그린 IT 보안 기술

전용희 | 장종수*
대구가톨릭대학교, 한국전자통신연구원*

요 약

본고에서는 녹색성장을 위하여 정부에서 추진하고 있는 그린 IT기술의 동반자로서 보안 기술의 필요성을 알아보고자 한다. 이를 위하여 먼저 그린 IT 보안 기술의 필요성과 그린 IT를 위한 핵심 보안 기술에 대하여 살펴본다. 다음으로 에너지 인터넷이라고도 불리는 지능형 전력망(Smart Grid)에서의 보안의 필요성과 보안 기술 개발 전략, Cisco 사의 사례연구 등에 대하여 기술하고자 한다. 본 논문은 녹색성장을 위한 전략 수립 단계에서 보안 기술의 중요성을 제시하는 것을 목표로 작성되었다.

I. 서 론

그린 IT 국가전략은 단순한 IT 강국을 넘어 글로벌 그린 IT 선도국으로의 도약을 목표로 하고 있다. 그린 IT는 환경을 의미하는 녹색(Green)과 정보통신기술(IT)의 합성어이다. IT 제품 및 서비스의 라이프 사이클 전반을 녹색화하고 신성장 동력으로 육성하는 "IT 부문 녹색화(Green of IT)"와 IT 융합으로 에너지/자원의 효율적 이용을 극대화하여 저탄소 사회 전환을 촉진하고, 실시간 환경 감시 및 조기 재난 대응 체계를 마련하여 기후 변화에 대한 대응역량을 강화하는 "IT 융합에 의한 녹색화(Green by IT)"를 포괄적으로 의미한다.

그린 IT 추진과제와 정보보호의 관계를 알아보기 위하여 핵심과제에 대하여 간략히 기술하고자 한다[1]. 먼저 IT 부문 녹색화 분야의 3대 정책 방향은 다음과 같다:

① World Best 그린 IT 제품 개발 및 수출전략화
② IT 서비스 그린화 촉진
③ 10배 빠른 안전한 네트워크 구축

다음으로 IT 융합에 의한 6대 녹색화 정책방향은 다음과 같다:

④ IT를 통한 저탄소 업무 환경으로 전환
⑤ IT 기반 그린 생활혁명 구현
⑥ IT 융합 제조업 그린화
⑦ 스마트 녹색 교통, 물류 체계로의 전환
⑧ 지능형 전력망 인프라 구축
⑨ 지능형 실시간 환경감시 및 재난 조기 대응 체계 구축

① 은 PC, 모니터 등 IT 기기를 에너지 절감 효과가 탁월한 그린 IT 제품을 개발하고, 공공 부분 및 민간 부분에 도입을 확산해 나간다는 내용이다.

② 에서는 IT 서비스의 그린화로 지식서비스 산업의 녹색성장 기반을 강화하기 위하여, IDC(Internet Data Center)의 그린화, 그린 클라우드 컴퓨팅(Cloud Computing) 서비스 기반 구축 및 방송통신 네트워크 인프라의 그린화 촉진 등이 포함되어 있다.

③ 은 세계 최고 수준 Giga 넷 구축을 통한 고품질, 실감형 서비스 제공 기반을 마련하고, WiBro, 4G, 센서망 등 무선 인프라 고도화 및 그린 정보보호 체계 강화 등의 추진 내용을 포함하고 있다.

④ 에서는 첨단 IT기반의 원격 협업/영상회의 확대, 전국

적 스마트워크 센터 구축을 통한 탄소 프리 출퇴근 환경 제공, 업무처리 전과정의 IT화로 탈종이 업무환경 확대, 건물 에너지 관리 시스템 보급, 확산 및 지원제도 개편 등의 추진과제를 포함하고 있다.

⑤는 미래형 학습환경 구현, IPTV 기반의 u-헬스 추진, 가상 체험 콘텐츠 구축 및 제공, RFID 기반의 음식 폐기물 관리 시스템 구축, 주택용 에너지 관리 시스템(HEMS) 개발 및 보급 등의 과제를 포함하고 있다.

⑥에서는 IT 기술을 활용한 제조 공정 그린화, 그린 산업단지 조성 및 관리, 제조업 등의 폐자원 관리를 위한 기반 정보 시스템 구축 등의 과제를 포함하고 있다.

⑦은 지능형교통체계(ITS) 고도화 및 확산, 지능형 물류거점 효율화 및 물류정보 연계 통합, 공용자전거와 IT 기술을 융합한 녹색교통 체계 기반 조성 등의 과제를 포함한다.

⑧에서는 지능형 전력망 인프라 구축, 조기 상용화를 위한 IT 인프라 연계 및 활용 등의 과제가 있다. 여기서는 첨단 검침 인프라(AMI: Advanced Meter Infrastructure)와 초고속 인터넷, 홈 네트워크 연동 기술 개발 및 표준화, IPTV, 홈서버, 휴대단말 기반의 사용자 전력 제어 서비스 개발 등이 세부적으로 포함되어 있다.

⑨에서는 종합적, 체계적 환경 감시를 통한 기후 변화 조기 대응 및 대규모 CO_2 발생을 유발하는 재난을 적극적으로 예방하고 대응하는 체계를 구축하는 과제를 포함하고 있다.

위의 9대 정책 방향과 추진내용을 보면, '그린 IT 보안 기술' 의 중요성을 쉽게 찾을 수 있다. 예를 들어, 그린 PC가 만약 악성 코드에 감염된다면 PC가 이상 작동을 하게 되고 따라서 전력 소모가 증가하고 탄소 배출량도 커지게 된다. 악성코드가 감염되었을 때 소비되는 전력량은 175W로 평상시 보다 25% 정도 증가하는 것으로 조사된바 있다. 환경부는 국내 1 KWh 전기 생산에 424g의 탄소가 발생하는 것으로 발표하였으며, 국내 PC 추정량 3,500만대 중 약 1%가 악성코드에 감염된다고 하드라도, 악성 코드로 인하여 추가로 배출되는 탄소량은 9,973톤에 해당된다[2].

또 다른 예로, 네트워크에 분산서비스거부 (DDoS: Distributed Denial of Service) 공격이 발생하면 대응 장비가 작동해야 하는데, 이때 추가적인 전력낭비가 발생한다. 한국정보보호 진흥원의 실험 결과에 의하면 웹 서버에 DDoS 대응 장비를 작동 시키는 경우, 연간 3,000 KWh의 전력을 소모하는 것으로 나타났다. 2009년 3월 현재 국내 도메인 수가 약 180만개이고, 도메인 100개당 대응장비 1대 설치를 가정할 때, 3,000KWh*18,000 = 54,000,000 KWh의 전력 소모량 계산이 나온다. 이를 1KWh 당 83.71원의 단가를 적용하면, 약 45억 원 정도의 비용이 산출되는 것으로 지적하고 있다. 또 1 KWh 당 탄소 배출량 424g를 적용하면, 2만 3,000 톤 정도의 연간 탄소 배출량이 나오게 된다는 것이다. 따라서, DDoS 공격에 대한 신속한 대응으로 전력 낭비를 줄이고, 환경도 보호할 수 있게 된다[3].

이와 같이 그린 IT 기술을 국가적으로 안전하게 구현하기 위하여 정보보호 기술이 필수적이라고 여겨진다. 그러므로 본 논문에서는 녹색성장에 중추적인 역할을 수행하고 있는 그린 시큐리티 기술에 대하여 알아보고자 한다.

II. 그린 IT 보안 기술의 필요성

본 장에서는 그린 IT 구현을 위한 보안 기술의 필요성을 몇 가지 측면에서만 기술하고자 한다.

2.1 클라우드 컴퓨팅

클라우드 컴퓨팅은 컴퓨팅 자원을 효율적으로 사용할 수 있도록 하기 위하여, 가상화(virtualization)와 분산처리를 통해 대규모 컴퓨팅 자원의 풀을 구축하고 네트워크를 통하여 필요한 서비스를 제공하는 새로운 컴퓨팅 서비스 모델이다. 주요한 서비스 형태로는 SaaS(Software as a Service), NaaS(Network as a Service), DaaS(Data as a Service) 등이 있다.

네트워크를 통하여 다량의 고객 정보가 분산 처리 및 저장되므로, 이에 따른 개인 정보의 침해 및 유출 가능성이 높아진다고 할 수 있다. 그 외에도 서비스의 중단 등에 따른 가용성 및 신뢰성 문제 등에 대한 대책이 필요하다. 따라서 IT 서비스의 그린화를 위하여 필요한 클라우드 컴퓨팅의 안전한 구현을 위하여 정보보호가 전제될 필요가 있다.

2.2 안전한 네트워크 구축

서론에서 기술된 바와 같이, DDoS 공격 발생으로 인한 국내 피해규모가 심각하다. 공격은 점점 더 정교화되고 조직화되고 있으며, 규모도 대형화되는 추세이다. 최근의 해외 DDoS 공격 통계를 보면, 초당 최대 5백만 패킷(MPPS: Million Packets Per Second)에 이르는 공격이 발생하고 있고, 백만 패킷 이상을 운반하는 공격들이 여러 개 있었다. 5MPPS는 대략 40Gbps의 대역폭을 소모한다. 이는 곧 100Gbps의 공격이 나타날 수 있음을 의미한다.

따라서 안전한 네트워크 구축을 위하여 국가망 인프라 전반에 걸친 근본적이고도 통합적인 차원에서의 DDoS 대응 전략을 개발할 필요가 있다.

2003년 1월 25일 발생한 '인터넷 대란'과 최근 7월초에 발생한 DDoS 공격이 이를 잘 보여주고 있다.

2.3 그린 소프트웨어

그린 IT 기술을 구현하기 위하여 필요한 그린 소프트웨어는 IT 자산 및 운영의 효율화에 기여하는 소프트웨어, 다양한 분야에서 IT 활용을 통한 에너지 효율화, 그리고 지속 가능한 지구환경을 위한 제반 연구나 기후 협약 등 환경규제에 대응하기 위해 필요한 기능들을 지원하는 소프트웨어이다[4].

그린 소프트웨어의 유형과 역할을 간단히 살펴보면 아래와 같다[4]:

- IT 자산 및 운영 효율화: 클라우드 컴퓨팅 및 데이터 센터 소프트웨어
- 기후 협약 대응 체계: 그린 컴플라이언스(compliance) S/W, 유해 환경물질 관리 S/W
- IT 활용을 통한 에너지 효율화: 지능형 전력망(Smart Grid), 지능형 전동기(Smart Motor), 지능형 빌딩, 지능형 물류 체계, 가상 사무실

이와 같이 하드웨어뿐만 아니라, 소프트웨어는 IT 자체의 에너지 절감뿐만 아니라, 산업, 물류, 건물, 전력, 사무실, 주거환경 등 사회 전반에서 배출되는 온실가스를 감축할 수 있는 중요한 솔루션으로 개발되고 있다. 이러한 소프트웨어가 그린 IT의 진정한 솔루션이 되기 위하여는 소프트웨어 설계 단계에서부터 보안 기술이 접목될 필요가 있다[5].

예를 들어, 보안 위반을 가져올 수 있는 전통적인 오류 형태로 버퍼 오버 플로우(Over Flow)가 있다. 버퍼는 메모리 안에 있는 데이터가 보관되는 장소이다. 메모리가 유한하기 때문에, 버퍼 용량도 유한하다. 이런 이유로, 많은 프로그래밍 언어에서 프로그래머는 버퍼 최대 크기를 선언함으로써 컴파일러가 그 정도의 공간을 준비하도록 한다. C++ 언어와 같은 프로그래밍 언어로 작성된 프로그램에서는 프로그램이 확보한 메모리 크기를 넘는 문자열이 입력되면, 오버플로우가 발생하게 되고, 예기치 않은 작동이 일어난다. 버퍼 오버 플로우 공격의 한 예로 공격자는 시스템 공간의 코드를 대체할 수 있고, 운영체제인 것처럼 가장하여 통제권을 얻을 수 있게 되고, 공격자는 많은 명령을 실행할 수 있게 된다. 배열을 가진 고급 프로그래밍 언어에는 버퍼 오버 플로우 문제가 거의 항상 존재하기 때문에, 이런 버퍼 오버 플로우 기반의 취약성을 이용한 공격에 대비하고, 불완전한 중재(Incomplete Mediation), 경주상황(Race Conditions) 등의 소프트웨어 결함을 방지하도록 개발되어야 한다. 대부분의 소프트웨어는 복잡하고 에러가 존재할 수 있고, 이러한 소프트웨어의 결함이 다름 아닌 보안문제로 연결된다. 따라서 안전한 소프트웨어(Secure Software)를 구현하기 위하여 개발 단계에서부터 보안 기술이 적용될 필요가 있다.

그린 IT의 요소기술로 개발되고 있는 센서망, IT 융합 제조업 및 ITS(Intelligent Transport System) 등에도 정보보호 기술이 필수적이다.

III. 그린 IT 보안 기술

본 장에서는 그린 IT 구현을 위한 중요한 보안 기술에 대하여 기술하고자 한다.

3.1 악성 코드 대응 기술

악성코드(Malware: Malicious Software)란 소유자의 허가 없이 컴퓨터 시스템에 침입하거나 손상을 주도록 설계된 소프트웨어를 말한다. 이러한 멀웨어는 웹사이트 훼손에서 인간의 생명 손실까지 영향을 미칠 수 있으며, 현재 인터넷이 직면하고 있는 스팸(Spam), DoS 공격, 봇넷(Botnets), 웜과 같은 심각한 문제의 대부분은 이 악성 소프트웨어 때문에

발생한다. 현대의 멀웨어는 점점 더 복잡하여 지고 있으며 그에 따른 대응 방법도 더욱 어려워지고 있다.

서론에서도 기술한 바와 같이, 정상적인 PC에 악성코드가 감염되면 일반 PC보다 25% 정도 전력소비가 증가하게 된다. 또한 미국 환경 관련 연구 단체인 ICF(Intelligent Community Forum)에 의하면, 스팸메일에 소모되는 에너지를 조사한 보고서에서, 스팸메일 1개는 0.3g의 탄소를 배출시키는 것으로 밝혀졌다. 스팸메일 1통이 자동차를 1m 운행했을 때 보다 많은 탄소를 배출한다고 지적하고 있다[3].

3.2 저전력, 초경량 암호 기술

정보보호를 위하여 사용되는 암호 기술이 복잡한 수학적 연산과정이 많기 때문에 처리과정에서 전력을 많이 소비하게 된다. 따라서 저전력, 초경량 암호기법을 개발함으로써 전력낭비를 줄일 경우 상당한 '그린' 효과를 거둘 수 있다는 것이다. 예를 들어, 국내에서 개발된 경량화 암호 알고리즘으로 HIGHT(HIGh security and lightweigHT)가 있다. 이를 적용할 경우, 전력 소비 효과가 최대 15% 정도될 수 있다. 해외에서도 저전력, 경량 암호화 기술 개발연구가 활발히 진행되고 있으며, 국제 표준화도 추진되고 있다[3].

이러한 기술을 PC나 웹사이트, 인터넷 전화, RFID 등에 적용할 경우 연간 절감할 수 있는 탄소량은 3만 6,710톤에 이른다는 것이다.

3.3 DDoS 대응 기술

DDoS 공격이 인터넷에 대하여 거대한 위협을 제공하고 있으며, 이에 대한 대응책들이 많이 제시되었다. 그러나 공격의 복잡성과 다양성으로 인하여 어떤 대응 기법이 효과적인지도 상당히 혼란스럽게 되었다. 공격자들은 보안 시스템을 우회하기 위하여 꾸준히 공격도구들을 변경하고 있으며, 이에 대한 방패로써 연구자들 역시 새로운 공격에 대한 대응책을 강구하고 있다.

DDoS 대응 연구의 진보를 방해하는 심각한 요인은 아래와 같다[6]:

- 인터넷 상의 많은 지점에서 분산된 대응 필요: DDoS 공격에 효과적인 대응을 위하여 분산 협동 대응 시스템을 가져야 하기 때문이다. 현재 인터넷의 관리 방법 상 이것이 쉽지 않다는 것이 문제이다.
- 경제적, 사회적 요인: 분산 대응 시스템이 DDoS 공격으로부터 직접적인 손해를 보지 않는 소스나 중간 네트워크에 의해서도 설치되어야 한다는 것이다. 따라서 대응 솔루션들이 드물게 설치되어, 매우 제한된 효과만 가져올 수 있다.
- 상세 공격 정보의 부족: 여러 가지의 공격 유형에 대한 정보와 공격율, 기간, 패킷 크기, 에이전트 머신의 수, 시도된 대응 및 유효성, 피해 규모 등에 대한 정보가 부족하다.
- 대응 시스템 벤치마크의 부족: 현재까지 대응 시스템 사이의 비교를 할 수 있는 공격 시나리오나 확립된 평가 방법론의 벤치마크 suite가 없다는 것이다.
- 대규모 시험의 어려움: DDoS 대응이 실제적인 환경에서 시험될 필요가 있는데, 인터넷상에서 실제 분산 시험을 수행할 수 있는 대규모 테스트 베드나 안전한 방법이 없다는 것이다. 대응 시스템의 성능이 소규모 실험과 시뮬레이션 기반이라 신뢰적이지 못하다는 지적이다.

효과적인 DDoS 대응을 위하여 다음과 같은 설계목표가 제시될 수 있다:

- 분산 방어 메커니즘: 확장성이 있고, 악성 집단이 메커니즘 공격을 하는 것을 더욱 어렵게 만들고, 합법, 악성 트래픽의 통합을 제한하는 방어 조처를 가능하게 한다.
- 협동 메커니즘: 전역적인 정보를 제공함으로써 분산 대응 방법의 효율성을 증가시킨다.
- 정보 요구의 최소화: 대응을 위하여 많은 정보가 필요할수록, 계산적, 메모리, 네트워크 대역폭 오버 헤드가 많이 요구된다.
- 독립적으로 유용한 메커니즘: 다른 노드의 간섭 없이 모든 노드는 독립적인 기능이 가능해야 한다.

3.4 기타 기술

녹색 성장과 그린 IT를 구현하기 위한 다른 정보보호 관련 기술로는 다음과 같은 기술이 있다[3]:

- 융합 정보보호 기술: 초경량 저전력 암호알고리즘의 사용과 함께, 네트워크 구성을 최소화함으로써 전력소모를 줄이고자 하는 방법이다. 예를 들어, 방화벽과 가상사설망(VPN), 침입탐지시스템(IDS), 컴퓨터 바이러스 백신 등을 통합한 제품을 사용할 경우 별도의 보안 제품

을 사용하는 것보다 전력 소모가 절반 이상 감소된다는 지적이다.

- 그린 시큐리티 컴플라이언스 기술: 컴플라이언스(Compliance)란 법규정을 준수하도록 보장하기 위한 환경이나 시스템을 의미하는데, 이 컴플라이언스 기술이 저탄소 녹색성장을 위한 기본 인프라를 형성하기 때문이다. 필수적인 그린 시큐리티 컴플라이언스 기술로 스마트 장치 침해 예방, 취약 계층 그린 시큐리티, 에너지 인터넷 안정성 확보 및 그린 프라이버시 보호 등을 제시하고 있다.

IV. 지능형 전력망 보안 기술

4.1 지능형 전력망 보안의 필요성

지능형 전력망(Smart Grid)은 기존 전력망에 정보기술(IT)을 융합하여 전력 공급자와 소비자가 양방향으로 실시간으로 정보를 교환함으로써 에너지 효율을 최적화하는 차세대 전력망이다. 즉, 전력망에 통신망을 접목시켜 전력계통시스템의 제어를 통하여 발전, 송전, 배전의 전 과정에 대한 통제가 가능하여 지고, 결과적으로 에너지 사용의 효율성을 높이는데 있다. 지능형 전력망의 핵심기술로 첨단 검침 인프라(AMI: Advanced Meter Infrastructure)가 있다. AMI는 지능형 전력망, 통신 하부구조 및 지원 정보 하부구조의 융합으로 이루어진다. 그 이외에 지능형 전력망을 구성하기 위하여 진보된 송배전 자동화, 분산된 발전, 전기자동차 충전 하부구조 및 재생 에너지 발전 등이 필요하다.

이른바 '똑똑한 전기'를 생산하는 신기술로 스마트 그리드가 구축되면, 소비자는 전기 사용 요금과 사용량 정보를 실시간으로 알 수 있게 되고 가장 경제적인 시간대를 선택하여 전기를 사용하게 된다는 개념이다. 소비자는 그 동안의 수동적인 전력 소비 패턴에서 벗어나 전력 사용 시간대를 요금에 따라 선택 조정하는 등의 능동적인 전력 소비 패턴으로 전환하게 된다.

그러나 모든 IT 융합에서와 마찬가지로, 스마트그리드 역시 사이버 보안문제가 해결되어야 한다. 미국 보안 컨설팅 업체인 IOActive는 수년간 스마트 기기들에 대한 보안성을 점검한 결과 간단한 해킹 기술을 이용하여 해커들이 네트워크에 접속하여 전기 공급을 중단시킬 수 있다고 확인하였다. 이 실험 결과 전기 및 소프트웨어에 대한 약간의 지식과 500 달러짜리 장비만 있으면 스마트 그리드 시스템에 침투할 수 있었다. 그리고 한 개의 장비를 해킹하면 다른 스마트 그리드 시스템 전체를 조종할 수 있는 것으로 나타났다. 전력 소비 출력을 무작위로 높이거나 줄일 수도 있고 정전 기능도 가능하여 광범위한 피해가 예상된다고 분석하고 있다. 실제로 지난 4월에는 미국의 전력망에 해커들이 침투하여 전력망을 교란 시키는 소프트웨어를 설치한 사건이 발생한 바 있다[7-9].

지능형 전력망의 효과적인 운용을 보장하는 사이버 보안의 역할에 대하여 미국의 에너지성(DOE) 에너지 부문 계획에 문서화되어 있다. 미국의 국가 하부구조 보호 계획(NIPP: National Infrastructure Protection Plan)에 의하면 사이버 보안은 다음과 같이 정의된다[10]:

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

그리드에 대한 위험 요소는 다음과 같다:

- 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.

4.2 지능형 전력망의 취약성

[9]에서는 지능형 계량기(스마트 미터)의 취약성을 이용하여 금적적 이득을 취할 수 있기 때문에, 악성 해커의 매력적인 타깃이 될 것임을 지적하고 있다. 계량기를 침해한 해커는 에너지 비용을 즉각 조작할 수 있고 발전 에너지 계량기

수치를 조작할 수 있다. 현재에서도 미국내의 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. 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 확실하다.

또한 지능형 전력망에 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 지능형 전력망의 도입과 함께 필요한 보안 관련 기술에 대하여도 조사될 필요성이 존재한다.

4.3 요구사항 문서

지능형 전력망에 적용될 수 있는 많은 요구사항 문서들이 존재한다. 현재로는 NERC Critical Infrastructure Protection(CIPs) 만이 지능형 전력망의 특정 도메인에 대하여 의무적이다. 다음의 문서들이 지능형 전력망 CSCTG(Cyber Security Coordination Task Group)의 구성원들에 의하여 보안 요구사항으로 식별되었다[10].

다음의 표준들은 지능형 전력망과 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, 2008
- *UtilityAMI Home Area Network System Requirements 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

4.4 보안 기술 개발 전략

지능형 전력망의 개발과 함께 지능형 전력망 보안 기술이 개발되어야 할 것으로 보이며, 아래와 같은 여러 가지 목표를 가지고 추진되어야 할 것으로 보인다[9].

- 소비자 보호를 위한 법적 제도가 확립되어야 한다. 의료정보보호를 위하여 미국에서 도입된 HIPAA(Health Insurance Portability and Accountability Act)와 마찬가지로 지능형 전력망을 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 지능형 전력망에 대한 보안 기술을 광범위하게 평가하고 시험해야 할 것이다. 특히 지능형 계량기에 대한 설계 단계에서 보안 기술이 포함되도록 하여야 할 것이다. 지능형 전력망 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.
- 지능형 전력망 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.

4.5 CISCO사 사례연구

시스코사에서 보는 지능형 전력망에 대한 보안 필요성을

다음과 같은 요인에서 지적하고 있다[11].

- 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

지능형 전력망 보안 기술이 효과적이기 위하여는 종단간에 걸친 보안 능력이 필요하며, 이렇게 하기 위하여는 위협을 탐지하고 완화하기 위하여 여러 지점에 방어 메커니즘을 보유하는 계층화 구조가 필요가 있다. 기능적인 보안 요구사항은 다음과 같다:

- 통합 물리 보안: 지능형 전력망에서 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 지능형 전력망에 접근을 할 수 있는 여러 사용자 그룹이 존재한다. 이런 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.
  - 페리미터와 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 구현한다. 안전하고 기밀성 데이터 전송을 위하여 암호 알고리즘을 적용한 가상사설망(VPN) 구조를 지원한다. 서버와 종단 장치 상의 중요 자산을 보호하기 위하여 호스트 암호화 및 데이터 저장 보안 능력을 허용한다. 유무선 연결 상에 유비쿼터스 보안을 제공한다.
- 실시간-감시, 관리 및 상호협동: 보안 사고의 타깃이 되거나 취약성 있는 네트워크 요소를 알기 위하여 실시간 감시체계가 수립되고, 관리 및 상호협동 하여야 한다.

V. 맺음말

본 논문에서는 그린 IT의 구현을 위한 보안 기술의 필요성에 대하여 살펴보았다. 먼저 그린 IT의 구현을 위한 핵심요

소인 클라우드 컴퓨팅, 안전한 네트워크, 그린 소프트웨어 분야에서의 보안 기술의 필요성을 기술하였다. 본 고에서는 특히 지능형 전력망의 도입에 따른 보안 기술의 필요성에 대하여 강조하고자 하였다.

2009년 7월 9일 이탈리아에서 개최된 G8 확대정상회의 기후변화 세션에서 지능형 전력망을 선도할 국가로 우리나라가 지정된바 있다. 한국이 스마트 그리드 선도국가로 지정된 만큼 안전한 그리드 구축을 위한 보안 기술의 중요성을 간과해서는 안될 것이다.

그린 IT의 실현을 위한 보안 기술의 중요성을 다시 한 번 더 강조하기 위하여, 두 보안전문가의 조언을 인용하면서 본 논문의 끝을 맺고자 한다 [2]. 임종인 고려대학교 교수는 "에너지 자원 소모를 최소화하기 위해 도입해야 하는 그린 IT에 정보보호의 뒷받침이 없으면 큰 문제를 초래할 수 있다"라고 했으며, 황중연 한국정보보호진흥원 원장은 "잘 알려지지 않았지만 그린 IT에 정보보호가 기여하는 바가 크다. 녹색성장을 위해서도, 깨끗한 인터넷 세상을 구현하기 위해서도 반드시 정보보호를 염두에 둬야 한다"라고 말했다.

참 고 문 헌

[1] 제 3차 녹색성장위원회, 그린 IT 국가 전략(안), 2009. 5.13.

[2] '정보보호 없이는 녹색성장도 위험하다', 전자신문 2009. 4. 9.

[3] '[녹색성장, 그린 시큐리티] DDoS 공격 시리즈', 전자신문, 2009. 4.16~2009.6.18.

[4] 지은희, 류혜숙, 녹색성장의 핵심 엔진, 그린 소프트웨어, SW Insight 정책리포트, 한국소프트웨어진흥원, 2008.11.

[5] Charles P. Pfleeger and Shari L. Pfleeger, Security in Computing(4th ed), Prentice Hall, 2007.

[6] Jelena Mirkovic and Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", Computer Communication Review, Vol. 34(20), pp.39-53, 2004.

[7] '스마트 그리드, 현재 보안 수준으론 안 돼', 전자신문, 2009.3.24.

[8] '지능형 전력망 관심, 우려 교차', 한국정보통신신문, 2009. 5.25.

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

[10] United States Department of Energy, Grid http 자료.

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

약 력

전 용 희

1978년 고려대학교 학사
1989년 미국 노스캐롤라이나주립대 석사
1992년 미국 노스캐롤라이나주립대 박사
1978년 ~ 1978년 삼성중공업㈜
1978년 ~ 1985년 한국전력기술㈜
1979년 ~ 1980년 벨기에 벨가롬사
1992년 ~ 1994년 한국전자통신 연구원 선임연구원
1994년 ~ 현재 대구가톨릭대학교 교수
2001년 ~ 2003년 대구가톨릭대학교 공과대학장
2001년 ~ 2006년 한국통신학회 학회지 편집위원회
2008년 ~ 현재 한국정보보호학회 부회장
관심분야 : 네트워크 보안, 통신망 성능 분석

장 종 수

1984년 경북대학교 학사
1986년 경북대학교 석사
2000년 충북대학교 박사
1989년 ~ 현재 한국전자통신연구원 지식정보보안연구부 책임연구원
2008년 ~ 현재 한국정보보호학회 부회장
2009년 ~ 현재 한국정보처리학회 정보통신응용연구회 위원장
관심분야 : 네트워크 보안, 정책기반 보안관리, 비정상트래픽탐지, 유해정보차단