[5C-105]

상호연동 기반의 SCADA 시스템에 대한 보안위험분석 프로세스

김인중[1], 정윤정[1], 박중길[1], 원동호[2]
전자통신연구원[1], 성균관대학교[2]
{cipher, yjjung, jgpark}@h.ac.kr[1] dosan@dosan.skku.ac.kr[2]

A Process of Security Risk Analysis in the Interoperability-based SCADA system

InJung Kim[1], YoonJung Jung[1], JoongGil Park[1], Dongho Won[2]
ETRI[1], Sungkyunkwan University[2]

요 약

최근 유비쿼터스 환경으로 진입하면서 SCADA 시스템에 대한 효율적인 운영에 많은 관심을 가지고 있으나 보안 문제로 인하여 계속 폐쇄 망으로 운영하고 있다. 이는 인터넷 기반으로 SCADA 시스템을 운영함으로써 발생되는 절감액보다 침해사고가 발생하였을 때 발생되는 피해액이 상대적으로 크다고 볼 수 있지만 정확한 위험분석을 통하여 산출된 결과라고 볼 수 없다. 또한 폐쇄 망으로 운영한다고 할지라도 내부자에 의한 침해 및 재난 재해에 의한 피해가 발생하는 경우에 대한 정확한 비교 산출 근거가 제시되고 있지 않다.

본 논문에서는 SCADA 시스템에 대해서 성능 분석 모델을 통하여 수준에 맞는 보안 환경을 유지하고 개방형으로 진화됨에 따라 보안 대책에 대한 방향을 제시하기로 한다.

I. 서론

SCADA 란 Supervisory Control And Data Acquisition 의 약어로 통합 원격감시제어시스템 또는 감시제어 데이터 수집시스템이라고 한다. 일반적으로 국가기간시설로 운영되고 있으며 점차 그 범위가 확대되어 가고 있다. 특히, 발전, 가스, 교통, 항공 등 국민 생활에 밀접하여 정보통신기반보호법 7 조 2 항[1]에서도 주기적으로 보호대책을 수립하도록 명시되어 있다.

기존의 SCADA 시스템은 현장 제어, 전용회선, 실시간 운영체제, 전용 프로토콜, 단말 PLC 등을 사용하여 해커로부터 독립적이고 안전한 운영이 가능하였다. 하지만 경영합리화를 통하여 SCADA 시스템이 중앙집중식 원격 관리, TCP/IP 네트워크 기반의 프로토콜, 범용 운영체제(Windows, Linux)를 탑재한 PC 등을 사용하기 시작함에 따라 점차 안전성이 떨어지고 보안 취약점이 증가하기 시작하였다[2]. 제어망과 정보망에 대한 비교는 표 1과 같다.

현재까지는 기존의 인프라 구조를 바탕으로 SCADA 시스템을 운영하고 있지만 향후 시스템이 노후화되고 새로운 시스템이 구축되는 경우 상호 연동에 따른 취약점 및 위협이 발생하게 되며 이러한 위험은 해커로부터 자유롭지 못하게 된다. 최근 테러의 경향을 보면 점차 SCADA 시설에 대한 공격으로 집중화되고 있으며 한번 피해가 발생하면 대규모 인명피해 및 국가적 이미지에 엄청난 실추시키게 되는 데 해커의 소행은 고도화 지능화됨에 따라 사이버테러에 대한 대비가 무엇보다도 중요하다. 특히, 사용자의 부주의에 의한 바이러스/웜 유포는 공격의 주체가 불분명하여 대응 및 복구에 대한 한계를 드러나게 한다.

표 1. 제어망과 정보망간의 비교

	제어망(SCADA)	정보망(MIS)
운영체제	실시간 OS(RTOS) 자체 OS	범용 OS (Windows,Linux)
주전산기	메인프레임	서버
단말기	PLC	PC
네트워크	폐쇄망	개방망/제한망
프로토콜	FieldBUS	TCP/IP
특징	Time Critical	Data Critical
운영 주체	전기/전자 직종	전산/컴퓨터 직종
구축	일괄적으로 진행	순차적으로 진행

지금까지는 정보망에 대한 취약점분석 평가 및 위험분석/관리는 활발하게 이루어졌지만[3] SCADA 시스템에 대해서는 개방형모델이 아니므로 취약점 연구에 상대적으로 소홀하였다. 하지만 SCADA 시스템이 점차 보편화되고 광역화됨에 따라 이에 대한 연구가 필요로 하게 되었다. 특히 SCADA 시스템은 여러 지역이 널리 분포되어 있으므로 타 시스템과의 연동이 필수적이다. 위성망, CDAM/TDMA 망, 유선/무선망, 전화망 등을 복잡하게 운영 관리하고 있으며 이로 인하여 운영자 및 관리자 조차도 응용업무의 흐름이 어떻게 진행되고 있는지를 파악하지 못하는 경우가 발생한다. 그림 1 은 일반적인 SCADA 시스템의 구조이다. 이러한 연동망에 대한