情 報 保 護 學 會 誌
第21卷 第7號, 2011. 10

스마트그리드 보안위협 및 보안 요구사항 분석

이 건 희*, 서 정 택**, 박 응 기***

요 약

최근 세계 각국의 전력산업에서 가장 큰 이슈가 되고 있는 스마트그리드는 정보통신 기술의 도움을 받아 고도로 지능화되고 자동화된 전력 운영 시스템이다. 전력사용의 효율성을 높이기 위해서 수용가와의 정보교환이 증가하고, 고객의 편의를 위해서 전기차, 수요반응 등 새로운 서비스가 증가했다. 이를 위해서 스마트그리드는 기존의 전력 시스템과 달리 다른 시스템과의 상호 연계성이 증가하고, 외부 시스템으로의 개방성 또한 높아졌다. 하지만 보안 관점에서는 외부 연계 증가 및 상호작용의 증가로 인해 보안위협이 증가하게 되는 문제가 발생했다. 스마트그리드는 국가주요기반시설 중 하나로 침해사고 발생 시 그 피해는 국가 전반에 걸쳐 발생할 것이다. 따라서 스마트그리드 구축에 있어 사이버 보안성 확보가 중요한 요소 중 하나이다. 이에 본 고에서는 스마트그리드의 주요 보안위협을 살펴보고, 보안위협을 제거하기 위해 필요한 보안 요구사항을 분석하도록 한다.

Ⅰ. 서 론

최근 컴퓨터 기술의 급속한 발전으로 인해 기존의 텍스트 위주의 사용자 환경에서 벗어나 이미지, 그래픽, 오디오 및 비디오 데이터 등을 제공하는 멀티미디어 사용자 환경으로 변환하고 있다.

기후변화 문제에 대한 대응책으로 세계 각국은 CO_2 발생 저감을 위해 노력하고 있다. 특히 전력 분야에서는 전력 사용 효율화, 신재생 에너지 활용 증가, 전기차 인프라 확보 등을 통해 전기 생산 감소, 화석 에너지 사용 감소 등을 유도함으로써 세계의 기후변화에 대한 대응 노력에 함께 하고자 하고 있다.

스마트그리드는 전력 분야의 이러한 노력을 지원하기 위한 지능화된 전력 시스템으로 발전 · 송전 · 배전 · 변전 시스템의 효율화와 소비자의 적극적인 참여를 유도하여 에너지 소비를 최소화할 수 있으며, 신재생 에너지를 이용한 발전설비의 안정화를 통해 신재생 에너지원 활용 비율을 늘리고, 전기차 및 충전 인프라를 활성화하여 CO_2 생산의 주범인 화석에너지를 사용하는 자동차의 이용 비율을 줄일 수 있다.

이를 위해 스마트그리드 시스템은 다양한 운영시스템과 단말기기 등이 상호 연계하여 유기적으로 동작되어야 한다. 특히, 소비자 영역에서 사용된 전력 사용 정보가 운영시스템으로 전송 되거나, 운영시스템에서는 소비자 영역으로 부하제어 또는 수요반응 신호를 송신하는 등 기존에는 분리되었던 일반 소비자 영역의 네트워크와 운영시스템의 네트워크가 연계되는 사례가 증가하게 된다.

이러한 전력 시스템 운영의 변화는 기존의 접근이 제한된 전력시스템에 비해 보다 많은 보안 위협을 발생시킬 수 있다. 특히 누구나 쉽게 접근할 수 있는 소비자 영역의 기기는 네트워크로 연결되어 있는 운영시스템으로 침투할 수 있는 연계점이 될 수 있어 기존에 없었던 큰 보안 위협이 될 수 있다.

2009년 CNN의 미국 전력망 악성코드 감염 사태 보도, 2009년 주요 해킹 컨퍼런스에서 스마트 미터 해킹 기법 발표, 2010년 스턱스넷(Stuxnet) 발견, 2011년 두쿠(Duqu) 발견 등의 일련의 사태는 스마트그리드에 대한 보안위협이 증가하고 있음을 방증한다[1-4]. 더불어 해커들의 기반시설에 대한 해킹 시도가 증가하고 있으

본 연구는 2010년도 지식경제부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구과제입니다. (2011101050001A)
* ETRI 부설연구소(icezzoco@ensec.re.kr)
** ETRI 부설연구소(seojt@ensec.re.kr)
*** ETRI 부설연구소(ekpark@ensec.re.kr)

며, 스턱스넷 및 두쿠 등의 정밀한 악성코드가 발견되고 있는 것은 향후 사이버전에서 전력망이 제1목표로 대두되고 있음을 방증하기도 한다.

전력망은 국가의 기반이 되는 시설로써 이러한 보안 위협으로 인해 테러 등과 같은 사이버 보안 침해사고가 발생될 경우 적절한 전력 공급을 하지 못해 국가 전체가 혼란에 빠질 수 있어 스마트그리드에 대한 보안이 무엇보다 중요하다. 사이버 공격으로 전력 공급이 중단될 경우 지난 9월 순환정전 사태보다 더욱 심각한 피해를 입게 될 것이다. 이에 미국 및 유럽 선진국에서는 스마트그리드에 대한 보안대책 마련을 서두르고 있다[5].

따라서 본 고에서는 스마트그리드 시스템, 기기, 네트워크의 사이버 보안 대책 마련을 위한 첫 단계로 스마트그리드 보안위협을 분석하고, 정의된 보안위협을 차단함으로써 안전한 스마트그리드 구축에 이바지 할 수 있도록 보안 요구사항을 식별한다.

Ⅱ. 스마트그리드

스마트 그리드는 전력망에 정보통신 기술을 접목한 새로운 형태의 전력 공급시스템이다. 기존의 전력 공급 시스템이 발전소에서 가정에 이르기까지 일방통행으로 이루어져 있었는데 비해, 스마트 그리드는 전력 공급을 위해서 전력 공급시스템과 사용자가 양방향으로 의사소통하는 시스템이다[6]. 공급자는 실시간으로 전력 사용 정보를 제공하여 사용자의 의사에 따라 전력 사용 시간과 양을 제어할 수 있게 한다. 즉, 각 가정의 개별 전자제품의 전력 소모량과 이로 인한 탄소배출량 등을 사용자가 직접 확인할 수 있게 된다.

스마트 그리드 환경에서는 각 가정과 건물이 실시간으로 에너지 사용량을 확인할 수 있어 언제 사용량이 폭증하며 어느 시간 때에 사용량이 줄어드는 지를 확인할 수 있다[7]. 또한 태양광 패널·연료전지·배터리 시스템 등 분산된 에너지 공급원을 활용해 전력 사용 피크 때를 대비해 에너지를 확보할 수 있으며 연료전지 및 소형 발전기 등을 상황에 따라 자동적으로 가동할 수 있도록 해준다. 이를 위해서 수요가 폭증할 때 가동되는 에너지 집약 설비의 가동을 차단하거나 늦추는 등의 수요 절감기술을 활용하기도 한다.

스마트 그리드 환경은 기존에 단순히 전력 소비만을 하던 소비자가 자신의 상황에 따라 전기를 공급하는 소규모 공급자가 될 수도 있게 한다. 태양광 발전으로 축전된 전기를 공급할 수 있도록 하는 분산전원 기술[8], 전기 자동차에 충전된 전력을 수요 피크 시 사용하거나 전력망에 되파는 'V2G(Vehicle-to-Grid)' 기술 등이 이러한 생각을 가능하게 한다[9].

스마트 그리드는 다양한 목적에 의해 연구 개발이 시도되어 왔다. 유럽의 경우 신재생 에너지 자원을 활용한 전력원이 발달하면서 이를 최대한 활용하기 위한 계통 운영 시스템이 필요하게 되었고 이를 위해 스마트 그리드를 연구하기 시작하였다[10]. 미국은 다양한 중소규모 정전 사태에 대응하기 위해서 노후한 설비의 최신화 및 디지털화를 꾀하기 위해서 스마트 그리드 연구를 수행하기 시작하였다[11].

특히 미국의 경우 2003년 발생한 북동부 대규모 정전사고로 인해 스마트 그리드 연구에 더욱 박차를 가하게 되었고[12], 2007년에는 에너지 안보법 (Energy Independence and Security Act of 2007, EISA 2007)을 제정하였다[13]. 이 법안은 스마트 그리드, 에너지 안보, 에너지 절약 등과 관계된 연구 개발 및 시작 적용을 유도하는 내용이다.

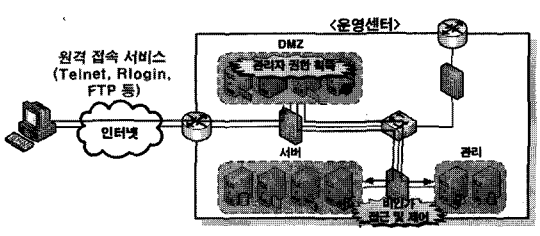
Ⅲ. 스마트그리드 보안위협

본 장에서는 스마트그리드 환경에서 발생할 수 있는 대표적인 보안위협에 대해서 분석한다.

3.1 운영센터 보안위협

3.1.1. 원격접속 서비스 운영에 따른 위협

[그림 1]에서 설명하는 바와 같이 운영센터의 내부 네트워크 장비 및 시스템에 기본으로 설정된 서비스를 수행하거나 Telnet, FTP 등과 같은 불필요한 원격 접속 서비스들을 허용할 경우, 공격자가 구성설정 및 불필요



[그림 1] 원격 접속 서비스 및 구성 설정 취약점을 이용한 보안위협 개념도

한 원격 접속 서비스의 취약점을 이용해 스마트그리드 운영을 위한 네트워크에 침입할 수 있다.

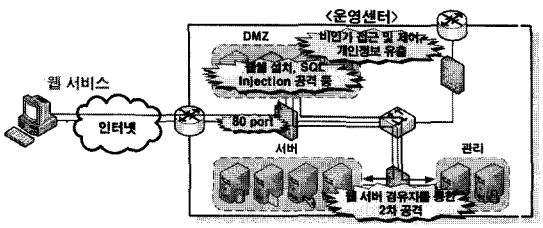
또한 시스템 유지·관리를 위해 인터넷 등 운영센터 외부 네트워크에서 시스템 접속을 허용하는 경우, 취약한 계정 관리나 원격 서비스 취약점을 이용해 운영센터 내부로 침입할 수 있다.

3.1.2. 웹 서비스 운영에 따른 위협

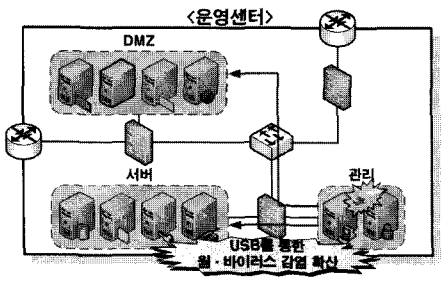
일반적으로 웹 서비스는 사용자가 접근하기 쉽고 취약점이 널리 알려져 있으므로 침해사고에 노출될 위험성이 크다. 스마트그리드 운영정보 제공을 위한 웹 서비스 운영 시 웹 해킹에 대한 보안대책이 미비한 경우, 침입차단시스템 등에서 허용된 포트(80, 8080, 8088 등)를 통해 웹쉘(WebShell) 설치, SQL Injection 공격 등을 수행하여 서버 제어, 악성스크립트 삽입, 서버 및 DB 시스템 개인정보 유출 등의 공격들이 가능하다. [그림 2]는 이와 같은 보안위협을 이용한 공격의 예를 설명하고 있다. 침해된 웹 서버는 운영센터의 다른 시스템들을 침입하기 위한 경유지로 활용될 수 있다.

3.1.3. 운영센터 시스템 악성코드 감염 위협

운영센터 내 시스템들이 바이러스 백신 소프트웨어



〔그림 2〕 웹 서비스 운영에 따른 보안위협 개념도



〔그림 3〕 USB 메모리 사용에 따른 웜·바이러스 확산 개념도

에 의해 보호되지 않을 경우, USB 메모리 등을 통한 웜·바이러스 감염 시 운영센터 전체로 확산될 수 있다. 운영센터가 완전하게 물리적으로 분리되어 운영되는 경우 또는 연계 접점에 대한 보안대책이 안전한 경우에도 운영센터 내부에서 USB 메모리 등 보조기억매체 사용에 따른 웜·바이러스 감염 위협에 노출될 수 있다. [그림 3]은 운영센터 내부에서 USB 메모리를 통한 악성코드 감염 및 확산에 대해 설명하고 있다.

3.1.4. 운영센터 내 인터넷 사용으로 인한 위협

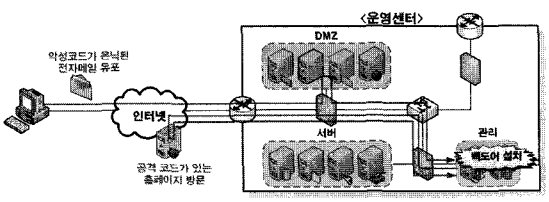
운영센터에서 내부 직원이 인터넷을 통한 전자메일 및 웹 서비스를 이용할 경우, 악성코드가 은닉된 전자메일 및 취약점을 가진 웹 브라우저를 통해 백도어 등이 설치되어 감염된 운영센터 내 PC를 해킹 경유지로 활용하여 운영센터 전체에 대한 공격이 가능하다. [그림 4]는 운영센터의 컴퓨터에서 인터넷을 사용하여 악성코드가 설치되는 사례를 설명하고 있다.

3.1.5. 잘못된 네트워크 구성 및 정책

운영센터 네트워크를 관리영역, 서버영역, DMZ영역 등으로 분리하지 않거나 분리된 영역 간 적절한 접근제어를 수행하지 않을 경우, 운영센터가 보안위협에 노출되었을 때 운영센터 전체로 피해가 확산될 수 있다. 또한 운영센터 내 라우터, 스위치와 같은 네트워크 구성 장치의 잘못된 설정 및 정책으로 운영센터 내·외부의 불필요한 데이터가 유입될 수 있고, 이로 인해 운영센터 주요 웹 서비스 접속 장애, 실시간 전력거래정보 전송 지연 등과 같은 네트워크 장애를 유발할 수 있다.

3.1.6. 잘못된 정보보호시스템 정책

침입차단시스템, 침입방지시스템, VPN(Virtual Pri-



〔그림 4〕 운영센터 내 인터넷 사용에 따른 보안위협 개념도

vate Network) 장비와 같은 정보보호시스템들의 잘못 구성된 설정 및 정책으로 인하여 운영센터 내부 네트워크 침입 경로가 발생할 수 있다. 정보보호시스템들의 설정 및 정책의 악의적인 변경에 대한 백업 대책이 없을 경우, 사고 발생 시 스마트그리드 운영 복구를 위한 즉각적인 대응이 어려울 수 있다.

3.2 운영센터 연계구간 보안위협

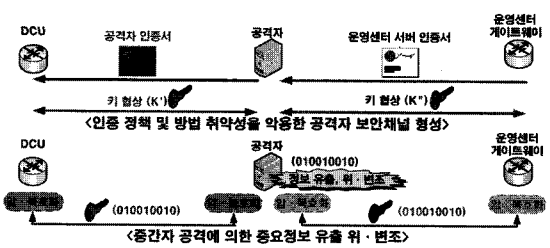
3.2.1. 연계구간 보안채널 형성 시 중간자 공격

운영센터 연계구간에서 안전한 데이터 전송을 위한 IPSec(Internet Protocol Security), SSL(Secure Socket Layer)/TLS(Transport Layer Security)와 같은 보안채널 형성 시 상호 인증이 안전하게 이루어지지 않을 경우, 보안채널 형성과정에서 [그림 5]에서 설명하고 있는 중간자(MITM, Man-in-the-Middle) 공격에 의해 중요정보 유출, 불법 위·변조, 삭제 공격이 가능하다. 특히 SSL/TLS 보안채널 형성 시 중간에서 공격자가 위조된 서버 인증서를 클라이언트에게 전송하여 중간자 공격이 가능한 취약점이 이미 공개되었다[14-15].

3.2.2. 연계구간 중요정보 유출 및 위·변조 위협

운영센터 연계구간에서 전력운영정보, 기간시스템 제어명령 및 감시정보의 불법 수집 및 조합을 통한 분석 결과를 추후 스마트그리드 운영 장애 공격을 위한 중요 정보로 악용할 수 있다. 또한 운영센터 연계구간에서 개인 전력정보의 불법 수집 및 조합을 통한 유출로 개인정보보호 침해가 발생할 수 있다.

운영센터 연계구간 통신매체에 제3자가 무단으로 접근할 수 있다면, 운영센터 연계구간에서 전력운영정보, 제어명령 및 감시정보가 권한이 없는 제3자에 의해 불법 위·변조 및 삭제될 수 있다. 이 위협을 이용하여 공격할 경우 스마트그리드의 실시간 전력 거래를 방해하거나, 심한 경우 스마트그리드 운영 장애를 유발할 수 있다. 특히 AMI 운영센터와 스마트 미터 간 연계구간에서 전력 사용정보를 불법 조작할 경우 스마트그리드 전력 거래의 신뢰성을 떨어뜨릴 수 있다.



[그림 5] 중간자 공격 개념도

3.2.3. 스마트그리드 기기를 통한 운영센터 불법 접근

기기 인증 및 접근제어를 완벽하게 수행하지 않을 시에 불법 조작된 기기나 기기를 가장한 PC와 같은 정보기기를 이용하여 운영센터로 침투할 수 있다.

3.2.4. 스마트그리드 기기 불법 제어

운영센터에 침입한 공격자가 스마트 미터와 같은 기기에 불법 제어 명령어를 전달하여 스마트그리드 수용가에 대한 임의의 전력 차단과 같은 위협을 가할 수 있다.

3.3 스마트그리드 기기 보안위협

3.3.1. 낮은 기기 성능으로 인한 위협

스마트그리드 환경에서는 전력수급상태 정보 수집, 전력설비 상태정보 수집, 전력설비 제어, 전력공급 등을 위해 다양한 기기가 설치된다. 스마트 미터, 데이터 수집기(DCU, Data Collector Unit), 스마트 가전, 전기차, 전기차 충·방전장치, 정보수집 센서, 풍력·태양력 발전기기 등이 그 예이다. 이러한 기기들은 성능 및 비용 문제로 암호 알고리즘을 적용하지 않거나 낮은 보안 강도의 암호 알고리즘을 적용할 수도 있다. 이 경우 공격자는 해당 기기들을 주요 공격 대상으로 삼을 수 있고, 해당 기기가 공격을 받게 되면 연계된 네트워크를 통해 운영센터로 침투할 수 있기 때문에 결국 스마트그리드 전체의 보안성이 낮아질 수 있다.

3.3.2. 기기 불법 접근

다양한 유·무선 통신 환경에서 운영되는 기기들에 대한 사용자 인증 및 접근통제가 이루어지지 않을 경우, 공격자에 의한 전력차단 등의 기기조작이나 전력요금 조작 등의 금전적 피해가 발생할 수 있다. 특히 스마트

미터의 경우 해당 기기에 대한 전력차단 등의 기기조작 뿐만 아니라 전체 소비자단 전력망에 대한 웜·바이러스, DDoS(Distributed Denial of Service) 등과 같은 대규모 공격으로 전개될 수 있다.

또한, 기기에 물리적으로 접근하여 기기의 암호 키를 추출하거나 운영체제, 펌웨어를 변조한 경우 기기의 악의적인 동작으로 인하여 운영센터나 기기 네트워크에 위협이 전이될 수 있다.

3.3.3. 기기 내 중요정보 유출, 위·변조 및 삭제

스마트 미터나 데이터 수집기와 같은 기기에 저장되는 전력 관련 정보가 보호되지 않을 경우, 해킹을 통해 기기 내 저장된 개인 전력정보 유출을 통한 사생활 침해 및 전력사용량 위·변조, 삭제를 통한 불법 전력 사용이 가능하다.

Ⅳ. 보안 요구사항

본 장에서는 앞서 언급한 스마트그리드 주요 보안위협을 제거하기 위한 스마트그리드 보안 요구사항에 대해서 분석하도록 한다.

4.1 관리적 보안 요구사항

4.1.1. 정보보호체계 수립

운영센터의 정보보호 업무를 책임지고 체계적으로 수행하기위하여, 정보보호 업무를 총괄하는 정보보호 담당자를 지정해야 한다. 운영센터 정보보호 담당자는 정보보호 현황 분석, 정보보호 대책 수립, 보안관제, 침해사고 대응 및 복구 등의 담당 업무를 총괄 운영 및 관리한다. 또, 운영센터는 정보보호 담당자가 수행해야 할 업무를 규정하고, 정보보호 담당자는 업무 내용 및 결과를 문서화(전자문서 포함)하여 보관 및 관리한다.

4.1.2. 보안관제 수행

운영센터는 운영센터가 관리하는 네트워크, 정보시스템에 외부 침입 사실을 감시할 수 있는 관제시스템을 설치·운영하여 외부로부터의 침입에 신속히 대응할 수 있어야 한다. 또한 운영센터에 대한 사이버 공격에 즉시 대응하기 위하여 실시간 보안관제를 수행해야 한다.

운영센터의 보안관제 활동은 다음과 같은 공격 여부를 주기적으로 점검하고 대응할 수 있도록 해야 한다.

- o 정보시스템 악성 코드 감염 여부
- o 인가받지 않은 자료 접근 및 유출, 훼손
- o 서비스 거부 공격

운영센터의 보안관제 인력은 침해사고 유형별 예상 징후와 이에 수반하는 피해 증상 및 대응요령을 숙지해야 한다.

4.1.3. 침해사고 대응계획 수립 및 시행

침해사고를 인지한 구성원이 침해사고에 신속하게 대응할 수 있도록, 침해사고 대응계획을 수립하고 시행해야 한다. 침해사고 대응계획에는 침해사고 확인 절차, 침해사고 응급조치 절차, 침해사고 보고 절차, 침해사고 복구 절차 등이 포함되어야 한다.

수립된 침해사고 대응계획을 시행함에 있어 운영센터 내 부서 및 업무 담당자 별 역할과 책임을 지정하여 침해사고에 유기적으로 대응할 수 있도록 한다. 또한 침해사고 징후가 있거나 발생한 경우 침해사고 대응센터에 즉각 연락하고 침해사고 대응계획에 따라 대응 및 복구를 수행한다. 침해사고 대응이 종료된 후, 침해사고에 대한 대응활동의 세부내역이 포함된 보고서를 작성하여, 문제점 해결 및 침해 대응 방법 개선의 자료로 활용해야 한다.

4.1.4. 보조기억매체 보안

운영센터가 완전하게 물리적으로 분리 운영 및 연계 접점에 대한 보안대책이 안전한 경우에도, 운영센터 내부에서 USB 메모리 등 보조기억매체 사용에 따른 웜·바이러스 감염 시 운영센터 전체로 확산 될 수 있으므로, 보조기억매체 관리를 수행해야 한다.

이를 위해서 운영센터는 보안적합성이 검증된 보조기억매체 통제시스템을 운영하거나, 물리적으로 보조기억 매체를 사용할 수 없도록 조치한다. 인가된 보안 USB 및 보조기억매체를 사용하기 위해서는 사용자 식별 및 인증이 필요하다. 또한 각 구성원이 인가된 보조기억매체를 정보시스템 또는 기기에 연결 할 경우, 보조

기억매체에 저장되어 있는 데이터를 안티 바이러스 제품을 사용하여 검사함으로써 최소한의 보안조치를 취하도록 해야 한다.

4.1.5. 개인정보보호

개인정보보호에 대한 관리 책임자 부재 시 개인정보 관리 소홀에 의한 개인 정보 분실, 도난, 누출, 변조 또는 훼손의 가능성이 있으므로, 개인정보보호 관리 책임자를 지정한다. 지정된 개인정보보호 관리책임자를 통해 운영센터 및 스마트그리드에서 취급되는 모든 개인정보는 통제 및 관리되어야 한다.

4.2 기술적 보안요구사항

4.2.1. 안전한 네트워크 구성

운영센터와 인터넷이 연결된 망과 접점이 존재할 경우, 공격자가 접점을 경유지로 하여 운영센터 내부로 침입할 수 있으므로, 인터넷과 연결된 망과 물리적으로 연결을 차단해야 한다. 이와 더불어 운영센터 정보시스템들을 기능, 보안 중요도에 따라 서버영역, DMZ영역, 관리영역 등의 별도 서브넷으로 구성하여 접근제어를 수행해야 한다. 운영센터 네트워크를 관리영역, 서버영역, DMZ영역 등으로 분리하지 않거나 분리된 영역 간 적절한 접근제어를 수행하지 않을 경우, 스마트그리드 운영센터가 보안위협에 노출되었을 때 운영센터 전체로 피해가 확산될 수 있으므로, 운영센터 네트워크 접근제어를 수행해야 한다.

운영센터 네트워크를 영역에 따라 구분하여 구성한 경우, 각 서브넷 간은 엄격한 접근제어를 수행할 수 있도록 해야 한다. 업무상 필요한 서브넷 간의 통신을 제외하고는 원칙적으로 통신을 제한하고, 네트워크 단위의 통신 제한보다는 시스템 및 서비스 단위에서의 접근제어를 수행해야 한다. 특히 제어시스템 등의 중요 시스템이 포함된 서브넷은 접점에 침입차단시스템을 구성하고, 제한된 시스템 및 서비스에 한정하여 통신을 허용한다.

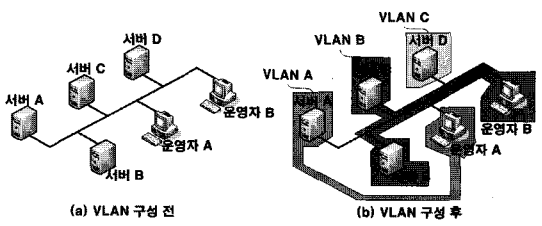
물리적인 서브넷 구성이 어렵거나 서브넷 구성의 보조 수단으로 VLAN (Virtual LAN) 설정을 통하여 운영센터의 시스템 운영에 필요한 시스템 간에만 통신이 가능하도록 설정함으로써 보안 안전성을 향상시킬 수 있다. [그림 6] (a)는 물리적으로 하나의 네트워크에 모든 서버와 운영자 PC가 구성된 형태로써, 임의의 한 시스템이 다른 모든 시스템에 접근이 가능하다. [그림 6] (b)와 같이 하나의 물리적 네트워크이지만, 상호 통신 및 연동이 필요한 시스템들만을 동일한 하나의 VLAN으로 구성하고, 서로 다른 VLAN들 간에는 통신을 제한함으로써 3개의 네트워크를 별도로 구성한 것과 같은 효과를 가진다.

또한 운영센터 내에 Wi-Fi 등과 같은 무선 네트워크를 구성할 경우, 무선 네트워크는 인터넷이 연결된 망 등과 연결될 수 있으며, 보안 설정이 미비할 경우 전파 범위 내에서 누구나 접근이 가능하므로, 무선 네트워크 사용을 금지해야 한다.

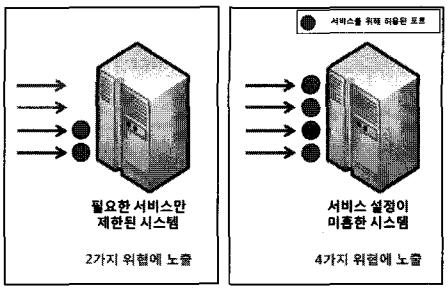
4.2.2. 정보시스템 접근제어

사이버 공격은 시스템의 각종 서비스, 응용 프로그램 등의 취약점을 이용하여 이루어지므로 시스템 운영과 관리에 필요한 최소한의 서비스만 제공하여 위협을 최소화해야 한다. [그림 7]에서 보는 바와 같이 서비스 개수에 비례해 시스템의 위협은 증가하거나 감소하게 된다.

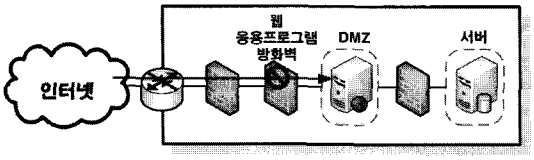
웹 서비스는 외부로 제공되는 경우가 많아 외부에서의 침입경로가 될 가능성이 높으나, 침입차단시스템 등의 일반적인 정보보호시스템으로는 탐지와 차단이 어려우므로 웹 응용프로그램에 대한 보안대책을 별도로 수



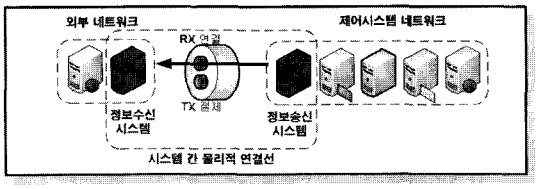
〔그림 6〕 VLAN 구성에 의한 접근제어 개념도



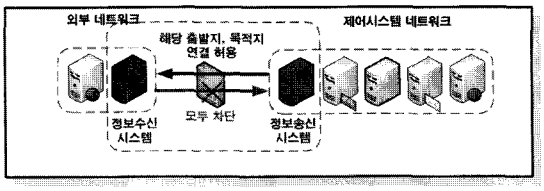
〔그림 7〕 서비스 관리 필요성



〔그림 8〕 웹 응용프로그램 방화벽 개념도



〔그림 9〕 물리적 일방향 통신 개념도



〔그림 10〕 논리적 일방향 통신 개념도

립·시행해야 한다. [그림 8]에서 웹 응용프로그램 방화벽을 통해 웹 서비스를 보호하는 방법의 개념에 대해 설명하고 있다.

웹 서버는 외부 네트워크와의 접점인 DMZ 구간에 위치하는 경우가 많아 외부에서의 주 공격 대상이므로, 반드시 웹 응용프로그램의 취약점을 제거하여야 한다. 웹 응용프로그램 취약점 공격은 정상적인 서비스 제공을 위하여 침입차단시스템 등에서 허용된 포트(e.g 80(HTTP), 8080, 8088 등)를 이용하여 이루어지기 때문에 기존의 일반적인 침입차단시스템 외에 웹 응용프로그램 방화벽을 추가로 구성하여 보호하는 것을 고려하도록 한다.

4.2.3. 전력제어시스템 보호

스마트그리드 운영에 있어 제어시스템은 매우 중요한 위치를 차지한다. 각 센서 및 기기로부터 수집된 정보를 바탕으로 운영에 필요한 결정을 하기 위한 정보로 가공을 하며, 경우에 따라서는 제어명령을 통해 설비 및 기기를 조작할 수도 있기 때문이다. 공격자가 제어시스템을 장악하게 되면, 스마트그리드 전반에 걸친 서비스를 제어할 수도 있는 상황에 이르게 되므로 소규모의 정전 또는 전국단위의 정전 등과 같은 피해가 발생할 수 있다.

따라서 제어시스템은 일반 서비스용 네트워크 등과 회선을 분리해 안전하게 보호되어야 한다. 이 경우 VPN 등을 이용한 동일 회선 내 논리적 알고리즘을 이용한 분리는 허용되지 않으며, MSPP(Multi-service Provisioning Platform) 등의 물리적 기술을 이용하여 하나의 회선을 여러 통신채널로 분리하여 사용하는 것은 가능하다.

제어시스템의 운영정보를 다른 네트워크에서 필요할 경우, 침입 경로를 원천적으로 차단하면서 자료를 전달하기 위하여 일방향 통신을 이용하여 연계하는 것이 좋다. 일방향 통신을 위해 물리적 일방향 통신과 논리적 일방향 통신 방법을 사용할 수 있지만, 물리적 일방향 통신 방법을 사용할 것을 권장한다. [그림 9]에서 설명하고 있는 물리적 일방향 통신은 제어시스템 네트워크에서 외부 네트워크로의 통신선은 있으나, 외부 네트워크에서 제어시스템 네트워크로의 통신선은 절체된 통신을 의미하며, [그림 10]에서 설명하고 있는 논리적 일방향 통신은 침입차단시스템을 이용하여 제어시스템의 특정 정보시스템에서 외부 네트워크의 특정 정보시스템으로의 통신만을 허용하는 통신을 의미한다.

4.2.4. 통신 보호

운영센터 내 정보시스템과 외부 시스템 간 통신 시 종단간 암호화 통신을 수행하여 통신 내용이 노출되거나 위·변조되는 것을 방지해야 한다. 이를 위해서는 안전하면서도 시스템 특성에 적합한 암호 알고리즘을 선택하여 적용하는 것이 필요하다.

현재 국내외 스마트그리드 표준화 및 기술 개발에서 주로 다루어지는 암호 알고리즘은 다양하다. [표 1] 각 표준에서 주로 다루어지고 있는 알고리즘을 나열하고 있다. 해당 알고리즘 중 국내에서 개발한 알고리즘은 ARIA, HAS-160, KCDSA, EC-KCDSA와 같으며, 이 외의 알고리즘은 국제표준이다.

HOMQV와 같이 현재 규격에서 제시하고 있는 암호 알고리즘보다 향상된 성능 및 보안성을 제공하는 암호 기술이 지속적으로 제안되고 있다[16]. 또한 해킹 등 공격위협 다양화 및 지능화로 인해 강화된 보안기술 적용

〔표 1〕 스마트그리드 암호알고리즘 목록

구분		암호알고리즘
대칭키 암호 알고리즘		AES, ARIA
해시함수		HAS-160, SHA-1/224/256/384/512
공개키 암호 알고리즘	인수분해	RSA
	이산대수	DSA, KCDSA, DH, MQV
	타원곡선	ECDSA,EC-KCDSA, ECDH, ECMQV

〔표 2〕 보안강도를 만족하기 위한 알고리즘 별 키 길이

보안강도		112bits	128bits
대칭키 암호 알고리즘		-	128bits
인수분해 방식		2048bits	3072bits
이산 대수 방식	공개키	2048bits	3072bits
	개인키	224bits	256bits
타원곡선 방식		224-225bits	256-383bits

이 요구될 것으로 예상되며 이로 인한 시스템의 성능 저하를 막기 위해서는 보다 고성능의 암호기술 적용이 요구된다. 따라서 국내 스마트그리드 구축 환경에 최적화된 암호기술에 대한 지속적 연구 개발 및 수용이 이루어져야 할 것이다.

암호 알고리즘 사용의 안전성을 보장하기 위하여 스마트그리드 시스템 및 기기에 적용되는 암호 알고리즘들은 일정 수준의 보안강도를 만족해야 한다. 미국 국립표준기술연구소(NIST, National Institute of Standards and Technology)에서는 2011년부터 2029년까지 128비트 이상의 대칭키 암호 알고리즘과 112 비트 이상의 공개키 암호 알고리즘 사용을 권장하고 있다[17-18]. 따라서 현재 구축되는 스마트그리드 시스템 및 기기는 최소 128bit 수준 이상의 보안강도를 지니는 알고리즘을 사용해야 한다. [표 2]는 보안강도 128bit를 만족하기 위한 알고리즘 별 키 길이를 나타낸다.

4.2.5. 시스템 및 기기 인증

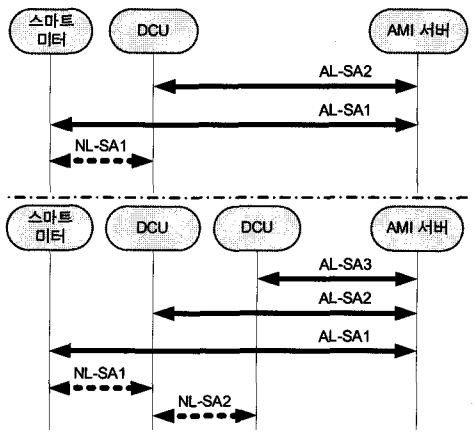
스마트그리드 환경에서 시스템 및 기기 인증은 네트워크 레벨 인증과 응용 레벨 인증으로 분류할 수 있다.

네트워크 레벨 인증(NL-SA, Network Level-Security Association)은 비인가 기기들의 통신 경로 중간 지점에서 특정 기기 및 시스템을 통해 네트워크에 접속하는 행위를 차단하는 암호학적 접근제어 방법이다. 예를 들어, 스마트 미터와 DCU 사이의 무선 통신 구간에서 비인가 시스템이 스마트 미터로 위장하여 DCU를 통해 AMI 서버에 접근 시도 또는 AMI 네트워크에 유해 트래픽을 발생 시킬 수 있다. 이러한 이상행위를 차단하기 위해 스마트그리드 네트워크에서 DCU와 같은 연계장치는 네트워크 레벨의 인증을 수행하고 MAC (Message Authentication Code)값을 사용하여 접근제어를 수행한다.

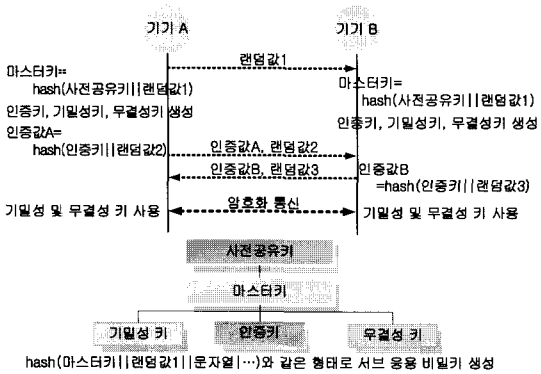
응용 레벨 인증(AL-SA, Application Level-Security Association)은 스마트그리드 기기 단에서 운영기관 서버 단으로 전달되는 전력 관련 데이터들을 보호하기 위해 상호 인증하는 과정이다. 응용 레벨 인증을 수행하는 통신 객체는 데이터 보호를 위한 무결성 및 기밀성 비밀키 교환에 앞서 상호 인증 과정을 수행한다.

스마트그리드 환경에서 시스템 및 기기의 네트워크 구성에 따라 네트워크 레벨 인증과 응용 레벨 인증을 모두 수행해야 하는 경우가 있으며, 이 경우 기기 성능을 고려하여 중복된 인증 절차 등에 대해 효율적인 인증 과정을 고려해야 한다. 예를 들어 AMI 네트워크에서 스마트 미터의 경우, 스마트 미터와 DCU 간에 네트워크 레벨 인증이 요구되며 스마트 미터와 AMI 서버 간에 응용 레벨 인증이 요구된다. 스마트 미터에서는 두 번의 인증 절차 수행으로 암호학적 연산량 및 인증 절차에 따른 추가 전력 소모가 예상된다. [그림 11]은 상기 예를 설명한다.

사전공유키 기반으로 시스템 및 기기를 인증할 경우,



〔그림 11〕 네트워크 및 응용 레벨 인증 구간 예



〔그림 12〕 공유비밀키 기반 계층적 비밀키 생성 구조 예시

시스템 및 기기에 오프라인으로 공유키가 설정되어야 하며, 사전공유키를 인증용도로 직접 사용해서는 안 된다. 사전공유키는 기기 설치 시 설정되는 가장 중요한 최상위 비밀키이므로 최대한 안전성을 보장하기 위해 설정 과정과 사용 측면에 있어서 외부 유출 가능성을 최소화해야 한다.

사전공유키 자체를 직접 사용할 경우 그 사용 빈도수가 높아져 유출 가능성이 높아지므로 인증, 데이터 무결성·기밀성 용도를 위한 각각의 응용 비밀키를 계층적으로 생성하여 사용해야 한다. [그림 12]는 사전공유키 기반 계층적 비밀키 생성 구조에 대한 예시이며, 네트워크, 서비스, 기기 특성을 고려하여 변경될 수 있다.

4.2.6. 기기 보호

스마트그리드 기기의 유·무선 로컬 인터페이스를 통해 공격자가 기기에 침투하는 것을 차단하기 위해 기기 접근 시 사용자를 인증해야 한다. 스마트그리드 기기에는 점검, 업데이트, 수리 등의 작업을 위해 현장 작업자에게 허용된 유·무선 로컬 인터페이스가 존재하므로, 공격자는 이를 통한 기기 접근 시도를 할 수 있다. 허용되지 않은 공격자가 기기에 접근하는 것을 막기 위해 로컬 인터페이스를 통한 데이터 송·수신 작업을 할 경우, 기기가 작업자를 인증하도록 한다. 예를 들어, 작업자가 유지보수용 기기를 스마트그리드 기기에 연결할 경우 두 기기 간 인증 절차를 수행하도록 할 수 있다.

4.2.7. 기기 펌웨어 및 소프트웨어 설치 보안

스마트그리드 기기에서 동작하는 펌웨어 및 응용 소프트웨어 등은 개발 당시 고려하지 못한 취약점이 설치 후 발생할 가능성을 항상 가지고 있다. 따라서 이러한 취약점 발견시 즉시 업데이트하여 안전하게 스마트그리드를 운영할 수 있도록, 스마트그리드 기기 펌웨어 및 소프트웨어 업데이트 기능이 포함되어야 한다.

펌웨어 및 소프트웨어는 배포 전 보안 취약성 분석을 면밀히 수행하고, 기능 검사를 수행하여, 설치(업데이트) 후 오동작하거나 보안 취약점이 발견되는 문제가 발생하지 않도록 한다.

2009년 7월 BlackHat USA에서 스마트 미터에서 작동하는 웜을 개발하고, 이를 스마트 미터 펌웨어 원격 업데이트 기능을 이용해 전파시키는 공격방법을 소개했다. 이와 관련하여 펌웨어 및 소프트웨어가 원격으로 배포될 경우, 해당 프로그램의 배포자와 배포 시스템을 인증하도록 한다. 배포되는 펌웨어 및 소프트웨어의 위변조를 방지해 무결성 보장을 위해 펌웨어 및 소프트웨어에 대한 암호화(또는 서명)된 검증코드를 함께 배포한다.

4.2.8. 스마트그리드 기기 데이터 보호

스마트 미터, 미터 데이터 수집기, 배전망 센서 등 스마트그리드 기기들은 공개된 장소에 설치되고, 물리적으로 완벽하게 보호되지 않아 임의의 공격자가 물리적인 접근을 통해 무단으로 데이터를 취득할 수 있다. 따라서 기기 별 기능에 따라 필수 저장 데이터를 식별하고, 식별된 데이터만 기기에 저장한다.

예를 들어, 스마트 미터에는 전기 사용량 및 실시간 가격 정보 등의 전기사용 정보는 저장 가능하나, 소비자 식별 가능한 개인 정보는 저장하지 않아야 한다.

또한, 스마트그리드 기기의 메모리는 데이터베이스 기능으로 사용되어서는 안 되며, 데이터 백업 및 서비스 효율성 제고를 위한 임시 저장소 개념으로 사용한다.

V. 결 론

본 고에서는 스마트그리드의 보안 위협을 분석하고, 각 보안위협을 해소하기 위한 보안 요구사항을 분석하였다. 본 논문에서 제시된 요구사항이 스마트그리드를 보다 안전하게 보호하여 국가안보 능력 향상에 큰 기여를 할 수 있을 것으로 기대된다.

향후 스마트그리드 사업자들은 "지능형전력망 구축 및 이용촉진에 관한 법률"에 따라 스마트그리드의 사이

버 안전성 확보를 위한 보안대책을 수립해야 한다. 본 고에서 제시한 보안위협 및 보안 요구사항은 각 사업자들이 보안대책을 수립하는데 도움이 될 것이다.

참고문헌

[1] Electric Utilities May Be Vulnerable to Cyberattack, CNN, April 2009. http://www.washingtonpost.com/wp-dyn/content/article/2009/04/08/AR2009040803904.html?referrer=emailarticle

[2] M. Davis, "Smart Grid Device Security : Adventures in a new medium", BlackHat USA 2009, July 2009.

[3] N. Falliere. L.O. Murchu, E. Chien, "W32.Stuxnet Dossier," Symantec Security Response, November 2010.

[4] N. Falliere. L.O. Murchu, E. Chien, "W32.Duqu : The precursor to the next Stuxnet," Symantec Security Response, November 2011

[5] NIST, "Guidelines for Smart Grid Cyber Security", NIST IR 7628, August 2010.

[6] E.W. Gunther, A. Snyder, G. Gilchrist, D. R. Highfill, "Smart Grid Standards Assessment and Recommendations for Adoption and Development", Technical Report, EnerNex Corporation, Feb. 2009

[7] D. von Dollen, "IntelliGrid Consumer Portal Telecommunications Assessment and Specification", EPRI Technical Report, Dec. 2005.

[8] UK Department of Trad and Industry, "Meeting the Energy Challenge: A White Paper on Energy", DTI Report, pp.14-15, May 2007.

[9] J. Tomic, W. Kempton, "Using Fleets of Electric-drive Vehicles for Grid Support", Journal of Power Sources, Elsevier, Vol. 168, Iss. 2, pp.459-468 Jun. 2007.

[10] A. Battaglini, J. Lilliestam, C. Bals, A. Haas, "The SuperSmart Grid", European Climate Forum, Jun. 2008.

[11] K.R. Nahigian, "The Smart Alternative: Securing and Strengthening Our Nation's Vulnerable Electric Grid", The Reform Institute, Jun. 2008.

[12] B. Pfundt, "Smart Grid: Fewer Blackouts, More Greenbacks For The Northwest", Climate Solutions Journal, Aug. 2005.

[13] F. Sissine, "Energy Independence and Security Act of 2007: A Summary of Major Provisions", CRS Report for Congress, Dec. 2007.

[14] P. Burkholder, "SSL Man-in-the-Middle Attacks", SANS Institute InfoSec Reading Room, February 2002.

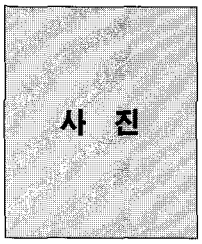
[15] M. Eriksson,"An Example of a Man-in-the-Middle Attack Against Server Authenticated SSL-sessions", International Conference on Applied Cryptography and Network Security, October 2003.

[16] S. Halevi, H. Krawczyk, "One-Pass HMQV and Asymmetric Key-Wrapping," Public Key Cryptography 2011, LNCS, Vol. 6571, pp.317-334, 2011.

[17] E. Barker, W. Barker, W. Burr, W. Polk, M. Smid, "Recomendation for Key Management - Part 1: General," NIST SP 800-57, May 2011.

[18] E. Barker, A. Roginsky, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths," NIST SP 800-131A, January 2011.

〈著者紹介〉



이 건 희 (Lee, Gunhee)
정회원
2001년 2월 : 아주대학교 정보및 컴퓨터공학부 졸업
2003년 2월 : 아주대학교 정보통신 전문대학원 정보통신공학과 석사
2009년 2월 : 아주대학교 정보통신 전문대학원 정보통신공학과 박사
2009년 3월~현재 : 한국전자통신 연구원 부설연구소 연구원
관심분야 : 스마트그리드 보안, 제어시스템 보안, 유무선 네트워크 인증 및 키 관리

서 정 택 (Seo, Jungtaek)
정회원
1999년 2월 : 충주대학교 컴퓨터 공학과 졸업
2001년 2월 : 아주대학교 컴퓨터 공학과 석사
2007년 2월 : 고려대학교 정보경 영공학전문대학원 정보보호 박사
2001년~현재 : 한국전자통신연구 원 부설연구소 선임연구원/과제책 임자
관심분야 : 스마트그리드 시스템 및 통신 보안, 제어시스템 보안, 제어시스템 통신 프로토콜 보안, 취약성분석 평가, DDoS공격 탐지 및 대응

박 응 기 (Park, Eungki)
정회원
1986년 2월 : 중앙대학교 전자계 산학과 졸업
1988년 2월 : 중앙대학교 전자계 산학과 석사
2005년 2월 : 아주대학교 컴퓨터 공학과 박사
1988년~1999년 : 한국전자통신연 구원 선임연구원
2000년~2002년 : (주)니츠 기술 이사
2002년~현재 : 한국전자통신연구 원 부설연구소 책임연구원/실장
관심분야 : 보안관제, 스마트그리 드 시스템 및 통신 보안, 제어시스 템 보안, DDoS공격 탐지 및 대응