情 報 保 護 學 會 誌
第19卷 第5號, 2009. 10

산업제어시스템 보안을 위한 네트워크 설계 및 구조

전 용 희*

요 약

본 논문에서는 산업제어시스템 보안을 위한 네트워크 설계 및 구조에 대하여 살펴보고자 한다. 산업제어시스템을 위한 네트워크 구조 설계에서, 통상적으로 제어 네트워크를 사내 망과 분리하는 것이 권고된다. 그러나 산업제어시스템과 사내 망의 연결이 필요한 실제 상황이 발생할 수 있다. 만약 이런 연결이 이루어진다면, 심각한 보안 위험을 유발하기 때문에 설계 및 구현에서 주의가 요구된다. 따라서 본 논문에서는 산업제어시스템 보안을 위한 네트워크 설계 원칙 및 네트워크 구조와 방화벽의 사용, DMZ의 생성, 효과적인 보안 정책을 갖춘 침입탐지 능력, 훈련 프로그램과 사고 대응 메커니즘을 포함하는 심층-방어 보안 구조에 대하여 소개하고자 한다.

Ⅰ. 서 론

산업제어시스템(ICS: Industrial Control System)과 IT 시스템 사이에는 주요한 운영적 차이점이 존재하기 때문에, 기존 IT 시스템에 적용하던 보안 제어 방법이 ICS에 적용되기 위하여 변경되어야 한다. 따라서 기존 보안 프로그램이 ICS 기술과 환경 요구사항 및 특성에 맞도록 개발되어야 한다.

서비스거부(DoS: Denial of Service) 공격과 웜, 바이러스 같은 멀웨어가 이미 보편화되었고 ICS에 영향을 미치고 있다. 만약 주요 하부구조에 침해가 발생하면 심각한 영향을 미칠 수 있다. 이는 ICS의 실패로 인한 인명 부상 및 손실, 환경 파괴와 같은 물리적 영향, 그리고 부차적으로 발생하는 경제적 및 사회적 영향이 있다.

ICS 보안의 초점은 단순한 장치가 아니라 PLC (Programmable Logic Controller), DCS (Distributed Control System), SCADA(Supervisory Control And Data Acquisition)와 HMI(Human Machine Interface) 같은 감시 장치를 사용하는 계기-기반 시스템을 포함하여야 하며, ICS 시스템에 대한 위험 평가를 수행하고 그 결과를 바탕으로 각 시스템에 대한 잠재적 영향을 기반으로 ICS 시스템의 우선순위를 정해야 한다.

ICS 내부 취약점의 식별도 대표적인 IT 시스템과는 다른 접근을 요구한다. 대부분의 경우, IT 시스템 상의 장치는 고객에 대한 서비스를 거의 중단하지 않고 재부팅, 재저장 및 대체될 수 있다. 반면에 ICS는 실제 프로세스를 제어하고 따라서 조처(행동)에 따른 실제 결과를 가져다준다. 어떤 행동은 시간에 민감하며 다른 것은 좀 더 여유 있을 수도 있다. [표 1]은 정보 시스템과 제어 시스템에서의 보안 특성 차이를 보여준다.

Ⅱ. 네트워크 설계 원칙

2.1 개요

ICS를 위한 네트워크 구조 설계는 일반적으로 사내 망(Corporate Networks)과 분리시키는 것이 권고된다. 사내 망에서 통상적으로 허용되는 인터넷 접근, FTP(File Transfer Protocol), 이메일 및 원격 접근 트래픽이 ICS 네트워크에서는 허용되지 않아야 한다. 분리된 네트워크를 보유함으로써, 사내 망에 대한 보안과 성능이 ICS 네트워크에 영향을 미칠 수 없도록 해야 한다.

그러나 ICS와 사내망의 연결이 필요한 실제 상황이 발생할 수 있다. 만약 이런 연결이 이루어진다면, 이것이 심각한 보안 위험을 유발하기 때문에 설계 및 구현에서 주의가 요구된다. 두 네트워크가 연결되어야 한다면, 최소한의 연결을 허용하고 방화벽과 DMZ(De-

* 대구가톨릭대학교 컴퓨터정보통신공학부(yhjeon@cu.ac.kr)

Militarized Zone)[1]를 통하는 것이 권고된다. DMZ는 방화벽에 직접 연결된 별도의 네트워크 세그먼트이다.

〔표 1〕 정보 시스템과 제어 시스템의 보안 특성 차이점

보안 특성	정보 시스템	제어 시스템
앤티바이러스/모바일 코드	통상적 광범위한 사용	비통상적/효과적인 설치가 불가능
지원 기술 수명	2-3년 다양한 공급자	최대 20년 단일 공급자
아웃 소싱	통상적 광범위한 사용	운영이 흔히 아웃소싱 되지만, 여러 제공자에게 다양화되지 않음
패치 응용	정기적 계획됨	드뭄, 비계획적 공급자 특정
변경 관리	정기적 계획됨	고도로 관리되고 복잡함
시간 민감 내용	일반적으로 지연 허용	지연 허용 안됨
가용성	일반적으로 지연 허용	연속적 사용
보안 인식	개인 및 공공 부문에서 중간 정도	물리적 보안을 제외하고 열악
보안 시험/감사	좋은 보안 프로그램의 부분	정지에 대한 일시적 시험
물리 보안	안전	원격/무인 안전

사내 망으로부터 접근될 필요가 있는 ICS 데이터를 포함하는 서버는 이 네트워크 세그먼트에 설치해야 된다. 단지 이 세그먼트만 사내 망에서 접근 가능해야 한다.

2.2 방화벽

방화벽은 다른 보안 입장을 채택하고 있는 네트워크 사이의 트래픽 흐름을 제어하는 시스템 혹은 장치이며, 패킷 필터링 방화벽, 상태유지(stateful) 감시 방화벽 및 애플리케이션-프락시 게이트웨이 방화벽 등이 있다. ICS 환경에서, 방화벽은 ICS 네트워크와 사내망 사이에 대부분 설치된다. 적절하게 방화벽 구성이 이루어진다면, 제어 시스템 호스트 컴퓨터와 컨트롤러에 대한 불필요한 접근을 제한할 수 있고 보안을 증진시킬 수 있다.

1) 여기서 DMZ는 인터넷 접근 가능 서버와 네트워크 내의 서비스들을 보호하기 위한 버퍼 역할을 하는 네트워크 장치에 추가된 인터페이스를 의미한다.

방화벽은 프로세스 제어 장치에서 수행할 수 없는 다음과 같은 보안 정책을 실행해야 한다:

- 비보호 LAN과 보호된 ICS 네트워크 상의 장치사이에 특정 실행 통신망을 제외하고 모든 통신을 차단한다. 차단은 외향 및 내향 패킷 모두에 대하여 발생하며, 소스와 목적지 IP 주소 쌍, 서비스 및 포트 기반으로 이루어진다.
- ICS 네트워크에 접근하는 모든 사용자의 보안 인증을 ICS 네트워크의 취약성에 따라 단순한 패스워드, 복잡한 패스워드, 복수-인자 인증 기술, 토큰, 바이오 메트릭 및 스마트카드 같은 특정한 방법을 사용하여 수행한다.
- 사용자의 업무 기능에 필요한 제어 네트워크 상의 노드에만 접근을 제한적으로 허용함으로써, 고의적 혹은 우연적인 사고 가능성을 줄이도록 한다.
- 트래픽 감시, 분석 및 침입 탐지를 위한 정보흐름을 기록한다.
- ICS에 적절한 운영 정책을 구현하도록 해야 한다.

ICS 환경에 방화벽을 설치할 때 다음과 같은 문제점이 존재 한다:

- 제어 시스템 통신에 지연 추가의 가능성
- 산업 응용에 적합한 규칙집합(rule set) 설계에서의 경험 부족

사이버 사고를 신속하게 탐지하고 대응하기 위하여 방화벽과 다른 보안 센서들의 실시간 감시가 필요하다.

2.3 제어 네트워크의 논리적 분리

ICS 네트워크는 물리적으로 분리된 네트워크 장치 상에서 사내 망으로부터 최소한 논리적으로 분리되어야 한다. 연결이 필요할 때는 아래와 같은 원칙들이 지켜져야 한다:

- ICS 네트워크와 사내 망 사이에 문서화되고 최소한의 액세스 포인트만 있어야 한다.
- ICS 네트워크와 사내 망 사이의 상태(stateful) 방화벽은 분명하게 권한이 부여된 트래픽을 제외하고 모든 트래픽을 거부하도록 구성되어야 한다.
- 방화벽 규칙은 TCP와 UDP(User Datagram Protocol) 포트 필터링, ICMP(Internet Control Message Protocol) 유형 및 코드 필터링 이외에 적어도 소스와 목적지 필터링를 제공해야 한다.

ICS 네트워크와 사내 망 사이의 통신을 하는 한 가지

바람직한 방법은 중간 DMZ 네트워크를 구현하는 것이다. 단지 사내 망과 DMZ 사이에, 그리고 ICS 네트워크와 DMZ 사이에서 제한된 특정 통신만 발생하도록 하기 위하여, DMZ는 방화벽에 연결되어야 한다. 사내 망과 ICS 네트워크는 서로 직접 통신하지 않아야 한다.

Ⅲ. 네트워크 구조

이 절에서는 여러 가능한 네트워크 구조에 대하여 기술하며 각각의 장단점을 설명한다. 이 절에 나오는 그림들은 네트워크를 분리하기 위하여 방화벽의 설치를 보여주기 위한 것이며, 모든 장치들을 모두 보여주기 위함은 아니다.

3.1 사내 망과 제어 네트워크 사이의 방화벽

사내 망과 제어 네트워크 사이에 단순한 두 포트 방화벽을 도입함으로써, 보안 개선을 상당 부분 얻을 수 있다. 방화벽을 적절히 구성한다면, 제어 네트워크에 대한 성공적인 외부 공격의 기회를 많이 감소시킨다.

그러나, 이 설계에서는 두 가지의 문제가 존재한다. 첫 번째로, 만약 데이터 서버가 사내 망에 존재한다면, 방화벽은 데이터 서버가 제어 네트워크 상의 제어 장치와의 통신을 허용해야 한다. 이 경우 사내 망의 악성 혹은 부적절하게 구성된 호스트에서 발생한 패킷이 개별 PLC/DCS에 전달될 수 있다.

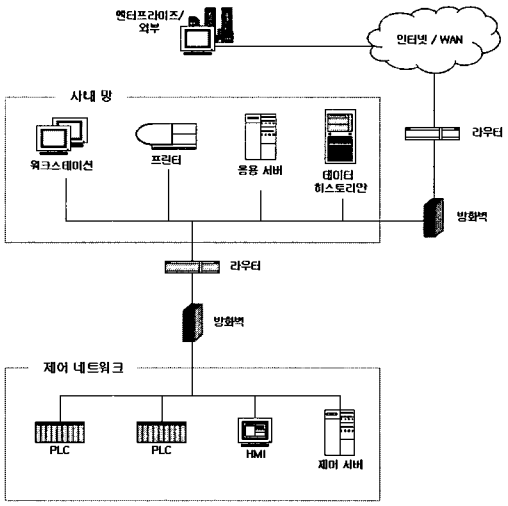
만약 데이터 서버가 제어 네트워크 상에 존재한다면, 사내 망으로부터의 모든 호스트가 데이터 서버와 통신하는 것을 허용하는 방화벽 규칙이 있어야 한다. 대표적으로, 이런 통신은 SQL(Structured Query Language)이나 HTTP(Hypertext Transfer Protocol) 요구와 같은 응용 계층에서 일어난다. 데이터 서버 응용 계층 코드의 결함이 서버 침해를 초래할 수 있다. 일단 서버가 침해되면, 제어 네트워크 상의 나머지 노드들이 웜 전파나 상호작용 공격에 취약하게 된다.

두 번째 문제점은 제어 네트워크에 영향을 줄 수 있는 위장된 패킷이 만들어질 수 있다는 것이다. 이 경우, 은밀한 데이터가 허용된 프로토콜 내에 터널 된다. 예를 들어, 만약 HTTP 패킷이 방화벽을 통하여 허용된다면, HMI나 제어 네트워크 컴퓨터에 우발적으로 유입된 트로이 목마 소프트웨어가 원격 엔티티에 의하여 제어될 수 있고, 합법적인 트래픽으로 위장하여 그 엔티티에게 포착된 패스워드 같은 데이터를 전송할 수 있다.

요약하면, 이 구조는 비-분리 네트워크에 비하여 상당한 개선이 있지만 사내 망과 제어 네트워크 장치 사에 직접 통신을 허용하는 방화벽 규칙의 사용을 요구한다. 이것은 매우 주의 깊게 설계되고 감시되지 않는다면 보안 침해 가능성을 초래 할 수 있다.

3.2 사내 망과 제어 네트워크 사이의 방화벽과 라우터

보다 조금 더 정교한 설계는 라우터/방화벽의 결합을 사용하는 것이다. 라우터는 방화벽 앞단에 위치하여 기본적인 패킷 필터링 서비스를 제공하며, 방화벽은 상태 감시나 프락시 기법을 사용하여 더욱 복잡한 문제를 다룬다. 이 형태의 설계는 신속한 라우터가, 서비스 거부(DoS: Denial of Service) 공격의 경우에서처럼, 대량의 입력 패킷들을 처리할 수 있게 하여 주고 방화벽에 대한 부하를 감소시켜 준다. 또한 공격자가 통과해야 할 두 개의 다른 장비가 있기 때문에 개선된 심층-방어를 제공한다. [그림 1]은 사내 망과 제어 네트워크 사이의 방화벽과 라우터의 배치를 보여준다.



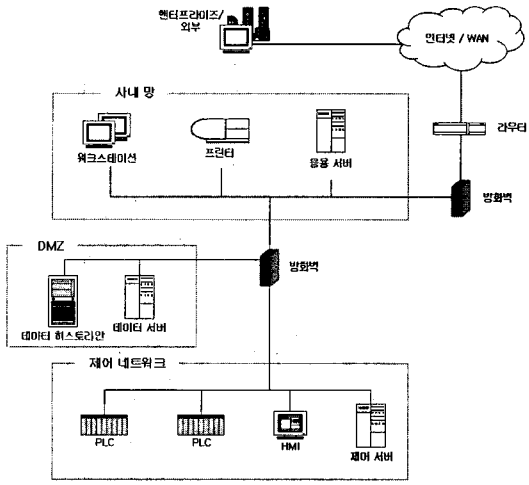
〔그림 1〕 사내 망과 제어 네트워크 사이의 방화벽과 라우터

3.3 사내 망과 제어 네트워크 사이에 DMZ를 가진 방화벽

보안이 훨씬 더 개선된 방법은 사내 망과 제어 네트

워크 사이에 DMZ를 설립하기 위한 능력을 가진 방화벽을 사용하는 것이다. DMZ는 데이터 서버, 무선 액세스 포인트, 혹은 원격 및 제 3자 액세스 시스템과 같은 한 개 이상의 중요 컴포넌트를 보유한다. DMZ 가능 방화벽을 사용함으로써 사실상 중간 네트워크의 생성을 허용하는 것이 된다.

DMZ의 생성은 방화벽이 대표적인 공공 및 사설 인터페이스뿐만이 아닌, 세 개 이상의 인터페이스를 제공하는 것을 요구한다. 인터페이스 중의 하나는 사내 망에 연결되며, 다른 한 개는 제어 네트워크에, 마지막으로 DMZ 네트워크 상의 데이터 서버나 무선 액세스 포인트와 같은 공유 혹은 보안이 취약한 장비에 연결된다. [그림 2]는 이 구조의 예를 보여준다.



〔그림 2〕 사내 망과 제어 네트워크 사이 DMZ를 가진 방화벽

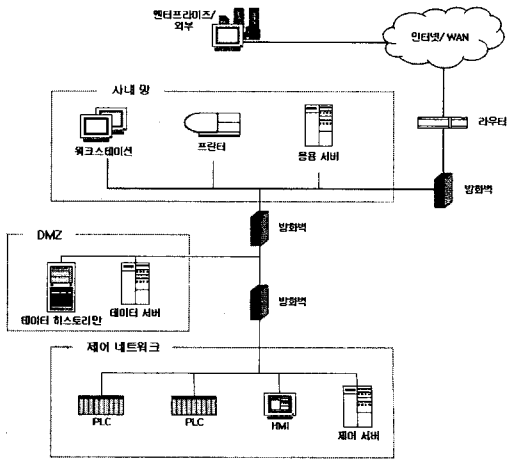
DMZ 내에 사내 망에서 접근할 수 있는 컴포넌트를 설치함으로서, 사내 망에서 제어 네트워크로의 직접 통신이 필요 없게 되고, 각 경로는 DMZ안에서 효과적으로 끝난다. 대부분의 방화벽은 복수의 DMZ를 허용할 수 있으며, 어떤 유형의 트래픽이 존(zone) 사이에 전달될 수 있는지 명시할 수 있다. [그림 2]에서, 방화벽은 사내 망에서 제어 네트워크로 진입하는 임의의 패킷들을 차단할 수 있으며, 또한 제어 네트워크를 포함하여 다른 네트워크 존으로부터의 트래픽도 규제할 수 있다. 룰-셋을 잘 설계하면 제어 네트워크와 다른 네트워크 사이에 확실한 분리를 유지할 수 있으며, 사내 망과 제어 네트워크 사이에 직접 통과하는 트래픽이 거의 없거나 전혀 없게 된다.

만약 패치 관리 서버, 앤티 바이러스 서버 혹은 다른 보안 서버가 제어 네트워크를 위하여 사용되어야 한다면, DMZ 상에 직접 위치하여야 한다.

이 형태의 구조에서 주 보안 위험은 DMZ 내의 컴퓨터가 침해된다면, DMZ에서 제어 네트워크로 허용되는 애플리케이션 트래픽을 통하여 제어 네트워크에 대한 공격을 개시하기 위하여 사용될 수 있다는 것이다. 이런 위협을 최대한 감소시키기 위하여 DMZ 내의 서버를 강화하고 능동적인 패치를 수행하며, 제어 네트워크와 DMZ 사이에서 단지 제어 네트워크 장치에 의하여 개시되는 연결에 대해서만 허용하는 방화벽 룰 셋을 적용해야 한다. 이 구조에 대한 다른 우려는 추가된 복잡성과 여러 개의 포트를 가진 방화벽의 잠재적인 증가된 비용이다.

3.4 사내 망과 제어네트워크 사이 방화벽 쌍

[그림 2]의 변형된 형태는 [그림 3]에서 보여주는 것처럼, 사내 망과 ICS 네트워크 사이에 한 쌍의 방화벽을 설치하는 것이다. 데이터 서버와 같은 공통 서버는 MES(Manufacturing Execution System) 계층이라고 하는 DMZ-같은 네트워크 존 내의 방화벽 사이에 위치한다. 첫 번째 방화벽은 제어 네트워크나 공유 데이터 서버로 향하는 임의의 패킷들을 차단하고, 두 번째 방화벽은 침해된 서버로부터의 원하지 않는 트래픽이 제어 네트워크로 진입하는 것을 막아주고, 제어 네트워크 트



〔그림 3〕 사내 망과 제어 네트워크 사이의 방화벽 쌍

래픽이 공유 서버에 영향을 미치는 것을 방지할 수 있다. [그림 3]은 사내 망과 제어 네트워크 사이에 설치된 방화벽 쌍을 보여준다.

두 개의 다른 제조사로부터의 방화벽이 사용되는 경우 장점이 있다. 만약 어떤 조직에서 제어 그룹과 IT 그룹이 자신의 방화벽을 관리할 책임을 가진다면, 이 구조는 분명하게 분리된 장비 책임성을 가지도록 한다. 주요 단점은 비용 증가와 관리의 복잡성이다. 엄격한 보안 요구사항이나 분명한 관리 분리가 필요한 환경에 대하여, 이 구조는 몇 몇 강한 장점을 가진다.

Ⅳ. 심층-방어 보안 구조

4.1 보안 특성과 공격 방법론

단 하나의 보안 제품, 기술이나 솔루션으로 ICS를 적절히 보호할 수 는 없다. 심층-방어(defense-in-depth) 기법은 두 개 이상의 다른 중복된 보안 메커니즘을 포함하는 복수 계층 전략을 의미하며, 어느 한 메커니즘에서의 실패의 영향이 최소화되기 때문에 바람직한 구조이다. 심층-방어 구조 전략은 방화벽의 사용, DMZ의 생성, 효과적인 보안 정책을 갖춘 침입탐지 능력, 훈련 프로그램과 사고 대응 메커니즘을 포함한다. 게다가, 효과적인 심층-방어 전략은 다음과 같은 ICS에 대한 가능한 공격 벡터의 철저한 이해를 요구한다.

- 네트워크 페리미터 내의 백도어와 허점: 제어 시스템은 충분한 보안 분석 없이 설치되는 경우가 많기 때문에, 백도어가 우연히 생성될 수 있다. 특히 네트워크 페리미터가 가장 중요하며 공격자가 이용할 수 있는 보안 취약성을 가질 수 있다. 무선 통신도 공격자에 의하여 SSID(Service Set Identifier) 브로드캐스팅, 제한된 접근 제어, 암호화 부족 및 제한된 네트워크 분할 등이 이용될 수 있다. 제어 시스템의 원격 제어 능력이 제어 데이터의 차단, 수정, 재주입 공격 등을 유발할 수 있다.
- 공통 프로토콜에서의 취약성: 제어 시스템에서 많이 사용되고 있는 공통 프로토콜인 OLE(Object Link and Embedding), DCOM(Distributed Component Object Model), RPC(Remote Procedure Call) 및 OPC(OLE for Process Control)와 같은 실시간 데이터 통신 표준들의 취약성들이 공격자에 의하여 이용될 수 있다. 또한 전통적으로 고립된 제어 네트워크와 비즈니스 환경과의 융합이 공격자에게 새로운 환경을 제공하고 있다.

제어 시스템을 위한 보안 패치의 설치도 기존 IT 시스템과는 다르다. 제어 시스템 동작에 어떤 영향을 미치는지 사전에 엄격한 시험이 이루어져야 한다. 실제로 패치의 설치로 생산 설비가 완전히 중단된 사건이 여러 건 보고된 바 있다.

- 필드 장치에 대한 공격: 필드 장치에 대한 접근을 통하여, 공격자가 센서 네트워크와 제어 시스템 네트워크로 진입할 수 있다.
- 데이터베이스 공격: 기존 IT 시스템의 데이터베이스에 대한 SQL 주입 공격이 제어 시스템에 발생한다면, 훨씬 더 큰 영향을 미칠 수 있으며, 제어 시스템 보안에 주요한 위협이 될 수 있다.
- 통신 하이재킹(hijacking)과 중간자(man-in-the-middle) 공격: 제어 시스템은 통상적으로 신뢰(trust)를 가정하며, 따라서 장치들 사이의 데이터 흐름에서 보안이 취약하다. 이 경우 아래와 같은 주요 보안 문제가 존재한다:

- 네트워크 상의 데이터를 공격자가 재 경로배정 할 수 있는 능력
- 평문 형식으로 된 중요 트래픽 포획 및 분석 능력
- 제어 통신에 대한 통제권을 얻기 위한 프로토콜 역공학 능력

이런 공격을 결합하여 공격자는 중간자 공격을 실행하게 되고, 네트워크 상의 데이터에 대한 제어권을 얻을 수 있다.

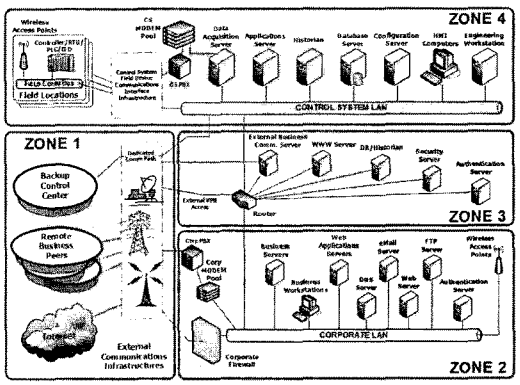
4.2 심층-방어 전략

[그림 4]는 zone으로 구분된 보편적인 제어시스템의 구조를 보여준다. 이 zone들은 다음과 같이 구분되어 있다:

- Zone 1: 인터넷, 피어 위치 및 백업 설비에 대한 외부 연결
- Zone 2: 사내 통신용 외부 연결
- Zone 3: 외부 서비스로부터의 제어 시스템 통신
- Zone 4: 프로세스-기반 혹은 SCADA 제어 시스템 운영

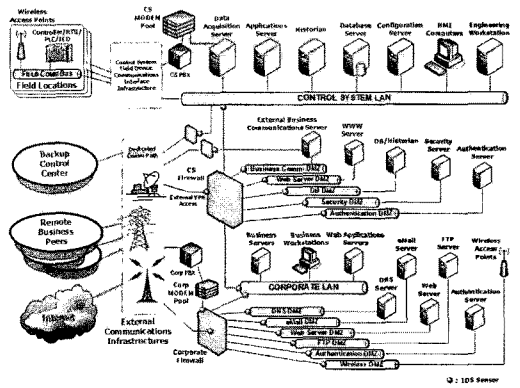
위의 존들은 각기 유일한 보안 요구사항을 가진다.

만약 제어 시스템 운영 존이 침해된다면, 제어 시스템 정보 자원의 조작은 치명적일 수 있다. 많은 부문에서 제어 시스템에 대한 악성 공격은 실제적인 결과를 초래한다.



〔그림 4〕 통상적인 구조에서의 존[3]

[그림 5]는 Control Systems Cyber Security: Defense in Depth Strategies 문서에 기술된 바와 같이 미국 국토안보부(DHS: Department of Homeland Security) CSSP(Control Systems Security Program) 권고 실제 위원회에 의하여 개발된 ICS 심층-방어 구조 전략을 보여준다.



〔그림 5〕 CSSP 권고 심층-방어 구조[3]

Control Systems Cyber Security: Defense in Depth Strategies 문서는 multi-tier 정보 구조를 유지하면서 제어 시스템 네트워크를 사용하는 조직을 위한 심층-방어 구조 전략을 개발하기 위한 지침 및 방향을 제공한다. 이 전략은 방화벽, DMZ의 사용과 ICS 구조 전체에 침입탐지 능력의 사용을 포함한다. 그림에서 여러 DMZ의 사용은 별도의 기능성에 대한 부가된 능력과 액세스 특권을 제공하고, 다른 운영 의무사항을 가진 네트워크들로 이루어진 대규모 구조를 보호하는데 매우 효과적인 것으로 증명되었다. 침입 탐지 설치는 다른 룰셋과 감시되는 각 도메인에 유일한 시그니처가 적용된다.

4.3 주요 보안 대책

제어 시스템 환경의 정보보호를 위하여 사용할 수 있는 다섯 가지의 보안 대책은 다음과 같다:

- 보안 정책: 제어 시스템 네트워크와 개별 컴포넌트를 위한 보안 정책을 개발해야 하며, 현재 위협 환경, 시스템 기능성 및 보안 요구 수준을 반영하도록 주기적으로 검토되어야 한다.
- 자원과 서비스에 대한 접근 차단: 네트워크 상에 방화벽이나 프락시 서버와 같은, 접근 제어 목록을 가진 페리미터 장치의 사용을 통하여 보통 채택된다. 호스트-기반 방화벽과 앤티-바이러스 소프트웨어를 통하여 호스트 상에서도 실행될 수 있다.
- 악성 행위 탐지: 네트워크 혹은 호스트 기반 탐지 행위는 로그 파일의 정기적인 감시를 필요로 한다. 침입탐지시스템이 네트워크 혹은 개별 호스트에 사용될 수 있다.
- 공격 가능성 완화: 취약성이 이용될 수 없도록, 필터 설정, 특정 구성(배열)을 가진 서비스와 응용의 운영 등을 통하여 취약성에 대한 접근을 통제할 수 있어야 한다.
- 핵심 문제 해결: 취약적인 응용의 제거, 소프트웨어 취약성 갱신 및 패칭과 같은 핵심 보안 문제를 해결해야 한다. 소프트웨어 허점이 있는 곳에는 관리자가 적용할 수 있도록 공급자나 개발자에 의하여 완화 기법이 제공되어야 한다.

V. 맺음말

심층-방어 보안 구조가 설치된 후, 방화벽을 통하여 어떤 트래픽을 통과시킬지는 정책을 통하여 결정되어야 한다. ISA(The Instrumentation, Systems, and Automation Society) 99의 기술보고서 부록 A에 의하면, 아래와 같은 일반적인 기준을 제시하고 있다:

- 제어 시스템에 대한 내향 트래픽은 차단되어야 한다. 제어 시스템 내부 장치 접근은 DMZ를 반드시 통과해야 한다.
- 제어 네트워크 방화벽을 통한 외향 트래픽은 긴요한 통신에 대해서만 제한되어야 한다.
- 제어 네트워크로부터 사내 망으로의 모든 외향 트래픽은 서비스와 포트에 의하여 소스(근원지)와 목적지-제한적이어야 한다.

또한 DNS(Domain Name System), HTTP(Hyper Transfer Protocol), FTP(File Transfer Protocol), SMTP(Simple Mail Transfer Protocol), SNMP(Simple Network Management Protocol), SCADA와 같은 특정 서비스에 대하여도 방화벽 규칙이 설정되어야 한다.

기존의 IT 시스템은 "data를 처리하기 위하여 physics"를 이용하는 반면에, 산업제어시스템은 "physics를 처리하기 위하여 data"를 이용하는 근본적인 차이가 존재한다. 그러므로 기존 IT 시스템을 위한 보안 기술이 산업제어시스템의 보안을 위한 필요 메커니즘이 될 수는 있지만, 산업제어시스템의 심층-방어를 위하여 충분하지 않을 수 있다. 따라서 산업제어시스템의 보안 특성에 대한 충분한 이해를 바탕으로 국가 주요 정보 하부구조를 구성하고 있는 산업제어시스템 정보보호 기술 개발 및 구현에도 관심을 기울어야 할 것으로 생각된다.

참고문헌

[1] Alvaro A. Cardenas et al., "Research Challenges for the Security of Control Systems", Proceedings of the 3rd conference on Hot topics in Security, 2008.

[2] Arvid Kjell, *Guide to Increased Security in Process Control Systems for Critical Societal Functions*, The Swedish forum for information sharing concerning information security-SCADA and Process control systems(FIDI-SC), Swedish Emergency Management Agency, Oct. 2008.

[3] Homeland Security, Control Systems Security Center, *Control Systems Cyber Security: Defense in Depth Strategies,* May 2006.

[4] ISA 99, Security for Industrial Automation and Control Systems, 2009.

[5] NIST(National Institute of Standards and Technology), U.S. Department of Commerce, Special Pub. 800-82, Final Public Draft, *Guide to Industrial Control Systems (ICS) Security,* Sep. 2008.

[6] Testimony of Joseph M. Weiss, *Control Systems Cyber Security-The Current Status of Cyber Security of Critical Infrastructures,* before the Committee on Commerce, Science, and Transmission, U.S. Senate, March 19, 2009,

[7] 전용희, "산업제어시스템 정보보호: 개요", 정보보호학회지 제 19권 제 5호, 한국정보보호학회, 2009년 10월.

〈著者紹介〉

전 용 희 (Yong-Hee Jeon)
종신회원

1971년 3월~1978년 2월: 고려대학교 전기전자전파공학부, 학사
1985년 8월~1987년 8월: 미국 플로리다 공대 대학원 컴퓨터공학과
1987년 8월~1992년 12월: 미국 노스캐롤라이나주립 대학원 Elec. and Comp. Eng. 석사, 박사
1978년 1월~1978년 11월: 삼성중공업(주)
1978년 11월~1985년 7월: 한국전력기술(주)
1979년 6월~1980년 6월: 벨기에 벨가톰사 연수
1989년 1월~1989년 6월: 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA
1989년 7월~1992년 9월: 미국 노스캐롤라이나주립대 부설 CCSP (Center For Comm. & Signal Processing) RA
1992년 10월~1994년 2월: 한국전자통신연구원 광대역통신망연구부 선임연구원
1994년 3월~현재: 대구가톨릭대학교 컴퓨터 · 정보통신공학부 교수
2001년 3월~2003년 2월: 대구가톨릭대학교 공과대학장
2004년 2월~2005년 2월: 한국전자통신연구원 정보보호연구단 초빙연구원
2007년 1월~2007년 12월: 한국정보보호학회 학회지 편집위원장
2008년 1월~현재: 한국정보보호학회 부회장
2009년 1월~현재: 한국정보과학회 정보보호연구회 위원장
<관심분야> 네트워크 보안, DDoS 탐지 및 대응 기술, 산업제어 시스템 정보보안, 통신망 성능분석