Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.2, Apr. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.2.295

발전소 주제어시스템 모의해킹을 통한 취약점 분석 및 침해사고 대응기법 연구

고 호 준,[1†] 김 휘 강[2‡]
[1]한국남동발전, [2]고려대학교

A study on vulnerability analysis and incident response methodology based on the penetration test of the power plant's main control systems

Ho-Jun Ko,[1†] Huy-Kang Kim[2‡]
[1]Korea South-East Power Co, [2]Korea University

요 약

발전소 주제어시스템(DCS, Distributed Control System)은 원격지의 설비를 계통현황에 따라 실시간 조작, 감시 및 운전 효율성을 향상시키기 위해 튜닝을 하도록 구현된 자동화 시스템이다. DCS는 IT 기술의 발전과 함께 점차 지능화, 개방화되고 있다. 많은 전력회사들이 DCS에 설비 관리용 패키지 시스템을 접목하여 예측진단을 통한 유지·보수 및 Risk Management를 실현시키기 위한 투자를 확대하고 있다. 하지만, 최근 해외사례에서 보듯이 원전·전력망 등 국가 주요기반시설인 산업 제어시스템(ICS)을 마비시키고 파괴할 목적으로 개발된 최초의 사이버 전쟁무기인 스턱스넷이 출현하는 등, 폐쇄형 시스템으로 구성된 발전소 주제어시스템도 점차 외부 공격으로부터 위협의 대상이 되고 있음을 알 수 있다. 높은 수준의 가용성(낮은 고장빈도와 신속한 복구)과 운영 신뢰성의 이유로 10년 이상 장기 사용이 요구되는 발전소 주제어시스템의 경우 전적으로 해외 기술에 의존하고 있고 패치 업데이트 등 주기적 보안관리가 이뤄지지 못해 잠재된 취약점이 노출될 경우 심각한 우려가 예상된다. 본 논문에서는 국내 발전회사에서 사용 중인 Ovation 1.5 버전의 간이 시뮬레이터 환경에서 범용 취약점 분석툴인 NESSUS를 활용하여 인가된 내·외부 사용자의 악의적 행위(모의해킹)를 수행하였다. 이를 통해 취약점 탐지 및 발전소 제어시스템 내 사이버 침해사고 발생 시 효과적으로 대응 할 수 있는 취약점 분석 및 로그분석 방안을 제시하고자 한다.

ABSTRACT

DCS (Distributed Control System), the main control system of power plants, is an automated system for enhancing operational efficiency by monitoring, tuning and real-time operation. DCS is becoming more intelligent and open systems as Information technology are evolving. In addition, there are a large amount of investment to enable proactive facility management, maintenance and risk management through the predictive diagnostics.

However, new upcoming weaponized malware, such as Stuxnet designed for disrupting industrial control system(ICS), become new threat to the main control system of the power plant. Even though these systems are not connected with any other outside network. The main control systems used in the power plant usually have been used for more than 10 years. Also, this system requires the extremely high availability (rapid recovery and low failure frequency). Therefore, installing updates including security patches is not easy. Even more, in some cases, installing security updates can break the warranty by the vendor's policy. If DCS is exposed a potential vulnerability, serious concerns are to be expected. In this paper, we conduct the penetration test by using NESSUS, a general-purpose vulnerability scanner under the simulated environment configured with the Ovation version 1.5. From this result, we suggest a log analysis method to detect the security infringement and react the incident effectively.

Keyword : DCS security, log analysis, vulnerability analysis, penetration test, incident response

접수일(2013년 6월 12일), 수정일(2013년 12월 9일) 게재확정일(2013년 12월 17일)
* 본 연구는 고려대학교 정보보호대학원 석사학위 논문임.

† 주저자, sunyujin@koreatech.ac.kr
‡ 교신저자, sangjin@koreatech.ac.kr (Corresponding author)

Ⅰ. 서 론

컴퓨터를 이용한 제어개념은 1960년대 중반부터 프로세스 제어분야에 도입되기 시작하였으며 초기의 컴퓨터를 이용한 제어개념은 1970년대 중반까지 한 대의 컴퓨터에 의한 DDC(Direct Digital Control) 시스템과 현장 아날로그 연결에 의한 제어 방식이 주종을 이루고 있었다. DDC 시스템이란 한 대의 컴퓨터에 프로세스 데이터의 입력, 출력 및 플랜트의 감시, 조작, 제어 등을 모두 집중화 시켜 관리하는 시스템이다.〔1〕

하나의 중앙처리 장치를 여러 개의 작은 중앙 처리 장치로 나누어 기능별로 분리하고 작은 용량의 중앙처리 장치를 갖는 각각의 컴퓨터를 통신 네트워크로 연결시켜 전체 시스템을 구성하도록 한 DCS (Distributed Control System)가 1975년에 탄생하였다.

DCS의 기본개념은 공정제어에 적용되는 시스템을 각 플랜트에 맞게 단위 서브시스템으로 분리하고 주어진 역할을 수행하며 상호간에 통신이 가능하도록 한 것으로서 소형 DDC 시스템 여러 개를 유기적으로 연결하여 전체 시스템을 구성한 것이라 볼 수 있다. 이후 감시와 조작은 집중시키고, 고장에 대한 위험성은 분산시키고자 하는 지속적인 사용자의 요구에 의해 분산제어시스템은 점차 향상되고 통합화 되고 있다. 또한 IT 기술의 향상으로 지능화, 개방화되고 있으며 발전소 자체적으로도 엔지니어링 기술이 집약되면서, DCS에 설비 관리용 패키지 시스템을 접목하여 OA망에서 예측진단을 통한 유지·보수 및 Risk Management를 할 수 있게 되었으며, 이를 정착시키기 위해 기술투자를 점차 확대하고 있다.

하지만 최근 해외사례에서 보듯이 원전·전력망 등 국가 주요기반시설인 산업 제어시스템(ICS)을 마비시키고 파괴할 목적으로 개발된 사이버 전쟁무기인 스턱스넷(Stuxnet)이 전 세계로 확산되고 있어 폐쇄형 시스템으로 구성된 발전소 주제어시스템도 점차 외부 공격으로부터 위협의 대상이 되고 있음을 알 수 있다. 스턱스넷은 폐쇄망으로 운용되는 독일 지멘스사의 산업자동화제어시스템(PCS7)만을 공격목표로 제작된 악성코드로서, 지금까지의 악성코드가 실력과시나 금전적인 이득을 목적으로 한 것과 달리 사회기반시설의 파괴만을 목적으로 하고 있다는 점에서 사이버 무기화된 최초의 사례로 알려져 있다. 스턱스넷은 PC를 감염시킨 후 이 PC에 연결되는 휴대용 저장장치(USB, 외장형 하드디스크 등)를 통해 산업시설 내 컴퓨터로 침투하는 것으로 밝혀졌다.〔2〕

발전소 주제어시스템은 높은 수준의 가용성(낮은 고장빈도와 신속한 복구)과 운영 신뢰성의 이유로 10년 이상 장기 사용이 요구된다. 더불어 전적으로 해외 기술에 의존하고 있기 때문에, 패치 업데이트 등 주기적 보안관리가 이뤄지지 못해 잠재된 취약점이 노출될 경우 심각한 우려가 예상된다. 특히 제어시스템이 제조사의 고유한 프로토콜을 사용하던 방식에서 벗어나 상호 호환성 확보를 위해 표준화 되어감에 따라, 공개된 표준을 통해 공격자는 제어시스템 및 네트워크 동작에 대해 손쉽게 지식을 습득할 수 있게 되었으며, 이에 따라 공격의 가능성과 위험성 역시 높아지고 있다. 신규 버전의 주제어시스템의 경우 세계적인 보안 이슈로 인해 제조사에서 알고리즘 암호화 및 패치 업데이트 전용 서버 구축 등 자체 보안정책을 수립하여 출시하고 있으나 이미 설치 운용중인 대다수의 발전소 DCS는 보안대책을 전혀 고려하지 않은 채 도입된 상태이다. 하지만, 보안 취약점에 대한 패치 업데이트 권고사항 조차 시스템 정지 및 오동작 사례가 있어 적용하기가 어려운 상황이다.

본 논문에서는 Ovation 1.5 버전(Emerson社, 1999년 출시)의 간이 시뮬레이터 환경에서 범용 취약점 분석툴인 NESSUS를 활용하여 인가된 내·외부 사용자의 악의적 행위(모의해킹)를 재현하였다. 이를 통해 취약점 발굴, 개선과 함께 효율적 로그 분석 기법을 연구하여 발전소 제어시스템 내 사이버 침해사고 발생 시 효과적으로 대응 할 수 있는 방안을 수립하고자 한다.

시뮬레이터 환경은 주제어기 2대, DB Server 1대, 운전원 조작용 HMI 1대를 CISCO2950 스위치로 구성하였으며, 스위치의 활성화된 포트에 비인가 노트북(NESSUS 탑재)이 연계되어 해킹툴을 실행시키면서 쌓이는 로그 분석을 통해 침해사고 시 효율적 대처 방법 및 예측 가능성을 모색하고자 하였다.

해당 발전소의 경우 운전정보시스템, 플랜트 성능감시 시스템이 망분리 장치를 통해 DCS와 OA망에 연계되어 있으며 이를 완벽한 폐쇄망이라 규정하였고, 정지 중 DCS 전용 네트워크 스위치의 로그확인을 위해 제작사 및 관리자의 노트북(Clean PC)을 연결시키는 사례가 있어 충분히 현실성이 있다고 보고 본 연구와 같은 가상 시나리오를 설정하여 실험을 실시하였다.

II. 관련연구

2.1 DCS의 기본 특징

프로세스 제어기능을 여러 대의 컴퓨터에 분산시켜서 신뢰성은 향상시키고 이상 발생 시 그 파급 효과를 최소화시키며 프로세스 정보처리 및 관리기능 등은 중앙의 주 컴퓨터(DOC : Distributed Operate Console)에 집중화시킴으로서 자료처리 및 운영관리를 원활히 하고 중앙제어실에서 플랜트 전반에 대한 감시, 제어, 운전 및 조작이 가능토록 설계되어 있다. 즉 "기능의 분산과 정보의 집중"이라는 2가지 특징 사이에서 균형을 유지하면서 개발되고 있으며 재래식 아날로그 계장시스템과 비교하여 DCS의 주요 장점은 다음과 같다. [1]

- 일관성 있는 공정 관리로 제어의 신뢰도가 향상되며 다양한 응용이 가능하고 유연성 있는 제어가능.
- 한 조작자가 처리공정에 대한 많은 정보처리 및 제어기능을 수행하며 집중관리 가능하여 인력의 효율적 활용 및 유지보수 용이.
- 복잡한 연산과 논리 회로를 구성할 수 있고 Data의 수집 및 보고서(Report) 작성 기능이 있으며 이중화(CPU, Power, Network 등) 적용으로 시스템 안정성이 높음.

2.2 Ovation System 구성현황

모든 컴퓨터 시스템에는 할당된 기능을 수행하기 위해 소프트웨어가 필요하다. 컴퓨터에 기반을 둔 DCS는 프로세스 정보, 제어 알고리즘 그리고 적절한 운전에 필요한 운전자 인터페이스 명령으로 프로그램되어야 한다.

또한 대부분의 분산제어설비 신호흐름은 현장에 설치된 각종 계측기에서 감지한 신호가 마셜링 패널 및 릴레이 패널을 거쳐 프로세스 제어유닛의 입출력 모듈로 인입된다. 이들 전송된 신호는 CPU에서 정해진 프로그램에 따라 연산되며 결과는 Data Highway를 통해 운전원 스테이션으로 전달되어 운전용 모니터의 그래픽 화면에 지시된다. 또한 운전원이 조작한 신호는 이와 역순으로 다시 제어기(CPU)를 거쳐 현장의 각종 구동기에 전달된다.

2.2.1. Ovation System 개략도

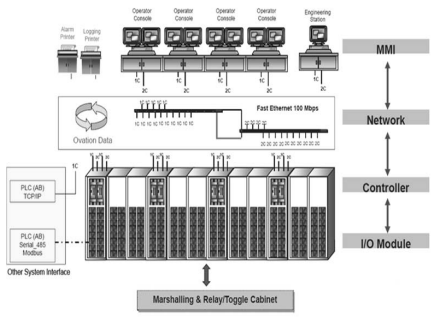

Fig.1. The outline of DCS

- Controller : P-133MHz Processor, 64MB 이상 Flash RAM, Redundancy
- I/O Module : Analog & Digital I/O, Local & Remote I/O, 시리얼 통신 등
- Network : Fast Ethernet(100Mbps), Broadcast 전송방식, Redundancy
- MMI : Engineering Console, Operator Console, OPC 등

2.2.2 주요 구성부

1) System Interface

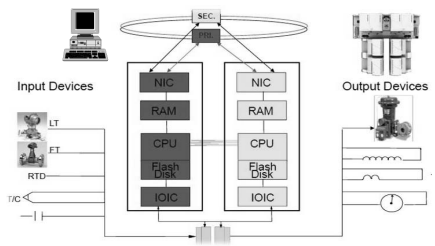

Fig.2. Ovation System Interface

- CPU : 제어대상인 프로세스 상태량(Analog or Digital)에 따라 다르나 32Bit 마이크로프로세서가 많이 사용되고 있다. 제어대상(기계설비, Plant Process)은 실시간에 변화하므로 엄격한 Real Time 처리가 요구된다.
- IOIC : I/O 신호와 CPU간 인터페이스
- Flash Memory(비활성) : Algorithm, 논리, 운영체제 저장
- DB Server : Master Database 구성 및 저장, 전용 SW Access Control

2) Data Highway

광케이블이나 UTP 케이블로 통신선로를 연결한 LAN (Local Area Network : 근거리통신망)의 하나이며 전송 거리는 보통 수 Km 이내 이다. 분산제어 시스템의 유일한 집중화 부분으로서 정보교환을 고속으로 하고 응답성도 좋아야 한다.

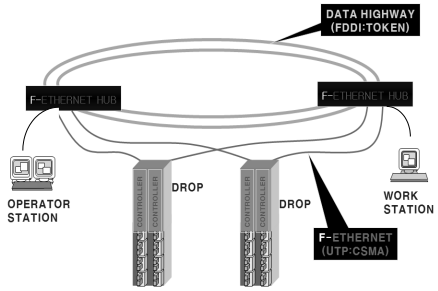

Fig.3. The outline of ovation system network

- TOKEN : 접속되어 있는 HUB들 사이를 토큰이라는 패킷이 순환하는 동안 자신이 전송하고자 할 때 토큰을 취득하여 DATA 전송을 한 후 전송이 완료되면 토큰을 반납하는 방식.
- CSMA : ETHERNET WORKSTATION이 데이터를 전송하기 전에 다른 STATION (DROP)에서 데이터 전송을 실행하고 있는지 여부를 감청한 다음 ETHERNET CABLE에 다른 데이터 신호가 없을 경우 DATA 전송.

3) Process Interface

제어대상과 직결해서 제어정보의 처리를 행하기 위한 컴퓨터의 입출력을 말하며 Analog 입력 및 출력, Digital 입력 및 출력 등이 있다. 24시간 연속 운전되는 공업시스템에 사용되어 기계설비의 제어나 감시를 행하기 때문에 신뢰성이 좋고 확장성이 좋아야 한다.

4) Operator Interface

운영자가 필요에 따라서 제어대상을 제어하기도 하고 공정상태를 감시하기 위해서 준비된 조작스위치 및 상태표시 장치를 총칭하여 말한다. 최근에는 MMI(Man Machine Interface)기능을 강화하여 운전원의 부담을 경감하고, 고도의 상황판단 능력을 가지는 방향으로 발전되고 있다.

2.2.3. DCS의 역할

1) 설비운영 측면

프로세스 제어대상의 In/Output Data 실시간 생성과 처리를 통해 플랜트 자동 운전을 가능하게하고 필요시 운전원 HMI에서 Parameter Value 변경 및 현장의 단위기기 기동, 정지 등 Remote 조작기능을 부여한다. 중요 신호의 다중화 구성을 통한 신뢰도 향상과 현장 기계설비 및 계측기 정비 시 자체적으로 Signal Bypass하여 발전소 운전 중 설비 교체 및 교정이 가능하다.

2) 설비감시 측면

HMI의 Monitor를 통해 운전원 및 제어원은 보다 효율적인 설비감시를 할 수 있으며 화면 체계는 플랜트 특성에 따라 다르다. 그래픽 화면은 제어될 프로세스의 도식화된 화면을 말하며, 프로세스의 조건에 대해 운전원에게 실시간 데이터를 제공하는 동적인 화면이다. 이 화면에는 루프의 태그 이름, 측정값, 출력값, 출력 모드, 공학 단위(engineering unit)가 표시된다. 운전원은 탱크 수위, 프로세스 온도 등과 같은 것을 색의 변화나 동화상의 심벌을 사용하여 그래픽 표현을 통해 직접 제어할 수 있다.

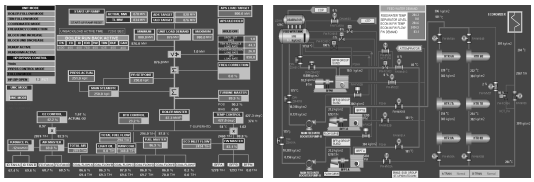

Fig.4. Ovation system graphic

Trend 화면은 실시간 또는 Historical (보통 1초부터 수개월) 모드를 선택할 수 있으며 모든 변수와 시간 축에 대해 퍼센트 또는 공학 단위의 크기 조절이 가능하다.

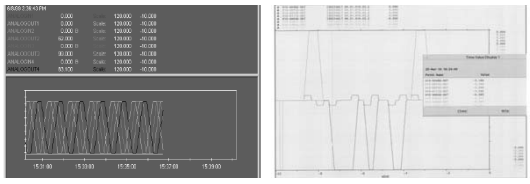

Fig.5. Ovation system trend

경보 화면은 태그, 경보 형태, 설명, 우선순위, 확

인 상태 등이 있는 경보 목록을 제공한다. 경보검출 시간에 따라 순서대로 경보 목록이 작성된다. 운전원은 실시간으로 취명되는 경보감시와 실제의 경보조건을 확인하고 상황에 따라 운전상태 지장유무를 판단, 조치할 수 있어야 하며, 제어원은 Alarm Historical Review를 통해 문제점을 분석하고 해결방안을 찾아 설비 이상상태 발생 전에 신속하게 복구하여야 한다.

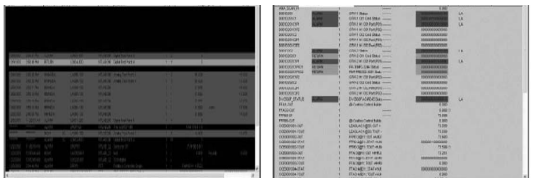

Fig.6. Ovation System Alarm View

3) 예측진단 측면

DCS의 통합화와 더불어 확장성이 향상되면서 여러 정보를 활용한 플랜트 예측 진단 시스템의 개념이 등장하였고 그 중요성은 날로 높아지고 있다. 가능한 많은 공정변수를 수용하여 운전설비의 특성에 맞는 Trend 및 그래픽 화면을 구성, 프로세스 주요변수의 변화율 분석 및 이상상태 조기 감지를 통해 운영자는 프로세스의 비정상 조건을 찾아내고 예측할 수 있게 된다. 또한 DCS와 연계한 설비 관리 감시용 시스템을 구축하여 전사적으로 활용하고 있으며, 모 발전소의 경우 예측진단 활성화의 일환으로 전 직원 마이머신 Trend Monitoring을 시행 중에 있다. 운전원의 감시범위를 벗어난 취약설비 계통이나 담당설비에 대한 운전 모니터링 및 예측진단 분석 Tool로 사용하며 아래와 같은 역할을 수행한다.

- 기동, 정지 및 운전 중 데이터 취득 및 분석
- 온도·압력 등 운전데이터의 Trend 분석
- 기간, 범위 설정하여 Alarm, Trip 등 경향 파악

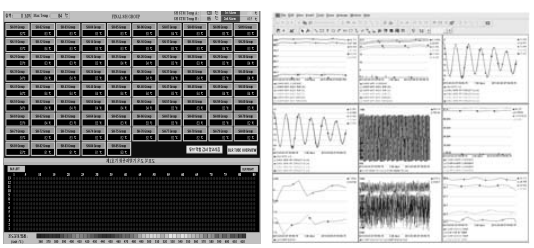

Fig.7. Plant Information System

2.3 Ovation 1.5 보안 적용 사항

2.3.1 주제어시스템 자산 중요도 산정

2011년도 발전제어망을 주요보안시설로 지정하였고 정보통신기반 보호법 제9조에 의거 국가 주요정보통신기반시설의 취약점을 주기적으로 분석·평가토록 하고 있다. 특히 2013년부터는 매년 9월까지 국정원에 제출토록 의무화 하였으며 발견된 취약점에 대한 위험등급 부여, 개선방향 수립 등 유기적인 평가를 통해 보안성 강화를 유도할 계획이다.

모 발전소 주제어설비의 중요자산 분류는 다음과 같다.

Table 1. The system of DCS assets

유 형	Host Name	주요 목적	운영체계	OS 버전
서버 시스템	Engineering Console	운전 조작 & Program 수정	UNIX	Solaris 8
	Operator Console	운전조작, OPC	Windows	Win NT 4.0
	Controller	알고리즘 연산, 실시간 Data 처리	UNIX	VxWorks
네트워크 장비	SWITCH (L2, L3)	Highway Interface	CISCO IOS	12.2
Data Base	DB Server	Program 수정, Oracle DB 저장	UNIX	Solaris 8

한편 전자정부 정보보호관리체계(G-ISMS)의 위험관리에 근거하여 올해부터 취약점 분석·평가대상 자산을 식별하고 각 자산에 대한 위험관리를 위해 대상 자산의 기밀성, 무결성, 가용성, 피해규모, 복구목표 등에 따라 중요도 가치 수준을 정해야 한다. 주요정보통신기반시설의 특성을 고려하여 상·중·하, 1~3등급 등으로 구분하며 보안등급 선정기준 근거하여 모 발전소 주제어설비에 대한 자산의 중요도를 산정하고 각 자산의 주요기능 및 목적에 대해 살펴보면 다음과 같다.

Table 2. The subject of grade for DCS importance(ex.)

NO.	OS	설비명	기능
US01	Solaris 8	Engineering Workstation	Logic 수정, DB 서버
US02	Solaris 8	Engineering Workstation	Logic 수정, WAVE 서버
US03	Solaris 8	Operator Console	운전 조작
US04	Solaris 8	Operator Console	운전 조작
US05	Solaris 8	Operator Console	운전 조작
US06	Solaris 8	Historian Server	Data 저장
WS01	Win NT 4.0 SP6	OPC	PLC 연계(Primary)
WS02	Win NT 4.0 SP6	OPC	PLC 연계(Secondary)
WS03	Win NT 4.0 SP6	Operator Workstation	Monitoring
WS04	Win NT 4.0 SP6	Operator Workstation	Monitoring
WS05	Win NT 4.0 SP6	Operator Workstation	AMS

Table 3. The assessment of DCS importance

자산	기밀성			무결성			가용성		
	H	M	L	H	M	L	H	M	L
US01	○			○			○		
US02	○			○			○		
US03	○			○			○		
US04	○			○			○		
US05	○			○			○		
US06	○			○			○		
WS01	○				○		○		
WS02	○				○		○		
WS03	○				○		○		
WS04	○				○		○		
WS05	○			○			○		

2.3.2. 자산별 취약성 분석·평가 및 개선

정부에서는 발전소 제어설비 보안감사를 매년 시행하고 있으며 주요 정보통신기반시설 취약점 분석·평가 점검항목(관리적/물리적/기술적 분류 총 453개)에 따라 일괄적으로 취약점 분석을 수행한다. 관리적 점검요령은 정보보호 정책/지침 등 관련 문서 확인과 정보보호 담당자, 시스템 관리자, 사용자 등과의 면담으로 확인하고, 물리적 점검 요령은 전산실, 현관, 발전제어실 등의 통제구역을 실사하여 확인하며, 기술적 점검요령은 점검도구, 수동점검, 모의해킹 등을 통해 확인하고 있으며 직전년도 발견된 취약점에 대해서는 중점적으로 감사하고 있다. 다음은 행안부 주관 보안감사 시 취약점 분석·평가 결과를 요약한 내용이며 모 발전소 기준으로 취약점 개선을 통해 평가점수가 전년대비 향상된 것을 볼 수 있다. 관리적 보안부분에서는 비밀번호 관리 미흡, USB 포트 물리적 봉인 및 통제구역 CCTV 미설치 등에 대한 취약점이 도출되어 즉시 개선하였으며, 서버시스템 부분에서는 윈도우즈 백신 미운용, 사용하지 않는 폴더 및 소프트웨어 미삭제 등 취약점이 도출되었으나 주제어시스템 운용에 민감한 부분으로 제작사의 정밀검토를 통해 향후 개선해나가야 할 과제로 남아있다.

네트워크 부분에서는 사용되는 취약서비스를 제거토록 권고 받았으나 시스템운영상 반드시 필요한 부분으로 수용하지 못한 사례도 있다. 주요 개선사항을 보면 UNIX는 계정관리 5항목, 파일 및 디렉토리 관리 4항목, 서비스 관리에서 6항목으로 [Fig. 8]에서 나타난 것처럼 전·후 향상 폭이 상당히 높음을 볼 수 있다.

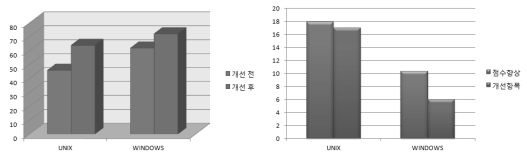

Fig. 8. The result of vulnerability estimate & improvement

반면 최초 취약점 평가결과를 봤을 때 제어시스템의 초기 도입 시 보안사항이 전혀 고려되지 않았음을 알 수 있고, 사용자 및 제작사 상호의 보안에 대한 인식도를 예상할 수 있다. 또한 제작사에서 취약점 평가결과에 대해 주로 패스워드와 파일 접근권한 등 기본적 사항에 대해서만 조치하도록 권고한 것을 보았을 때 아직 보안적용에 따른 시스템 운영 문제점 등 상세한 기술검토는 미미한 것으로 판단된다.

III. 제어시스템 개방화와 동향

3.1. 제어시스템 개방화와 보안문제

제어시스템은 개별성이 높아 전통적으로는 그 대부분이 응용 영역별로 장치 벤더가 개발한 독자 기술을 핵으로 실현되었다. 그러나 비용절감 압력 속에서 사용자가 요구하는 고도의 기능을 실현하기 위해 서서히 개방화된 시스템 기술을 활용하고 있다. 개방화라는 용어는 사양이 일반적으로 공개된 표준 프로토콜이나 표준 인터페이스를 사용하고, 인터넷 등의 광역이나 범용 네트워크상에서 가동 되는 시스템을 의미한다. 예를 들면 Windows OS나 VxWorks와 같은 상용 OS, 모듈/Linux와 같은 오픈 소스 소프트웨어, 이더넷이나 Wi-Fi와 같은 표준 네트워크 인터페이스, TCP/IP 프로토콜 등을 사용하고 있는 시스템이 해당된다. 다양한 기존 제품과의 호환성을 얻을 수 있고 표준 모듈을 사용함으로써 개별적으로 개발하는 것보다 선진적인 기능을 비교적 저렴하게 실현할 수 있다. 반면에 개방화된 시스템에 사용된 프로토콜이나 인터페이스 등의 기술자료는 공개되어 있어 누구나 쉽게 입수할 수 있는데, 이러한 기술정보는 공격 방법을 짜내는 힌트가 될 수 있다. 또 완전히 같은 코드로 만들어진 모듈을 내장한 제어시스템이 다수 존재한다는 것은 공격자가 그 코드에 대한 공격툴을 별도로 만들어내지 않고도 같은 툴을 사용해 다수의 제어시스템을 표적으로 한 공격이 가능하게 되는 것을 의미한다. 즉, 개방화는 이용자에게 편익을 주는 한편, 공격자에 대해서도 공격 준비에 필요한 비용을 낮추거나 혹은 같은 수고로 큰 효과를 얻을 수 있다는 것을 의미한다. 오늘날에는 제어 시스템을 대상으로 한 공격용 툴이 인터넷을 통해 다수가 공개되어 있으며, 블랙마켓을 통한 거래 역시 존재한다. 또한 광역 네트워크와의 접속연동은 악의를 품은 자가 원격에서 숨어서 표적이 되는 시스템을 노리고 공격하는 리스크나 네트워크 바이러스가 침입하여 피해를 발생시키는 리스크를 높이게 된다. 실제로 제어 시스템을 대상으로 침입 가능한 지점을 탐색하고 있는 것을 추정되는 인터넷상에서의 네트워크 스캐닝 활동도 보고되고 있다. 이러한 개방화와 보안 문제의 인과관계는 네트워크 보안 역사와도 표리관계에 있다. 벤더의 독자적인 OS를 탑재한 메인프레임이 주로 이용됐던 1980년대 이전에도 학술적으로는 보안 사고의 가능성이나 대책이 논의되었지만, 큰 문제가 되는 경우는 극히 드물었다. 보안 문제가 대두한 것은 개방화가 진행된 이후의 일이다. 예를 들면, 모리스 웜 사건이나 1990년대 전반에 연이은 네트워크 침입 사건은 UNIX를 탑재한 서버나 워크스테이션을 중심으로 한 인터넷 이용이 급격히 확대된 시기와 겹치고 2003년 전후로 매년 맹위를 떨친 컴퓨터 바이러스나 네트워크 웜 발생은 네트워크 접속된 Windows PC가 널리 보급된 시기와 겹친다. 과거의 제어 시스템은 제어기기 벤더 고유의 특수한 프로토콜이나 기본 소프트웨어가 주로 이용되었기 때문에 공격 방법이 유포되는 경우는 적었고 제어 시스템이 관련된 정보보안 사고의 사례 역시 거의 발견되지 않았지만, 제어시스템의 개방화가 현저히 진행된 오늘날에는 제어 시스템을 포함한 정보 보안 관리가 중요한 경영 과제가 되었다. [3]

3.2 제어시스템 보안 동향

미국의 경우 에너지부(DOE)는 2003년에 국립 SCADA 테스트베드(NSTB)를 설립하면서 국내 전력회사 및 그 소유주, 시스템 공급회사, 연방 정부 등이 자율적으로 협조하는 민-관 협조체계를 발족시키면서 전력공급을 제어하는 전자 시스템에 대한 사이버 보안이 크게 개선되었다. 또한 미국 전력시장에 진입하는 신규 SCADA 시스템 공급 회사의 80% 이상이 적극적으로 참여하고 있다. NSTB 회원들은 날로 지능화 되어가는 위협적 환경에서 제어시스템을 보호하기 위한 지식, 방법론, 기술을 지속적으로 키워가며 평가 프로그램은 신·구 제어시스템 모두에 대하여 그 보안성을 강화시켰고 전력회사에서는 공급회사가 제공하는 업그레이드와 소프트웨어 패치를 신속하게 설치하면서 이전보다는 훨씬 높은 평가점수를 획득하였다고 밝혔다. NSTB의 주요 활동은 제어시스템 공급사의 표준제품에 내재하고 있는 취약점을 노출시킴으로써 보안 문제점에 대한 명확한 이해를 돕고 그 결과에 대한 수정사항을 시스템에 적용하여 기반시설 제어시스템을 더욱 안전하게 만들고 있다. 또한 제품 제작사들도 자사 제품의 보안 신뢰성을 공증 받고 이로 인한 마케팅 효과가 증가하고 있다고 한다. [4]

우리나라의 경우 2012년 11월 제16차 “정보통신기반보호위원회”에서 새로운 유형의 사이버공격에 대비한 기반시설 보호강화 대책을 논의하고 각종 제도와 기준을 정비하였다. 선진국에 비해 다소 뒤늦기는 했지만 사이버 해킹 등의 보안위협에 선제적으로 대응하기 위해 한국인터넷진흥원에 제어시설 보호 전담지원

센터를 설립하고 "산업제어시스템 테스트베드" 구축을 논의중에 있다. 제어시스템의 사이버 보안 강화를 위한 좋은 프로그램이 운영되어도 가용성이 극히 중시되기 때문에 보안을 강화하는데 소극적일 수 있다. 이에, 사전에 충분한 테스트를 해볼 수 있도록 테스트베드 구축 및 경영진에 대한 보안인식 재고 프로그램과 같은 정부차원의 지원이 필요하다.

IV. Ovation System 모의해킹

4.1 사용 툴(Nessus) 및 실험방법 소개

Nessus는 Local과 Remote 시스템에 대한 보안 취약점 점검도구로 그 특성을 살펴보면 다음과 같다.〔5〕

- 사용이 자유롭고, 업데이트가 편리함.
- 서버와 클라이언트 구조로 동작.
- Plug-in 방식으로 유연한 점검항목 선택 가능
- 결과보고서를 HTML, ASCII 등 여러 가지 형태로 리포팅

〔Fig. 9〕는 Ovation 1.5 버전의 간이 DCS 환경으로 모의해킹을 수행한 구성도이며, 자산별 사용 OS에 맞는 취약점을 도출할 수 있도록 Nessus plug-in을 변경 하면서 실험하였다. 또한 전체 plug-in을 활성화 하여 모든 호스트로 공격하는 실험도 병행하였으며, 각 상황에 따른 로그 유형을 분석하여 사이버 침해 시 효과적인 대응방안이 도출될 수 있도록 연구해 보고자 하였다.

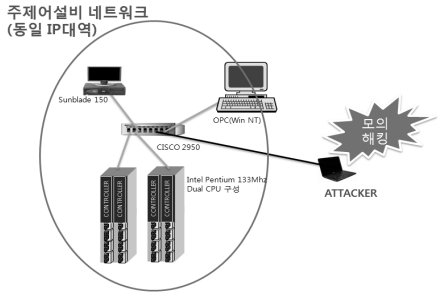

Fig.9. The composition of DCS simulator

Table 4. The subject of grade for simulator

유 형	Host Name	주요 목적	운영체계	OS 버전
서버 시스템	Operator Console (모델명 : Dell 650)	운전조작	Windows	Win NT 4.0
네트워크 장비	L2 SWITCH (모델명 : Cisco2950)	Highway Interface	CISCO IOS	12.2
Data Base	DB Server & EWS (모델명 : Sunblade 150)	Program 수정, Oracle DB 저장	UNIX	Solaris 8
RTU	Controller (제작사 자체 모델)	알고리즘 연산, 실시간 Data 처리	UNIX	VxWorks

4.2 자산별 침해유형 분석

앞서 설명한 바와 같이 시뮬레이터 환경에 맞게 해킹툴의 항목을 활성화 시키고 Scan을 해본 결과 자산의 특성에 따라 각각 다른 취약점이 발견되었다. Nessus Homefeed 버전에서 지원되는 여러 플러그인 항목 중 테스트 실험결과 주제어시스템의 성능저하 및 Fail Mode로 진행되는 항목을 자산별로 구분하여 모의해킹을 시현하였고 그 기준은 〔Table 5〕와 같다. 그 결과 DB Server(Solaris)의 경우 Risk High(2), Medium(4), Information(40) 항목에 대한 취약점 리스트가 Reporting 되었으며 Operator Console(WinNT)의 경우 Critical(2), Medium(1), Information(31), Controller(VxWorks) Information(7) 및 스위치(CISCO 2950)는 Medium(5), Low(1), Information(16)항목에 대한 취약점이 발견되었다. 세부 내용을 살펴보면 다음과 같다.

Table 5. The item of penetration testing

구 분	Plugins	DB Server	OWS	Controller	Switch
Backdoors	Backdoors	○	○	○	○
OS	CISCO				○
	SOLARIS	○			
	Default Unix Accounts	○			
	Windows		○		
Databases	Databases	○			
DoS	DoS	○	○	○	○

구 분	Plugins	DB Server	OWS	Contr oller	Switch
FTP	FTP	○	○	○	
Network	Gain a shall remotely	○	○	○	○
	General	○	○	○	○
	RPC	○	○	○	○
	Service detection	○	○	○	○
	SNMP	○	○	○	○

Table 6. The vulnerability list of DB server

Family	plug-in	Risk
Net work	10833 (1) - CDE Subprocess Control Service (dtspcd) Detection	I
	10884 (1) - Network Time Protocol (NTP) Server Detection	I
	11154 (1) - Unknown Service Detection: Banner Retrieval	I
	11367 (1) - Discard Service Detection	I
	11819 (1) - TFTP Daemon Detection	I
	11936 (1) - OS Identification	I
	12053 (1) - Host Fully Qualified Domain Name Resolution	I
	17975 (1) - Service Detection (GET request)	I
	25220 (1) - TCP/IP Timestamps Supported	I
	35296 (1) - SNMP Protocol Version Detection	I
	40448 (1) - SNMP Supported Protocols Detection	I
	53335 (1) - RPC portmapper (TCP)	I
	54615 (1) - Device Type	I
DoS	11901(1) - TCP/IP Multicast Address Handling Remote DoS	M
	14274(182) - Nessus SNMP Scanner	I
	11111 (33) - RPC Services Enumeration	I
	22964 (11) - Service Detection	I
	10263 (2) - SMTP Server Detection	I
	10092 (1) - FTP Server Detection	I
	10180 (1) - Ping the remote host	I
	10223 (1) - RPC portmapper Service Detection	I
	10281 (1) - Telnet Server Detection	I
	10884 (1) - Network Time Protocol (NTP) Server Detection	I
	11936 (1) - OS Identification	I
	17975 (1) - Service Detection (GET request)	I
Back door/ FTP/ OS	14274 (183) - Nessus SNMP Scanner	I
	10180 (1) - Ping the remote host	I
DB	14274 (184) - Nessus SNMP Scanner	I
	11111 (33) - RPC Services Enumeration	I
	22964 (10) - Service Detection	I
	10263 (2) - SMTP Server Detection	I
	10092 (1) - FTP Server Detection	I

Family	plug-in	Risk
	10180 (1) - Ping the remote host	I
	10223 (1) - RPC portmapper Service Detection	I
	10281 (1) - Telnet Server Detection	I
	10884 (1) - Network Time Protocol (NTP) Server Detection	I
	11936 (1) - OS Identification	I
	17975 (1) - Service Detection (GET request)	I

Table 7. The vulnerability list of controller

Family	plug-in	Risk
Back door/ FTP/ DoS	14274 (182) - Nessus SYN Scanner	I
	10180 (1) - Ping the remote host	I
Net work	14274 (182) - Nessus SYN Scanner	I
	10114 (1) - ICMP Timestamp Request Remote Date Disclosure	I
	10281 (1) - Telnet Server Detection	I
	10287 (1) - Traceroute Information	I
	10884 (1) - Network Time Protocol (NTP) Server Detection	I
	11936 (1) - OS Identification	

Table 8. The vulnerability list of operator console

Family	plug-in	Risk
DoS	10335 (15) - Nessus TCP scanner	I
	11111 (6) - RPC Services Enumeration	I
	22964 (4) - Service Detection	I
	10736 (2) - DCE Services Enumeration	I
	10150 (1) - Windows NetBIOS / SMB Remote Host Information Disclosure	I
	10180 (1) - Ping the remote host	I
	10223 (1) - RPC portmapper Service Detection	I
	10884 (1) - Network Time Protocol Server Detection	I
	11011 (1) - Microsoft Windows SMB Service Detection	I
	11936 (1) - OS Identification	I
Net work	54586 (1) - Multiple Vendor RPC portmapper Access Restriction Bypass	M
	11219 (14) - Nessus SYN scanner	I
	11111 (6) - RPC Services Enumeration	I
	22964 (4) - Service Detection	I
	10180 (1) - Ping the remote host	I
	10223 (1) - RPC portmapper Service Detection	I
	10287 (1) - Traceroute Information	I
	10884 (1) - Network Time Protocol Server Detection	I
	10919 (1) - Open Port Re-check	I

Family	plug-in	Risk
	11936 (1) - OS Identification	I
	12053 (1) - Host Fully Qualified Domain Name Resolution	I
	45590 (1) - Common Platform Enumeration (CPE)	I
	53335 (1) - RPC portmapper (TCP)	I
	54615 (1) - Device Type	I
OS	13852 (1) - MS04-022: Microsoft Windows Task Scheduler Remote Overflow(841873) (uncredentialed check)	C
	19699 (1) - Microsoft Windows NT 4.0 Unsupported Installation Detection	C
	11219 (14) - Nessus SYN scanner	I
	10736 (2) - DCE Services Enumeration	I
	11011 (1) - Microsoft Windows SMB Service Detection	I
	10180 (1) - Ping the remote host	I
	10150 (1) - Windows NetBIOS / SMB Remote Host Information Disclosure	I
Back door/ FTP	14274 (183) - Nessus SNMP Scanner	I
	10180 (1) - Ping the remote host	I

Table 9. The vulnerability list of Network Switch

Family	plug-in	Risk
Net work	10882 (1) - SSH Protocol Version 1 Session Key Retrieval	M
	35291 (1) - SSL Certificate Signed using Weak Hashing Algorithm	M
	42873 (1) - SSL Medium Strength Cipher Suites Supported	M
	51192 (1) - SSL Certificate Cannot Be Trusted	M
	57582 (1) - SSL Self-Signed Certificate	M
	65821 (1) - SSL RC4 Cipher Suites Supported	L
	22964 (5) - Service Detection	I
	11219 (4) - Nessus SYN scanner	I
	10114 (1) - ICMP Timestamp Request Remote Date Disclosure	I
	10267 (1) - SSH Server Type and Version Information	I
	10281 (1) - Telnet Server Detection	I
	10287 (1) - Traceroute Information	
	10863 (1) - SSL Certificate Information	I
	10881 (1) - SSH Protocol Versions Supported	I
	11936 (1) - OS Identification	I
	21643 (1) - SSL Cipher Suites Supported	I
	42980 (1) - SSL Certificate Expiry - Future Validity	I
	45590 (1) - Common Platform Enumeration (CPE)	I
	54615 (1) - Device Type	I
	56984 (1) - SSL / TLS Versions Supported	I
	62563 (1) - SSL Compression Methods	I
	Supported	
DoS	10180 (1) - Ping the remote host	I
	11219 (4) - Nessus SYN scanner	I
Back door/ FTP	10180 (1) - Ping the remote host	I
	11219 (4) - Nessus SYN scanner	I

4.2.1 DB Server의 취약점 분석

〔H〕 NFS Share User Mountable

Configure NFS on the remote host so that only authorized hosts can mount the remote shares.

The remote NFS server should prevent mount requests originating from a non-privileged port.

- ◆ NFS 서비스 비활성화 여부 : NO 〔로그파일 저장을 위해 필요〕
- ◆ NFS 설정 파일에 대한 접근 권한 적절성 : YES 〔750〕
- ◆ NFS 공유 관련 디렉토리를 설정 및 접근 권한 적절성 : NO ☞ 재검토 사항

〔H〕 SNMP Agent Default Community Name (public)

Disable the SNMP service on the remote host if you do not use it.

Either filter incoming UDP packets going to this port, or change the default community string.

- ◆ 불필요한 SNMP 서비스 구동 여부 : NO
- ◆ SNMP community string 값의 복잡성 만족 여부 : NO ☞ 재검토 사항

〔M〕 TCP/IP Multicast Address Handling Remote DoS(spank.c)

Contact your operating system vendor for a patch.

Filter out multicast addresses (224.0.0.0/4)

- ◆ 최신 보안패치 및 벤더의 보안 권고사항 적용 여부 : Partially

〔M〕 RPC bootparamd Service Information Disclosure

Filter incoming traffic to prevent connections to the portmapper and to the bootparam daemon, or deactivate this service if you do not use it.

- ◆ RPC 서비스 제거 여부 : NO 〔시스템 상 다수의 RPC 서비스 존재〕

〔M〕 RPC rusers Remote Information Disclosure

Disable this service if not needed.

〔M〕 NFS Exported Share Information Disclosure

Configure NFS on the remote host so that only authorized hosts can mount its remote shares

〔L〕 X Display Manager Control Protocol Detection

Disable the XDMCP if you do not use it, and do not allow this service to run across the Internet

4.2.2 Operator Console의 취약점 분석

〔C〕 MS Windows Task Scheduler Remote Overflow (841873)

Microsoft has released a set of patches for Windows 2000, XP and 2003 :

http://technet.microsoft.com/en-us/security/bulletin/ms04-022

- ◆ 최신 서비스팩 적용 여부 : YES〔sp6〕
- ◆ 최신 Hotfix 적용 여부 : NO ☞ 재검토 사항
- ◆ 바이러스 백신 프로그램 업데이트 유무 : NO ☞ 재검토 사항

〔C〕 Microsoft Windows NT 4.0 Unsupported Installation Detection

Upgrade to a supported version of Windows.

- ◆ 제어시스템 특성상 버전 업그레이드에 맞춰 즉시 교체 불가

〔M〕 Multiple Vendor RPC portmapper Access Restriction Bypass

Apply the relevant patch from the referenced documents for EMC Legato Networker, IBM Informix Dynamic Server, or AIX.
If a different application is being used, contact the vendor for a fix.

- ◆ 재검토 사항 : 서버 단종에 따른 산업용 제작 PC의 문제점

4.2.3 Network Switch의 취약점 분석

〔M〕 SSH Protocol Version 1 Session Key Retrieval (18882)

Disable compatibility with version 1 of the protocol.

- ◆ Ovation 1.5 버전에서는 사용하지 않음

〔M〕 SSL Certificate Signed using Weak Hashing Algorithm (35291)

Have to the certificate reissued.

- ◆ Ovation 1.5 버전에서는 사용하지 않음

〔M〕 SSL Medium Strength Cipher Suites Supported (42873)

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

- ◆ Ovation 1.5 버전에서는 사용하지 않음

〔M〕 SSL Certificate Cannot Be Trusted (51192)

Purchase or generate a proper certificate for this service.

- ◆ Ovation 1.5 버전에서는 사용하지 않음

〔M〕 SSL Self-Signed Certificate (57582)

Purchase or generate a proper certificate for this service.

- ◆ Ovation 1.5 버전에서는 사용하지 않음

〔L〕 SSL RC4 Cipher Suites Supported (65821)

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.

- ◆ Ovation 1.5 버전에서는 사용하지 않음

위에서 살펴본 바와 같이 현재 모 발전소에 채용된 Ovation 1.5 버전의 제어시스템은 1999년도에 출시된 제품으로 일반 IT 환경에서 발견된 많은 취약점들을 반영하지 않은 채 운용되고 있음을 볼 수 있다. 실제 모 발전소에서 제어시스템 서버에 OS 패치를 설치 후 제어 프로그램을 바이러스로 인식하면서 오작동 한 사례가 존재한다. 이와 같이 취약점은 존재하지만 보안조치를 적용하지 못하는 사례가 제어시스템 운영환경에 다수 존재한다. 향후 사용 편의성 및 원가 절감을 위해 범용 OS 및 프로토콜을 채용한 DCS가 주를 이룰 것으로 예상되므로, 제어시스템의 취약점에 대한 정보가 벤더와 사용자간 공유가 되어 DCS 도입단계에서부터 보안성을 검토하고, 지속적으로 취약점을 제거해 나갈 수 있는 프로세스가 마련되어야 한다.

4.3 효율적 로그분석 기법 연구

4.3.1 로그분석의 필요성

IDS, IPS, 방화벽과 같이 네트워크 단의 탐지 및 차단 시스템만으로는 오탐지 및 미탐지의 가능성이 있어 피해현황을 정밀하게 분석하기에는 한계가 존재한다. 이에 대한 보완책으로, 시스템의 다양한 로그파일을 교차분석 하여 시스템의 보안상황 및 피해상황에 대해 정확히 파악할 수 있다. 로그란 시스템에 접속한 사용자들의 행위들을 저장해 놓은 기록들로 외부에서

침입을 해온 공격자가 시스템에서 어떠한 일을 행했는지, 또는 사용자가 어떠한 명령어들을 이용하고 있는지 등의 보안상 의미 있는 정보들과 시스템이 처리한 업무와 에러 등의 운영정보를 포함하고 있다.

특별한 징후 없이 침해사고가 발생하기도 하지만 보통은 해커가 공격을 하기 전에 정보수집 등의 행위를 할 수 있는데, 정기적인 취약점 진단과 함께 주기적인 로그분석을 통해 침해사고 발생 이전에 공격 및 이상증후를 감지할 수 있는 보안 대응 체계를 구축할 수 있다.〔6〕

4.3.2 시스템별 로그 현황 및 분석방법

시스템 로그의 생성 및 저장 단계를 살펴보면 다음과 같다.

- Authentication : 계정과 정상적인 패스워드를 입력하는 과정
- Authorization : 올바른 패스워드 입력해서 시스템에 의해 로그인이 허락된 사용자라고 판명되어 로그인 되는 과정
- Accounting : 시스템에 로그인 한 후 이에 대한 기록을 남기는 과정
- Audit Trail(감사추적) : Accounting하여 남긴 로그정보를 통한 추적

또한 시뮬레이터 환경에서 사용하는 OS인 Windows 시스템과 유닉스 로그의 차이를 보면 Windows 시스템은 로그(이벤트)가 중앙 집중화되어 있어 관리가 편한 반면 삭제당할 위험이 크며, 유닉스는 로그가 분산되어 있어 관리 및 삭제가 힘든 특징이 있다. 먼저 전반적인 시스템별 로그 분석과 설정을 살펴보고 모의해킹 시 서버의 Status와 남겨진 로그를 검토하여 침해유형에 따른 대응책을 도출하도록 한다. Ovation 시스템의 경우 네트워크 및 Controller 등 중요 설비에 대한 Error Log를 DB Server로 수집하도록 하여 실시간 정보가 General Messages 창에 Display 되고 있다. 보통 Configuration 되어 있는 정보에 대한 에러와 시스템 부팅에 대한 로그로 이것만으로 시스템 상태를 전반적으로 진단하는 데는 무리가 있어 개별 설비의 자체로그와 함께 분석하는 것이 필요하다. 〔Fig. 10〕은 Windows NT의 이벤트 Logging의 구성현황을 도식화하여 보여주고 있다.

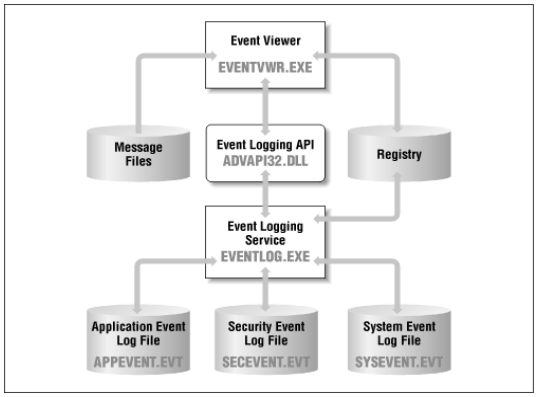

Fig. 10. Interaction of a Win32 program with the event logging service〔7〕

Windows NT의 Event Logging Service는 모든 이벤트 로그의 접근을 통제하며 윈도우즈의 시작과 함께 자동적으로 실행되고 다른 로그파일로의 읽기, 쓰기 등을 관장하고 있다. 또한 보안 로그에 성공 액세스 시도 또는 실패 액세스 시도를 기록할 사용 권한 유형을 설정하여 컴퓨터의 개별 파일 및 폴더에 감사 정책을 적용할 수 있다.

일반적으로 윈도우즈 서버를 사용하는 경우 침해사고 발생 시 로그 분석 절차 및 점검내용은 다음과 같다.〔8〕

가. 사용하지 않는 IP 대역이나 비정상적인 행위를 하는 로그를 점검한다.
나. 사용자 계정과 그룹을 점검한다.
다. 모든 그룹에서 불법사용자를 점검한다.
라. 사용자권한을 점검한다.
마. 비인가된 응용프로그램이 실행되었는지 점검한다.
바. 변경된 시스템 바이너리 파일을 점검한다.
사. 시스템과 네트워크 환경설정을 점검한다.
아. 비인가된 파일공유를 점검한다.
자. 실행중인 스케줄러를 점검한다.
차. 불법프로세스를 점검한다.
카. 이상한 파일이나 숨겨진 파일을 찾는다.
타. 파일 퍼미션 변경이나 레지스트리 키값의 변경을 점검한다.
파. 사용자나 컴퓨터의 정책변화를 점검한다.
하. 시스템이 다른 도메인으로 변경되었는지 점검한다.

솔라리스 운영체제에서 메시지 생성에 관해서는 syslogd 데몬에 의해서 총괄 관리된다. 시스템 메시지가 생성되면 메시지는 syslogd 데몬에게 전달되고 syslogd 데몬은 /etc 디렉토리에 존재하는 syslog.conf 파일의 설정을 확인하여 적당한 위치로 로그 기록을 출력하게 된다. /etc/syslog.conf 파일은 m4(전 처리기)에 의해서 해석된 상태로 syslogd 데몬에게 전달되므로 시스템 관리자는 /etc/syslog.conf 파일을 관리하는 것이 중요하다. 특히 솔라리스는 로그가 분산되어 있으며 윈도우처럼 GUI 형식이 아니므로 관리자 및 사용자의 접근과 관리가 어렵다. 따라서 시스템 관리자는 주요 로그 디렉토리 위치를 파악하고 있어야 하며 주기적으로 수집하고 분석하여 지속적으로 침입탐지 활동을 해야 한다. [Table 10]에 솔라리스 시스템의 주요로그 설명 및 저장위치를 정리하였다.

Fig. 11. principles of syslog

Table 10. The explanation of solaris log

로그파일	저장 위치	출력명령	Description
utmp(x), wtmp(x)	/var/ adm	w : 현재 last : 누적	사용자의 Account 정보 (확장정보) - login, logout, reboot 등의 누적정보
syslog	/var/ log	vi, more	운영체제 및 응용프로그램의 주요 동작내역
sulog	/var/ adm	vi, more	su 명령에 의한 결과 기록
pacct	/var/ adm	lastcomm, acctcom	각 사용자에 의해 실행된 프로세스 기록 (Ovation 1.5 미적용)
authlog	/var/ log	vi, more	시스템 내 인증관련 이벤트 기록
messages	/var/ adm	vi, more	각종 메시지들을 기록
loginlog	/var/ adm	vi, more	5번 이상의 로그인 실패에 대한 기록
lastlog	/var/ adm	lastlog	사용자의 마지막 로그인 시간 기록
access_log	/var/ log/ httpd	common	접속요청 및 시도에 대한 로그(Web)
error_log	/var/ log/ httpd	tail -f	접속요청 및 에러에 대한 로그(Web)

유닉스(솔라리스) 서버를 사용하는 경우 침해사고 발생 시 로그 분석 절차 및 점검내용은 다음과 같다. [8]

가. lastlog, 프로세스 기록, syslog에 의해 생성된 모든 로그 파일 및 보안로그를 조사한다.
나. 침입당한 시스템의 setuid와 setgid 파일을 모두 찾아본다.
다. 침입당한 시스템의 바이너리 파일이 변경 되었는지 여부를 확인한다.
마. corn과 at 에 의해 실행되는 모든 파일을 조사한다.
바. 불법적인 서비스가 없는지 확인한다.
사. /etc/passwd 파일이 변경되었는지 여부를 확인한다.
아. 네트워크 config 파일에 불법적인 내용이 들어가 있지 않은지 확인한다.
자. 시스템에 침입자가 사용할 만한 프로그램이나 히든파일이 있는지 확인한다.
차. 로컬 네트워크 상에 있는 모든 시스템을 함께 조사한다.

기본적인 공격시도나 해킹 등은 대부분 열려져있는 port를 통해 이루어지고 해킹툴들의 기본 셋팅값들이 대부분 거의 변경 없이 사용되는 기본 포트번호를 그 공격통로로 삼는다는 점 때문에 보안측면에서 user 전용 포트로 변경하여 사용하는 것은 중요하다고 할 수 있으며, 시스템 관리자들은 현재 서비스 중인 장비들의 포트사용 목록을 관리할 수 있도록 해야 한다.

4.3.3 공격 유형별 로그 및 시스템 상태 분석

Nessus Homefeed 버전에서 지원하는 플러그인 항목 중 실험결과 시뮬레이터 환경(Ovation 1.5)에 영향을 주는 6가지 카테고리(Family)별 영향도를 〔Table 11〕에서 나타내었으며 이에 따른 공격 유형별 로그를 정리하였다.

Table 11. The influence of penetration testing

구 분	SWITCH	CONTROLLER				DB SERVER	OWS
	ROOT(S)	DROP 1	DROP 51	DROP 18	DROP 68	DROP 200	DROP 186
DoS	이상무	REBOOT	REBOOT	REBOOT	REBOOT	FAIL	FAIL
NET WORK	이상무	이상무	이상무	이상무	이상무	FAIL	FAIL
FTP	-	이상무	이상무	이상무	이상무	FAIL	FAIL
BACK DOOR	-	이상무	이상무	이상무	이상무	FAIL	FAIL
OS	이상무	-	-	-	-	FAIL	FAIL
DATA BASE	-	-	-	-	-	FAIL	FAIL

서버시스템의 경우 평상시와는 다른 비정상적인 로그들이 남아있음을 확인할 수 있었으나 침해 유형별 특징적인 로그를 구분하는 것은 현재의 시스템 구성상 한계가 있었다. 특히 4.3.2의 시스템별 로그 현황 및 분석방법에 근거하여 로그 수집을 시도하였으나 DB Server(Solaris)의 경우 Default 이외에 수동으로 설정해야 생성되기 시작하는 몇몇 유용한 로그들이 있는데, 이를 적용하지 않음으로 인해 모든 로그가 생성되지 않아 효율적 분석에 어려움이 있었다.

서버시스템은 DoS Attack이 아닌 Port Scanning 만으로도 장애가 발생하여 조작이 불가하였으며 이는 소프트웨어의 보안기능 고려 없이 산업용 컴퓨터들이 개발, 운용되고 있음을 보여주는 예라 할 수 있다. 요컨대, 산업용컴퓨터의 내구성 평가 외에도 안전 및 신뢰도를 평가하여 도입하는 정책이 반드시 필요하다. 또한, 시스템 점검 및 정비 시 반드시 Clean PC를 사용하도록 하여 사소한 악성프로그램이라도 접근되는 것을 철저히 통제, 운전·조작 불가에 따른 발전소 불시정지 등 침해사고 방지를 위한 절차 및 정책 수립을 하여야 한다.

발전소 주제어시스템에서 문제발생시 가장 심각한 타격을 줄 수 있는 부분이 컨트롤러이며 이의 기능상실 및 Reboot는 즉시 발전기 정지를 유발시킬 수 있을 만큼 시스템 상 보호해야 할 최우선 순위에 해당된다. 본 실험결과에서 보듯 서버시스템 보다 사양이 훨씬 낮은 CPU를 사용함에도 컨트롤러는 DoS 공격에 의해서만 문제가 발생하여 일반 IT 설비에서 사용되는 범용 OS가 적용되지 않은 것이 오히려 취약점에 덜 노출되고 있음을 확인할 수 있었다.

Ovation 1.5 버전의 주제어시스템에 모의해킹 시도 후 DB Server 및 OWS(Win NT)는 1분 이내 Fail Mode가 되어 자체 로그분석 및 운전·조작이 불가하였으며, 특히 DB Server 문제발생시 컨트롤러를 포함하여 시스템 전반적인 로그를 확인 할 수 있는 백업장치가 없어 복구시점까지 상황판단이 어려웠다. 이를 보완하기 위해, 발전소 주제어시스템 환경에도 IDS나 IPS을 적극 도입하여 서버 장애시 네트워크 상에서 탐지한 공격 및 이상증후와 교차분석을 할 수 있도록 해야 한다. 또한, 앞서 설명하였듯이 기본적으로 생성되는 로그 이외에 환경 설정에 의해서 만들어지는 로그들 중 유용한 대상에 한해 관리자가 반드시 생성해 주어야 하며, Ovation 1.5 버전의 주제어시스템에도 동일하게 적용되어야 한다.

다음은 Ovation 1.5 버전에서 적용되지 않았던 각 사용자에 의해 실행된 프로세스 기록을 저장하는 pacct 로그파일을 직접 생성하여 침해 유형별 특징적인 부분만 정리해 보았다.

Table 12. DB Server pacct Log

No	명령어	Before	DoS	Net work	FTP	DB	OS	Back door
1	drvconfig				O		O	
2	dtexec	O	O	O				
3	finger		O	O				
4	get_peer		O					
5	in.fingerd		O	O				
6	in.ftpd		O	O				
7	in.tftpd			O				
8	in.uucpd		O					
9	inetd.qu		O					
10	last		O					
11	login		O	O				
12	prtconf		O					
13	rpc.ruse					O	O	O
14	ss_downl		O	O	O	O	O	O
15	ss_failo		O	O	O	O	O	O
16	ss_query		O	O	O	O	O	O
17	ss_switc		O	O	O	O	O	

솔라리스 OS를 사용하는 DB Server의 경우는 자체적으로 저장되고 있는 Log(/var/adm/messages, /usr/wdpf/log)와 〔Table 12〕의 pacct 로그를 시간대별로 종합적으로 분석하면 어떤 유형의 침해가 발생되었는지 유추할 수 있겠지만, Operator Work Station으로 사용하고 있는 Windows NT와 컨트롤러의 경우는 시스템 Up/Down 관련 메시지만 남아있어 침해 유형을 판단하는데 어려움이 존재 하였다. 특히 이번 실험결과에서 보면 공격시도 후 시스템 동작불능 전에 상황을 예견하여 대처하도록 관련 로그가 제공되지 않았고 거의 공격과 동시에 Fail Mode가 되어 이미 손을 쓸 수가 없는 상황에서야 침해 감지가 가능하였다. 또 하나 확인할 수 있었던 것은 IT 시스템 보다 오히려 주제어시스템이 Nessus 공격에 더 취약하였으며 주기적인 OS 패치 업데이트 및 보안 취약점 개선의 필요성을 재확인 할 수 있었다.

V. 결론

발전소 주제어시스템에서 네트워크 스위치와 컨트롤러는 가장 중요설비로 이중화 구성이 되어 있으며 동작불능 시 1분 이내에 발전정지를 유발하므로 최우선적으로 보호해야 된다. 특히 컨트롤러의 경우는 외부로의 접속점이 네트워크 스위치 밖에 없으므로 네트워크 단에서 강력한 보안정책이 요구되며 사이버 침해 및 문제발생시 확실한 원인규명을 위한 지원 프로세스들이 필요하다. 즉, 빈약한 자체 로그를 보완할 수 있는 방어시스템 및 모니터링 시스템 등을 도입하여 사고 시 효율적 분석을 통한 신뢰성 있는 원인파악을 이끌어 내어야 한다.

어떤 공격에서도 안전한 시스템은 현실적으로 존재하기 어려우므로 미사용 포트봉인 등의 물리적 방법과 자산별 보안정책을 세분화하여 관리하고 벤더와의 협력을 통한 시스템 보안취약점 개선 활동을 꾸준히 지속해야 한다. 또한 향후 설비단종에 따른 Upgrade 및 발전소 건설시 설계단계에서부터 주제어시스템 보안사항을 명기하고 벤더별 보안정책 등을 면밀히 검토하여 표준화 시킬 수 있도록 유도해야 한다. 특히 정보보호제품 평가·인증처럼 제도적으로 관련 사항을 강제할 수 있는 범위를 발굴하여 기준을 정하도록 사용자 및 벤더 상호간 노력하여 제어시스템의 보안 신뢰성을 높일 수 있다.

Ovation 시스템의 통상적인 Network Switch 부하율을 보면 CPU 사용량 5% 이내, Memory 사용량 40% 이내, Port별 트래픽(Broadcast packet) 20% 즉 20Mbps 이하로 사실상 일반 웹 전산망을 기준으로 비교해 보아도 네트워크상 여유는 충분함을 알 수 있다. 그럼에도 불구하고 현재 Ovation 제작사에서 Network Management System 도입에 대해 네트워크 부하율 증가를 우려하여 부정적으로 보고 있다. 이처럼 벤더에서 적극적으로 사용자의 입장을 고려하지 못하고 있으나, 향후 제작사에서 신제품 사양에서 뿐만 아니라 기 운영 중인 시스템에 대해서도 지속적인 보완이 이루어지도록 제품 보안 강화정책을 통해 사용자와의 신뢰를 유지해야 할 것으로 판단된다.

범용화된 OS를 사용하고 시스템간 TCP/IP 통신이 주를 이루게 되면서 발전소 주설비에 속하진 못하지만 단위시스템을 제어토록 구성된 PLC를 DCS에 수용하고 있고 두 시스템이 연계되는 루트로 사이버 침해 위협이 증가하고 있다. 점점 발전소 내에서도 보안관할 범위가 증대되고 있으며 포괄적으로 시스템화하여 관리하지 않으면 비인가 노트북 및 USB 등 사용에 따른 예기치 못한 악성프로그램에 의한 침해사고 사례가 빈번해 질 것으로 예상된다. PLC 설비는 통제구역에 위치하지 않아 접근제어가 어렵고 설비 영향도가 적어 정비 및 관리자의 보안 의식이 낮기 때문이다. 궁극적으로 보안 관련 최근의 이슈와 사고의 심각성에 대한 경각심을 통해 조속히 경영진의 의식 변화를 이끌어 내야하며 최소한 본부급 사업소만큼은 보안 전문조직이 운영되어 체계적 관리를 통한 사이버침해 대응 및 예방활동을 전담할 수 있도록 해야 한다.

References

〔1〕 Y. S. Kim, “Automation of Sewage Treatment Facilities by DCS,“ Monthly journal of automation systems, pp. 115~116, Jan. 1997

〔2〕 J. O. Kwon, Y. J. Hong, “A study on the security management plan of ICS,” Samsung SDS Journal of IT Services Vol.8/No.2, pp. 114~115, Sep. 2011

〔3〕 The Japan Society Of Automation, “The opening and security problems for DCS,” Automation System, v.26, pp. 52~57, Aug. 2010

〔4〕 Matt Tani ″DOE Focuses on Cyber

Security" Transmission & Distribution World, pp. 97, Mar. 2007
〔5〕 Y. S. Jang, "Report of Nessus analysis," CERTCC-KR, pp. 5, Jul. 2001
〔6〕 H. K. Kim, K. H. Im, and S. C. Park, "DSS for computer security incident response applying CBR and collaborative response," Expert Systems with Applications, Vol 37, Issue 1, pp. 852-870, Jan. 2010
〔7〕 James D. Murray "Windows NT Event Logging" O`Reilly, newton.ma.us, pp. 105, Sep. 1998
〔8〕 D. Y. Ha, "The analysis procedures for Hacking damages(Win NT/2000)," CERTCC-KR , pp. 4~7, Apr. 2001

〈저자소개〉

고 호 준 (Ho-Jun Ko) 정회원
2003년 2월: 제주대학교 전기공학과 졸업
2012년 6월: 고려대학교 정보보호대학원 석사
2003년 8월~현재: 한국남동발전 근무
〈관심분야〉 제어시스템 보안, 네트워크 보안, 전자공학

김 휘 강 (Huy-Kang Kim) 종신회원
1998년 2월: KAIST 산업경영학 학사
2000년 2월: KAIST 산업공학과 석사
2004년 5월 ~ 2010년 2월: NC소프트 정보보안실장, Technical Director
2009년 2월: KAIST 산업 및 시스템공학과 박사
2010년 3월~현재: 고려대학교 정보보대학원 조교수
〈관심분야〉 온라인게임 보안, 네트워크 보안, 네트워크 포렌직, 침입탐지시스템, 봇넷탐지