情 報 保 護 學 會 誌
第22卷 第5號, 2012. 8

# AMI 보안 취약점 점검 항목에 관한 연구

김 신 규*, 전 유 석*, 서 정 택*

요 약

스마트그리드는 기존 전력망에 IT 기술을 융합한 차세대 전력망이다. 전력망에 IT 기술을 도입함으로써 운영효율이 증가하고 다양한 부가서비스가 창출되지만 반대로 사이버 보안위협은 증가하게 된다. 사이버 보안위협의 기술적 증가요인으로는 신재생에너지의 보급으로 인한 전력망 연결 접점 증가와 실시간·양방향 통신으로 인한 스마트그리드 기기 공격, 양방향 통신 프로토콜 공격 가능성 존재 등이 있다. 또한, 환경적 증가요인으로는 스마트그리드는 전력망 특성상 사고 발생시 피해 규모가 크므로, 상대국 및 테러집단에 의한 주요 공격대상이 되고 있다는 점이다. 본 논문에서는 이러한 스마트그리드 사이버 보안위협을 사전에 차단하기 위해, 스마트그리드의 핵심 기술이라 할 수 있는 AMI의 보안 취약점을 발견할 수 있는 현실적인 취약점 점검 항목을 제시한다.

## Ⅰ. 서 론

스마트그리드는 기존 전력망에 IT 기술을 융합한 차세대 전력망이다. IT 기술의 도입으로 인해, 운영효율이 증가하고 다양한 부가서비스가 창출되지만 반대로 사이버 보안위협은 증가하게 된다[1].

사이버 보안위협 증가요인은 풍력, 태양광 등 녹색기술인 신재생 에너지가 전력계통에 연계됨으로써 전력망 연결 접점이 많아지고, 기존 폐쇄적이던 전력망에 다양한 이해당사자가 참여하여 실시간·양방향 정보교환이 증가함에 따라, 스마트 미터 공격, 양방향 통신 프로토콜 공격 등 다양한 사이버 공격이 가능하기 때문이다. 이러한 기술적 원인 외에 환경적 원인도 존재한다.

전력망은 사고 발생시 피해가 크므로 사이버 전쟁 시 주요 공격대상으로 지목되어 왔으며, 2010년 스턱스넷(Stuxnet)이 발견된 이후 그 가능성은 더 높아지고 있다.

스턱스넷은 이란의 핵관련 시설에 대한 물리적 파괴를 위해 개발된 사이버 무기이다. 이로인해, 실제로 이란에서 1000여대의 원심분리기가 손상되는 피해가 발생하였으며, 이러한 사이버 무기가 스마트그리드를 대상으로 사용될 경우에는, 지난 2011년 9월 15일 발생한 순환정전사태와 비교할 수 없는 큰 피해가 발생할 것이다.

또한, 국외에서는 전력망에 대한 사이버 공격이 실제로 발생하고 있다. [표 1]은 전력망 및 스마트그리드에 대한 해킹 사례를 정리한 것이다.

〔표 1〕 전력망 및 스마트그리드 해킹사례

| 일자 | 주요 내용 | 출처 |
|---|---|---|
| 2007년 | 브라질의 2007년 대규모 정전사태가 전력망 해킹 사고로 인해 발생<br>- 700만 달러의 피해 발생 | 美 前 국가정보국장 마이크 맥코넬 |
| 2009년 3월 | 스마트 미터 해킹을 통한 운영센터 침입<br>- 광역 정전 가능성 확인 | 미국 CNN |
| 2009년 4월 | 미국 전력망 내에 중국·러시아 사이버 스파이가 설치한 것으로 추정되는 악성 프로그램 발견<br>- 유사시 전력망 마비 목적으로 추정 | 미국 CNN |
| 2009년 9월 | 스마트미터 취약점을 공격하는 웜·바이러스 전파 시뮬레이션<br>- 24시간만에 25000대 스마트 미터 감염 추정 | BlackHat 2009 |

본 논문에서는 스마트그리드에 대한 사이버 보안위협을 사전에 차단하기 위해, 현실성을 고려하여 스마트그리드의 핵심 기술이라 할 수 있는 AMI(Advanced Metering Infrastucture)의 보안 취약점 점검 항목을 제

본 연구는 2011년도 지식경제부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다.
(No. 2010101040046A)

* ETRI 부설연구소 (skkim, jys0710, seojt@ensec.re.kr)

시하고자 한다. 이를 위해 2장에서는 스마트그리드의 사이버 보안위협을 설명하고, 3장에서는 AMI 구성 및 기존 연구에 대해 설명하며, 4장에서 현실적인 AMI 취약점 점검 항목을 제안한다. 마지막으로, 5장에서는 추후 연구되어야 할 분야에 대해 제안한다.

## Ⅱ. 스마트그리드 사이버 보안위협

스마트그리드는 개방형 아키텍처를 가지고 있어 기존 전력망에 비해 전력망과 연결되는 단말장치의 수가 급증한다. 예를 들어, 우리나라 1,750만 가구에 스마트 미터가 설치되고, 공장 및 상업시설 등에도 스마트 미터가 설치된다는 점을 볼 때, 향후 전력망에 수천만대의 스마트 미터가 연결될 것이다. 또한, 전력 공급자와 소비자간 양방향 통신의 사용으로 인하여 스마트 미터에서 스마트그리드 운영센터로의 통신경로가 생기게 되며, 이를 통해 운영센터와 연결된 송·변전 시스템 등 기존 전력시스템에 접근할 수 있는 경로가 발생한다. 이로 인해, 스마트그리드에 연결된 수천만개의 스마트 미터를 이용한 DDoS 공격, 악성코드 확산 등의 사이버 공격이 가능하다.

이러한, 스마트그리드 특성을 고려할 때 스마트그리드에 대한 사이버 공격 가능성을 증가시키는 보안위협 요인으로는 양방향 통신 사용으로 인한 침투경로 제공, 상용제품 사용으로 인한 공개 취약점 발생, 일반인이 접근하기 쉬운 곳에 스마트그리드 접근을 위한 경로 노출, 스마트그리드 기기간 상호 연결로 인한 통신 복잡도 증가 및 물리적으로 광범위하게 분산되어 설치되는 스마트그리드 장비가 있다. 각각의 보안위협에 대한 세부내용은 [표 2]와 같다.

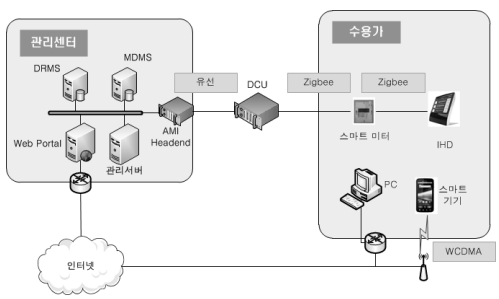
〔표 2〕 스마트그리드 사이버 보안위협 증가 요인

| 보안위협 | 설명 |
|---|---|
| 양방향 통신기술 사용으로 인해 보안위협 증가 | 스마트그리드는 스마트 미터기, 전력공급업체, 관리업체 사이에 양방향 통신기술을 사용(불법적인 데이터 위·변조 공격으로 전력계통 운영 방해나 과금정보 조작을 통한 금전적 피해 발생 가능) |
| 상용 하드웨어와 소프트웨어 사용 증가 | 스마트그리드는 시스템정보 및 취약점이 외부에 노출되는 상용 기술을 많이 사용하여 기존 전력망에 비해 보안위협 증가 |
| 소비자단에서 스마트그리드 시스템으로의 수많은 접점 | 수천만대의 스마트 미터, 전기차 등이 전력망에 연결되므로 인해, 소비자단에서 스마트그리드 시스템으로 접근 가능한 지점이 대폭 증가 |
| 스마트그리드 기기간 상호연결 증가 | 지능화된 서비스 제공을 위해 기존 수직적 통신 구조를 벗어나, 주변의 스마트그리드 기기와 통신을 수행하는 등 상호연결성 증가로 인해 위험관리가 어려움 |
| 광범위한 지역에 분산된 스마트그리드 장비 | 스마트 미터, 배전 센서 등의 스마트그리드 장비가 광범위한 지역에 물리적으로 산재하여 위험관리 및 보안관제가 어려움 |

## Ⅲ. 관련 연구

### 3.1 AMI 구성

AMI는 크게 3가지 구성 요소를 가진다. 관리센터에는 전력검침정보를 관리하는 MDMS(Metering Data Management System), 실시간 요금을 관리하는 DRMS(Demand-Response Management System)가 위치하고, 수용가에는 전력사용량을 검침하는 스마트 미터(Smart Meter), 전력사용량을 사용자에게 알려주는 IHD(In-Home Display) 등이 위치한다. 이 둘 사이에는 여러 스마트 미터로부터 정보를 수집하여 관리센터에 전달해 주는 DCU(Data Concentration Unit)가 위치한다[2][3].




〔그림 1〕 일반적인 AMI 구성도

일반적으로 수용가에서는 설치의 편리성을 위해 근거리무선통신 표준인 Zigbee 및 무선 Mesh 네트워크, 전력선 통신인 PLC(Power Line Communication)를 주로 사용하고, DCU와 관리센터 간에는 유선통신, WCDMA(Wideband Code Division Multiple Access), WiMAX(Worldwide Interoperability for Microwave Access), GPRS(General Packet Radio Service)를 주로 이용한다. 본 논문에서는 AMI의 가장 일반적 구성인 수용가 영역은 Zigbee 통신, DCU와 관리센터 구간은 유선

〔표 3〕 AMI 장치별 CPU 및 OS 사양

| 장치 | CPU | OS | 기타 |
|---|---|---|---|
| 스마트 미터 | ARM 계열 | 임베디드 OS | 저전력, 저 연산능력 |
| DCU | ARM 계열 | 임베디드 OS | 저전력, 중 연산능력 |
| MDMS, DRMS | 서버급 | Solaris, Linux, Windows | 고 연산능력 |

을 사용하는 구성에 대해 취약점 점검 항목을 제시한다.

AMI를 구성하는 각 장치의 소프트웨어, 스마트 미터와 DCU는 ARM CPU 기반의 저전력 하드웨어로 구성되며, 운영체제는 임베디드 OS 특히, 임베디드 리눅스를 주로 사용한다. MDMS, DRMS는 일반 서버급 하드웨어와 운영체제 사양을 가진다. 그 세부내용은 [표 3]과 같다.

### 3.2 AMI 취약점 관련 연구

2011년 InGuardians 社에서는 AMI 공격 방법이라는 주제로 문서를 발표하였다[5]. 이 문서에서는 AMI 환경에서 발생가능 한 취약요소를 18종으로 분류하고 각 취약요소에 대해 설명하였다. 제시한 취약요소는 통신관련 평문전송, 보안성 없는 적외선통신 사용, 하드웨어 접근을 통한 정보취득, 암호알고리즘 및 암호키 관련 취약점, 인증 취약점 등이 있다. 각각의 취약요소에 대한 설명은 [표 4]와 같다.

## Ⅳ. AMI 취약점 점검 항목

AMI의 주요 구성요소인 스마트미터, DCU는 주로 임베디드 시스템을 사용하고 있어, 기존 IT 시스템에 대한 취약점 점검에 비해 물리적 접근을 통한 취약점 점검과 Zigbee 등의 근거리무선통신 취약점 점검이 추가적으로 필요하다. 하지만, 일부 취약점 점검을 위해서는 고가의 전용 장비가 필요하며, 일주일 이상의 장시간 점검이 요구되기도 한다. 그러므로, 실질적으로 주어진 시간(일주일 이내) 내에 취약점 점검을 수행하는 것은 장비적, 시간적 제약이 따른다. 이러한 문제점을 해결하기 위해, 본 장에서는 쉽게 구입가능한 장비들을 선정하고 해당 장비를 이용해 단기간 내에 점검할 수 있는 AMI 취약점 점검항목에 대해 제시하고자 한다.

AMI 취약점 점검에 필요한 장비는 크게 하드웨어 정

〔표 4〕 AMI 취약요소

| 취약요소 | 설명 |
|---|---|
| 암호화되지 않은 통신 | AMI 통신 데이터를 암호화하지 않고 평문으로 전송 |
| 하드웨어 통신정보 가로채기 | 하드웨어에 접근하여 EEPROM으로부터 직접 정보를 획득하거나, SPI(Serial Peripheral Interface), I2C(Inter Integrated Circuit) 버스(Bus)로부터 통신 정보를 획득 |
| 부적절한 암호기술 사용 | 키 생성알고리즘 취약점, 키스트림 재사용 문제, Replay 공격 취약점, 취약한 암호알고리즘 사용, 부적절한 무결성 검사, 짧은 키 사용, 부적절한 IV(Initial Vector) 사용 등 |
| 직접적인 하드웨어 접근 | 직접적인 하드웨어 접근을 차단하기 위한 Tamper-Protection 기능에 취약점이 존재하여 하드웨어에 직접 접근 가능 |
| 저장된 키와 패스워드 취약점 | 인증, 암호화, 무결성 검증을 위해 키와 패스워드가 미터에 저장됨 |
| 암호키 분배 취약점 | 훔친 키나 검증되지 않은 인증서로 통신 내용을 복호화 가능 |
| 안전하지 않은 인터페이스 | 적외선 통신과 같은 경우 짧은 통신 거리를 가지기 때문에 다른 통신 방식에 비해서 덜 위험할 것이라고 생각하여 공격 대비 미흡 |
| 미터 인증 취약점 | 스마트 미터와 NAN 장치 사이의 인증에는 다양한 절차가 존재하므로, 잘못된 Nonce 값 선택, Replay 공격, 서비스거부 공격으로 인한 메모리고갈 등 발생가능 |
| NAN 기기 인증 취약점 | NAN 장치가 스마트미터의 인증을 받는 절차에 취약점 존재이 존재하여, 미터 인증 취약점과 동일한 취약점 발생 가능 |
| 펌웨어 구현 취약점 | 펌웨어의 구현상의 오류는 공격의 대상이 될 수 있으며, 대표적인 공격으로 Buffer overflow, Off-by-one overwrite, Format String, integer Overflow 공격이 있음 |
| DNS 취약점 | 스마트그리드 환경에서 사용되는 Name Resolution 기법에 Name server DoS 공격, Meter name resolution cache poisoning, Response manipulation through race condition exploits 등의 취약점 존재 가능 |
| 취약한 기본 설정 정보 | 일부 기기들은 보안 설정을 사용자에게 위임하고 있어 적절한 환경 설정이 이루어 지지 않는 기기들은 공격에 노출 가능 |
| 통신경로 취약점 | 통신 경로를 정할 때 악의적인 공격자가 중간에 자신을 거치게 만들어 MITM(Man-In-The-Middle) 공격 가능 |
| 서비스 거부 공격 취약점 | DoS(Denial of Service) 공격을 발생시켜, 리소스를 독점하거나 다른 사용자의 이용을 방해 가능 |
| 정보 누출 취약점 | 일부 통신에서 특정 정보(헤더, 트레일러, 인증) 등을 평문으로 전송하여 정보가 유출 가능하고, 특정 정보(가전제품의 종류, 이용패턴등)는 개인 프라이버시를 침해 가능 |
| 고정된 인증값 사용 취약점 | 변경되지 않는 고정된 인증값(인증서, 암호키)을 사용할 경우 이를 이용한 공격 가능 |
| 난수 생성기 취약점 | 난수 생성기술은 무결성, 기밀성을 보장하기 위한 중요한 기술이나 RNG(Random Number Generation)을 구현하는 것은 어려움 |
| 시간 서비스 취약점 | Network Time Protocol(NTP), Global Positioning System(GPS) 취약점을 이용하여 예기치 않은 펌웨어 업데이트, 검침정보의 무결성 문제 등 발생 가능 |

보 취득, 무선통신 정보 취득 및 해킹, 시스템 해킹으로 분류할 수 있다. 시스템 해킹의 경우 기존 IT 시스템 취약성 분석 도구와 동일하며, 무선통신의 경우 Zigbee에 특화된 장비가 필요하다[6]. 하드웨어 정보 취득의 경우 임베디드 시스템 디버깅 관련 장비를 요구한다. 이를 고려해 선별한 AMI 취약점 점검 장비는 [표 5]와 같다.

선정한 AMI 취약점 점검 장비와 점검 소요시간을 고려할 때, AMI 취약점 점검 항목은 다음과 같이 도출할 수 있다.

취약점 점검 항목은 크게 물리적 접근을 통한 취약점과 네트워크 접근을 통한 취약점으로 구분된다. 물리적 접근의 경우 스마트그리드 장치에 물리적으로 접근하여 정보를 추출하는 취약점으로, 물리적으로 쉽게 접근가능 한 위치에 설치되는 스마트 미터, DCU가 해당된다. 네트워크 접근은 데이터 통신을 통해 발생 가능한 취약점으로, 기존 IT 시스템에 존재하는 취약점 외에 Zigbee 관련 취약점, 스마트 미터와 DCU 특징에 따른 특화 취약점으로 구분할 수 있다.

스마트 미터에 대한 물리적 취약점 점검 항목으로는 물리적으로 접근이 가능한지, 가능할 경우 정보를 추출할 수 있는지와 관리용 포트를 통해 관리 프로그램 접근이 가능한지 확인하는 항목이 있다. 네트워크적 취약점 점검 항목으로는 Zigbee 통신에서 키 교환시 정보 탈취, 시퀀스(Sequence) 넘버 조작을 통한 재전송

〔표 5〕 AMI 취약점 점검 장비

| 목적 | 장비 | 설명 |
|---|---|---|
| 하드웨어 정보 취득 | Beagle I2C/SPI Protocol Analyzer | I2C/SPI 프로토콜 분석기 |
| | Aardvark I2C/SPI Host Adapter | I2C/SPI 명령 주입기 |
| | JTAG In Circuit Debugger | JTAG 포트 연결 장치 |
| 무선통신 정보 취득 및 해킹 | USRP(Universal Sofrware Radio Peripheral) | 소프트웨어 기반 무선통신 분석 도구 |
| | Daintree Sensor Network Analyzer | Zigbee 프로토콜 분석 도구 |
| | KillerBee | Zigbee 해킹 지원 도구 |
| | AVR RZ Raven USB Stick | KillerBee 프로그램 구동 Zigbee 장치 |
| 시스템 해킹 | Nessus | 시스템 취약점 점검 스캐너 |
| | MetaSpolit | 시스템 취약점 이용 침투 도구 |
| | Paros | 웹 응용프로그램 해킹 지원 도구 |

〔표 6〕 AMI 취약점 점검 항목

| 대상기기 | 구분 | 취약점 분류 | 취약점 세부분류 |
|---|---|---|---|
| 스마트 미터 | 물리적 접근 | Tamper Protection 공격 | |
| | | Data bus Sniffing | |
| | | 메모리덤프 | |
| | | 디버깅 정보 추출 | |
| | | 관리용 통신포트 접근 | 적외선, 시리얼 등 관리용 통신포트 접근 |
| | 네트워크 접근 | Zigbee 통신 공격 | 키 교환시 정보 탈취 |
| | | | 재전송(Replay) 공격 |
| | | | 재밍(Jamming) 공격 |
| | | | PAN 코디네이터 위장공격 |
| | | 관리 S/W 공격 | 인증우회 |
| | | | 불법명령 전송 |
| | | | 설정정보(비밀키 등) 열람 |
| | | 응용 프로토콜 공격 | 불법 전원차단 명령 |
| | | | 악성 펌웨어 업데이트 |
| | | 스마트미터 공격 | 임베디드 시스템 취약점 |
| | | | 응용프로그램 취약점 |
| | | 타 시스템 공격 | DCU 공격 경로 활용 |
| | | | 다른 스마트미터 공격 경로 활용 |
| DCU | 물리적 접근 | Tamper Protection 공격 | |
| | | Data bus Sniffing | |
| | | 메모리 덤프 | |
| | | 디버깅정보 추출 | |
| | | 관리용 통신포트 접근 | 시리얼, 이더넷 등 관리용 통신포트 접근 |
| | 네트워크 접근 | Zigbee 통신 공격 | 키 교환시 정보 탈취 |
| | | | 재전송(Replay) 공격 |
| | | | 재밍(Jamming) 공격 |
| | | 관리 S/W 공격 | 인증우회 |
| | | | 불법명령 전송 |
| | | | 설정정보(비밀키 등) 열람 |
| | | 응용 프로토콜 공격 | 불법 제어명령 |
| | | | 악성 펌웨어 업데이트 |
| | | DCU 공격 | 임베디드 시스템 취약점 |
| | | | 응용프로그램 취약점 |
| | | 타 시스템 공격 | MDMS, DRMS 시스템 공격 |
| | | | 다른 DCU 시스템 공격 |
| MDMS/DRMS | 네트워크 접근 | 스마트 기기 서비스 공격 | 응용프로그램 취약점 |
| | | | 인증우회 |
| | | | 불법제어 명령 |
| | | MDMS, DRMS 공격 | 시스템 취약점 |
| | | | 응용프로그램 취약점 |
| | | 응용 프로토콜 공격 | 불법 제어명령 |
| | | | 악성 펌웨어 업데이트 명령 |
| | | 타 시스템 공격 | DCU 공격 경로 활용 |
| | | | 스마트미터 공격 경로 활용 |

(Replay) 공격, 무선 통신을 방해하는 재밍(Jamming) 공격, Zigbee 코디네이터 관련 공격과 스마트 미터 관리용 프로그램의 취약점에 대한 점검과 스마트 가전 기기 전원제어 및 펌웨어 업데이트 관련 프로토콜 취약점, 스마트 미터 운영체제 및 응용프로그램에 대한 취약점, 타 시스템 공격 경로로의 활용 가능 취약점으로 구분할 수 있다.

DCU의 경우 취약점 점검항목은 스마트 미터와 유사하다. 이는 스마트 미터와 DCU가 유사한 하드웨어와 운영체제를 가지기 때문이다. 이로 인해 DCU는 스마트 미터와 물리적 취약점 점검항목은 동일하며, Zigbee의 경우 DCU가 Coordinator 역할을 수행하여, 관련 취약점 이 제외된다. 관리 S/W 공격, 응용 프로토콜 공격, DCU 공격은 대상이 스마트 미터에서 DCU로 변경되며, 타 시스템 공격은 DCU의 네트워크 위치에 따라 대상 MDMS, DRMS, DCU로 달라진다.

MDMS, DRMS의 경우 일반 IT 시스템 취약점이 동일하다. 단, 스마트폰 등의 스마트 기기를 위한 서비스가 추가적으로 제공되어 관련 취약점 점검 항목이 추가되며, 응용 프로토콜 공격과 타 시스템 공격 대상이 변경된다.

이러한 내용을 세부적으로 정리하면 [표 6]과 같다.

## Ⅴ. 결 론

우리나라는 2020년 광역단위, 2030년 국가단위 스마트그리드 구축을 목표로 정책을 추진하고 있다. 이에 따라 2020년까지 광역단위 스마트그리드 구축을 위해 많은 투자가 이루어 질 것으로 예상된다. 하지만, 스마트그리드는 기존 전력망에 비해 효율성이 증가하는 반면에 사이버 보안위협에 더 많이 노출됨으로 인해, 스마트그리드가 구축되기 전 사이버 보안 취약점을 제거하는 것이 매우 중요하다. 이를 위해서는 스마트그리드에 대한 취약점 점검 항목을 식별하고 이에 대해 취약점 존재여부를 점검하는 것이 필요하다.

본 논문에서는 시간적, 장비 제약이 존재하는 현실을 반영하여 취약점 점검 도구를 선정하였으며, 이를 이용하여 점검가능한 스마트그리드 AMI의 핵심 구성요소인 스마트 미터, DCU, MDMS, DRMS에 대한 취약점 점검항목을 제시하였다.

앞으로 AMI 외에 전기자동차, 신재생에너지 시스템, 마이크로그리드 등 스마트그리드 전체에 대한 취약점 점검항목에 대해 추가 연구가 필요하며, 최종적으로는 취약점 점검항목 연구결과를 바탕으로 스마트그리드 각 시스템의 특성을 반영한 취약성 분석 방법론을 연구하는 것이 필요하다.

## 참고문헌

[1] 이건희, 서정택, 이철원, “스마트그리드 사이버 보안 추진 현황”, *정보보호학회지*, 20(5), pp. 7-13, 2010. 10.

[2] KEPCO, “KEPCO T&D New Products”, KEPCO, pp. 11, 2011. 01.

[3] 이일우, 이정인, “스마트그리드 정보통신기술”, *한국통신학회지*, 27(11), pp. 3-11, 2010. 10.

[4] 최재덕, 서정택, 이철원, “제주 스마트그리드 실증단지 보안대책 현황”, *정보보호학회지*, 20(5), pp. 14-19, 2010. 10.

[5] Justin Searle, “Advanced Metering Infrastructure Attack Methodology”, BlackHat EU 2011, 2011. 3.

[6] Joshua Wright, “KillerBee: Practical Zigbee Exploitation Framework”, ToorCon11, 2009. 10.

## 〈著者紹介〉


사 진

**김 신 규 (Sin-Kyu Kim)**
정회원

2000년 2월: 연세대학교 기계전자공학부 졸업
2002년 2월: 연세대학교 컴퓨터과학과 석사
2007년 8월: 연세대학교 컴퓨터과학과 박사수료
2003년 12월~현재: ETRI 부설연구소 선임연구원/스마트그리드보안팀장
<관심분야> 스마트그리드 보안, 국가기반시설 보안, 취약점 분석

사 진

**전 유 석 (Yu-Seok Jeon)**
정회원

2007년 8월: 인하대학교 컴퓨터공학과 졸업
2010년 2월: 포항공과대학교 정보통신학과 석사
2010년 2월~현재: ETRI 부설연구소 연구원
<관심분야> 취약성 분석, 스마트그리드 보안

사 진

**서 정 택 (Jung-Taek Seo)**
정회원

1999년 2월: 충주대학교 컴퓨터공학과 졸업
2001년 2월: 아주대학교 컴퓨터공학과 석사
2006년 2월: 고려대학교 정보보호대학원 정보보호공학과 박사
2000년 11월~현재: ETRI 부설연구소 선임연구원/스마트그리드보안연구실장
<관심분야> 스마트그리드시스템 및 통신보안, 제어시스템 보안, 취약성 분석평가, DDoS 공격탐지 및 대응