제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003. 5)

가스 SCADA 시스템 보안 취약성 분석 및 대책에 관한 연구

김윤의*, 윤천균**, 이현관*, 김영일*
*호남대학교 정보산업대학원 인터넷 비지니스학과
**호남대학교 정보기술원
e-mail:happyzip@empal.com

A Study on Vulnerability Analysis and Countermeasure for Gas SCADA

Yun-Eui Kim*, Chun-Kyun Youn**, Hyun-Kwan Lee*
yong-Il Kim*
*Dept of Internet Business, Ho-nam University Gradı School Information & Industry
**Dept of Information Technology Center, Ho-nam Univ

요 약

이 연구는 국가 기간산업망인 전력, 철도, 가스, 항공 등의 SCADA(Supervisory Control And Data Acquisition) 시스템 보안을 목적으로 현재 운영중인 가스 SCADA에 대해 시스템, 네트워크, 관리방법에 대해 보안 취약성 평가분석 및 모의해킹을 실시하고 취약분야별 대응방안을 제시하였다. 또한 이들의 결과를 종합하여 Gap 분석을 실시함으로써 사이버 테러 및 해킹 등에 보다 안전한 시스템을 구축하기 위한 방안을 제시하였다.

1. 서론

정보산업의 발전과 더불어 컴퓨팅과 네트워킹 기술의 발전 및 보급으로 산업현장에서도 이들을 이용하여 다양한 프로세스를 제어하고 있다.

SCADA(Supervisory Control And Data Acqtion)란 정보수집, 처리, 분석, 제어 및 송수신 기능들을 이용하여 원거리에 분산되어 있는 현장 Field로부터 Data를 수집하고 수집된 Data를 바탕으로 생산공정·계통 등의 프로세스 상황들을 일정한 장소에서 종합적으로 감시하고 제어하기 위한 시스템을 말하며 송·배전, 송유관, 가스배관, 항공, 철도 등의 산업에 이용하고 있다.

SCADA 시스템은 그동안 독립된 LAN(Local Are Network) 형태로 운영되어 왔기 때문에 사이버 위험 및 보안에 관한 관심도 그다지 크지 않았었다. 그러나 최근 SCADA System이 경영정보를 지원하여 비즈니스 결정 도구로 이용되면서 외부 네트워크와 연결되는 추세이며, 사이버 침입을 통해 국가기간산업망인 전기, 가스, 철도 등을 공격하여 서비스를 중단시킨다면 국가 혼란을 초래할 수도 있다.

본 논문에서는 정보보호 관리자를 위해 개발된 국제 기업보안 표준규격인 BS7799와 정수장 SCAD의 사이버 공격 위험 연구 그리고 해킹기법을 이용한 내부망 보안 평가방법을 연구하여 운영중인 가스 SCADA 시스템의 보안평가 방법에 적절한 체크시트를 만들고, 모의해킹을 통해 보안 취약점을 분석하여 Gap 분석을 통한 종합적인 SCADA 시스템 취약점을 평가함으로써 사이버 침입에 대응할 수 있는 시스템 구축방안을 제시하고자 한다.[1][2] 2장에서는 본 연구와 관련된 BS7799, 정수장 SCADA 사이버 공격의 위험 연구, 해킹기법을 이용한 내부망 보안 평가 방법에 대해 언급하고, 3장에서 가스 SCADA 시스템의 보안 취약성 평가·분석 및 대응방안에 관해 자세히 설명하였으며, 제 4장에서 사이버 공격의 위험에 대응할 수 있는 SCADA System 구축방법을 제시하였고, 5장에서 결론을 기술한다.

2. 관련 연구

시스템의 보안 취약성 평가 및 분석을 위하여 적용하고 있는 방법에 대한 연구로 BS7799, 정수장 SCADA 사이버 공격 위험, 해킹기법을 이용한 내부망 보안평가, Security For Unix, 정보시스템의 위관리 및 재난복구 등 다양한 방법이 있으나, 본 논문에서는 아래의 3가지를 이용하려 한다.[1][2][3]

2.1 국제 기업보안 표준규격(BS7799)

조직의 정보보안을 구현하고 유지하는 관리자를 위해서 개발된 것으로 크게 두 부분으로 구성된다.

1부에서는 정보보호 정책 수립을 위한 표준적인 실무지침으로 10개의 주요분야 127개의 통제항목으로 구성된 종합적인 보안 통제 목록이다. 보안정책, 보안조직, 자산분류와 통제, 인적보안, 물리적 및 환경적 보안, 전산기 및 네트워크 관리, 시스템 접근통제, 시스템 개발 및 유지보수, 업무지속성 계획 및 준수 등을 다루고 있으며 이러한 항목들이 본 연구와 연관성을 가지고 있다.

2부에서는 정보관리시스템(ISMS)에 대한 구축방법을 6단계로 제시하고 있다.

2.2 정수장 SCADA 사이버 공격의 위험

미국 버지니아 대학교 Captain Barry가 1998년 연구한 내용으로 미국의 정수장 SCADA에 대한 사이버 공격 위험에 대해 취약성을 크게 기능, 하드웨어, 소프트웨어, 인간, 도구, 접근, 지리학적 위치의 7가지로 분류하여 평가하고 이벤트와 오류분석을 통해 사이버 공격에 대응할 수 있는 시스템을 구현하는 방법을 제시하고 있다.[2]

2.3 해킹기법을 이용한 내부망 보안 평가 방법

네트워크를 지대별 및 공격 경로로 분리한 후 해킹 및 해커수준의 분류를 적용하여 실제적인 내부망의 보안수준을 평가하도록 방법을 제시하였으며 보안수준을 5개 등급(ISL1~ISL5)으로 분리하여 ISL5의 보안수준을 가장 고수준으로 평가하고 있다.[1]

3. 보안 취약성 평가·분석 및 대응방안

가스 SCADA의 취약성 평가는 4단계로 구분하여 실시하였다. 1단계로 BS7799와 내부망 보안평가 방법 및 정수장 SCADA의 사이버 공격 위험을 연구하여 현재 국내에서 사용하고 있는 가스 SCADA 시스템의 실정에 맞게 적용, SCADA 보안 취약성 평가용 체크시트를 만들어 취약성 평가·분석 및 대응방안을 제시하였다. 2단계로는 시스템에 대해 정밀 및 자동진단을 실시하여 취약성을 평가·분석 및 대응방안을 제시하였으며, 3단계로 내부 및 외부영역 수준의 모의해킹을 실시하여 취약성을 평가·분석하였고, 마지막으로 1단계~3단계의 평가결과를 바탕으로 Gap 분석을 실시하여 SCADA 시스템의 종합적인 취약성을 평가·분석하였다.

3.1 체크시트에 의한 취약성 평가 분석

정보보호 정책 및 조직 외 9개 항목에 대한 인터뷰를 실시하고 그 결과를 주요 수행업무에 대해 위협영역을 6가지로 분류하여 평가한 결과는 〈표1〉와 같으며, 시스템/네트워크 유지관리 업무중 인간적 실수가 가장 높게 평가되었다.

〈표1〉 주요 수행업무 위협분석 평가 결과

위협영역 / SCADA업무	정보 시스템	전자 제어 시스템	통신 시스템	기술적 오류	인간적 실수	물리적 환경적	업무 평균
공급감시 및 제어	1.6	1.0	1.0	1.7	2.0	1.0	1.4
계통분석 및 데이터관리	1.6	1.0	1.0	1.7	1.5	1.0	1.3
시스템/네트워크 유지관리	1.1	1.0	1.0	1.0	**2.5**	1.0	1.3
경영정보시스템 지원	1.1	1.2	1.0	1.3	1.5	1.0	1.2
위험도 평균	1.4	1.1	1.0	1.4	1.9	1.0	1.3

※ 위험도 분석 (3등급이 가장 위험요소가 큼)

- 1등급(1.0~1.3) : 19개 영역
- 2등급(1.4~2.0) : 8개 영역
- 3등급(2.1~2.5) : 1개 영역

3.1.1 정보시스템 대응방안

24시간 상시 근무로 인한 해당업무별 동일한 계정 사용문제에 대해 컴퓨터 사용권한을 근무자의 업무시간대별로 제한할 수 있도록 프로그램을 개발하여 계정관리 강제 적용을 실시한다. 네트워크 장비에 대해 인증체계를 적용하여 장비의 인증을 강화한다. 내부 및 외부인의 불법 침입을 탐지하기 위해 침입탐지 시스템을 구축하고 중요 저장매체의 폐기 체계를 수립하여 폐기절차를 강화한다.[5]

3.1.2 기술적 오류 및 인간적 실수

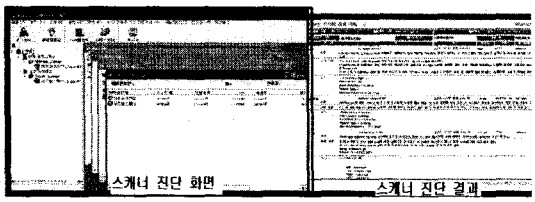
SCADA 시스템의 소프트웨어에 대해 보안기술을 이전 받아 습득하여 기술적 오류를 예방하고 운영자 및 관리자에 대해 보안인식 및 기술교육을 통해 인간적 실수를 예방한다.

3.2 시스템 보안 취약성 평가 분석

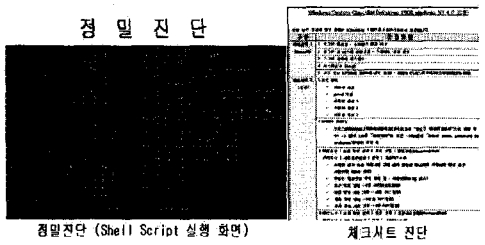
시스템 진단은 서비스별, 용도별, 운영체제별로 중요도를 고려하여 정밀 및 자동진단을 실시하였다. 자동진단은 서버 기반의 취약점 점검 시스템인 NeoScanner를 이용하였으며 결과는 (그림1-1)과 으며, 정밀진단은 DEC Unix가 갖고있는 취약점 파악하기 위해 Shell Script를 작성하여 이용하였고 결과는 (그림1-2)와 같다. 〈표2〉는 자동 및 정밀진단 평가결과를 종합하여 분석한 결과이며 가장 높은 취약점은 사용자 환경관련 취약점이었다.[3]

〈표2〉 자동 및 정밀 진단 평가결과

위협구분	세부항목	취약점 갯수	평균
사용자 계정 관련 취약점	불필요한 계정관련 취약점 외 6항목	34	2.8
불필요한 서비스 파일 취약점	Startup 서비스 취약점 외 10항목	53	4.4
사용자 환경관련 취약점	Root 사용자 Path 관련 취약점 외 2	11	0.9
비정상적인 파일 권한 취약점	World Writable한 파일 취약점 외 2	17	1.4
시스템 환경관련 취약점	시스템 파라미터 취약점 외 7	24	2.0
추가위협 요구사항	포트취약점 외 1	14	1.1
총계	총 34 항목 점검	153	12.6



(그림1-1) 자동 진단 결과



(그림1-2) 정밀 진단 결과

3.2.1 대응방안

시스템내 불필요한 계정을 삭제하고 권장하는 암호정책을 적용하여 계정관련 취약점을 제거하며, 불필요한 서비스는 중지시키고, Root Path설정 및 host 파일을 점검하여 사용자 환경관련 취약점을 제거하며, 쓰기 권한을 제한하고 비정상적인 파일, 스케쥴리, 시스템로그, 파라미터, 레지스트리 보안 옵션 등을 점검하여 취약점을 제거한다.[3][4][5]

3.3 모의해킹을 통한 취약성 평가 분석

모의해킹은 외부영역, 인트라넷 영역(MIS), 내부(SCADA)영역으로 분류하여 실시하였으며, 인터넷 공중망을 통한 외부영역 및 인트라넷 영역에서 SCADA 망으로의 모의해킹은 실패하였으며 내부영역의 모의해킹은 성공하였다.

3.3.1 인터넷 공중망을 통한 외부영역 모의해킹

외부영역 모의해킹은 외부에서 회사 웹사이트를 접속하여 정보를 습득하고 Shell을 획득한 후 인트라넷에 침투, MIS Gateway를 점령하고 SCADA망 침입하는 단계로 시행하였으나, MIS Gateway의 보안수준이 높게 설정되어 있어 실패하였다. MIS Gateway는 Windows NT Server 4.0을 사용하고 었으나 모든 서비스 포트를 Close하여 운영함으로써 외부에서의 접근은 완전히 차단되었으며 Databas 통신은 자체 제작 소프트웨어를 사용하고 있었다.

3.3.2 인트라넷을 통한 모의해킹

인트라넷을 통한 모의해킹은 회사 내에서 경영정보 시스템 서버에 침입하여 MIS Gateway를 점령하고 SCADA망에 침입하는 단계로 시행하려 하였으나 외부영역 모의해킹 실패로 인트라넷 영역의 모의해킹은 실시하지 않았다.

3.3.3 내부영역 모의해킹

각 지역에 있는 SCADA망을 이용, 지역 SCADA 서버로 침투하여 계정정보를 획득하고 이를 통해 중앙 상황실의 SCADA 서버로 침입을 시도한 결과 서버에 대한 사용자 및 패스워드 정책은 중간 이상의 보안 레벨을 설정하고 있으나 패스워드 정책 및 불필요한 서비스의 Open으로 내부해킹 위협에 노출되어 있었다.

3.3.4 대응방안

외부와의 연결은 가급적 피하고 외부와의 데이터 송·수신이 불가피한 경우 Gateway Server를 중간에 설치하여 모든 서비스 포트를 막고 자체 소프트웨어를 제작하여 운영하며, 시스템에 대한 패스워드 정책을 강화하고 필요로 하는 클라이언트에 한하여 서비스 및 DBMS에 대한 접근제어를 설정하여 보안레벨을 강화한다.

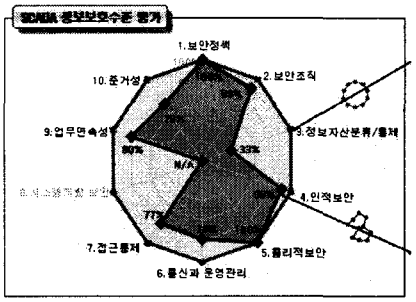
3.4 Gap 분석을 통한 취약성 종합평가

시스템 보안의 종합적인 평가를 위해 상기 3.1, 3.3.3의 평가·분석 결과를 토대로 가장 높은 보안수준인 보안정책 및 물리적 보안을 100%로 기준을 설정하여 Circle을 만들어 Gap 분석을 실시하였다.

평가결과는 (그림2)와 같고 정보자산 분류 및 통제 부분이 가장 낮은 보안수준을 보이고 있었다.

시스템에는 불필요한 서비스 파일 및 비정상적인 파일권한, 시스템 환경설정 오류 등이 존재하고 네트워크에는 경로통제 및 시스템 접근 제어미비, SNMP 보안설정 미비, 네트워크 장비 접근통제 설정 미비 등이 위협요소로 나타났다.

완벽한 보안 수준을 유지하기 위해서는 Gap 분석 결과를 바탕으로 가장 취약한 부분부터 우선 순위를 결정하여 Gap 극복방안을 도출, 전 부분의 균형 있는 정보보호 체계를 확립해야됨을 알 수 있었다.



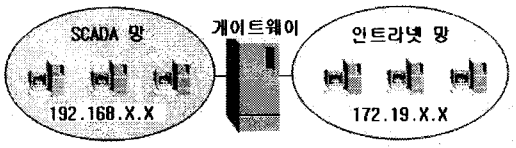
(그림2) Gap 분석을 통한 취약성 평가결과

4. 사이버 공격에 대응할 수 있는 SCADA 시스템 구축 방안 제시

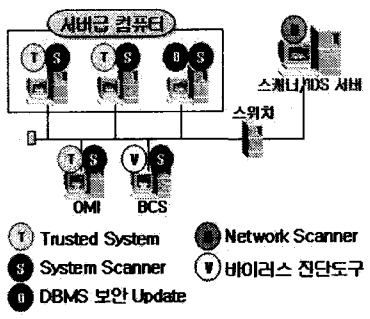
사이버 위험으로부터 시스템을 보호하고자 한다면 정보보호 지침 및 절차수립, 변경관리 보안 타당성 검토, 취약점 체크항목 마련, 보안기술강화 계획수립에 대한 정보보호 관리 체계를 구축하여 시행한다.

시스템 및 네트워크에 대한 접근경로를 완벽히 차단하며 가급적 외부와의 연결은 피하고 부득이한 경우 Gateway 서버를 설치하고 IP는 사설 I (192.168.X.X)를 사용한다. (그림3-1)

시스템에는 중요도에 따라 시스템 스케너 및 바이러스 진단도구를, 네트워크에는 네트워크 스캐너 및 IDS를 설치하고, 시스템간에는 Trusted System으 구축하며, 운영체제는 항상 최신버전의 Patch 프로그램을 Up-date한다. 기타사항들은 본지의 각 평가분석에 대한 대응방법에 준해서 구축한다. (그림3-2



(그림3-1) SCADA망과 외부망과의 연결방법



(그림3-2) 시스템 중요도에 따른 진단도구

4. 결론

본 연구에서는 현존하는 가스 SCADA의 취약점을 평가하기 위하여 적용 가능한 방법을 연구하여 적용하였으며, 그 결과를 평가 분석하여 향후 사이버 공격에 대응할 수 있는 SCADA 시스템 구축을 위하여 필요한 대응방안을 제시하였다.

여기서 시도한 취약점 평가 분석 방법 및 정보보호 관리체계 구축, 외부와의 접속경로 완전 통제, 사설 IP 사용 및 시스템 중요도에 따른 진단도구 설치 등의 대응책은 현재 운영중인 가스 SCADA 시스템에 대한 보안 대책이지만 이와 유사한 전력, 수도, 철도, 항공 등의 SCADA 시스템에도 적용할 경우 사이버 테러 및 해킹을 효과적으로 방어할 수 있을 것이다.

참고문헌

[1] 서동일, 최병철, 손승원, 이상호,"해킹 기법을 이용한 내부망 보안 평가 방법",정보처리학회논문지 C 제9-C권 제3호(2002.6)

[2] Captain Barry C. Ezell,Yacov Y. Haimes of Cyber Attack to Supervisory Control and Acquisition for Water Supply",Center for Management of Engineering Systems(May 19

[3] 포항공과대학교 전자계산소,"Security+ for Un

[4] http://www.c-cure.org.

[5] http://www.kisa.or.kr