SCADA 시설에 대한 보안강화 방안에 관한 연구

정 윤 정*

요 약

현재 제어시스템은 국가 기간시설 및 대규모 산업 플랜트 등 우리 생활에 있어서 매우 중요한 역할을 수행하고 있다. 일반적으로 제어시스템을 관리하기 위하여 SCADA 시스템을 운영하고, 이런 SCADA 시스템은 정보시스템과 연동하여 운영하는 추세이다. 또한 SCADA 시스템의 운영체제는 사용자에게 편의성과 다양한 기능을 제공하기 위하여 잘 알려진 운영체제인 윈도즈나 유닉스로 변화하고 있다. 이러한 변화는 과거에 물리적으로 별도 네트워크로 안전하게 운영되던 시스템을 정보시스템에 대한 위협요소인 사이버테러에 노출하는 원인을 제공하였다. 정보시스템보다 제어시스템에 대한 사이버테러 가능성은 아직까지는 미비하지만 점차 증가하는 추세이고, 사이버테러가 발생하면 국가, 사회전반에 매우 큰 규모의 피해영향을 주게 된다. 그러므로 본 논문은 SCADA 시설에 대한 보안강화 방안을 제시하여 체계적인 보안전략을 마련하고 구현함으로써 보안수준을 향상시키고자 한다.

The Study on a Security Safeguard Plan for SCADA Infrastructure

Yoon Jung Chung*

ABSTRACT

The control system is accomplishing very important role in our life currently as the national critical Infrastructure and large scale industry plant. We manage SCADA system to manage generally the control system interconnected with the information system. The operating system of SCADA is changing also to the well-known OS like Windows or UNIX for offer various convenience and facility to the user. We offered the reason why such change of the system makes so that it is exposed to cyber terror. In the traditional SCADA system is managed safely by an isolated network system physically. It is the trend to increase gradually though a cyber terror possibility is thinner on a control system than a information system but the cyber terror gives a nation or community wide damage influence of large scale if it happens. Therefore this paper presents a security safeguard plan about SCADA system and helps prepare systematic security strategy and enhance the security level implement.

Key word : SCADA, Information Security, Cyber Terror, Risk Analysis

* 국가보안기술연구소

1. 서 론

급속한 인터넷의 보급과 보편화는 많은 조직들이 기존의 조직 경영을 위한 시스템에서 고객 중심의 시스템으로 전환하도록 유도하였다. 또한 개인도 정보 생활을 영위하며 다양한 서비스를 제공받고 있다. 다양한 정보와 서비스를 위하여 정보시스템과 네트워크는 상호연동을 하는 추세인데, 이를 위하여 각종 프로토콜도 표준화되어 이기종간의 접속이나 연동이 가능하도록 발전하고 있다. 이러한 정보시스템과 네트워크의 상호연동 추세로 인하여 각 장비, 네트워크와 프로토콜의 취약점이 다른 시스템에 전이되는 결과를 초래하고 있다.

SCADA 시스템은 집중원격감시제어시스템으로 통신 경로상의 아날로그 또는 디지털 신호를 사용하여 원격장치의 상태정보 데이터를 수집, 수신, 기록하고, 수집한 정보를 이용하여 중앙제어시스템의 원격 장치를 감시하고 제어하는 시스템이다. 이 시스템은 발전, 송배전시설, 석유화학플랜트, 제철 공정시설, 석유, 송유관 등의 다양한 제어시스템을 원격관리하기 위하여 사용한다.

과거에는 이러한 산업제어시스템은 정보시스템과 물리적으로 분리된 별개의 네트워크로 구성되었다. 그러나 많은 정보를 제공받고자 하는 국민이나 고객에게 제어시스템에서 발생하는 다양한 정보를 제공하거나 조직의 경영자에게 제어시스템의 주요 정보를 신속하게 제공하기 위하여 정보망(business network)과 연동하고 있는 추세이다. 이러한 연동을 통해서 제어시스템에 비하여 잘 알려진 프로토콜과 서비스를 사용하는 정보망의 다양한 취약점으로 인하여 제어시스템의 보안에 대한 중요성이 부각되었다.

본 논문은 SCADA 시설의 보안수준 향상을 위하여 요구되는 보안 강화방안을 제시하고자 한다. 본 논문의 구성은 SCADA 보안 현황을 제 2장에서 설명하고, 제 3장에서 SCADA 시설에서 요구되는 보안요구사항을 기술하였다. 제 4장은 SCADA 시설을 위한 보안강화 방안을 제시하고, 마지막 제 5장은 결론 및 향후 추진해야 할 연구사항을 기술하였다.

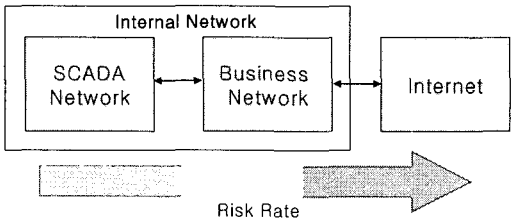
2. SCADA 보안 현황

SCADA 보안활동은 미국 국토안보부(DHS : Department of Homeland Security)에서 주도적으로 진행하고 있다. 활동의 목적은 국가 주요 기반시설로 운영되는 제어시스템에 잠재되어 있는 취약점을 제거하고 위협에 대응하기 위하여 정부와 산업 간의 협력을 강화하는 것이다. 제어시스템 프레임워크는 토폴로지, 기능, 시스템 보안 목표, 산업 사례, 보안 요구사항, 권고안 등으로 구성되는 사이버 안전 매트릭스를 제공한다. 또한 제어시스템을 운영하는 사이트들을 위한 안전 보증등급과 보안조건을 충족시킬 수 있는 도구를 개발하고, 이를 사이트에 제공한다.

SCADA 시스템에 대한 자산 우선순위화를 하고, 위협과 취약점을 식별하여 이로 인한 피해영향을 산정한다. 보안등급에 따라 관련 연구소와 산업체가 공동 테스팅을 수행하고 가능한 공격의 패턴을 개발하여 제어시스템 산업에 대한 인식을 높이고 있다. 이러한 국가 테스트베드를 운영하면서 운영체제 및 프로토콜에 대한 연구를 지속적으로 수행하고, 표준화 활동을 수행하고 있다. 정보시스템 및 SCADA 시스템에 대한 위험분석 관련 표준으로는 보안 분류에 관한 FIPS 199와 SP800-60, 보안 컨트롤 영역에 관한 FIPS 200과 SP800-53, 보안 컨트롤 문서들에 관한 SP 800-18, 보안 컨트롤 구현에 관한 SP800-70, 시스템 인증 관련 SP800 등이 있다[1-6].

현재 공격에 필요한 지식수준이 낮아지고 공격기술 수준은 고도화 되고, IT 시스템 뿐만 아니라 SCADA 시스템의 경우 공격자들 사이에서 점차적으로 관심도가 높아지고 있다. 그러나 SCADA 시

스템을 보호하기 위한 방법은 IT 시스템에 비해 미비한 수준이다. IT 네트워크의 경우 다양한 공격도구들로 인해 공격에 대한 전문지식이 없이도 공격이 가능하지만, 기존에 특화된 OS 사용과 분리된 네트워크 사용으로 제어 시스템은 아직은 안전하다. 그러나 (그림 1)과 같이 점차적으로 IT 네트워크와의 통합이 이루어지고 있으므로 보안 예방 및 대응을 위한 수준을 향상시켜야 한다. (그림 1)에서 보는 바와 같이 SCADA 시스템이 Business 네트워크와 연동이 되고, Business 네트워크와 인터넷이 연동이 된다면 SCADA 시스템의 보안 수준을 인터넷에서 필요한 보안수준으로 적용해야 한다. 인터넷으로 연동될수록 위험 가능성은 높아지므로, 이러한 연동형태로 구성되었다면 SCADA 시스템, Business 네트워크, 인터넷에 대한 모든 보안 메커니즘을 구축해야 한다[7].



(그림 1) SCADA 시스템 연동

실제로 이러한 위협으로 인하여 일부 제어 시스템에 보안 사고가 발생하였다. SANS SCADA Security Summit에 의하면 Davis-Besse 핵발전소는 블래스터 웜에 감염되었고 호주 Sewage Release에서는 불만이 많은 직원에 의해 밸브가 열리는 사건 발생하였다 .또한 Worcester 공항에서는 10대에 의해 PBX 스위치가 해킹되어 활주로 등이 꺼지는 보안 사고가 발생하였다[9].

과거에는 사이버 보안사고 발생에 대한 가능성은 희박하였지만, 네트워크와 정보시스템 간 연동으로 인하여 점차 침해사고도 늘어가고 있는 현실이다.

3. 보안 요구사항 및 자산평가 방안

3.1 SCADA 침해사고

본 시나리오는 SANS SCADA Security Summit에서 데모를 한 공격 시나리오이다[9]. 본 시나리오를 통하여 필요한 정보보안 요구사항을 분석하였다.

3.1.1 시나리오

본 시나리오는 한 전력회사의 SCADA 시스템을 장악하는 보안침해 시나리오이다.

① 공격자는 HTML 공격코드를 가진 파워포인트를 첨부한 메일을 전력회사 직원의 이메일로 전송한다.
② 공격자는 사용자에 의해 파워포인트가 오픈되기를 기다린다.
③ 사용자가 첨부된 파워포인트를 열고 이미지 위로 마우스가 이동하면 인터넷익스플로러는 사용자의 컴퓨터 c:에 컴파일된 help 파일을 오픈한다.
④ 공격자의 help 파일은 공격자의 컴퓨터로부터 루트킷을 다운받아 실행하여 공격자가 사용자의 컴퓨터에 연결 가능하다.
⑤ 공격자는 사용자의 업무상 컴퓨터를 제어할 수 있게 되어 업무용 네트워크를 조사하고 방화벽을 찾기 위해 ARP 스캔을 수행한다.
⑥ ARP 스캔은 업무용 네트워크상의 컴퓨터를 찾아내고 ARP back scatter 공격으로 SCADA 네트워크와의 연결 지점인 방화벽이나 게이트웨이에 대한 정보를 수집한다.
⑦ 공격자는 SCADA 방화벽과 DNS 서버 사이에 중간자 공격을 수행한다.
⑧ 감염된 png 이미지를 포함하고 있는 웹사이트를 위조한 후 DNS 요청을 기다린다
⑨ 운영자가 DNS 서버에 요청을 시도하면 공격자

는 중간에 패킷을 가로채서 위조 사이트로 연결시킨다.

⑩ 공격자는 운영자의 컴퓨터에 pnp 이미지 공격 코드를 전송하고 공격자의 컴퓨터로부터 루트킷을 실행함으로써 SCADA 사용자 컴퓨터를 제어 가능하다.

이러한 침해사고 시나리오는 제어시스템과 IT 시스템의 연동으로 공격이 가능하다. IT 시스템의 위협을 이용하여 시스템을 장악하고 SCADA 시스템에 대한 명령어 등을 학습하여 최종적으로 SCADA 시스템에 대한 제어도 가능하게 된다.

3.1.2 시나리오 관련 보안대책

상기 보안침해 시나리오 대한 공격 방법들을 예방하기 위하여 필요한 보안대책을 분석한다.

- Phishing 등을 예방하기 위해서 정상적인 웹 사이트를 판별할 수 있도록 교육을 해야한다.
- HTML Help 공격코드를 탐지하기 위해선 시스템 업데이트와 IDS를 설치해야 한다
- ARP 스캔을 탐지하기 위해선 IDS를 설치해야 한다.
- DNS spoofing을 방지하기 위해서 SCADA 네트워크로부터 웹 브라우징이 불가능하게 설정해야 한다.
- Libpng 버퍼 오버플로우를 방지하기 위해서는 시스템을 업데이트하고 패치를 수행해야 한다.
- SCADA 명령어를 가로챌 수 없게 하기 위해서는 SCADA 통신을 위한 인증을 수행해야 한다.

SCADA 시스템과 IT 시스템에 연동이 되어 있기 때문에 IT 시스템에서 사용하는 취약점을 통하여 SCADA 시스템까지 보안침해가 발생할 가능성이 높아진다. 그러므로 SCADA 시스템에 대한 보안과 함께 연동되어 있는 IT 시스템에 대한 보안 대책 적용도 매우 중요하다.

3.2 SCADA 보안요구사항

IT 정보망과 제어 시스템은 운영환경이 다르므로 보안에 대한 적용에 차이점이 있다. <표 1>은 IT 시스템과 제어시스템의 보안에 대한 관점 차이점을 분석하였다.

〈표 1〉 제어시스템과 IT 시스템 비교

내용	IT 시스템	제어시스템
보호대상	정보	물리적인 처리
피해영향	정보노출, 재정적 영향	생활, 생명, 환경, 사회, 재정적 영향
평가방법	취약점 평가	위험평가
운영체제	대화형, 단위처리, 잘 알려진 OS	대화형 실시간, 특화된 OS (최근 SCADA 서버는 알려진 OS 사용추세)
안티바이러스 및 모바일코드	일반적으로 발생	일반적이지 않으며 적용 역시 거의 불가능
제공기술의 생명주기	대부분 3~5년	20년 이상
보안패치	정기적으로 수행	업체별로 느리게 적용
처리시간	상대적으로 지연 허용	안전성으로 인해 매우 시간에 민감
가용성	유지보수를 위해 일시적 중단 허용	24시간 365일 항상 동작 필요
장애허용	몇 시간 ~몇 달 정도	백만분의 일초~몇 시간
문제에 대한 대응	재부팅 가능	복구(재부팅 불가)
보안 인식	매우 필요하다고 인식	물리적 보안을 제외하고 매우 열악
보안 테스트 및 감시	필수적으로 스케줄에 의하여 수행	기계 정전에 대비한 테스트에 중점을 두어 수행

<표 1>에서 분석한 바와 같이 제어시스템은 정보시스템보다 실시간 운영과 가용성이 매우 중요한 시스템이다. 그러므로 제어시스템에 보안대책을 적용하려면 가용성에 영향을 주지 않도록 개발해야 한다.

3.3 제안하는 자산평가 방법

SCADA 시스템에 대한 보안 적용을 위해서는 기본적으로 위험평가를 수행하여야 한다. 위험평가는 첫 번째 프로세스인 자산 평가를 통하여 SCADA 시스템의 자산가치 산정와 주요 자산식별이 가능하다, 본 논문에서는 SCADA 시스템에서 자산평가 방법을 제안하고자 한다. 자산평가는 자산 자체의 가치와 보안현황 수준을 통하여 위험평가의 대상 시스템 식별이 가능하다. 자산가치 산정은 업무의 지원성, 정보보안 요구사항의 정도, 피해영향을 분석하여 결정한다. 마지막으로 보안현황 수준은 네트워크 연결정도, OS의 알려진 정도와 현재 적용되어 있는 보안수준으로 파악한다.

$$AE = AV \times SS$$
$$AV = BI \times SF \times DI$$
$$SS = (NWC \times OS)/PS$$

여기서 AE는 Asset Evaluation, AV는 Asset Value, SS는 Security Status, BI는 Business Importance, DI는 피해영향, NWC는 Network connectivity, OS는 OS의 알려진 정도, PS는 Present Safeguard이다. 자산평가는 수식에 <표 2>~<표 4>에 제시된 등급별 점수를 대입하여 산정한다.

〈표 2〉 정보보안 요구사항 등급분류

등급	기밀성	무결성	가용성
5	비밀성이 있는 데이터	데이터의 수정·변경에 매우 민감	시스템이 정지에 매우 민감
3	민감하지만 비밀은 아닌 데이터	데이터 수정·변경에 일부 영향	시스템이 정지에 일부 영향
1	평문데이터	데이터 수정·변경이 크게 상관없음	시스템이 정지와 크게 상관없음

〈표 3〉 OS 사용에 따른 등급분류

등급	내 용
5	정보시스템에서 사용하는 잘 알려진 OS 사용하는 경우(Windows, UNIX, Linux 등)
3	SCADA 개발 업체에 특화된 OS를 사용하고, SCADA 시스템의 OS로 대중화가 되어 있는 경우
1	- SCADA 개발 업체에 특화된 OS를 사용하고, SCADA 시스템의 OS로 대중화가 낮은 경우 - 기관요구에 의하여 별도 OS를 수정하거나 개발을 한 경우

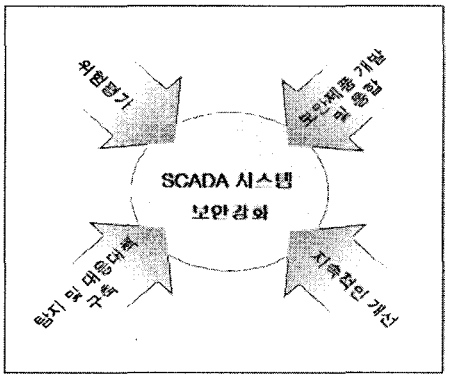
〈표 4〉 네트워크 연동현황에 따른 등급분류

등급	내 용
5	SCADA 시스템이 인터넷과 직접 연동할 경우
4	SCADA 시스템과 연동한 정보망이 직접적으로 인터넷과 연동할 경우
3	SCADA 시스템과 연동한 정보망이 간접적으로 인터넷과 연동할 경우
2	SCADA 시스템과 연동한 정보망이 인터넷과 연동하지 않을 경우
1	SCADA 망일 물리적으로 별도망 구성일 경우

4. 제안하는 보안강화 방안

본 절은 국가 기간시설의 주축을 이루는 SCADA 시스템의 보안을 강화하기 위한 방안을 (그림 2)와 같이 제시하였다. 강화 방안으로는 첫째 예방활동에 해당하는 위험평가를 수행하고, 둘째는 위험평가를 수행하여 제시한 보호대책을 적용하기 위한 보안제품을 개발을 해야 한다. 셋째는 신속대응을 위한 방법으로 보안침해 탐지 및 대응대책을 구축해야 하고, 마지막으로 이러한 활동들을 지속적으

로 수행하고 개선해야 하는 것이다[10].



(그림 2)

4.1 위험평가

SCADA 시스템의 운영 컴포넌트 식별, 네트워크 연동현황 등을 파악하고, 위협 및 취약점을 식별한다. 또한 식별한 위협 및 취약점을 제거하기 위한 활동을 정의하고 구현 계획을 세워야 한다[14, 15].

위험은 위협, 취약점, 이로 인한 손실로 산정되는데, 위협은 사람, 환경, 사건을 의미하고 취약점은 우발적 사고 혹은 공격이 가능한 시스템의 보안약점이며 손실은 예상되는 피해의 양이다. 이러한 위험분석 수행을 통하여 시스템의 현재 운영현황과 보안 수준을 파악할 수 있다[11-13].

위험분석은 현재 운영하는 시스템의 위협 노출 정도를 파악하고, 이를 제거하기 위한 보안 통제를 수립하는 일련의 프로세스이다. 시스템의 위협에의 노출 정도에 따른 보안 수준을 결정하는 과정은 취약한 컴포넌트 식별, 위협 식별, 감소 방안 파악의 3단계로 이루어진다.

① 취약한 컴포넌트 식별을 위해 사용 네트워크, OS, 사용 장비 등을 식별
② 취약한 컴포넌트에 대해 알려진 공격을 연관시킴으로써 발생 가능한 위협과 취약점을 식별
③ 특정 공격을 방어하기 위한 수단으로 수정, 차단, 탐지 등을 확인하여 위험감소 방법 파악

제어 시스템은 문제 해결을 위해 빈번한 수정적용이 쉽지 않고, 계층별 방어를 고려하여 적절한 보안전략을 구축해야 한다.

4.2 보안제품 개발 및 통합

위험평가에서 보안 위험이 식별되고, 이를 제거하거나 감소시키기 위한 보호대책을 적용해야 한다. 또한 조직 환경에 필요한 보안제품이 식별된다면 개발해야 한다. 보안도구를 개발할 때 고려해야 할 사항이 있다.

제어시스템에서 가장 민감한 보안요구 사항인 가용성에 영향을 주지 않도록 개발해야 한다. 가능한 호스트에 영향을 주지 않도록 안티 바이러스, 방화벽 등 안전한 게이트웨이의 구축이 필요하다[8]. 또한 이러한 보안제품을 개발한 후 조직에 정합 테스트를 한 후 통합을 수행해야 한다.

SCADA 시스템에 적합한 보안제품들을 개발을 하면서 장기적 비전으로 동일 보안제품에 대한 표준화의 고려도 필요하다.

4.3 탐지 및 대응체계 구축

사이버침해는 항상 위협으로 존재하므로 이를 탐지하고 신속하게 대응하기 위한 보안침해 탐지 및 대응체계를 구축해야 한다. 제어시스템에 침해의도가 발견되면 자동적으로 대응 조치가 가능한 시스템을 구현해야 한다. 이를 지원하기 위한 SCADA 시스템에 적합한 IDS, IPS와 감사활동을 위한 시스템 개발이 필요하다

4.4 지속적인 개선

SCADA 시설 보안강화를 위한 방안으로 예방활동, 보안제품 개발, 대응활동 등을 제안하였다. 이러

한 활동은 운영환경, 위협과 취약점의 변화에 의하여 지속적으로 개선하여 안전하게 운영해야 한다. 또한 이러한 활동들을 수행하기 위한 보안 교육 및 훈련도 체계적이고 지속적으로 마련되어야 한다.

5. 결 론

제어시스템은 컴퓨터시스템을 기반으로 하고, 민감한 처리와 물리적인 기능을 제어하고 감시하기 위하여 많은 기반구조와 산업에서 사용 중이다. 과거에는 제어시스템의 보안은 물리적 공격에 대한 보호와 시설의 오동작을 대처하기 위한 것이었다. 그러나 최근에는 적대국가, 테러그룹, 불만있는 고용인 또는 악성침입자에 의하여 사이버침해가 발생하고 있다. SCADA 시스템은 기간시설로 매우 중요하고, 침해사고가 발생하면 대규모 피해 영향을 줄 가능성이 높다.

본 논문은 SCADA 시설의 환경변화로 사이버 침해 가능성이 높아졌고, 이를 보호하기 위한 방안을 제안하였다. 이러한 보안대책 강화방안이 적용되기 위해서는 체계적인 전략이 필요하고, 아직 SCADA 시설은 보안이 초보단계이므로 많은 시간이 소요될 것이다.

향후 SCADA 시설의 보안을 위하여 연구할 내용은 본 논문에 제시한 4가지 방안에 대한 세부 활동을 정의하는 것이다. 우선 수행할 연구 내용은 위험평가를 제대로 수행하기 위하여 SCADA 시설의 보안 Best Practice를 정의해야 한다. Best Practice는 SCADA 시설의 도메인 별로 다르므로 전력 Grid에 대한 보안 Best Practice에 초점을 맞추어 연구할 계획이다.

참 고 문 헌

[1] Guideline for Developing Security Plans for Federal Information Systems, SP800-18, http://csrcnist.gov/publications/nistpubs/index.html.

[2] Recommended Security Controls for Federal Information Systems, SP800-53, http://csrcnist.gov/publications/nistpubs/index.html.

[3] Guideline for Mapping Types of Information and Information Systems to Security Categories, SP800-60, http://csrcnist.gov/publications/nistpubs/index.html.

[4] Security Configuration Checklists Program for IT Products : Guideline for Checklists Users and Developers, SP800-70, http://csrcnist.gov/publications/nistpubs/index.html.

[5] Standards for Security Categorization of Federal Information and Information Systems, FIPS 199, http://csrcnist.gov/publications/fips.

[6] Minimum Security Requirement for Federal Information and Information Systems, FIPS 200, http://csrcnist.gov/publications/fips.

[7] The integration of SCADA and corporate IT, Ian Wiese, http://www.iinet.net.au.

[8] Cyber security tools for SCADA, Dennis K. Holstein, OPUS publishing, October 2004.

[9] SANS, SCADA 2006 Security Summit, http://www.SANS.org.

[10] Roadmap to secure control systems in the energy sector, DOE&DHS, January 2006.

[11] Harold F. Tipton and Micki Krause, "Information Security Management Volume 3~4th Edition", Auerbach Publications, pp. 417-430, 2002.

[12] BS 7799-Guide to Risk Assessment and Risk management, BSI, 1998.

[13] B. D. Jenkins, "Security Risk Analysis and management", Countermeasures, Inc., 1998.

[14] Information Technology Security techniques Guidelines for the management of IT security, ISO/IEC JTC 1/SC 27, 1997.

[15] Gary Stonebumer, Alice Goguen, and Alexis Feringa, "Risk Management Guide For Information Technology Systems", NIST, 2001.

정 윤 정

1997년 성균관대학교 정보공학과(공학사)

1999년 성균관대학교 전기전자 및 컴퓨터공학과 (공학석사)

1999년~2000년 하나로통신 IDC 근무

2000년~현재 한국전자통신연구원 근무