情 報 保 護 學 會 誌
第20卷 第3號, 2010. 6

스마트 그리드의 취약성, 특성, 설계 원칙 및 보안 요구사항 분석

전 용 희*

요 약

기존의 전력망에 정보기술(IT)을 융합하여 전력 공급자와 소비자가 양방향 통신을 통하여 생산과 소비 효율을 최적화할 수 있는 스마트 그리드가 개발되고 있다. 그러나 전력망에 IT 기술이 융합되면서 정보통신 인프라에서 발생하고 있는 보안 문제가 전력망에서도 그대로 재현되고 있다. 스마트 그리드와 같은 제어 시스템 보안 기술은 기존의 IT 보안 기술과는 특성상 여러 가지 차이점이 존재한다. 따라서 전력 인프라에 대한 사이버 공격을 방지하고 대응하기 위하여 보안 기술이 개발단계 초기부터 고려될 필요가 있다. 본 논문에서는 국가 주요 정보하부구조를 구성하게 될 스마트 그리드의 취약성, 특성, 보안 필요성과 요구사항 및 네트워크 설계 원칙 등에 대한 분석 결과를 제시한다.

Ⅰ. 서 론

전력망에 통신망을 접목시켜 전력계통시스템의 제어를 통하여 발전·송전·변전·배전의 전 과정에 대한 통제가 가능하여 지고, 결과적으로 에너지 사용의 효율성을 높이고자 하는 것이 에너지 인터넷이라고 불리는 스마트 그리드(Smart Grid)의 목표이다[1,2]. 즉 기존 전력망에 정보기술(IT)을 융합하여 전력 공급자와 소비자가 양방향으로 실시간으로 정보를 교환함으로써 에너지 효율을 최적화하는 차세대 전력망이라고 할 수 있다. 그러나 모든 IT 융합에서와 마찬가지로, 스마트그리드 역시 사이버 보안문제가 해결되어야 한다[3].

스마트 그리드의 통신 방식은 BPL(Broadband over Power Line), WiFi, WiMax, 3G 셀룰라, TDMA/CDMA, VSAT(Very Small Aperture Terminal) 위성과 같은 여러 형태의 무선망 및 고속 인터넷 백본망, 전력선(PLC: Power Line Carrier) 통신, RFID(Radio Frequency IDentification) 통신 같은 통합된 통신 형태가 될 것이다[4]. 이런 다양하게 서로 연결된 통신망이 취약점을 유입 시킬 수 있다.

스마트 그리드의 효과적인 운용을 보장하는 사이버 보안의 역할에 대하여 미국의 에너지 성(DOE) 에너지 부문 계획에 문서화되어 있다. 미국의 국가 하부구조 보호 계획(NIPP: National Infrastructure Protection Plan)에 의하면 사이버 보안은 다음과 같이 정의된다[4]:

"기밀성, 무결성 및 가용성을 보증하기 위하여 전자정보 및 통신 시스템과 서비스(그리고 그 속에 포함된 정보)에 대한 손상, 권한이 없는 사용 및 남용을 방지하고, 필요한 경우, 복구까지를 포함 한다".

그리드에 대한 위험 요소는 다음과 같다[4]:

- 그리드의 복잡성이 취약성을 도입할 수 있고, 잠재적인 공격 노출 및 비고의적 에러를 증가시킬 수 있다.
- 상호 연결된 네트워크가 통상적인 취약성을 도입할 수 있다.
- 통신 붕괴에 대한 취약성 및 서비스 거부(DoS: Denial of Service) 공격이나 소프트웨어 및 시스템 무결성을 침해할 수 있는 악성 소프트웨어 유입의 가능성을 증대시킨다.
- 잠재적인 공격을 위한 진입점과 경로의 수가 증가한다.
- 고객의 비밀성을 포함하여 데이터 기밀성의 침해가 가능하다.

시스코사에서 보는 스마트 그리드에 대한 정보보호

* 대구가톨릭대학교 컴퓨터정보통신공학부(yhjeon@cu.ac.kr)

필요성은 다음과 같은 요인에서 지적하고 있다[5,6].

- 그리드 하부구조와 IP-기반 유선 및 무선망과의 혼합
- 지능형 계량기, 센서, 원격 검침 및 제어 시스템 같은 새로운 네트워크 종단점의 유입
- 입상적(granular) 접근 정책 및 고용원, 계약자 및 소비자와 같은 원격 사용자 그룹을 위한 제어에 대한 요구 증가
- 사이버 위협을 은폐하기 위한 위협 기술의 진화
- 규제적 컴플라이언스 요구사항

미국 DOE에서도 현대적인 그리드를 도입하는데 해결해야 할 기술적인 장벽 중에 보안 기술을 명시하고 있다[7]. 특히 분산 에너지 자원 소유주, 독립 전력 생산자, 소비자의 수요 대응 및 자동화 검침 프로그램 등에 반드시 보안 기능이 구축되어야 하며, SCADA(Supervisory Control And Data Acquisition) 및 보호 계전기 시스템의 보안이 보장되어야 함을 명시하고 있다.

우리나라가 스마트 그리드 선도국가로 지정된 만큼, 스마트 그리드의 안전한 구현을 위한 보안 기술의 개발에 대하여도 구체적인 계획을 수립하여야 할 것이다[8-11]. 따라서 본 논문에서는 스마트 그리드와 같은 국가적인 주요 인프라를 보호하기 위한 보안 기술의 요구사항을 분석하고 설계 원칙에 대한 분석 결과를 제시하고자 한다.

Ⅱ. 스마트 그리드의 취약성

대표적으로 전력 송배전망에서 지역적으로 분산된 SCADA 제어 기술을 사용한다. SCADA 시스템이 지역 원격 필드 제어 스테이션으로부터 데이터를 수집하여 전력 분배를 감시하고 제어하며 중앙 위치로부터의 명령을 내린다[12-16].

SCADA는 흔히 네트워크로 서로 연결된다. 이것은 전력 제어 센터와 발전 설비의 경우에 해당한다. 발전 설비 운영이 디지털 제어 시스템(DCS: Digital Control System)에 의하여 제어되지만, DCS는 전송과 배전 명령과 생산 출력을 조정하기 위하여 SCADA 시스템과 통신하여야 한다.

이와 같이 스마트 그리드는 물리적이고 또한 수많은 정보 통신 기술을 통하여 복잡하게 고도로 연결되어 있으며 상호 의존적이다. 한 하부구조에서의 사고가 연속적으로 증폭되어 다른 하부구조에 직·간접적으로 영향을 미칠 수 있다.

전력이 상호의존적인 주요 하부구조의 가장 광범위한 소스 중의 하나로 여겨진다. 한 예로써, 전력 전송 SCADA 시스템에서 사용되는 마이크로웨이브 통신 네트워크의 붕괴로 연속적인 실패가 개시될 수 있다. 감시 및 제어 능력이 없어 대규모 발전 단위가 격리되고 전송 변전소에서의 전력 손실을 초래하는 이벤트가 발생할 수 있다. 이런 손실이 주요 불균형을 일으키고 전력 그리드를 통한 연속 실패를 야기 시킬 수 있다. 이것은 다시 대규모 정전 사태를 불러오고, 석유 및 가스 생산, 정유소 운영, 수 처리 시스템, 폐수 수집 시스템과 같은 전력에 의존하는 모든 산업에 심각한 영향을 미칠 수 있다.

스마트 그리드의 핵심 기술인 첨단 검침 인프라(AMI: Advanced Meter Infrastructure)의 취약성을 이용하면 금전적 이득을 취할 수 있기 때문에, 악성 해커의 타깃이 될 것으로 예상된다[17]. 만약 해커가 계량기를 침해하게 된다면, 에너지 비용을 즉각 조작할 수 있고 발전 에너지 계량기 수치를 조작할 수 있다. 이미 미국 내의 전력망에 대한 소비자 사기 행위가 발생하고 있으며, 그 액수는 60억불에 달하는 것으로 평가하고 있다.

기계적인 계량기에서 디지털 계량기로 전환됨에 따라, 공격 행위가 조잡하고 위험한 물리적 시스템 조작에서 원격 침투와 복잡하고 여러 가지 상태 정보를 보유한 컴퓨터의 조작으로 이동하게 될 것이다. 이것으로 더욱 정교한 공격이 가능하여 지고, 개인 전력 사용량에 대한 변경과 같은 소규모 공격이나, 전력망에 대한 대규모 공격 개시 형태로 전개될 수 있다. 예를 들어, 지능형 계량기 사이에서 확산되는 웜이 최근에 실제로 제작되었다[17]. 계량기 봇(meter bots), 분산 서비스 거부(DDoS: Distributed Denial of Service) 공격, 사용 기록기(usage logger), 지능형 계량기 루트킷, 계량기-기반 바이러스 및 다른 악성 소프트웨어가 출현할 것이 거의 확실하다고 분석하고 있다.

또한 스마트 그리드에 저장된 에너지 사용 정보를 통하여 고객의 비밀성이 침해될 수 있다. 전력 소비 습관과 행위 등이 노출된다. 예를 들어, TV 시청과 같은 특정 활동이 탐지될 수 있는 전력 소비 징후를 가지게 된다.

따라서 스마트 그리드의 도입과 함께 필요한 보안 관련 기술에 대하여도 조사될 필요성이 존재한다.

Ⅲ. 특성분석

기존 그리드는 특별한 하드웨어와 소프트웨어를 사용하여 독점적인(폐쇄적인) 제어 프로토콜을 수행하는 고립 시스템이었기 때문에 전통적인 IT 시스템과는 상당히 거리가 있다.

〔표 1〕 IT 시스템과 제어 시스템 차이

분류	IT 시스템	제어 시스템
성능 요구	비실시간, 일정한 응답, 처리력 속도에 대한 엄격한 요구, 지연 및 지터 허용	실시간, 시간에 민감한 응답, 적당한 처리력 속도 허용, 지연 및 지터는 심각한 문제
가용성 요구	rebooting 허용, 시스템 운영 요구사항에 따라 가용성 편차가 허용됨	rebooting 불허용, 높은 가용성 요구, 계획된 가동 정지
위험 관리 요구	데이터 비밀성과 무결성이 가장 중요, 일시적인 가동 중지 허용(결함 감내 시스템 불급), 비즈니스 운영 방해가 최대 위험	인명 및 생산 시스템 관점의 안정성이 가장 중요, 일시적 가동 중지 불허용(결함 감내 시스템 중요), 인명, 프로세스 장비 혹은 생산 능력의 손실이 최대 위험
보안 구조	컴퓨터 관련 자산 및 저장/전송 정보 보호 목적, 중앙 서버 보안	제어 장치와 PLC 같은 필드 장치 보호
보안 솔루션	대표적인 IT 시스템을 대상으로 설계	시스템 운영을 보증하도록 설계되지 않음
시간 민감 상호작용	비상사태 시 상호작용이 덜 민감, 원하는 정도로 시스템 자원에 대한 접근 통제 제한	비상사태 시 인간 혹은 다른 상호작용에 대한 대응이 매우 중요, 시스템에 대한 접근이 엄격이 규제되어야 함.
시스템 운영 및 변경 관리	표준 운영 체제 사용하도록 설계, 갱신이 단순하고 자동화된 도구 이용가능.	특별히 채택된 운영체제와 표준 운영체제 혼용, 소프트웨어 변경은 단계적 수행, 공급자 참여 필요.
자원 제한	보안 솔루션과 같은 제3자 응용의 추가를 지원하는 충분한 자원이 이용가능	프로세스를 위한 특화된 설계, 보안 솔루션을 위한 메모리 용량 및 컴퓨팅 자원이 제한
통신	표준 통신프로토콜, 주로 유선 네트워크 및 지역 무선 네트워크, 대표적인 IT 네트워크 실제 기반으로 구축	많은 독점적 통신 프로토콜 존재, 전용선/광섬유/무선링크/위성과 같은 다양한 형태의 매체 사용, 네트워크가 복잡하고 전력시스템에 대한 지식 요구
관리 지원	다양한 지원형태 가능	소수의 벤더에 의해서만 가능
서비스 생명	3~5년의 짧은 생명주기	15~20년의 긴 생명주기
요소 접근	지역에 설치되고 접근 용이	고립되고 지역적으로 원격지에 있어 접근이 어려움

근래에 와서, IP(Internet Protocol) 장치가 독점적인 솔루션들을 대체하고 있어, 사이버 보안 취약성 및 사고의 가능성을 증대시키고 있다. 그러나 스마트 그리드의 보안 특성은 기존 IT 시스템 보안과는 큰 차이가 존재한다[12,14-16]. 예를 들어, 일반적으로 기존 IT 시스템의 보안 목적은 기밀성, 무결성, 가용성(CIA: Confidentiality, Integrity, Availability)의 순서를 따르나, 스마트 그리드에서는 그 순서가 AIC로 바뀐다. 그러므로 스마트 그리드 환경에 적합한 새로운 보안 솔루션이 필요하다고 할 수 있다.

스마트 그리드에서 연결성과 원격 접근 능력을 증진시키기 위하여 IT 솔루션들을 많이 채택하고 있다. 그러나 IT 시스템과 전력망 제어시스템 사이에는 표 1과 같은 차이가 있다[12,14,15].

표 1에 몇 가지 중요한 차이점이 요약되어 있다. 스마트 그리드 보안관련 연구를 위하여 이런 개별적인 특성을 잘 이해하는 것이 필요하다.

표 2는 일반적인 정보 시스템과 스마트 그리드 제어 시스템의 보안 특성 상 차이점을 보여준다[12,16].

요약하면, 스마트 그리드와 IT 시스템 사이의 운영

〔표 2〕 정보 시스템과 스마트 그리드 제어 시스템의 보안 특성 차이점

보안 특성	정보 시스템	제어 시스템
앤티바이러스/모바일 코드	통상적 광범위한 사용	비통상적/효과적인 설치가 불가능
지원 기술 수명	2-3 년 다양한 공급자	최대 20 년 단일 공급자
아웃 소싱	통상적 광범위한 사용	운영이 흔히 아웃소싱 되지만, 여러 제공자에게 다양화되지 않음
패치 응용	정기적 계획됨	드물, 비계획적 공급자 특정
변경 관리	정기적 계획됨	고도로 관리되고 복잡함
시간 민감 내용	일반적으로 지연 허용	지연 허용 안됨
가용성	일반적으로 지연 허용	연속적 사용
보안 인식	개인 및 공공 부문에서 중간 정도	물리적 보안을 제외하고 열악
보안 시험/감사	좋은 보안 프로그램의 부분	정지에 대한 일시적 시험
물리 보안	안전	원격/무인 안전

및 위험 차이가 보다 정교화 된 보안 전략 적용에 대한 필요성을 증대시킨다. 스마트 그리드 운영과 관련된 보안 솔루션의 설치, 운영 및 유지보수가 가지는 가능한 의미를 이해하기 위하여, 전력망 제어 엔지니어, 제어 시스템 운영자 및 보안 전문가의 협동 팀이 밀접하게 일할 필요가 있다.

Ⅳ. 스마트 그리드의 설계 원칙

4.1 개요

스마트 그리드의 정보 네트워크 구조 설계는 일반적으로 Corporate Networks와 분리시키는 것이 권고된다. Corporate Networks에서 통상적으로 허용되는 인터넷 접근, FTP(File Transfer Protocol), 이메일 및 원격 접근 트래픽이 스마트 그리드에서는 허용되지 않아야 한다. 분리된 네트워크를 보유함으로써, 사내 망에 대한 보안과 성능이 그리드 네트워크에 영향을 미칠 수 없도록 해야 한다[18,19].

그러나 스마트 그리드와 Corporate Networks의 연결이 필요한 실제 상황이 발생할 수 있다. 만약 이런 연결이 이루어진다면, 이것이 심각한 보안 위험을 유발하기 때문에 설계 및 구현에서 주의가 요구된다. 두 네트워크가 연결되어야 한다면, 최소한의 연결을 허용하고 방화벽과 DMZ(De-Militarized Zone)를 통하는 것이 권고된다. DMZ는 방화벽에 직접 연결된 별도의 네트워크 세그먼트로써, 인터넷 접근 가능 서버와 네트워크 내의 서비스들을 보호하기 위한 버퍼 역할을 하는 네트워크 장치에 추가된 인터페이스를 의미한다.

Corporate Networks로부터 접근될 필요가 있는 그리드 데이터를 포함하는 서버는 이 네트워크 세그먼트에 설치해야 된다. 단지 이 세그먼트만 Corporate Networks에서 접근 가능해야 한다.

4.2 방화벽

방화벽은 다른 보안 입장을 채택하고 있는 네트워크 사이의 트래픽 흐름을 제어하는 시스템 혹은 장치이며, 패킷 필터링 방화벽, 상태유지(stateful) 감시 방화벽 및 애플리케이션-프락시 게이트웨이 방화벽 등이 있다. 그리드 환경에서, 방화벽은 그리드 네트워크와 Corporate Networks 사이에 대부분 설치된다. 적절하게 방화벽 구성이 이루어진다면, 그리드 시스템 호스트 컴퓨터와 컨트롤러에 대한 불필요한 접근을 제한할 수 있고 보안을 증진시킬 수 있다.

방화벽은 프로세스 제어 장치에서 수행할 수 없는 다음과 같은 보안 정책을 실행해야 한다[19]:

- 비보호 LAN과 보호된 그리드 네트워크 상의 장치 사이에 특정 실행 통신망을 제외하고 모든 통신을 차단한다. 차단은 외향 및 내향 패킷 모두에 대하여 발생하며, 소스와 목적지 IP 주소 쌍, 서비스 및 포트 기반으로 이루어진다.
- 그리드 네트워크에 접근하는 모든 사용자의 보안 인증을 그리드 네트워크의 취약성에 따라 단순한 패스워드, 복잡한 패스워드, 복수-인자 인증 기술, 토큰, 바이오 메트릭 및 스마트카드 같은 특정한 방법을 사용하여 수행한다.
- 사용자의 업무 기능에 필요한 제어 네트워크 상의 노드에만 접근을 제한적으로 허용함으로써, 고의적 혹은 우연적인 사고 가능성을 줄이도록 한다.
- 트래픽 감시, 분석 및 침입 탐지를 위한 정보흐름을 기록한다.
- 그리드에 적절한 운영 정책을 구현하도록 해야 한다.

그리드 환경에 방화벽을 설치할 때 다음과 같은 문제점이 존재 한다:

- 제어 시스템 통신에 지연 추가의 가능성
- 산업 응용에 적합한 규칙집합(rule set) 설계에서의 경험 부족

사이버 사고를 신속하게 탐지하고 대응하기 위하여 방화벽과 다른 보안 센서들의 실시간 감시가 필요하다.

4.3 그리드 네트워크의 논리적 분리

그리드 네트워크는 물리적으로 분리된 네트워크 장치 상에서 Corporate Networks로부터 최소한 논리적으로 분리되어야 한다. 연결이 필요할 때는 아래와 같은 원칙들이 지켜져야 한다:

- 그리드 네트워크와 Corporate Networks 사이에 문서화되고 최소한의 액세스 포인트만 있어야 한다.
- 그리드 네트워크와 Corporate Networks 사이의 상태(stateful) 방화벽은 분명하게 권한이 부여된 트래픽을 제외하고 모든 트래픽을 거부하도록 구성

되어야 한다.

- 방화벽 규칙은 TCP와 UDP(User Datagram Protocol) 포트 필터링, ICMP(Internet Control Message Protocol) 유형 및 코드 필터링 이외에 적어도 소스와 목적지 필터링를 제공해야 한다.

그리드 네트워크와 Corporate Networks 사이의 통신을 하는 한 가지 바람직한 방법은 중간 DMZ 네트워크를 구현하는 것이다. 단지 Corporate Networks와 DMZ 사이에, 그리고 그리드 네트워크와 DMZ 사이에서 제한된 특정 통신만 발생하도록 하기 위하여, DMZ는 방화벽에 연결되어야 한다. Corporate Networks와 그리드 네트워크는 서로 직접 통신하지 않아야 한다.

4.4 심층-방어 보안 구조

4.4.1 보안 특성과 공격 방법론

단 하나의 보안 제품, 기술이나 솔루션으로 스마트 그리드를 적절히 보호할 수 는 없다. 심층-방어(defense-in-depth) 기법은 두 개 이상의 다른 중복된 보안 메커니즘을 포함하는 복수 계층 전략을 의미하며, 어느 한 메커니즘에서의 실패의 영향이 최소화되기 때문에 바람직한 구조이다. 심층-방어 구조 전략은 방화벽의 사용, DMZ의 생성, 효과적인 보안 정책을 갖춘 침입탐지 능력, 훈련 프로그램과 사고 대응 메커니즘을 포함한다. 게다가, 효과적인 심층-방어 전략은 다음과 같은 제어 시스템에 대한 가능한 공격 벡터의 철저한 이해를 요구한다[19].

- 네트워크 페리미터 내의 백도어와 허점: 제어 시스템은 충분한 보안 분석 없이 설치되는 경우가 많기 때문에, 백도어가 우연히 생성될 수 있다. 특히 네트워크 페리미터가 가장 중요하며 공격자가 이용할 수 있는 보안 취약성을 가질 수 있다. 무선 통신도 공격자에 의하여 SSID(Service Set Identifier) 브로드캐스팅, 제한된 접근 제어, 암호화 부족 및 제한된 네트워크 분할 등이 이용될 수 있다. 제어 시스템의 원격 제어 능력이 제어 데이터의 차단, 수정, 재주입 공격 등을 유발할 수 있다.
- 공통 프로토콜에서의 취약성: 제어 시스템에서 많이 사용되고 있는 공통 프로토콜인 OLE(Object Link and Embedding), DCOM(Distributed Component Object Model), RPC(Remote Procedure Call) 및 OPC(OLE for Process Control)와 같은 실시간 데이터 통신 표준들의 취약성들이 공격자에 의하여 이용될 수 있다. 또한 전통적으로 고립된 제어 네트워크와 비즈니스 환경과의 융합이 공격자에게 새로운 환경을 제공하고 있다.

제어 시스템을 위한 보안 패치의 설치도 기존 IT 시스템과는 다르다. 제어 시스템 동작에 어떤 영향을 미치는지 사전에 엄격한 시험이 이루어져야 한다. 실제로 패치의 설치로 생산 설비가 완전히 중단된 사건이 여러 건 보고된 바 있다.

- 필드 장치에 대한 공격: 필드 장치에 대한 접근을 통하여, 공격자가 센서 네트워크와 제어 시스템 네트워크로 진입할 수 있다.
- 데이터베이스 공격: 기존 IT 시스템의 데이터베이스에 대한 SQL 주입 공격이 제어 시스템에 발생한다면, 훨씬 더 큰 영향을 미칠 수 있으며, 제어 시스템 보안에 주요한 위협이 될 수 있다.
- 통신 하이재킹(hijacking)과 중간자(man-in-the-middle) 공격: 제어 시스템은 통상적으로 신뢰(trust)를 가정하며, 따라서 장치들 사이의 데이터 흐름에서 보안이 취약하다. 이 경우 아래와 같은 주요 보안 문제가 존재 한다:
  - 네트워크 상의 데이터를 공격자가 재 경로배정할 수 있는 능력
  - 평문 형식으로 된 중요 트래픽 포획 및 분석 능력
  - 제어 통신에 대한 통제권을 얻기 위한 프로토콜 역공학 능력

이런 공격을 결합하여 공격자는 중간자 공격을 실행하게 되고, 네트워크 상의 데이터에 대한 제어권을 얻을 수 있다.

4.4.2 심층-방어 전략

그림 1은 zone으로 구분된 보편적인 제어시스템의 구조를 보여준다. 이 zone들은 다음과 같이 구분되어 있다[20]:

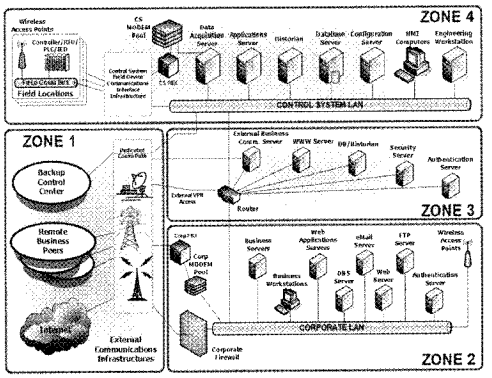
- Zone 1: 인터넷, 피어 워치 및 백업 설비에 대한 외부 연결
- Zone 2: 사내 통신용 외부 연결
- Zone 3: 외부 서비스로부터의 제어 시스템 통신

• Zone 4: 프로세스-기반 혹은 SCADA 제어 시스템 운영

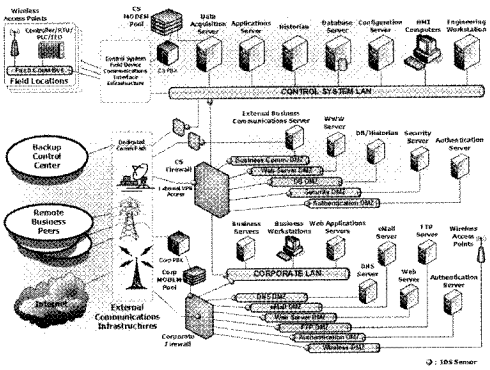
위의 존들은 각기 유일한 보안 요구사항을 가진다. 만약 제어 시스템 운영 존이 침해된다면, 제어 시스템 정보 자원의 조작은 치명적일 수 있다. 많은 부문에서 제어 시스템에 대한 악성 공격은 실제적인 결과를 초래한다.

그림 2는 Control Systems Cyber Security: Defense in Depth Strategies 문서에 기술된 바와 같이 미국 국토안보부(DHS: Department of Homeland Security) CSSP(Control Systems Security Program) 권고 실제 위원회에 의하여 개발된 제어 시스템 심층-방어 구조 전략을 보여준다[20].

Control Systems Cyber Security: Defense in Depth Strategies 문서는 multi-tier 정보 구조를 유지하면서 제어 시스템 네트워크를 사용하는 조직을 위한 심층-방어 구조 전략을 개발하기 위한 지침 및 방향을 제공한다. 이 전략은 방화벽, DMZ의 사용과 제어 시스템 구조 전체에 침입탐지 능력의 사용을 포함한다. 그림에서



〔그림 1〕 통상적인 구조에서의 존[20]



〔그림 2〕 CSSP 권고 심층-방어 구조[20]

여러 DMZ의 사용은 별도의 기능성에 대한 부가된 능력과 액세스 특권을 제공하고, 다른 운영 의무사항을 가진 네트워크들로 이루어진 대규모 구조를 보호하는데 매우 효과적인 것으로 증명되었다. 침입 탐지 설치는 다른 룰셋과 감시되는 각 도메인에 유일한 시그니처가 적용된다.

심층-방어 보안 구조가 설치된 후, 방화벽을 통하여 어떤 트래픽을 통과시킬지는 정책을 통하여 결정되어야 한다. ISA(The Instrumentation, Systems, and Automation Society) 99의 기술보고서 부록 A에 의하면, 아래와 같은 일반적인 기준을 제시하고 있다[21,22]:

• 제어 시스템에 대한 내향 트래픽은 차단되어야 한다. 제어 시스템 내부 장치 접근은 DMZ를 반드시 통과해야 한다.
• 제어 네트워크 방화벽을 통한 외향 트래픽은 긴요한 통신에 대해서만 제한되어야 한다.
• 제어 네트워크로부터 사내 망으로의 모든 외향 트래픽은 서비스와 포트에 의하여 소스(근원지)와 목적지-제한적이어야 한다.

또한 DNS(Domain Name System), HTTP(Hyper Transfer Protocol), FTP(File Transfer Protocol), SMTP(Simple Mail Transfer Protocol), SNMP(Simple Network Management Protocol), SCADA와 같은 특정 서비스에 대하여도 방화벽 규칙이 설정되어야 한다.

V. 요구사항

5.1 요구사항 문서

스마트 그리드에 적용될 수 있는 많은 요구사항 문서들이 존재한다. 현재로는 NERC Critical Infrastructure Protection(CIPs) 만이 스마트 그리드의 특정 도메인에 대하여 의무적이다. 다음의 문서들이 스마트 그리드 CSCTG(Cyber Security Coordination Task Group)의 구성원들에 의하여 보안 요구사항으로 식별되었다[3].

다음의 표준들은 스마트 그리드와 직접 연관이 있다.

• NERC CIP 002, 003-009
• IEEE 1686-2007, IEEE Standard for Substation Intelligent Electronic Devices Cyber Security Capabilities
• AMI System Security Requirements, 2009
• UtilityAMI Home Area Network System Require-

ments Specification, 2008

- IEC 62351 1-8, Power System Control and Associated Communications-Data and Communication Security

그 외에 제어 시스템에 적용할 수 있는 문서로는 다음과 같은 것이 있다:

- NIST SP 800-82, DRAFT Guide to Industrial Control Systems(ICS) Security, Sept. 2008.
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems, Dec. 2007.
- ANSI/ISA-99, Manufacturing and Control Systems Security, Part 1: Concepts, Models and Terminology and Part 2: Establishing a manufacturing and Control Systems Security Program
- 기타

5.2 개발 전략

스마트 그리드의 개발과 함께 스마트 그리드 정보보호 기술이 개발되어야 할 것으로 보이며, 아래와 같은 여러 가지 목표를 가지고 추진되어야 할 것이다[17].

- 소비자 보호를 위한 법적 제도가 확립되어야 한다. 의료정보보호를 위하여 미국에서 도입된 HIPAA (Health Insurance Portability and Accountability Act)와 마찬가지로 스마트 그리드를 위한 법제화가 이루어져야 한다. 이 법에서는 소비자 데이터 수집 방법, 데이터의 사용 권한, 정보 오남용에 대한 벌칙 등에 대하여 규정하여야 할 것으로 보인다.
- 정부, 학계 및 산업계가 스마트 그리드에 대한 보안 기술을 광범위하게 평가하고 시험해야 할 것이다. 특히 지능형 계량기에 대한 설계 단계에서 보안 기술이 포함되도록 하여야 할 것이다. 스마트 그리드 시스템에 대한 평가 기준도 확립되어야 할 것이다. 관련 기술 개발의 경쟁 체제 도입, 표준 제정 및 보안 전문가에 의한 독립적인 소스 코드 검토, 공공 시험 기관의 설립 등을 통하여 시스템의 품질을 개선할 수 있도록 유도하여야 한다.
- 스마트 그리드 실패에 대한 복구 전략이 확립되어야 한다. 복잡한 소프트웨어 시스템으로 하여금 자연스럽게 이용될 수 있는 버그를 가질 수 있으며, 이에 대한 소프트웨어 패치 관리 대책을 수립하고, 침해 시스템의 신속한 식별과 고립이 가능하도록 해야 할 것이다.

NIST 산하의 CSCTG에 의하여 작성된 "Smart Grid Cyber Security Requirements"에서는 스마트 그리드의 사이버 보안 전략을 다음과 같이 명시하고 있다[3].

- 위험 평가 수행
- 보안 아키텍처와 사이버 보안 요구사항의 명세를 개발하기 위한 공용 프레임워크를 제공하는 적용 사례(Use Case) 선택
- 스마트 그리드 개념 아키텍처와 연관되는 보안 아키텍처 개발
- 사이버 보안 요구사항의 명세 개발

[23]에서는 인터넷의 역사로부터 배울 수 있는 스마트 그리드 구축을 위하여 지켜야 할 12가지를 다음과 같이 제시하고 있다:

① 확장성 있는 서비스-지향 스마트 그리드 구조
② 통신 프로토콜의 정의 및 표준화
③ 보안 및 암호화
④ 에너지 관리 및 통신 도구
⑤ 개방 API(Application Programming Interface)
⑥ 킬러(killer) 애플리케이션의 발견
⑦ 소비자에 대한 다양한 인터페이스 제공
⑧ 인터넷에서의 IETF(Internet Engineering Task Force)와 같은 소위 "SGTF(Smart Grid Task Force)"의 결성
⑨ 명령 및 제어(C&C: Command and Control) 통신과 같은 특정 접근만을 허용하는 시큐어 그리드 계층(secure grid layer) 구축
⑩ 자동화된 자가-복구 능력
⑪ 국가 단위의 기술 시험 환경 구축
⑫ 스마트 그리드에 대한 경제성, 라이프스타일 증진, 에너지 보존 및 재생 에너지 통합 효과 측정 및 평가

스마트 그리드의 성공적인 구축을 위하여 인터넷으로부터 구축된 그 동안의 지식을 잘 사용해야 한다는 것이다.

5.3 기능적 보안 요구사항

스마트 그리드 보안 기술이 효과적이기 위하여 종단

간에 걸친 보안 능력이 필요하며, 이렇게 하기 위하여 위협을 탐지하고 완화할 수 있도록 여러 지점에 방어 메커니즘을 보유하는 계층화 구조가 필요하다. 기능적인 보안 요구사항은 다음과 같다[6]:

- 통합 물리 보안: 스마트 그리드에서 고려해야 할 첫 번째 사항으로 침입자로부터 그리드를 보호하는 물리적 보안을 지적하고 있다. 이를 위하여 IP 백본에 통합될 수 있는 비디오 감시, 카메라, 전자 접근 통제 및 긴급 대응 능력을 포함하여야 한다. IP 망과의 통합을 통하여 중앙 관리 및 통제, 모니터링 및 기록 능력, 정보에 대한 신속한 접근 등이 가능하여 진다.
- 신분 및 접근 통제 정책: 고용자, 계약자, 고객을 포함하여 스마트 그리드에 접근을 할 수 있는 여러 사용자 그룹이 존재한다. 이러 사용자 그룹에 대한 접근은 입상적(granular)으로 이루어져야하며, 권한부여는 "알 필요가 있는(need to know)" 자산에만 허용되어야 한다. 예를 들어, 종업원은 특정 지능형 제어 시스템에 접근할 수 있고, 계약자는 타임카드 응용에만 접근하고, 그리고 고객은 온라인으로 에너지 소비와 계산서(bill)를 볼 수 있도록 하는 인터넷 가능 접근을 할 수 있다.

강한 인증 메커니즘을 통하여 신분이 검증되어야 한다. 강한 패스워드를 사용해야 하고, 모든 시도는 기록되어야 한다. 지능망에 대한 접근은 명시적인 접근 허용을 통해서만 부여되는 "디폴트 거부" 정책을 구현해야 한다. 게다가, 허용되지 않는 접근을 방지하기 위하여 모든 접근점은 강화되어야 하며, 정상 운용을 위하여 필요한 포트와 서비스만이 실행되어야 한다.

- 강화된 네트워크 장치 및 시스템: 효과적인 보안 구조의 기반은 인프라 자체를 보호하는 것이다. 라우터와 교환기 같은 핵심 요소가 취약성이나 접근을 위한 방법을 제공하지 않도록 적절히 보호되어야 한다. 만약 이런 장치들이 침해된다면, DoS 공격을 통하여 전력망 운용을 방해하기 위하여 혹은 더욱 중요한 제어 시스템에 접근 하기 위하여 사용될 수 있다.
- 위협 방어: 효과적이고 계층적인 방어를 구축하기 위하여 전체 인프라에 걸친 광범위한 보안 원칙을 주의 깊게 적용해야 한다.
  - DoS 공격이 전력망의 기능을 약화시킬 수 있다. 네트워크 분할 및 접근 제어로 인하여 인터넷에서 기원하는 DoS 공격이 제어 시스템에 어떠한 영향을 미치지 않도록 해야 한다.
  - 중요 클라이언트 시스템, 서버 및 종단 기기를 보호하기 위하여 호스트-기반 침입방지시스템(IPS)과 앤티 바이러스 능력을 갖추어야 한다.
  - 인프라에 진입을 시도하는 외부 위협을 식별하기 위하여 네트워크-기반 IPS도 설치되어야 한다.
  - 페리미터(perimeter)와 인터페이스를 가지는 요소가 안전함을 보장하도록 취약성 평가가 주기적으로 수행되어야 한다.
- 전송 및 저장 데이터 보호: 다른 네트워크 세그먼트 사이의 접근 정책을 시행하기 위하여 방화벽 기능을 구현해야 한다. 안전하고 기밀성 데이터 전송을 위하여 암호 알고리즘을 적용한 가상사설망(VPN) 구조를 지원해야 한다. 서버와 종단 장치 상의 중요 자산을 보호하기 위하여 호스트 암호화 및 데이터 저장 보안 능력을 허용하여야 하며, 유무선 연결 상에 유비쿼터스 보안을 제공해야 한다.
- 실시간-감시, 관리 및 상호협동: 보안 사고의 타깃이 되거나 취약성 있는 네트워크 요소를 알기 위하여 실시간 감시체계가 수립되고, 관리 및 상호협동 하여야 한다.

5.4 주요 보안 대책

스마트 그리드 시스템 환경의 보안을 위하여 사용할 수 있는 다섯 가지의 보안 대책은 다음과 같다[20]:

- 보안 정책: 제어 시스템 네트워크와 개별 컴포넌트를 위한 보안 정책을 개발해야 하며, 현재 위협 환경, 시스템 기능성 및 보안 요구 수준을 반영하도록 주기적으로 검토되어야 한다.
- 자원과 서비스에 대한 접근 차단: 네트워크 상에 방화벽이나 프락시 서버와 같은, 접근 제어 목록을 가진 페리미터 장치의 사용을 통하여 보통 채택된다. 호스트-기반 방화벽과 앤티-바이러스 소프트웨어를 통하여 호스트 상에서도 실행될 수 있다.
- 악성 행위 탐지: 네트워크 혹은 호스트 기반 탐지 행위는 로그 파일의 정기적인 감시를 필요로 한다. 침입탐지시스템이 네트워크 혹은 개별 호스트에 사용될 수 있다.

- 공격 가능성 완화: 취약성이 이용될 수 없도록, 필터 설정, 특정 구성(배열)을 가진 서비스와 응용의 운영 등을 통하여 취약성에 대한 접근을 통제할 수 있어야 한다.
- 핵심 문제 해결: 취약적인 응용의 제거, 소프트웨어 취약성 갱신 및 패칭과 같은 핵심 보안 문제를 해결해야 한다. 소프트웨어 허점이 있는 곳에는 관리자가 적용할 수 있도록 공급자나 개발자에 의하여 완화 기법이 제공되어야 한다.

VI. 결론

스마트 그리드 시스템은 수도, 수송, 화학, 제지, 자동차, 석유 및 가스와 같은 산업제어 시스템과 더불어 국가적인 주요 기반시설에 해당된다. 스마트 그리드는 여러 가지 환경적인 변화로, 특별한 하드웨어와 소프트웨어를 사용하여 폐쇄적인 제어 프로토콜을 수행하는 기존 전력망의 고립 시스템에서, MS 윈도우, Unix, TCP/IP와 같은 표준 기술 및 프로토콜로 전환되고 있고 IT 망과의 통합이 이루어지고 있어, 정보통신 인프라에 존재하는 사이버 보안 취약성 및 사고의 가능성이 그대로 재현될 가능성이 증대되고 있다[24]. 그러나 스마트 그리드의 보안 특성은 기존 IT 시스템 보안과는 큰 차이가 존재한다. 그러므로 스마트 그리드 환경에 적합한 새로운 보안 솔루션이 필요하다고 할 수 있다.

기존의 IT 시스템은 "data를 처리하기 위하여 physics"를 이용하는 반면에, 스마트 그리드 제어시스템은 "physics를 처리하기 위하여 data"를 이용하는 근본적인 차이가 존재한다[12]. 그러므로 기존 IT 시스템을 위한 보안 기술이 스마트 그리드 시스템의 보안을 위한 필요 메커니즘이 될 수는 있지만, 심층-방어를 위하여 충분하지 않을 수 있다. 따라서 스마트 그리드 제어시스템의 보안 특성에 대한 충분한 이해를 바탕으로 국가 주요 정보 하부구조를 구성하고 있는 스마트 그리드 보안 기술 개발 및 구현이 개발 초기부터 이루어져야 할 것으로 생각된다.

2009년 7월 초에 발생한 7.7 DDoS 공격처럼, 만약 전력 인프라에 사이버 공격이 발생하면 국가적인 정전 사태와 같은 초유의 비상사태가 생길 지도 모른다. 따라서 국내에서도 정부와 산업체, 학계 및 연구소 등이 컨소시엄을 형성하여 점차 지능화·다양화되고 있는 사이버 공격에 대응할 수 있는 개발 전략을 수립하여야 할 것이다[1].

스마트 그리드를 위한 보안을 구현하기 위해서는 전체적인 보안 위험 관리 프레임워크가 개발되어야 한다. 이 프레임워크는 민간 및 공공부분에서 개발된 기존의 위험 관리 방식을 기초로 하여야 할 것이다. 이 프레임워크에서 스마트 그리드의 위험을 평가하기 위하여 전체 시스템에 대한 영향, 취약성 및 위협 정보를 결합하기 위한 프로세스를 확립해야 할 것으로 생각된다.

마지막으로 본 논문이 안전한 한국형 스마트 그리드의 구축을 위한 참고 자료가 되었으면 하는 바람이다.

참고문헌

[1] (재)한국스마트그리드사업단, 스마트그리드 2030, 웹 자료(2010년 3월 17일 검색).

[2] Wikipedia encyclopedia, Smart Gird. May, 2009.

[3] NIST, Smart Grid Cyber Security Strategy and Requirements, CSCTG(Cyber Security Coordination Task Group), Sep. 2009.

[4] U.S. Department of Energy, National Energy Technology Lab., Modern Grid Initiative, http 자료.

[5] Venkat Pothamsetty and Saadat Malik, Smart Grid: Leveraging Intelligent Communications to Transform the Power Infrastructure, Cisco White Paper, Feb. 2009.

[6] Cisco White Paper, Security for the Smart Grid, 2009.

[7] DOE Office of Electricity Delivery and Energy Reliability, Barriers to achieving the modern grid, July 2007.

[8] 정수환, "융합보안 R&D 이슈 및 방향", 정보보호학회지 제 19권 제 3호, 한국정보보호학회, pp.11-13, 2009년 6월.

[9] 전용희, "지능형 전력망(Smart Grid)과 정보보호", 정보보호학회지 제19권 제4호, pp.65-71, 2009년 8월.

[10] 이경복, 박태형, 임종인, "정보보호정책 관점에서의 한국형 스마트 그리드 추진 방안에 관한 연구", 정보화정책, 제 16권 제 4호, pp.73-96, 2009년 겨울호.

[11] 정나미, 전용희, 장정숙, "스마트 그리드를 위한 안전한 통신 요구사항에 대한 연구", 2010 동계종합

학술발표회 논문집,pp.11, 한국통신학회, 강원도 용평, 2010년 2월.

[12] Arvid Kjell, Guide to Increased Security in Process Control Systems for Critical Societal Functions, The Swedish forum for information sharing concerning information security-SCADA and Process control systems(FIDI-SC), Swedish Emergency Management Agency, Oct. 2008.

[13] NIST(National Institute of Standards and Technology), U.S. Department of Commerce, Special Pub. 800-82, Final Public Draft, Guide to Industrial Control Systems (ICS) Security, Sep. 2008.

[14] 이철수, "산업제어시스템 정보보안 감리 프레임워크 연구", 정보보호학회논문지, 제 18권 제 1호, pp.139-148, 한국정보보호학회, 2008년 2월.

[15] 전용희, "산업제어시스템 정보보호: 개요", 정보보호학회지 제 19권 제 5호, pp. 52-59, 한국정보보호학회, 2009년 10월.

[16] 전용희, "산업제어시스템 보안을 위한 네트워크 설계 및 구조" 정보보호학회지 제 19권 제 5호, pp.60-67, 한국정보보호학회, 2009년 10월.

[17] Patrick McDaniel and Stephen McLaughlin, "Security and Privacy Challenges in the Smart Gird", Secure Systems, May/June, pp. 72-74, IEEE, 2009.

[18] Alvaro A. Cardenas et al., "Research Challenges for the Security of Control Systems", Proceedings of the 3rd conference on Hot topics in Security, 2008.

[19] Arvid Kjell, Guide to Increased Security in Process Control Systems for Critical Societal Functions, The Swedish forum for information sharing concerning information security-SCADA and Process control systems(FIDI-SC), Swedish Emergency Management Agency, Oct. 2008.

[20] Homeland Security, Control Systems Security Center, Control Systems Cyber Security: Defense in Depth Strategies, May 2006.

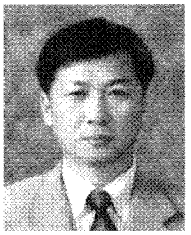
[21] ISA 99, Security for Industrial Automation and Control Systems, 2009.

[22] 에너지경제연구원, 미국 스마트그리드 시장 현주소와 도전과제, 2009년 12월.

[23] Balaji Natarajan, A dozen things the Smart Grid can learn from the Internet, earth2tech. 2009. 4.30.

[24] Testimony of Joseph M. Weiss, Control Systems Cyber Security-The Current Status of Cyber Security of Critical Infrastructures, before the Committee on Commerce, Science, and Transmission, U.S. Senate, March 19, 2009,

〈著者紹介〉



전 용 희 (Yong-Hee Jeon)

종신회원

1971년 3월~1978년 2월: 고려대학교 전기전자전파공학부, 학사
1985년 8월~1987년 8월: 미국 플로리다 공대 대학원 컴퓨터공학과
1987년 8월~1992년 12월: 미국 노스캐롤라이나주립 대학원 Elec. and Comp. Eng. 석사, 박사
1978년 1월~1978년 11월: 삼성중공업(주)
1978년 11월~1985년 7월: 한국전력기술(주)
1979년 6월~1980년 6월: 벨기에 벨가톰사 연수
1989년 1월~1989년 6월: 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA
1989년 7월~1992년 9월: 미국 노스캐롤라이나주립대 부설 CCSP (Center For Comm. & Signal Processing) RA
1992년 10월~1994년 2월: 한국전자통신연구원 광대역통신망연구부 선임연구원
1994년 3월~현재: 대구가톨릭대학교 컴퓨터·정보통신공학부 교수
2001년 3월~2003년 2월: 대구가톨릭대학교 공과대학장 역임
2004년 2월~2005년 2월: 한국전자통신연구원 정보보호연구단 초빙연구원
2007년 1월~2007년 12월: 한국정보보호학회 학회지 편집위원장
2008년 1월~현재: 한국정보보호학회 부회장
2009년 1월~2010년 2월: 한국정보과학회 정보보호연구회 위원장
<관심분야> 네트워크 보안, 스마트 그리드 보안, IT 융·복합 보안, 통신망 성능분석