Regular paper http://dx.doi.org/10.13067/JKIECS.2014.9.1.137

산업제어시스템의 사이버보안을 위한 취약점 분석

김도연*

Vulnerability Analysis for Industrial Control System Cyber Security

Do-Yeon Kim*

요 약

산업제어시스템(Industrial Control System)은 전력, 가스, 수도, 하수, 오일 및 교통시스템과 같은 국가주요기반시설 및 산업분야에서 원거리에 산재된 시스템의 효과적인 원격모니터링 및 제어를 위해 필수적으로 사용되는 컴퓨터 기반의 시스템을 말한다. 고도로 발전된 IT 및 네트워크 관련 기술들이 산업제어시스템에 적용되어 효율성을 높이는 장점이 있지만, 일반적인 IT 환경에서의 각종 정보시스템이 가지는 사이버보안 취약성 및 사고의 가능성이 증대되는 단점을 가지게 되었다. 산업제어시스템에서 통상적으로 발견되는 취약점은 우선순위, 발생빈도 및 영향의 심각성들과는 무관하게 정책 및 절차, 플랫폼 및 네트워크 등으로 분류된다. 이러한 취약점들은 첫째, 패스워드의 강제 사용등과 같은 보안 정책 및 절차를 적용함으로서 취약점을 경감 시킬 수 있다. 둘째로, 운영체제 및 응용프로그램의 패치 적용, 물리적인 접근제어, 보안프로그램 사용등과 같은 다양한 보안통제를 적용함으로서 취약점을 경감 및 완화 시킬 수 있다. 셋째로, 심층방호개념의 네트워크 설계, 네트워크 통신의 암호화, 네트워크 트래픽 제한, 네트워크 장비에 대한 물리적 접근제어 방법 등과 같은 다양한 보안통제를 적용함으로서 취약점을 제거하거나 완화 시킬 수 있다.

ABSTRACT

Industrial control system (ICS) is a computer based system which are typically used in nation-wide critical infra-structure facilities such as electrical, gas, water, wastewater, oil and transportation. In addition, ICS is essentially used in industrial application domain to effectively monitor and control the remotely scattered systems. The highly developed information technology (IT) and related network techniques are continually adapted into domains of industrial control system. However, industrial control system is confronted significant side-effects, which ICS is exposed to prevalent cyber threats typically found in IT environments. Therefore, cyber security vulnerabilities and possibilities of cyber incidents are dramatically increased in industrial control system. The vulnerabilities that may be found in typical ICS are grouped into Policy and Procedure, Platform, and Network categories to assist in determining optimal mitigation strategies. The order of these vulnerabilities does not necessarily reflect any priority in terms of likelihood of occurrence or severity of impact. Firstly, corporate security policy can reduce vulnerabilities by mandating conduct such as password usage and maintenance or requirements for connecting modems to ICS. Secondly, platfom vulnerabilities can be mitigated through various security controls, such as OS and application patching, physical access control, and security software. Thirdly, network vulnerabilities can be eliminated or mitigated through various security controls, such as defense-in-depth network design, encrypting network communication, restricting network traffic flows, and providing physical access control for network components.

키워드

Industrial Control System, Cyber Security, Vulnerabilities Analysis
산업제어시스템, 사이버보안, 취약점분석

* 교신저자(corresponding author) : 순천대학교 컴퓨터공학과(dykim@sunchon.ac.kr)
접수일자 : 2013. 11. 11 심사(수정)일자 : 2013. 12. 16 게재확정일자 : 2014. 01. 13

I. 서 론

산업제어시스템(Industrial Control System)은 전력, 가스, 수도, 교통 등의 주요 국가주요기반시설 및 산업 분야에서 원거리에 산재된 시스템의 효과적인 원격모니터링 및 제어를 위해 필수적으로 사용되는 컴퓨터 기반의 시스템을 말한다.

주요 기반시설의 산업 제어시스템은 일반 IT시스템과 비교해 볼 때 폐쇄성, 자원의 특수성, 운용 가용성 등의 측면에서 차이점이 있다. 폐쇄성은 인터넷과 같은 외부 네트워크와 분리된 내부의 필드 장비들만 연결하는 폐쇄적인 네트워크를 사용하면서 독자적인 설비 시설에서 개별적으로 운영되는 특징이 있으며, 특수성은 산업 제어시스템의 사용 분야에 따라 독자적인 프로토콜 및 임베디드 운영체제가 사용되고 하드웨어 역시 독자적인 변형을 가지는 장비가 사용되며, 가용성은 전력, 수도, 가스, 교통 등 기반시설은 중단될 수 없는 특징을 가지고 365일 24시간 상시 작동할 수 있도록 운영되는 특징을 가진다 [1].

산업 제어시스템은 주요 기반시설로써 사이버 공격으로 인해 기능이 마비되면 국민의 생명, 생활, 재산, 국가 경제에 중대한 영향을 끼쳐 국가경제에 혼란 초래할 수 있다.

본 논문에서는 산업제어시스템의 사이버보안을 위한 취약점을 분석하고자 하며, 2장에서 산업제어시스템의 사이버침해 사례를 열거하고, 3장에서는 산업제어시스템의 구성요소 및 IT 정보시스템과의 비교되는 산업제어시스템의 특성에 대해 기술하며, 4장에서는 산업제어시스템의 일반적인 취약점을 나열하고 분석하여, 결론으로 필요한 해결방안 및 대책을 논하고자 한다.

II. 산업제어시스템 침해 사례

2.1 Stuxnet 침투 사고

스턱스넷은 SCADA 시스템 중 독일 지멘스(Siemens)사의 SIMATIC PCS7 시스템을 공격하도록 설계 되어 있다. PCS7의 다양한 컴포넌트 중 SIMATIC WinCC7와 SIMATIC Step7이라 불리는 통합 관리 도구를 공격 대상으로 삼고 있다. SIMATIC WinCC는 통제 및 모니터링 시스템으로서 PLCs(programmable logic controllers)와 통신을 담당하는 소프트웨어인데, 스턱스넷은 WinCC의 존재하는 취약점을 이용하여 침투하게 된다. 또 다른 컴포넌트인 Step7은 제어 PC와 산업자동화 제어시스템 간에 블록(동작명령)파일 교환을 담당한다. 스턱스넷은 Step7의 일부 구성 요소를 자신이 생성한 파일로 교체시켜 산업자동화 제어 시스템을 모니터링 하거나 임의의 블록(악성 명령어 블록)을 생성시켜 제어하게 된다. 이렇게 장악된 시스템은 공격자가 제어하게 된다. 이렇게 장악된 시스템은 공격자가 의도한 명령으로 동작하게 되는데, 현재 발견된 스턱스넷은 모든 PLC의 영향을 주진 않고, PLC 타입 6ES7-315-2와 6ES7-417만 감염의 영향을 받는 것으로 알려졌다 [2].

2.2 하수처리시스템 제어권 탈취사고

2000년 호주의 퀸즈랜드에서 발생한 사고로, 회사에 불만을 가진 전직 직원이 하수처리시스템의 제어권을 탈취하여 수백만 리터의 처리되지 않은 오/폐수를 인근 공원 및 강으로 방류한 사건으로 분류된다. 사고를 일으킨 전직 직원은 본인의 노트북에 회사의 소프트웨어를 설치하고, 회사의 통신망에 최소한 46번 이상 무단 침입하여 하수처리시스템의 제어권을 탈취하였다 [3].

2.3 CSX 기차신호시스템 사고

2003년 Sobig 컴퓨터바이러스가 미국 동해안의 기차신호시스템을 정지시키는 원인이 되었다. 플로리다 잭슨빌에 위치한 CSX사의 컴퓨터시스템의 바이러스감염으로 인해 신호 및 급전 등의 이상으로 기차운행중단 및 지연 등의 원인이 되었다[4].

2.4 Davis-Besse 원자력발전소 사고

2003년 SQL 슬래머 웜이 미국 오하이오에 위치한 Davis-Besse 원자력발전소의 감시계통 컴퓨터에 감염되어, 관련 설비의 작동이 5시간 이상 불능 상태로 유지되었으며, 여타 발전소 제어망 통신에도 영향을 미친 것으로 보고되었다 [5].

III. 산업제어시스템의 구성 및 특성

산업제어시스템은 전형적으로 전력, 상/하수, 오일 및 천연가스, 운송, 화학 및 제약, 제지, 음식료 및 분산 제조업(자동차, 우주산업, 내구재산업) 등에 사용되고 있다. 산업제어시스템은 SCADA(Supervisory Control and Data Acquisition) 시스템, DCS(Distributed Control System) 시스템, PLC(Programmable Logic Controllers) 기기 및 PCS(Process Control System) 시스템 등으로 구성된다.

3.1 산업제어시스템의 구성

SCADA 시스템은 중앙데이터 획득 및 감시 제어기능을 이용, 분산된 장치를 제어할 목적으로 사용된다. DCS는 감시 및 제어기능을 이용, 공장과 같은 근거리 지역 내의 생산/제조 시스템을 제어하기 위해 사용된다. PLC는 특정 응용을 위한 이산제어를 위해 사용되며 제어기능을 제공한다. PCS는 특정 프로세스의 출력을 제어하기 위한 구조, 메커니즘 및 알고리즘을 적용한 시스템으로, 통상적으로 PLC로 구현될 수 있으며, 복잡한 시스템은 DCS나 SCADA 시스템 형태로 구현될 수 있다 [4].

3.2 산업제어시스템의 사이버보안 특성

초기의 산업제어시스템은 릴레이, 카운터 및 타이머 등과 같은 소자들을 배치하며 하드웨어 형태의 서킷보드를 직접 제작하여 구현되었다. 이러한 형태의 제어기들은 집적회로 및 마이크로프로세서의 등장으로 프로그램이 가능한 PLC 제어기 형태로 발전하게 된다. 또한, 가속화된 IT 및 네트워크 관련 기술들을 산업제어시스템에 적용하는 단계로 발전하게 되었으나, 일반적인 IT 환경에서의 각종 정보시스템이 가지는 사이버보안 취약성 및 사고의 가능성이 증대되는 단점을 가지게 되었다. 하지만 산업제어시스템이 가지는 사이버보안 특성은 기존의 IT 산업의 정보시스템이 가지는 보안 특성과는 차이점을 가지고 있다.

산업제어시스템이 연결성 및 원격 접근성을 증진시키기 위하여, IT 관련 기술을 점진적으로 수용하고 있고, IT 정보시스템과 산업제어시스템과의 통합이 증가하고 있지만, 표 1에서 보여 지는 것과 같이 사이버보안 특성의 많은 차이점을 가지고 있다 [6].

표 1. 정보와 산업제어시스템의 보안 특성 비교 [6]
Table 1. Security comparison Between IT and ICS [6]

Security Characteristics	Information System	Industrial Control System
Anti-Virus/ Mobile Code	commonly, wide-spread usages	uncommon, difficult to install
Life of Support Technology	2-3 years various supplier	maximum 20years single supplier
Outsourcing	commonly, wide-spread usages	restricted on operation
Applied Patch	periodic / planning	non-periodic / no planning
Configuration Management	periodic / planning	planning / managed
Time Sensitivity	allowed delay	not allowed delay
Availability	allowed delay	continuously
Security Awareness	medium range of awareness	worst except physical protection
Security Testing/Audit	part of security program	irregular testing
Physical Protection	secure	remote/ secure

Ⅳ. 산업제어시스템 취약점 분석

정부 및 기업체에서 일반적으로 사용하는 정보시스템의 사이버보안 통제를 위해서는 미국 국립표준기술연구소에서 발간한 SP800-53을 준용하고 있다. NIST SP800-53은 연방정부 행정기관을 지원하는 정보시스템에 대한 보안평가를 선택 및 지정할 수 있는 지침 제공을 목적으로 하는 권고안이다. 권고안의 대상으로는 정보시스템 및 정보보안 관리 및 감독 책임이 있는 개인, 정보시스템 개발 책임이 있는 개인, 정보보안 실행 및 운영 책임이 있는 개인, 정보시스템 및 정보보안 평가 및 감독책임이 있는 개인을 대상으로 한다 [7]. 반면에, 일반적인 정보시스템의 보안과는 달리 산업제어시스템에 대한 보안 사항은 NIST SP800-82에서 다루어지고 있다 [8].

산업제어시스템에서 통상적으로 발견되는 취약점은 우선순위, 발생빈도 및 영향의 심각성들과는 무관하게

정책 및 절차, 플랫폼 및 네트워크 등으로 분류할 수 있다 [8].

4.1 정책 및 절차의 취약성

산업제어시스템에서의 통상적인 취약점들은 정책 및 절차를 포함하는 문서들의 부재 또는 불완전성 및 부적절성 으로 인해 기인된다.

정책 및 절차와 관련된 취약점은 다음과 같다.

- ICS에 대한 부적절한 보안정책
- 공식적인 보안교육 및 인지프로그램의 부재
- 부적절한 보안구조 및 설계
- 설정된 ICS 보안정책에 근거한 보안절차의 부재 또는 비구체화
- ICS 장비 구현을 위한 지침서의 부재 및 결함
- 보안 실행을 위한 행정절차의 부족
- ICS에 대한 보안감사의 부재 또는 부족
- ICS의 재난극복계획 및 구체화된 연속운전계획의 부재
- ICS에 특화된 구성변화관리 프로그램의 부족

4.2 플랫폼의 취약성

산업제어시스템의 취약점들은 하드웨어, 운영체제 및 ICS 응용을 포함하는 플랫폼의 결함, 잘못된 환경설정 및 빈약한 유지보수들로 인해 기인한다.

플랫폼 구성과 관련된 취약점은 다음과 같다.

- 보안취약점이 발견된 이후에도 운영체제 및 벤더 소프트웨어의 패치가 개발되지 않음
- 운영체제 및 응용프로그램의 패치가 유지되지 않음
- 철저한 시험 없이 운영체제 및 응용프로그램의 패치가 구현됨
- 기본 구성을 사용함
- 필수적인 구성이 저장되지 않거나 백업되지 않음
- 휴대용 장치의 보호되지 않은 데이터
- 적절한 패스워드 정책의 부족
- 패스워드를 사용하지 않음
- 패스워드 노출
- 패스워드 추측
- 부적절한 접근제어 방법 적용

플랫폼 하드웨어와 관련된 취약점은 다음과 같다.

- 변화된 보안에 대한 부적절한 시험
- 필수시스템에 대한 부적절한 물리적인 방어
- 장비의 물리적인 접근이 비인가자에 허용
- ICS 장비에 대한 보안되지 않은 원격 접근
- 네트워크 연결을 위한 이중의 네트워크 어댑터 사용
- 문서화 되지 않은 자산
- 무선주파수 및 전자기 펄스의 간섭
- 비상전원의 부족
- 환경 통제의 부재
- 필수적인 장비의 중복성 부족

플랫폼 소프트웨어와 관련된 취약점은 다음과 같다.

- 버퍼 오버플로우
- 설치됐지만 실행시키지 않은 보안 기능
- 서비스 거부
- 정의되지 않거나, 적절히 정의되지 않은 상태에서의 부주위한 취급
- RPC 및 DCOM의 의존적인 OPC 사용
- ICS에서 광범위하게 사용되지만 보안되지 않은 프로토콜의 사용
- 평문의 사용
- 필요하지 않은 서비스의 실행
- 컨퍼런스 또는 잡지에 소개된 소프트웨어의 사용
- 소프트웨어 개발 및 형상관리에 부적절한 인증 및 접근제어 사용
- 침입탐지 또는 차단시스템의 미설치
- 로그를 유지하지 않는 경우
- 사건을 탐지하지 못하는 경우

플랫폼 멀웨어 방어와 관련된 취약점은 다음과 같다.

- 멀웨어 방어 소프트웨어의 미설치
- 최신의 멀웨어 방어 소프트웨어 또는 정의파일을 사용하지 않는 경우
- 철저한 시험 없이 구현된 멀웨어 방어 소프트웨어 사용

4.3 네트워크의 취약성

산업제어시스템의 취약점들은 ICS 네트워크의 결함, 잘못된 환경설정 및 빈약한 관리들로 인해 기인한다.

네트워크 구성과 관련된 취약점은 다음과 같다.

- 네트워크의 보안구조가 빈약한 경우
- 데이터 흐름제어를 적용하지 않은 경우
- 빈약하게 구성된 보안장비의 사용

- 네트워크 장비의 구성 파일을 저장 및 백업하지 않은 경우
- 암호화하지 않은 패스워드 전송
- 네트워크 장비에 계속 존재하는 패스워드
- 부적절한 접근제어를 적용한 경우

네트워크 하드웨어와 관련된 취약점은 다음과 같다.
- 네트워크 장비에 대한 부적절한 물리적 방호
- 안전하지 않은 물리적 포트의 사용
- 환경 통제의 부재
- 필수적이지 않은 인원들이 네트워크 연결 및 장비에 접근하는 경우
- 필수적인 네트워크의 중복성 부족

네트워크 경계와 관련된 취약점은 다음과 같다.
- 보안 경계가 정의되지 않은 경우
- 방화벽이 설치되지 않았거나 부적절하게 구성된 경우
- 제어네트워크에서 비 제어 트래픽을 사용한 경우
- 제어네트워크가 아닌 영역에서 제어네트워크 서비스를 사용한 경우

네트워크 감시 및 로깅과 관련된 취약점은 다음과 같다.
- 방화벽 및 라우터의 부적절한 로그
- ICS 네트워크상에서 보안감시를 하지 않는 경우

통신과 관련된 취약점은 다음과 같다.
- 필수적인 감시 및 제어 경로가 정의되지 않은 경우
- 표준화 및 문서화된 통신프로토콜 적용 시 평문을 사용하는 경우
- 사용자, 데이터 및 장비의 인증에 열악한 방법을 사용하는 경우
- 통신 시 무결성 확인이 부족한 경우

무선 연결과 관련된 취약점은 다음과 같다.
- 클라이언트와 AP 간의 부적절한 인증 방법을 사용하는 경우
- 클라이언트와 AP 간의 부적절한 데이터 방어 방법을 사용하는 경우

V. 결 론

산업제어시스템(Industrial Control System)은 전력, 가스, 수도, 교통 등의 주요 국가주요기반시설 및 산업분야에서 원거리에 산재된 시스템의 효과적인 원격모니터링 및 제어를 위해 필수적으로 사용되는 컴퓨터 기반의 시스템을 말한다.

고도로 발전된 IT 및 네트워크 관련 기술들이 산업제어시스템에 적용되고 있지만, 일반적인 IT 환경에서의 각종 정보시스템이 가지는 사이버보안 위협[9-11], 보안취약성 및 사고의 가능성이 증대되는 단점을 가지게 되었다.

산업제어시스템에서 통상적으로 발견되는 취약점은 우선순위, 발생빈도 및 영향의 심각성들과는 무관하게 정책 및 절차, 플랫폼 및 네트워크 등으로 분류된다. 이러한 취약점들은 첫째, 패스워드의 강제 사용등과 같은 보안 정책 및 절차를 적용함으로서 취약점을 경감 시킬 수 있다. 둘째로, 운영체제 및 응용프로그램의 패치 적용, 물리적인 접근제어, 보안프로그램 사용등과 같은 다양한 보안통제를 적용함으로서 취약점을 경감 및 완화 시킬 수 있다. 셋째로, 심층방호개념의 네트워크 설계, 네트워크 통신의 암호화, 네트워크 트래픽 제한, 네트워크 장비에 대한 물리적 접근제어 방법 등과 같은 다양한 보안통제를 적용함으로서 취약점을 제거하거나 완화 시킬 수 있다.

참고 문헌

[1] Y.-T. Cha, B.-H. Cho, and J.-C. Na, "Security Technology Trends and Prospective of Industrial Control System,". *KEIT PD Issue Report*, vol. 13-6, 2013, pp. 79-100.

[2] N. Falliere, L. O. Murchu, and E. Chien, "Win32.stuxnet Dossier," *Symantec Security Response*, 2011.

[3] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA Security in the light of Cyber- Warfare," *Computer & Security*, 2012, pp. 418-436.

[4] Y.-H. Chen, "Introduction of Information Security for Industrial Control System," ***Korea Institute of Information Security and Cryptology,*** vol. 19, no. 5, 2009, pp. 52-59.

[5] NRC Information Notice 2003-14, "Potential

Vulnerability of Plant Computer Network to Worm Infection," *Nuclear Regulatory Commission,* 2003.
[6] Y.-H. Chen, "Network Design and Architecture for ICS Security", *Korea Institute of Information Security and Cryptology,* vol. 19, no. 5 2009, pp. 60-67.
[7] NIST SP800-53, "Recommended Security Controls for Federal Information System," *National Institute of Standards and Technology,* 2009.
[8] NIST SP800-82, "Guide to Industrial Control System Security," *National Institute of Standards and Technology,* 2011.
[9] W.-S. Seo and M.-S. Jun, "A Direction of Convergence and Security of Smart Grid and Information Communication Network," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 5, no. 5, 2010, pp. 477-486.
[10] I.-S. Koo, K.-W. Kim, S.-B. Hong, G.-O. Park, and J.-Y. Park, "Digital Asset Analysis Methodology against Cyber Threat to I&C System in NPP," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 6, no. 6, 2011, pp. 839-847.
[11] C.-H. Yoon, G.-J. Kim, and C.-S. Jang, "Embedded-based Power Monitoring Security Module Design," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 8, no. 10, 2013, pp. 1485-1490.

저자 소개

김도연(Do-Yeon Kim)

1986년 충남대학교 계산통계학과 졸업(이학사)
2000년 충남대학교 대학원 정보통신공학과 졸업(공학석사)
2003년 충남대학교 대학원 컴퓨터공학과 졸업(공학박사)
1986년~1996 한국원자력연구원 선임연구원
1997년~2008 한국전력기술(주) 책임연구원
2008년~현재 순천대학교 컴퓨터공학과 교수
※ 관심분야 : 영상보안, 산업제어시스템보안