전력 제어시스템의 보안성 향상기술

최문석
KEPCO 전력연구원 선임연구원

1. 개 황

정보통신기반시설은 사이버 공격 발생 시 국민의 안녕을 위협하고 국가 전반에 걸쳐 사회적 혼란을 야기하는 등 그 파급효과가 크기 때문에 사이버테러 집단의 최우선 공격대상으로 분류되고 있다.

정보통신기반보호법에 의하면 정보통신기반 시설은 에너지 · 국방 · 금융 · 통신 등의 전자적 제어시스템 및 정보통신망을 의미하며, 국민 생활과 긴밀하게 연계되어 있어 국가 안전보장에 막대한 영향을 미치는 핵심시설이다.

2001년 정보통신기반보호법 시행 이후 주요 정보통신기반시설로 지정된 시설은 현재 139개 기관, 209개 기반시설로 국가에 의해 특별 관리하고 있다.

한국전력공사의 경우 송 · 변전 시스템, 배전자동화 시스템과 같은 제어시스템(SCADA)이 정보통신기반시설로 지정되어 있다. 안정적인 전력 공급을 위해서는 전력 제어시스템에 대한 사이버 공격을 차단하고 제어시스템의 이상 징후를 사전에 탐지할 수 있는 보안기술이 필요하다.

2. 현 황

가. 국내외 제어시스템 침해 사례 및 보안위협

1) 국외 침해 사례

2010년 7월 이란 부쉐르 원자력발전소의 원심분리기 1000여 대가 스턱스넷(Stuxnet) 악성코드에 의해 고장나는 사고가 발생했다. 스턱스넷은 독일 Siemens사의 제어시스템을 대상으로 정교하게 제작된 악성코드이며, 제어시스템에 대한 최초의 사이버 무기로 불린다.

이후 2011년 10월에는 스턱스넷과 악성코드의 구조 및 공격방법이 유사하여 차세대 스턱스넷이라 불리는 듀큐(Duqu)가 출현하여 제어시스템에 대한 핵심정보를 공격하기도 하였다.

또한, 2012년 5월 발견된 플레임의 경우 이란 등 중동국가의 정보탈취를 목적으로 미국과 이스라엘에 의해 제작된 악성코드의 존재가 밝혀져 사이버전쟁의 서막을 열었다는 평가를 받고 있다.

2) 국내 침해 사례

2013년 3월 20일 KBS, MBC 등 주요 방송사와 신한은행, 농협 등 금융권 전산망이 악성코드에 감염되어 총 3만 여대의 컴퓨터가 마비되었다. 3.20 전산 대란은 북한이 8개월간 준비해 실행한 것으로 밝혀졌다.

또한, 2013년 6월 25일 발생한 사이버 공격에 의해 청와대 홈페이지와 일부 언론사 등 69개 기관이 피해를 입었고 그중 14개 기관의 하드디스크가 파괴되었다. 6.25 사이버테러에 사용된 해킹방법과 악성코드가 3.20 전산 대란과 유사하였고 북한 IP가 발견되어 6.25 사이버 테러의 배후세력 역시 북한으로 추정되고 있다.

3) 보안위협

이와 같이 실질적인 침해 사례 외에도 제어시스템에 대한 보안 위협은 매년 증가하고 있다. 미국 ICS-CERT의 통계에 따르면 제어시스템의 사이버 침해사례 횟수가 2010년 39건에서 2011년 140건으로 350% 이상 증가하였고, 관련 취약점의 침해 횟수도 18건에서 139건으로 770% 이상 급증하고 있다.

또한, 현재까지 국내 사이버 침해사고는 방송 · 금융 등에 집중되어있지만 향후 공격대상은 산업 기반시설인 전력, 원자력, 수도, 교통 등으로 확대될 것이라는 예측이 보안 전문가의 공통된 의견이다.

북한은 정찰총국 내에 사이버전 지도국을 운영하고 있으며 해킹을 전담하는 사이버 전사 3천 명을 보유하고 있어 미국, 러시아에 이어 세계 3위 수준의 사이버 테러 능력을 보유하고 있다는 평가를 받고 있으며, 우리나라의 주요 정보통신기반시설을 공격할 경우 실제 전쟁과 유사한 피해가 발생할 것으로 예상되고 있다.

이처럼 꾸준히 증가하고 있는 보안위협으로부터 주요 정보통신기반시설인 전력 제어시스템을 보호하기 위해서는 보안 정책의 강화와 보안기술의 연구개발이 필요하다.

나. 국내외 기반시설 보호정책

1) 미국

미국은 9.11 테러 이후 국토안보법을 제정하고 국토안보부(DHS)를 신설하면서 22개 연방정부 기관을 통합하여 국토안보 업무를 효율적으로 수행하기 위한 조직체계를 마련하였다. 오바마 정부는 사이버보안정책을 최우선 과제로 두고 부시 정부에서 수립한

사이버보안 종합계획(CNCI)을 포함시켰다. 또한 정보통신 인프라 방어대책에 대한 전면적인 재검토를 수행하여 2009년 5월 사이버공격 정책 논평을 발표하며 거시적이고 일관성 있는 국가 사이버보안 전략을 추진하고 있다.

2) 영국

영국은 미국 · EU 등 타 국가들의 정보보안정책을 적극적으로 받아들이고 있다. 국가기반시설 보호를 담당하는 MI5와 민간과 공공 부분을 담당하는 국가기반시설보호센터(CPNI)는 통신, 교통 등 9개 카테고리로 기반시설을 분류하여 관리하고 있다. 또한, 2009년 6월 '사이버보안 전략'을 발표하고 사이버 테러에 대한 전략적 목표로 제시하고 있다.

3) 독일

독일은 정보통신기술의 신뢰를 조성하기 위해 자체 정보보안 가이드라인을 운영하고 있다. 독일의 정보통신기반보호에 관한 안전조치는 연방정보보안청(BSI)이 담당하며 정보보호 및 공적 안전 등은 연방망관리청(BNetzA)이 담당하고 있다. 연방정보보안청은 2011년부터 스마트그리드와 스마트 미터 보안에 대한 투자를 강화하고 있다.

4) 일본

일본은 국가기관협의체를 구성하여 사이버전에 대비하기 위한 체계적인 정보보안대책을 마련하고 있다. 2003년 10월 국가정보보안종합전략을 수립하고 2005년 4월 정보보안센터(NISC)를 설치하였으며 정보보호 위협 국제적 대응, 국제경쟁력 강화를 위한 글로벌 정보보호전략을 추진하고 있다.

4) 한국

우리나라는 국가기반시설 사이버 테러에 대비한 국가 차원의 대책으로 2001년 정보통신기반보호법을 제정하였다. 정보통신기반시설에 대한 취약점 분석 · 평가를 수행하고 취약점에 대한 보호조치 및 시행사항을 중점 관리하고 있다.

2011년 1월에는 지능형 전력망의 보호전력망을 구축 및 이용촉진에 관한 법률을 제정하여 스마트그리드 보안성 확보를 위한 기본계획, 보호 대책 이행점검 등의 제도적 장치를 제시하고 있으며 안전행정부에서는 정보통신기반시설의 위협요인을 분석하고 제거하기 위한 '주요 정보통신기반시설 취약점 분석 · 평가 기준'을 2012년 12월 고시하였다.

또한 3.20 전산 대란 이후 정부에서는 정보통신기반시설을 보호하기 위해 취약점 분석 · 평가 기준을 개선하고 내 · 외부 망과의 연동이 필요할 경우 반드시 일방향 통신을 사용토록 권고하는 등의 사이버 공격 대비책을 마련하고 있다.

다. 전력 제어시스템 보안성 향상 기술 개발

1) 사업 개요

정부에서 마련하고 있는 보안대비책을 구현할 수 있는 보안기술은 그 자체가 보호대상이며 선진국의 자국기술 보호 정책으로 인해 도입이 어렵다. 또한 도입이 가능하다 하더라도 국내 제어시스템 환경에 맞게 최적화하는데 오랜 시간과 노력이 필요하다. 이와 같은 문제를 해결하기 위한 국산 보안기술의 확보는 매우 시급한 국가 현안 과제라 할 수 있다.

이에 한국전력공사 전력연구원은 전력 제어시스템 보안성 향상기술 개발을 위하여 지난 3년간(2010년 6월~2013년 5월) 산업통상자원부 전력산업융합 원천기술개발사업 지원으로 총 129억의 연구비를 투입하여 '전력 제어시스템 보안기술 개발' 과제를 수행하였다. 본 연구과제에는 한국전력공사, 국가보안기술연구소, 한전KDN이 참여하고 있다.

본 연구과제에서는 제어명령 암호 및 인증을 통해 전송과정에서의 제어명령 변경을 방지하는 제어통신

보호시스템, 외부침입 경로를 물리적으로 차단하는 일방향 자료전달 시스템, 사이버 공격 시도를 사전에 탐지할 수 있는 이상 징후 감시시스템 등 전력 제어시스템 내 · 외부의 교란행위를 차단하거나 사전에 탐지하는 기술들을 개발하였으며 연구 성과물을 한국전력공사 사업소에 적용하여 성능 검증을 완료하였다.

2) 제어통신 보호시스템

제어통신 보호시스템은 전력 제어시스템의 통신 프로토콜인 DNP(Distributed Network Protocol)에 메시지 암호 및 인증기능을 부가하여 제어명령을 안전하게 전송하는 시스템으로 DNP 메시지 암호 및 인증 기능을 수행하는 보안통신장치와 암호 및 인증에 사용되는 보안 키 관리시스템(KMS : Key Management System)으로 구성되어 있다.

보안기능 적용을 위해 전국에서 운영 중인 전력 제어시스템을 교체할 경우 막대한 비용이 소요되고, 전력 공급이 일시적으로 중단되는 등 많은 문제가 발생되기 때문에 보안통신장치는 BITW[1] 형태로 구현하였다.

DNP 관련 국제표준인 IEEE 1815에서는 Secure Authentication을 추가하였다.

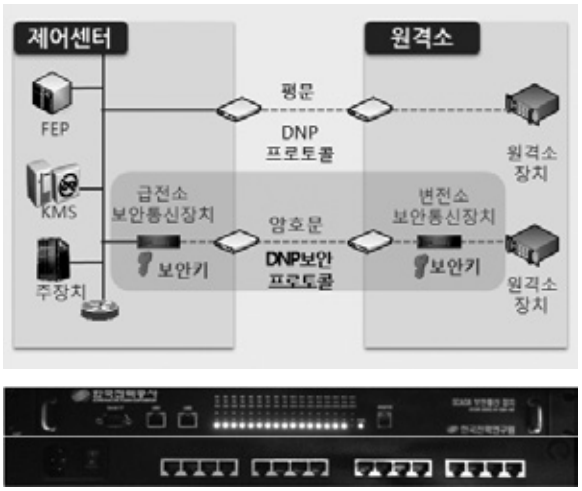
Secure Authentication는 전력 자동화 프로토콜의 정보보안을 위해 IEC 62351의 Part 3와 Part 5의 권고사항을 수용하고 이를 실질적으로 구현하기 위한 통신흐름, function code, object group, variation 등을 구체화하여 기존 DNP 규격에 인증과 무결성 보장을 위한 메커니즘이다.

IEEE 1815 Secure Authentication 규격은 응용계층만 변경하여 메시지 무결성 기능을 제공하고 체계적인 키 구조를 가지고 있다는 장점이 있다. 하지만 보안비용을 고려해 BITW 형태로 보안 기능을 구현할 경우 DNP 메시지 생성주체와 보안기능 수행주체가 다르기 때문에 메시지 재조립 및 분할과정이 부가적으로 발생하며 전송시간이 지연되는 단점이 생길 수 있다.

이러한 문제를 해결하기 위해 본 연구과제에서는 데이터 링크 계층에서 보안기능을 제공하도록 개발하고 응용계층에서 보안기능을 수행함으로써 전송시간 증가를 해결하였다.

또한, 메시지 인증 절차를 간략화하고 데이터 수신 대기시간이 최소화되도록 데이터 전송 알고리즘을 개선하여 제어통신 보안시스템이 제어시스템 전송성능에 영향을 미치지 않도록 개발하였다.

제어통신 보호시스템은 전력설비를 제어하기 위한 제어명령에 직접적으로 보안기능을 부가하는 시스템인 만큼 시스템 안정성 및 신뢰성을 검증하기 위해 전력연구원의 SCADA 보안 테스트베드와 연동하여 장기 성능시험을 수행하였다.



[그림 1] 제어통신 보안시스템 개요 및 시제품

3) 일방향 자료전달시스템

일방향 자료전달시스템은 보안성이 낮은 네트워크(업무망)에서 보안성이 높은 네트워크(제어망)으로의

1) BITW(Bump In the Wire) : 통신보호를 위해 보안기능을 별도의 하드웨어로 구현하는 방식

물리적 통신 경로를 제거하여 중요 시스템에 대한 사이버 공격 경로를 완전히 제거할 수 있는 시스템이다. 국가기반시설의 전자제어시스템 보안가이드 라인에서는 부득이하게 제어시스템 정보를 외부 네트워크로 전달해야 할 경우 안전한 일방향 전송장비의 도입을 권고하고 있다.

네트워크 연계 구간의 대표적인 보안솔루션인 방화벽은 관리적 설정 오류 및 시스템 자체의 보안 취약점에 의해 공격 경로가 발생할 수 있지만 일방향 자료전달시스템은 제어망에 대한 물리적인 접근 경로가 존재하지 않아 공격이 불가능하다.

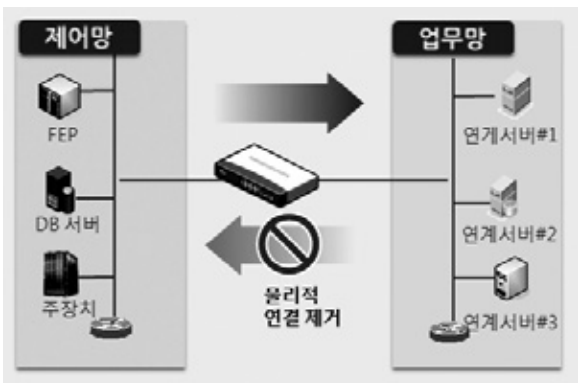
그러나, 일방향 자료전달시스템은 공격 경로를 완전히 제거한다는 장점이 있지만 업무망에서 제어망으로의 데이터 전송이 불가능하기 때문에 제어망의 운영정보를 업무망으로 전달하는 TCP기반의 자료연계 서비스의 TCP 세션 연결이 어렵게 되고 데이터 전송 성공 여부를 확인할 수 없다.

이러한 문제점을 해결하기 위해 TCP 세션 및 응답 생성 역할을 담당하는 서비스 에이전트를 개발하고 자가 에러 복구 알고리즘을 적용하여 데이터 전송 신뢰성을 향상시킴으로서 기존 자료연계 서비스의 변경 없이 일방향 자료전달시스템 적용이 가능하다.

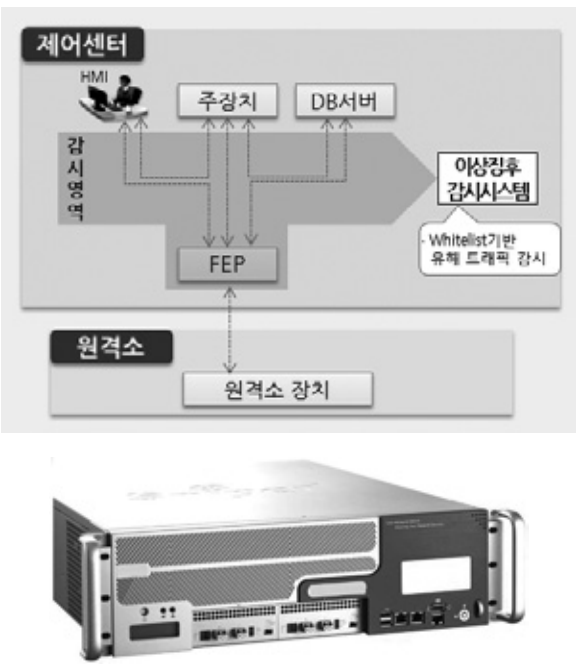
4) 이상 징후 감시시스템

이상 징후 감시시스템은 제어시스템 정상 통신패턴을 화이트 리스트(White list)로 정의하고 이를 위반하는 제어시스템의 내부 트래픽을 실시간 감시함으로써, 제어시스템의 비정상 동작을 유도하는 이상 징후를 조기에 발견하는 세계 최초의 제어시스템 특화 침입 감시시스템이다.

화이트 리스트 기반 감시기술은 사용자의 행위와 신규 서비스 등에 의해 통신패턴이 시시각각 변화하는 IT시스템에서는 적용이 어려우나 통신패턴 및 업무흐름이 일정한 제어시스템에 적합하고 블랙리스트 기반 감시기술에 비해 자원소비율 및 탐지율이 월등하여 최근 제어시스템 대상 공격감시방안으로 주목



[그림 2] 일방향 자료전달시스템 개요 및 시제품



[그림 3] 이상 징후 감시시스템 개요 및 시제품

받고 있는 기술이다.

기존 블랙리스트 기반 감시기술은 유해트래픽 감시규칙인 시그니처를 주기적으로 업데이트해야 하고 방대한 양의 시그니처를 관리해야 하는 반면 화이트리스트 기반감시기술은 감시규칙의 관리 부담이 적다. 또한, 기존의 방화벽과 침입 탐지 · 방지 시스템 등 블랙리스트 기반의 보안장비는 DNP3, Modbus, ICCP와 같은 제어 프로토콜 및 제어시스템 운영상의 특성을 반영하지 않기 때문에 제어시스템에 특화된 공격 트래픽 탐지에 한계가 있지만 본 연구과제 성과물은 제어메시지의 전송 흐름과 제어 트래픽의 통계적 특성을 반영하여 제어시스템에 특화된 공격 트래픽 및 제로데이터 공격*의 탐지가 가능하다.

3. 향후 계획

본 연구 과제를 통해 개발된 연구 개발품은 사업소 현장 시험을 통하여 성능 검증이 완료되었으며 연내 시범사업을 수행할 계획이다.

향후, 시범사업을 통해 개발된 기술을 지속적으로 보완하고 최적화하여 한국전력공사 전체에 확대 보급할 계획이다.

연구 개발품은 한국전력공사뿐만 아니라 발전그룹사, 한국가스공사, 한국수자원공사, 한국철도공사 등 다른 국가 기반시설에 적용이 가능하여 범국가 차원의 기반시설 보안성 향상에 기여할 것으로 전망된다.

* 제로데이 공격(Zero-Day Attack) : 소프트웨어상의 알려지지 않은 보안 취약점을 이용해 공격하는 기법