산업제어시스템을 위한 사이버 보안 시스템적용 방안

한경수*, 정현미*, 이강수*, 장수진**
*한남대학교 컴퓨터공학과
**보건대학교 컴퓨터 정보통신 학과
e-mail: psksmail@hnu.kr, mihj@se.hannam.ac.kr, gslee@eve.hannam.ac.kr, sjjang@hit.ac.kr

An application method for industrial control cyber security system

Kyung-su Han*, Hyun-mi Jung *, Gang-Soo Lee * , Su Jin Jang**
*Dept of Computer Engineering, Hannam University
**Dept of Computer Information communication, Daejeon Health college

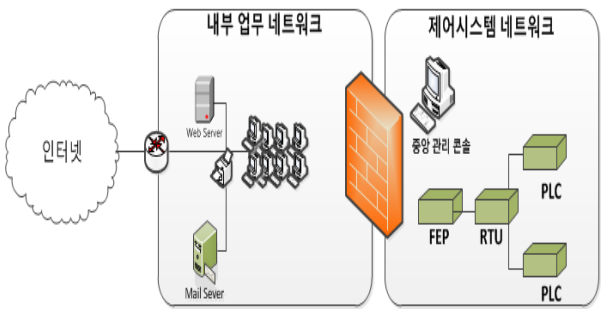
요 약

산업제어시스템(ICS: Industrial Control System)은 전력 생산, 댐 운영, 가스 생산, 수자원 관리, 원자력 발전 설비 등의 운영을 제어하고 관리하는 시스템이다. 대부분의 국가 기반 시설은 이러한 제어시스템에 의해 관리되고 있으며, 정보통신 기술이 발전하면서 업무망과 제어시스템망을 나누워 구축하며 점차 개방화되어 가고 있다. 이로 인한 IT측면에서 발생하는 사이버 공격이 비교적 폐쇄적인 제어 시스템 망으로 언제든지 이루어질 수 있으며, 실제 국내에서 독립적인 네트워크를 사용함에도 불구하고 금융권의 전산망이 마비되는 사태가 발생하였다. 또한 국외에서는 이란의 원자력 발전소 제어 시스템을 목적으로 하는 'Stuxnet' 악성코드로 인해 발전소 운용이 중단돼는 사례도 발생하였다. 산업용 시스템의 목적과 특성상 사이버 침해사고 발생 시 국가적 손실 및 생명에도 위협을 받을 수 있다. 본 논문은 과거에 보안을 고려하지 않고 구축되었던 제어시스템을 사이버 침해로부터 보호하기 위해 제어시스템을 위한 통신 프로토콜 암호화 및 화이트리스트보안 기술을 이용한 시스템 적용 방안을 소개하며, 네트워크 접속시 인가된 산업용 PC의 안전성을 평가하기 위해 요구되는 보안 플랫폼 설계를 한다.

1. 서론

전력 생산, 분배, 댐 운영, 가스 생산, 유통, 수자원 관리등 대규모 플랜트 시설들을 제어하는 제어시스템은 정보통신 기술을 활용함에 따라 점차 개방화 표준화 되어가고 있다. 이로 인한 사이버 침해인 네트워크로 인한 해킹, 사이버 테러 등의 위협으로부터 안전할 수 없게 되었다.

미국의 경우, 제어 시스템 침투 및 파괴 가능성을 테스트하여 취약점을 식별하고 대책을 세우기 위한 민·관 합동의 다양한 노력을 진행하고 있으며, 미국 원자력 규제 위원회(NRC)에서는 '원자력 설비를 위한 사이버 보안 프로그램' RG(Regulatory Guide)5.71 과 같은 사이버 보안에 대한 새로운 규정 지침을 제시하고 있다**[1]**.



(그림 1) 전형적인 제어시스템 네트워크 구성도**[2]**

제어시스템의 대표적인 SCADA(supervisory Control and Data Acquisition)시스템은 (그림 1)과 같이 플랜트 설비와 대개 PLC(Programmable Logic Controller)를 통해 연결 되며 제어권한이 공격자에게 절취 당하거나 서비스를 하지 못할 경우 실생활에 피해를 줄 수 있다.

SCADA시스템은 비교적 격리된 환경에서 운용되며 주로 독점 소프트웨어와 하드웨어, 통신 기술에 의존하였으나 제어 시스템과 업무 시스템간 상호 연동 필요성 및 연계를 위한 상호운용성이 강조 되어 Windows나 UNIX와 같은 상용 운영체제의 사용과 인터넷 및 VOIP전화망 네트워크와 같은 일반 통신기술이 사용되고 있다. 제어 시스템의 상호 연결로 인한 접속점이 증가하고 시스템 복잡도가 증가함에 따라 제어 시스템에 대한 사이버 침해 및 사례는 여러 분야에서 감지되었다.

제어시스템에 대한 취약성이 발견됨에 따라 보안 시스템의 적용 방법과 그 특성을 파악함으로써 효과적인 산업용 제어시스템에 대한 적용 방안이 필요하다.

본 논문은 제어시스템의 가장 큰 특징인 24시간 항상 운용되어야하는 점과 비교적 인터넷과 격리된 망에서의 바이러스 침해를 예방하기위해, 산업용 시스템을 위한 전체적인 보안 플랫폼의 필요성과 함께 설계를 제안한다. 2장에서는 제어시스템이 사이버보안으로부터 안전하지 않은 사례와 IT시스템

과의 차이에 대하여 기술하고, 3장에서는 산업용 제어시스템에 적용 가능한 보안 제품들과 함께, 4장에서 사이버 보안을 위한 보안 플랫폼 설계를 제시하며, 5장을 끝으로 결론을 맺는다.

2. 연구 배경

2.1 제어시스템 사이버 보안 침해 사례[4].

- 1988년, “Eligible Receiver”라고 알려진 2주간의 미국의 사이버테러 모의훈련 중에 미국의 전력제어 시스템을 대상으로 NSA직원이 다양한 방법을 이용하여 사이버 공격이 가능함을 확인하였다.
- 1999년 6월 워싱턴주의 ‘Olympic Pipe Line’이라는 회사에서 16인치 직경을 가진 파이프라인이 파열되어 237,000 개런의 개소린이 샛강과 공원에 유출되고 90분간 발화하여 1.5마일의 샛강을 따라 화재가 전개 되었다. 이사고로 3명의 어린이가 희생되었고 8명이 부상을 입었으며 수도 공급시설이 심각한 손실을 입었다.
- 2000년 봄에 호주 지방정부의 사업에 사용하기 위해 공장 자동화 소프트웨어를 개발한 어느 기업의 전직직원이 해고에 불만을 품고, 하수처리 시스템을 무선으로 원격 침입하여 264,000갤런에 달하는 하수를 강과 공원에 방출하였다.
- 2003년 1월에 MS사의 SQL 서버 웜인 Slammer가 오하이오의 오크하버에 있는 핵발전소(Davis-Besse Nuclear Power Plant)의 사설 컴퓨터 네트워크에 감염되어 5시간동안 시스템의 안전성을 감시할 수 없었고 플랜트 러치 컴퓨터가 작동하지 않아 다시 복구하는데 6시간이 소요되었다.
- 2005년 8월, 미국의 Daimler Chrysler 13개 자동차 공장이 단순한 인터넷 바이러스(Zotob worm) 하나로 인해 멈추어선 적이 있다. 인터넷 망과 사내 망 사이에는 Firewall이 당연히 설치되어 있었지만 worm은 제어시스템으로 들어갔고 수초 안에 이 공장 저 공장으로 확산되었으며 이로 인한 피해액은 1400만 달러에 이르렀다.
- 2006년 8월 Browns Ferry Nuclear Plant의 시설 운영자는 ‘high power, low flow condition’ 상태에서 원자로를 끌 수 밖에 없었다. 냉각수 시스템을 제어하는 이중화되어 있는 장치가 제어 네트워크에서 ‘excessive traffic’을 감지하였기 때문이다.
- 2009년과 2010년 이란 핵시설이 악성코드에 감염되어 가동 중단 사태가 발생하였다.

이러한 제어시스템이 사이버 공격에 취약한 이유는 폐쇄망로 운영되는 환경으로 인식하여 정보보호 시스템이 구축이 되어있지 않으며, 관리자의 보안의식이나 대처 능력이 부족할 수밖에 없다. 제어시스템의 보안 침해 사례와 같이, 보이지 않는 사이버 공격은 국가의 주요 산업 기반시설을 제어하는 시스템에 침투해 오작동을 유도하며 시스템을 마비 또는 파괴시킬 수 있다는 것을 알 수 있다.

2.2 제어시스템 과 IT시스템 차이

산업제어시스템(ICS: Industrial Control System)의 구조는 IT 시스템과 비교해봤을 때 목적의 특성상 차이점이 있기 때문에 이로 인한 보안 요구사항도 달라진다. 제어시스템은 특정 장비 전용으로 사용함으로 사양이 IT시스템보다 상대적으로 낮다. 솔루션 패치나 업데이트로 인한 장애를 최소화해야 하며, 불필요한 프로그램으로 인한 리소스낭비가 없어야한다.

ICS를 위한 네트워크 구조 설계는 업무망과 분리시킬 것이 권고 된다. 업무망에서 일반적으로 허용되는 웹서버를 통해 외부에서 제어시스템 네트워크로 침입하는 경우가 발생할 수 있기 때문이다.

다음 <표 1>은 산업용 제어시스템을 IT측면과 비교한 내용이다.

<표 1>제어시스템과 IT측면에서의 시스템 차이 비교

제어시스템 측면	IT 측면
우선순위는 무결성(relibility)과 가용성(availability).	보안성>무결성>가용성의 우선순위로 관리됨.
다수 프로토콜 차이로 여러 솔루션이 필요하다.	일반보안 tool은 제어 시스템에 적용되어 작동되지 않음.
운전정지등이 허용되지 않음.	일반적으로 지연 허용
네트워크 및 사내망 과 독립되어있음.	사내 시스템 망 또는 인터넷 망과 제어 시스템 망이 서로 연결되어 있음.
엔드 포인트 끝단의 장비중심	서버중심의 보안정책
Default password를 사용	특별한 규정 없음
시스템 updata & patch가 어렵거나 운영 중 불가능함.	updata & patch가 정기적으로 계획되어 있음

2.2 제로데이 취약성 이용한 악성코드

제로 데이란 윈도우 익스 플로우나 여러 응용프로그램의 취약점을 해커들이 보안 패키지가 나오기 전에 공격이 시작됨으로써 이름이 붙여졌다. 점차 제어시스템에서도 범용 OS를 사용하는 추세이며, 운영체제 자체 취약성을 이용한 사이버 공격이 이루어질 수 있다. 세계적인 전기전자 기업인 지멘스(siemens)의 WinCC, SCADA 시스템을 타켓으로 공격이 이루어진 사례가 있다. 제어시스템 제품 조사결과 지멘스 테크노매트릭스 팩토리 링크, 아이코닉스 제네시스 32와 64, 7테크놀로지스의 IGSS, DARAC 리얼윈의 버그트랙 보안 e메일 리스트 등 제품이 보안 위협에 노출됐다고 발표되었기 때문에 앞으로 제로데이 위협이 국내에도 도입될 스마트 그리드와 같은 국가 중요 패쇄 망 시스템을 노리고 있을 가능성이 크다.

2.3 SCADA시스템 바이러스 웜 Stuxnet

SCADA와 같은 폐쇄적인 환경에서 악성코드에 감염될 경우 백신프로그램으로는 대응이 어려울 수밖에 없다. 또한 산업용 PC의 경우 인터넷에 접속할 수 없기 때문에 백신 프로그램을 설치하지 않는 경우도 많다.

하지만 업무용 PC와 데이터를 공유하는 과정에서 USB메모리를 사용함에 따라 악성코드의 유입 경로가 될 수 있으며, 범용 OS를 사용하는 시스템에서 실제 2009년과 2010년 이란 핵시설에 악성코드가 감염되어 가동이 중단되는 사태가 발생했다. 사이버공격이 일부 성공한 것으로 알려졌으며 사용된 악성코드는 'Stuxnet'이다. 'Stuxnet'악성코드가 이용한 시스템의 취약점은 아래 <표 2>와 같다.

<표 2> 'Stuxnet'악성코드가 사용하는 시스템의 취약점**[5]**.

구 분	코드명	취약점
윈도우 취약점	MS08-067	서버 서비스의 취약점으로 인한 원격코드 실행 문제점.
	MS10-0426	윈도우 쉘 취약점으로 인한 원격코드 실행문제.
	MS10-061	프린트 스풀러 서비스의 취약점으로 인한 원격 코드 실행 문제점.
WinCC, PCS7	CVE-2010-2722	지멘스 SCADA시스템의 하드코드 패스워드로 인한 보안 취약점.

미국표준기술연구소 (NIST: National Institute of Standards and Technology)에서 제공하는 Nateional Vulnerability database에서 'Stuxnet'악성코드 검색결과 'Win32k Keyboard Layout Vulnerability'으로 windows 커널 모드 드라이버의 취약점으로 인한 권상 상승 문제점을 이용한다는 것 또한 알 수 있다.

3. 관련 연구

3.1 산업용 시스템에 적용 가능한 보안 시스템

3.1.1 화이트리스트 보안

산업용 시스템에서의 중앙 관리 서버에 적용 가능한 보안 솔루션은 크게 블랙리스트 기반의 방식과 화이트 리스트 기반의 방식으로 나눌 수 있다. 블랙리스트 방식의 대표적인 솔루션은 안티바이러스 솔루션으로 위험성이 입증된 악성 코드에 대해 시그니처를 제작하고, 차단하는 방식이다. 이러한 방식은 편의성이 높지만 알려지지 않은 신종 공격에 취약할 뿐만 아니라 발견되는 악성코드 및 IP에 대해 수없이 많은 업데이트가 필요하다. 국내 화이트리스트 기반 솔루션으로는 안철수 연구소 'Trusline'이 있다. 블랙리스트 와 반대되는 개념으로 허용된 프로그램만 실행 가능하게 함으로써 알려지지 않은 악성코드 및 침입을 좀 더 효과적으로 대처할 수 있는 보안 기술이다.

특히 화이트 리스트의 단점으로는 인가된 사용자라고 할지라도 외부에서 내부로 접근이 어렵다. 하지만 특정한 업무만 수행하는 서버나 산업용 컴퓨터와 같이 변화가 적고 운용되는 애플리케이션 숫자가 많지 않은 기기에서는 효용의 가치가 높다.

3.1.2 바이러스 대응 PC포트 차단 프로그램[6].

대부분 산업용 제어 PC는 업무망과 분리되어 운영되는 폐쇄 환경에서 운영된다. 제어 프로그램과 애플리케이션등의 업데이트가 요구되기 때문에 외부 네트워크와 연결되어 있지 않은 산업용 PC는 USB메모리 등을 이용하여 업데이트를 실행하게 된다. 이때 'Stuxnet'과 같은 악성코드에 감염된 PC에서 사용된 메모리 일 경우 산업용 자동화 시스템에 악성코드가 침입할 수 있게 된다.

산업용 시스템에 적합하게 제작되고 있는 USB는 보안기능으로 자동실행 방지와 사용자 식별인증, 지정 데이터 암복호화, 저장된 자료의 임의 복제 방지, 분실시 저장 데이터의 보호를 위한 삭제 등의 기능을 한다.

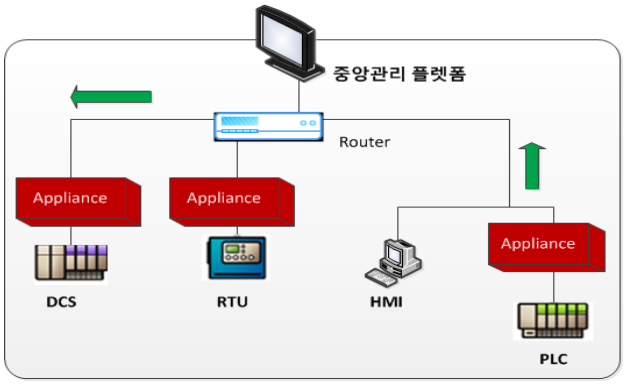
하지만 기업의 정보 유출을 차단하기 위해서 가장 기본적으로 제어를 해야 하는 것은 산업용 PC의 포트이다. 보안 USB를 사용하더라도 포트 자체를 제어하지 못한다면 일반 USB나 외장 HDD를 이용하여 더 많은 정보가 유출 될 수 있다. 국내 브레인즈스퀘어 회사에서는 컴퓨터에 부착된 다양한 장치를 제어할 수 있는 S/W인 SecuDrive Device Control 제품을 제공한다. 권한이 있는 사용자에 한에서 일시적으로 모든 장치 제어를 해제 또는 설정 할 수 있으며, 장치 제어가 해제 되더라도 해당 사용자의 장치 사용 로그는 모두 중앙에 수집된다.

3.1.3 SCADA 시스템 통신 프로토콜 보안[7].

전형적인 SCADA시스템 구조는 HMI(Human-Machine Interface), 관리시스템(Supervisory System), 센서에 연결되어 수집된 센서 신호를 디지털 데이터로 변환 하는 RTU(Remote Terminal Unit), 복합적인 입/출력을 위한 PLC(Programmable Logic Controller) 등으로 구성되어 있다.

광대역 통신 요구사항을 맞추기 위해 무선통신과 시리얼 또는 라우터에 연결을 통해 통신 인프라를 구성하며 이는 RTU에서 중앙 관리 시스템으로 연결을 뜻한다.

통신 프로토콜은 Modbus, IEC60870-50101 또는 104, IEC61850, DNP3.0등 이 있으며 직렬 통신구조로 이루 워 져 있다.



(그림 2) SCADA시스템 네트워킹보안 구성도

직렬 통신 보호를 위한 Tofino 제품군 'Starter Pack'은 (그림 2)과 같이 제공되는 Appliance를 각 제어장치에 설치할 수 있다. 네트워크 장치와 쉽게 통신이 가능하며 어떤 프로토콜이든 규칙을 정할 수 있다. 자산관리 모듈을 통해 수신하는 모든

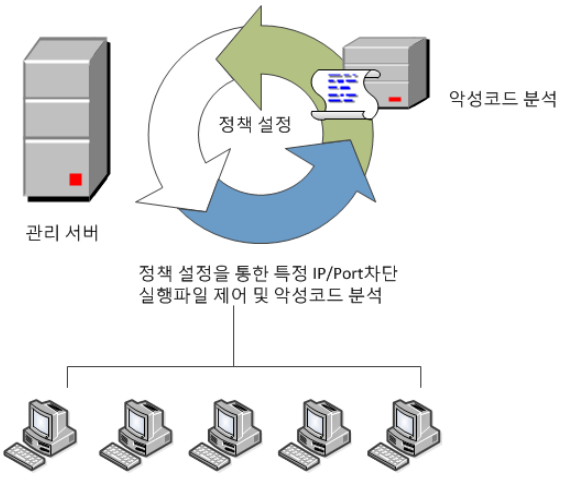
장치를 추적할 수 있으며 Firewall Loadable 기능으로 지정된 프로토콜과 일치하지 않는 트래픽을 확인하고 차단할 수 있다.

중앙관리 플랫폼에서는 보안 어플라이언스를 신속하게 구성하며 관측 및 모니터링 기능이 가능하다.

SCADA시스템의 기본 프로토콜 DNP3.0 및 Modbus 등을 사이버 위협으로부터 보호하기 위해서는 제어시스템 프로토콜 보안 정책과 함께 하드웨어 기반의 암호화 엔진의 연동이 필요하다.

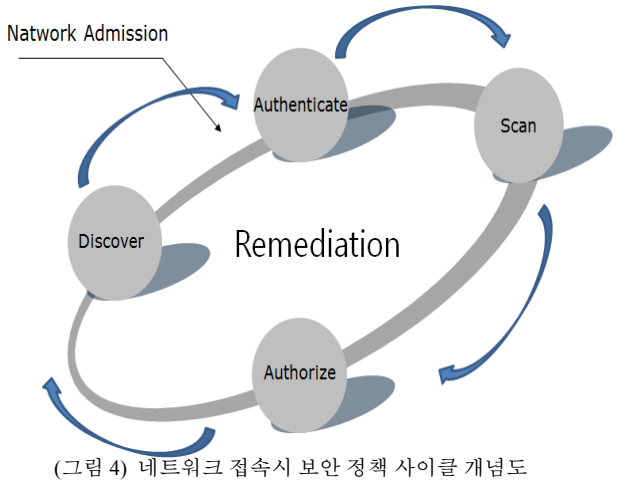
4. ICS 사이버 보안을 위한 설계

전형적인 ICS 구조는 Central Server서버를 통해 제어시스템 PC와 네트워크 구조를 갖는다. Central Server에서는 모든 방역과 실행파일 제어를 통해 시스템의 리소스를 최소화 하여야 하며, 악성코드 또한 분석되어야 한다.



(그림 3) 화이트 리스트 보안 기술 적용 중앙관리 서버 구성도**[8].**

서버에서는 인가된 단말에 대한 실행파일 제어와 악성코드 분석 및 악성코드를 유포하는 IP/Port를 차단할 수 있어야 하며 (그림 3)와 같이 'Trustline'의 구성 컨셉에 네트워크 접속하려는 제어PC에 대해 네트워크 보안을 위한 일련의 정책이 필요하다.



(그림 4) 네트워크 접속시 보안 정책 사이클 개념도

(그림 4)과 같이 Policy Manager에서 인터넷으로부터 악성코드의 유포를 막기 위해 보안 절차를 통한 안전성이 검증된 단말 만이 네트워크에 접속할 수 있도록 하는 보안 플랫폼이 필요하다. 구조는 화이트 리스트 보안 설정에 따른 네트워크에 접속하려는 인가된 단말에 대한 발견과, 인증, 정밀 검색 작업과 승인으로 이어지는 사이클 구조로 Discover, Authenticate, Scan, Authorize의 모든 단계에서는 정책 위반을 검출 하는 기능이 있어야 하며, 위반 사항에 대해서는 경고 메시지나 해결 방안을 제시할 수 있도록 해야 한다[9].

5. 결론

SCADA시스템 및 산업용 시스템은 제어 창치 상에 시그니처의 최소화 문제와 항시 운용 보안 장치를 운영하기가 어려운 환경이다. 제어시스템은 IT시스템과 그 요구사항과 운용환경 다른 특성을 가지고 있으며, 기존제어 시스템 보안제품이 제어시스템에 적용하기 어려운 문제점을 고려할 때, 제어스템을 위한 보안 제품은 실시간 응답, 24시간 운영이 보장되어야 하며 독립망 형식으로 운영 되어야한다. 데이터를 전달하는 대상이 고정적인 특성 또한 고려해야한다.

전송 데이터에 대한 IT측면에서의 기밀성보다는 무결성을 중요하게 접근해야한다.

상용솔루션을 적용하기 위해서는 우선 네트워크 기반의 IPS방식을 고려해야 하며 부가적인 보안 모듈설치가 가능한 경우에는 화이트 리스트 형태의 어플리케이션을 이용하여 알려지지 않은 악성코드를 좀 더 효과적으로 차단할 수 있다.

향후 ICS에 대한 공격을 통해 사회 기반 시설에 대한 혼란을 통해 국가안보를 저해할 수 있다. 차세대 제어시스템의 보안을 위해서는 사이버 공격에 대한 방역 기능과 일련의 보안 절차를 수행할 수 있는 정책 및 설계를 갖춘 ICS용 보안 솔루션 개발을 향후 과제로 남긴다.

[참고문헌]

[1] U.S.NUCLEAR REGULATORY COMMISSION, "REGULATORY CUIDE 5.71", JANUARY 2010.
[2]김영진외, "SCADA시스템의 안전성 확보방안에 관한 연구", 정보보호학회 논문지, 2009, 12, PP 146.
[3] 이철원, "주요제어시설의 사이버 보안 동향", 국가 보안기술 연구소(NSRI), 2007,4.
[4] 한국 정보 보호 진흥원, "국외 시스템 기반 평가 사례 및 기술 분석", PP 19~21.
[5] 박형근,"Stuxnet 상세분석 보고서", IBM Secufirty, 2010,12, pp 6.
[6] www.secudrive.co.kr,"SecuDrive Device Control PRODUCT CATEGORY".
[7] www.tofinosecurity.com,"Starter Pack PRODUCT CATEGORY".
[8] www.ahnlab.com,"TrusLine PRODUCT CATEGORY".
[9]www.innocore.co.kr,"mirage NAC MAP".