공격 등을 막을 수 있다.

물리적, PC기반 논리적, 서버기반 논리적 망분리 모두 업무를 위한 외부망과 내부망 사이 접점이 있다. 이 과정에서 내부망에 악성코드가 침투하면 망분리 이전보다 더 위험한 상황이 발생할 수 있다. 내부망의 아킬레스건은 내부망 자체를 보안하기 어렵다는 점이다. 그 때문에 보안의 강도는 추가적인 보안 솔루션을 얼마나 구축하느냐에 달려있다.

폐쇄망 보안을 강화하는 방안으로는 크게 퍼징(fuzzing)기법과 데이터흐름분석 기법을 제시한다. 퍼징 기법은 의도적으로 타당하지 않은 데이터를 보내서 시스템의 오류를 검출하는 기술이다. 이 기법은 시스템 설계단계에서부터 취약점을 찾아서 해결할 수 있다는 장점을 갖춰 미 국방부, 북대서양조약기구(NATO), 영국 국가기반보호센터(CPNI), 일본 제어시스템보안센터(CSSC) 등 많은 국가기관에서도 사용하고 있다. 메타디펜더 (Metadefender)와 같은 보안솔루션은 중간영역(DMZ) 에서 들어오는 파일을 비롯해 외부저장매체(USB 등)에서 흘러들어온 데이터를 실시간으로 탐지하고 악성행위 여부를 파악하여 폐쇄망 내 데이터 흐름을 추적해 사고를 예방한다. 사용자별로 규칙(rule)을 지정할 수 있고 제로데이 공격에 대한 보호도 가능하다.[7]

외부 서비스 제공 서버의 경우 기반시설 점검 기준으로 취약점 점검 및 조치를 수행하여 제어망에 대한 침투를 미리 방지하여야 하며, 화이트리스트 기반의 보안기술을 적용하여 타 시스템 간 허용된 프로토콜 및 프로그램을 사용하도록 하고, 이러한 통신환경에 대한 주기적인 모니터링을 수행해야 한다.

2. 교통신호제어기 물리 접근 해킹

1) 공격 시나리오

모든 교차로에는 1개 이상의 교통신호제어기가 설치되어 있다. 해당 제어기는 기본적으로 중앙 센터와 통신하며 동작하지만, 중앙 센터에 접근하지 않고 제어기에 직접 접근하여 조작하는 것으로 제어기와 연결된 다른 기기들을 제어할 수 있고, 중앙센터와 통신하는 내용을 확인 및 수정할 수 있다. 문제는 현재 통신 시 사용하는 프로토콜에서 교통신호제어기의 개폐 상태는 알 수 있지만 누가 어떤 목적으로 해당 제어기에 접근했는지는 알 수 없다는 점에 있다.[8]

제어기에 직접 접근하여 시도하는 공격은 노출의 위험도가 높지만, 비상시나 민방위 훈련 시 사용할 수 있는 수동 조작판을 이용하여 신호를 임의로 변경할 수 있듯 공격자가 충분히 접근 할 수 있는 공격 벡터이다.[9] 빠른 시간 내로 조치를 취하지 않는다면 신호가 임의 조작되어 교차로가 마비될 수 있으며 다른 교차로의 제어기와 상호 간의 정보교환을 하는 C-ITS 특성상 다른 교차로까지 피해가 확산될 우려가 있다.

2) 예방 및 대응 방안

제어기의 개폐 시 인증 절차를 추가하여 어떤 사용자가 어떤 목적을 가지고 제어기에 접근했는지 특정할 수 있어야 한다. 해당 제어기 관리자의 생체정보를 저장한 후 개폐 시 생체 인식 기술을 활용한 인증 절차(FIDO)를 통해 현재 제어기를 개폐하는 사람이 허가받은 관리자임을 특정할 수 있다.

중앙 센터에서 특정한 신호를 보낸 상태에서만 개폐하도록 하여 제어기의 개폐 상태의 변화를 중앙 센터에서 쉽게 감지할 수 있도록 하는 방법도 있다. 해당 절차들을 밟지 않고 강제로 개폐했을 경우에는 바로 중앙 센터에 경고를 알림과 동시에 시스템을 방어할 수 있도록 해야 한다.

3. V2X 통신 주파수 간섭

1) 공격 시나리오

ITS의 단방향 교통서비스의 한계를 보완하여 도입하는 것이 양방향 교통서비스 제공이 가능한 C-ITS이며, 이를 통해 주행 중 주변 차량 및 도로와 끊김 없는 상호 통신을 하여 교통정보를 교환 및 공유할 수 있다. C-ITS는 DSRC, WAVE, 이동통신(3G, LTE), WiFi 등 다양한 무선 통신 기술을 혼용해서 이용하는데, WAVE를 이용하고 있다는 것이 가장 큰 특징이다.

WAVE는 Wireless Access in Vehicular Environment의 약자로, IEEE 기술 표준이다. 이동성을 거의 충족시키지 못하며 주로 실내에서 사용하는 IEEE 802.11 a/g 와 달리 WAVE는 높은 이동성을 제공하고, 도플러 천이 등의 간섭이 잘 발생하는 실외 환경에 적합한 기술이며 통신 교환시간이 짧은 차량망(VANET) 에서 도로나 차량의 위험 상황을 특정 차량에 전달할 수 있다.

〈표 2〉 IEEE 1609.2에 적용되는 암호 알고리즘
〈Table 2〉 Encryption algorithm applied to IEEE 1609.2

Name	Function	Standard	Remarks
ECDSA	Digital Signature	FIPS 186-3	P-224, P-256
ECIES	Public-key cryptography	IEEE 1363a	P-256, SHA-256
AES-CCM	Symmetric-key algorithm	FIPS 197 NIST SP 800-38C	
SHA-256	Hash	FIPS 180-3	

WAVE 통신의 보안 표준은 1609.2 Security에 정의되어있으며, 공개키(Public Key)를 이용한 암호화 기법과 비 익명 인증(Non-anonymous Authentication) 기법을 이용한다. 하지만 사용자 보호를 위한 익명 인증 메커니즘에 관해서는 아직도 표준화가 진행중이므로 현재 대부분의 시스템엔 이 표준을 포함하고 있지 않다.

WAVE 통신 기술은 차량 주행과 안전성에 직결되는 문제이므로 스푸핑, 패킷 변조 등의 공격으로부터 메시지를 보호할 필요가 있다. WAVE의 현재 문제점은 보안 기능으로 인한 메시지 전송시간의 지연 가능성이다. 보안 처리를 통해 시간이 지연될 경우, 비정상적인 통신이 이루어질 수 있기 때문이다.

이에 대역폭에 맞는 전파를 이용한 재밍 공격 시나리오를 구상해볼 수 있다. 실외 환경에 최적화 되어있는 통신망이라 할 수 있지만, 무선 통신 특성상 불가능하지는 않다. 재밍 공격이 이루어 지면 차량과 차량 간의 통신 중 패킷이 손실되거나 지연될 가능성이 있다.

2) 예방 및 대응 방안

C-ITS 장비를 설치하기에 앞서, 주파수에 의한 공격을 막기 위해선 전파의 간섭이 있을 수 있는지 사전 환경조사가 필요하다. 국내 C-ITS 장비는 WAVE 통신뿐만 아니라, 여러 통신망을 혼용할 예정이며, 모두 무선통신을 이용하는 네트워크로 구성되어있다. 그러므로 주파수의 제약이 없는 깨끗한 환경에서 원활한 통신이 이루어져야 한다. 만약 전파의 간섭이 받는 환경이라고 한다면, 중앙 전파관리연구소에 전파간섭 사실을 신고해야 한다.

사전 조사뿐만 아니라 주기적으로 주파수 대역에 장애가 있는지 모니터링 할 수 있는 장비나 시스템 또한 필요하며, 무선통신 자체에 대한 보안에도 힘을 써야 한다. 공격자 입장에서 주파수 대역폭을 찾았다 하더라도, 그 정보를 획득하거나 변조하기 어렵도록 통신을 암호화해야 한다.

C-ITS 통신 기술에 보안 기능이 들어있어도 치명적인 문제가 되는 점은 메시지 지연 현상과 패킷 손실 가능성이다. 고속인 차량과 차량 간 혹은 도로 간의 정상적인 통신이 이루어져야 한다. 최대한 패킷 손실을 막으면서 원활한 통신이 가능하게 하는 명확한 표준 개정이 필요하다.

4. 장비 내부시스템 및 관리자시스템 접근

1) 공격 시나리오

C-ITS 장비 중 하나인 교통신호제어기와 같은 장비들은 주로 임베디드시스템을 사용한다. 여기서

발생 가능한 취약점은 메세지정보 누출(Message Information Leak)이다. 소프트웨어를 개발할 때 개발자가 프로그램상의 오류 검출을 위하여 테스트 용도로 사용 하거나, 개발에 사용되는 임베디드 하드웨어 자체의 기본적 환경에 의해 오류 발생 시 디버그 메시지(Debug message)가 출력되는데, 공격자는 이를 악용하여 해당 기기의 임베디드 환경에 대한 정보를 알아내고 그에 맞는 취약점을 공격, 해킹에 성공할 수 있다. 이는 지난 2012년에 처음 발생한 스마트 TV 해킹 사례에서도 실제로 사용된 취약점이다.[10]

공격자는 도로에 있는 C-ITS 장비에 유무선으로 연결한 후, 위와 같이 하드웨어에 기본으로 탑재되어있는 시스템의 취약점을 통해 시스템을 장악 할 수 있게 되며, 언제든 해당 망에 접근할 통로(백도어)를 만들어 정보를 수집하거나 신호 체계에 혼란을 야기 시킬 수 있다.

2) 예방 및 대응 방안

개발자의 보안의식 강화를 통해 디버그 메시지가 충분히 취약점으로 사용되어 질 수 있다는 점을 인지시켜 소프트웨어 개발이 끝나면 개발 시 사용했던 디버그 메시지가 출력되지 않도록 해야 한다.

Ⅲ. 결론

교통시스템과 같은 국가 주요 기반 시설은 사이버 공격으로 인해 가동이 중단될 경우 막대한 사회적, 경제적 손실을 유발한다. 많은 국민들이 일상생활에서 자동차, 철도 등 교통수단에 크게 의존하여 이동하고, 특히 C-ITS는 교통사고를 예방하는 기능을 하여 국민의 생명에도 직접적으로 영향을 미칠 수 있음에 따라 안전한 환경을 지원하는 차세대 지능형 교통 시스템(C-ITS)의 필요성은 더욱 증가하고 있다.

본 논문에서는 2016년부터 국내에서 활성화 될 예정인 C-ITS에서 발생할 수 있는 사이버 공격 시나리오를 연구하여 그 예방 및 대응 방안을 제시했다. 과거와 달리 많은 제어시스템의 환경이 개방형으로 변화했고, 다양한 서비스들을 제공하며 연계성이 높아지면서 보안 위협으로부터 취약한 접점들이 점차 많아지고 있는 상황이다. C-ITS는 제어시스템이 ITS센터 내부에 존재하는 폐쇄망 이라는 점, V2X 통신 중 발생할 수 있는 WAVE 주파수 간섭이 가능할 수 있다는 점 및 외부기기에 물리적인 접근이 가능하다는 점을 악용하여 공격이 이루어질 수 있다.

전 세계적으로 C-ITS를 교통 기술 발전의 새로운 진행 방향으로 인식하고 있으며, 여기에 보안적인 요소들을 분리할 수는 없다. 구축 단계에서부터 보안에 강화된 C-ITS를 만든 뒤에 평창올림픽 등 주요 시범 사업 등을 안전한 C-ITS 구축 및 서비스 기술의 발전 기회로 삼아 국내 전문가 양성과 산업 경쟁력을 증진시킬 필요가 있다.

REFERENCES

[1] H. Jo, “Status and Future Trend of Cooperative ITS(2012),” *Weekly technology trends of National IT Industry Promotion Agency*, vol. 1547, pp.1-25, May. 2012.

[2] The Korea Transport Institute, *C-ITS technical investigations and methods to introduce on domestic*, pp.183-184, 2013.

[3] M. Gyu, *‘C-ITS construction’ on development from this year*(2014), Retrieved Sep. 25, 2015, from http://www.koit.co.kr/.

[4] J. Moon, *C-ITS; the status and prospect*(2014), Retrieved Sep. 25, 2015, from http://www.its.go.kr.

[5] P. Cho, J. Lim and H. Kim, “A Study on the Improvement of Security Vulnerabilities in Intelligent Transport Systems,” *Journal of The Korea Institute of Information Security & Cryptology*, vol. 23, no. 3, pp.531-543, Jun. 2013.

[6] Special report team, *Korea Hydro & Nuclear Power(KHNP) Cyber attack scenarios*(2014), Retrieved Sep. 25, 2015, from http://http://www.

boannews.com/.

[7] M. Lee, *Security market for SCADA systems rise after KHNP situation…'Closed network being unsafe' awareness ↑*(2015), Retrieved Sep. 25, 2015, from http://www.ddaily.co.kr/.

[8] Intelligent Transport Society of Korea, *Variable Message Sign(VMS) System standards Part6. VMS-Center Information exchange*, 2013.

[9] National Police Agency, *Traffic Signal Controller Standard specifications*(2010), Retrieved Sep. 25, 2015, from http://www.police.go.kr.

[10] S. Lee, *Smart TV Security*(2013), Retrieved Sep. 25, 2015, from http://beistlab.wordpress.com.

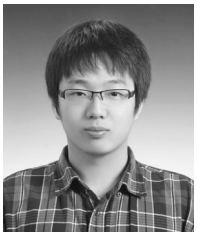
저자소개

장 윤 서 (Jang, Yoonsuh)
2015년 7월 ~ 현 재 : 한국정보기술연구원 차세대보안리더양성프로그램 Best of the Best 교육생
2015년 3월 ~ 현 재 : ISACA Korea Chapter 정보보호경영연구회 간사
2013년 3월 ~ 현 재 : 서울여자대학교 정보보호학과 학사과정 재학
e-mail : scintille@naver.com

이 동 섭 (Lee, Dong-Seob)
2015년 7월 ~ 현 재 : 한국정보기술연구원 차세대보안리더양성프로그램 Best of the Best 교육생
2012년 3월 ~ 현 재 : 부산대학 정보컴퓨터공학과 학사과정 재학
e-mail : dal4segno@gmail.com

안 소 희 (Ahn, So-Hee)
2015년 7월 ~ 현 재 : 한국정보기술연구원 차세대보안리더양성프로그램 Best of the Best 교육생
2011년 3월 ~ 현 재 : 동명대학교 정보보호학과 학사과정 재학
e-mail : conchiholic@naver.com

임 동 호 (Lim, Dong-Ho)
2015년 7월 ~ 현 재 : 한국정보기술연구원 차세대보안리더양성프로그램 Best of the Best 교육생
2015년 5월 ~ 현 재 : 경기지방경찰청 사이버명예경찰 누리캅스
2014년 1월 ~ 현 재 : 대한민국 육군 학사예비장교(KAOCS) 후보생
2013년 3월 ~ 현 재 : 강남대학교 컴퓨터공학과 학사과정 재학
e-mail : korea.devsec@gmail.com



신 정 훈 (Shin, Jeonghoon)
2015년 7월 ~ 현 재 : 한국정보기술연구원 차세대보안리더양성프로그램 Best of the Best 멘토
2012년 7월 ~ 2012년 3월 : Best of the Best 1기 수료, 정보보안최고인재 BEST 6
2006년 3월 ~ 2014년 8월 : 세종대학교 컴퓨터공학과 학사 수료
e-mail : sjh21a@gmail.com