논문 18-43-03-13 The Journal of Korean Institute of Communications and Information Sciences '18-03 Vol.43 No.03
https://doi.org/10.7840/kics.2018.43.3.572

기반시설 보안위협 분류 및 분석

이 경 률◆, 이 선 영*, 임 강 빈°

Classification and Analysis of Security Threats in the Infrastructure

Kyungroul Lee◆, Sun-Young Lee*, Kangbin Yim°

요 약

기반시설의 규제가 법제화되고 강화되면서 이를 만족하기 위한 대응체계의 개발 및 인허가에 대한 대응이 시급한 실정이다. 따라서 본 논문에서는 기반시설에서의 대응체계 구축을 위하여 발생 가능한 보안위협을 조사하고, 이를 그 특징에 따라 분류하며, 위협을 유발할 수 있는 취약점에 대하여 분석하였다. 분류한 보안위협은 크게 오프라인 위협과 온라인 위협으로 분류되며, 위협이 발생하는 보안 취약점은 정책 및 절차에 의한 취약점, 플랫폼 설정 취약점, 악성코드 취약점, 소프트웨어 취약점, 네트워크 취약점으로 분류된다. 본 연구결과를 통하여 기반시설에서 발생 가능한 위협에 대응하기 위한 지침서 및 평가서로 활용이 가능할 것으로 사료된다.

Key Words : infrastructure, security threats, vulnerability, attack example, security analysis

ABSTRACT

As the regulation of infrastructure is legislated and strengthened, development of security system is urgent. Therefore, we survey possible security threats to build up a security system in infrastructure, and the threats are classified according to their characteristics. Moreover, we also analyze vulnerabilities that can cause threats. Classified and analyzed results are expected to serve the guideline and evaluation to counteract possible threats in the infrastructure.

Ⅰ. 서 론

최근 2014년 12월, 원전 해커집단에 의한 사이버위협으로 원전 안전에 대한 국민적인 불안감이 증폭되기 시작하면서, 원전 사이버보안이 이슈화되었고, 이에 따라, 2013년 12월 24일, 원자력 시설 등의 방호 및 방사능 방재대책법[1]과 같이 기반시설의 규제가 법제화되고 강화되면서 이를 만족하기 위한 대응체계의 개발 및 인허가에 대한 대응이 시급한 실정이다. 법제화되고 강화된 원전 사이버 보안 규제를 살펴보면, 한국원자력통제기술원 (KINAC, the Korea Institute of Nuclear nonproliferation And Control)의 기술기준서 RS-015 (원자력시설등의 컴퓨터 및 정보시스템 보안 기술기준)에서 2018년 10월까지 가동원전의 사이버보

※ 본 연구는 한국연구재단 이공분야기초연구사업(No. NRF-2015R1D1A1A01057300), 순천향대학교 학술연구비 지원 및 순천향대학교 산학협력단 관리로 수행되었습니다.

◆ First Author : (ORCID:0000-0003-1477-7569)Soonchunhyang University R&BD Center for Security and Safety Industries (SSI), carpedm@sch.ac.kr, 정회원

° Corresponding Author : (ORCID:0000-0002-1361-1455)Soonchunhyang University Department of Information Security Engineering, yim@schac.kr, 정회원

* (ORCID:0000-0002-4686-9436)Soonchunhyang University Department of Information Security Engineering, sunlee@sch.ac.kr, 정회원

논문번호 : KICS2017-11-333, Received November 13, 2017; Revised January 31, 2018; Accepted March 15, 2018

안 대응체계 구축[2]을 요구하였으며, 한국원자력안전기술원 (KINS, Korea Institute of Nuclear Safety)의 규제지침 8.13 (안전계통의 디지털 컴퓨터 사용)에서 보안기술로 인하여 고유 안전성을 저해하는 개발환경, 운영환경 측면의 규제를 의미하는 SDOE (Secure Development and Operational Environment) 측면의 사이버보안 설계 및 보안성 검증 요구[3], 산업부/국정원의 정보통신기반보호법에서 "주요 정보통신기반시설"로 지정된 원전의 주기적 취약점 분석 수행 및 보호대책 요구[4] 등이 개정되어 시행되었다. 따라서 본 논문에서는 상기와 같이 기반시설에서의 대응체계 구축을 위하여 발생 가능한 보안위협을 조사하고, 이를 그 특징에 따라 분류하며, 위협을 유발할 수 있는 취약점에 대하여 분석하였다. 이를 자세히 설명하면, 기반시설에서의 대응체계 구축을 위하여 발생 가능한 보안위협을 조사하고, 이를 그 특징에 따라 크게 오프라인 위협과 온라인 위협으로 분류하며, 위협을 유발할 수 있는 취약점을 분석하여 정책 및 절차에 의한 취약점, 플랫폼 설정 취약점, 악성코드 취약점, 소프트웨어 취약점, 네트워크 취약점으로 분류하고 각 취약점을 상세히 분석한다. 본 논문의 구성은 다음과 같다. 제2장에서는 기존에 발생하였던 기반시설에서의 공격사례를 서술하고, 제3장에서는 기반시설에서 발생 가능한 보안위협, 제4장에서는 기반시설에서의 보안 취약점을 서술하며, 제5장에서 결론을 맺는다.

Ⅱ. 기반시설에서의 공격사례

원전 사이버보안 규제 법제화 및 강화의 원인 중 하나는 악성코드에 의하여 원전과 같은 기반시설의 특정 시스템이 장악되는 문제가 발생할 가능성이 존재하기 때문이며, 실제로 2010년에 발생한 스턱스넷 (Stuxnet)의 지능형지속위협 (APT, Advanced Persistent Threat)으로 인하여 특정 시스템이 공격당한 사례가 존재한다. 이와 같이 원전 등의 기반시설이 내/외부로부터의 위협에 의하여 발생한 공격사례는 다음과 같다[5-15].

전 세계적으로 환경, 수력, 수자원, 수처리, 석유, 원자력, 전력, 교통, 제조, 산업제어시스템 등의 기반시설에서 활용되는 제어 시스템 및 모듈이 내/외부로부터의 위협에 의한 공격사례가 존재하며, 이러한 공격사례는 바이러스, 원격 접속, 악성코드 감염, 내부관리자, 모의해킹 등으로 인하여 발생하였다. 상기 공격사례 중 대표적인 사례로는 슬래머 웜과 스턱스넷이 있다.

슬러머 웜은 2003년 미국 Davis-Besse 원전의 디지털 계측제어 시스템을 감염시켰으며, 이로 인하여 제어 시스템이 기능을 상실하는 사례가 발생되었다. 실제 상황은 기능이 상실된 제어 시스템이 정상적으로 운영되는 상태였지만, 전반적인 유지보수를 위하여 원자로가 정지된 상태이었으며, 실제로 안전성에 영향을 미치는 사례가 발생하지는 않았다. 슬래머 웜이 공격에 성공한 이유를 살펴보면, 원전 내부에서 마이크로소프트 윈도우즈 기반의 데이터베이스를 관리하기 위한 시스템인 SQL 서버 2000의 취약점으로 인하여 침입에 성공하였다. SQL 서버 2000은 1443/TCP 포트를 세션을 위한 목적으로 할당하며, 두 개 이상의 데이터베이스가 사용될 경우에는 해당 포트를 사용하지 못하는 특징이 있다. 이를 보완하기 위하여 클라이언트에서의 쿼리와 같은 요청이 각 SQL 서버에 올바르게 전달되도록 SQL 모니터 포트인 1434/UDP를 활용하였지만, 이러한 과정에서 취약점이 드러나게 되었다. 해당 포트로의 요청은 버퍼를 체크하지 않는 문제점이 존재하였으며, 공격자는 조작된 패킷을 해당 포트로 요청하여 메모리의 일부분을 덮어쓰는 버퍼오버플로우를 활용함으로써 서버의 권한을 획득하여 침입을 시도하였다. 공격 과정을 보다 자세히 살펴보면, 공격자는 ① 조작된 웜 패킷을 전송하여 1차 감염대상 SQL 서버의 1434 UDP 포트로 접속한 후, ② SQL 서버의 확인 서비스 취약점을 이용하여 버퍼오버플로우 공격을 시도하며, ③ 공격자의 악의적인 코드가 메모리에 삽입된 후, 자동으로 실행된다. 이를 통하여 1차 감염대상 SQL 서버의 침입에 성공하며, 슬래머 웜은 ④ 자신을 전파하기 위하여 SQL 서버의 확인 서비스에서 보안패치가 적용되지 않은 2차 감염대상 서버를 검색한 후, 침입을 시도한다. ⑤ 이러한 침입 시도는 IP 주소를 무작위로 생성하여 1~3의 과정을 자동으로 반복하며, ⑥ 새로운 공격대상의 IP 주소를 발견하면, 1434 UDP 포트로 접속을 시도한다. ⑦ UDP 포트에 정상적으로 연결되면, 버퍼오버플로우 공격을 시도하며, ⑧ 삽입된 악의적인 코드가 메모리에 로드되어 실행됨으로써 2차, 그리고 3차 감염대상 서버로 웜이 전파된다. 하지만 Davis-Besse 원전의 내부 네트워크는 방화벽을 통하여 외부로 연결되도록 구성되어 있었고, 방화벽을 통하여 1434 포트를 차단함으로써 외부로부터의 접근은 허가되지 않았다. 그럼에도 불구하고 이러한 공격이 가능하였던 이유는 방화벽 뒤에서 T1 연결을 통하여 원전의 서버에서 운영되던 응용소프트웨어를 제공하는 회사가 접속하는 것이 가능하기 때문에, 공격자는 해당 소프트웨어 공급사의 서버

를 슬래머 웜에 감염시킨 후, 방화벽 뒤에 연결된 T1 통신라인을 통하여 내부 네트워크로의 침입에 성공하였다. 이러한 공격과정을 통하여 안전과 관련된 변수를 운전원에게 지시하는 안전변수 지시계통 시스템 (SPDS, Safety Parameter Display System)과 모든 자료를 취득하고 저장하는 기능을 수행하는 발전소 컴퓨터 계통 시스템 (PCS, Plant Computer System)이 감염되어 6시간 정도 시스템이 정지되었다[16-19].

스텍스넷은 2009년에 최초로 발견되었으며, 2010년에는 이란 원자력발전소의 제어 시스템과 중국의 산업기반시설의 제어 시스템 등에 침투하여 시스템의 오동작을 발생시킨 악성코드이다. 주로 원자력발전소, 전력설비, SCADA, 철강, 댐 등과 같은 국가의 주요 산업제어 시스템에 침투한 후, 오동작을 유발시키는 명령코드를 입력함으로써 시스템을 마비시킨다. 시스템에 침투하기 위하여 USB 메모리 및 네트워크 공유 프린터 등의 취약점을 활용하며, 분리된 제어망 내의 시스템을 감염시키고 취약한 비밀번호를 가진 공유 네트워크로 자신을 복사하여 전파하는 특징이 있다. 특히, 침투한 시스템에서 자신이 탐지되지 않도록 은닉하는 기술인 루트킷 (rootkit) 기술을 활용하며, 공격을 위하여 특정 회사인 Siemens의 PLC가 engineering tool (Step-7)에 연결되었는지 확인한다. 이를 자세히 설명하면, Siemens 사의 PLC는 제어용 프로그램을 작성하기 위한 engineering tool과 원격 공정제어 감시를 위한 WinCC 프로그램을 제공하기 때문에, engineering tool을 통하여 PLC로의 공격을 시도한다. 따라서 engineering tool이 설치된 경우에는 해당 도구가 활용하는 라이브러리인 "s7otbxdx.dll" 파일의 이름을 변경하여 백업한 후, 변조된 악의적인 "s7otbxdx.dll" 파일로 변경하며, 이후 engineering tool이 실행될 때, 변조된 라이브러리가 로드되고 해당 라이브러리를 통하여 PC와 PLC 간의 블록 파일이 교환되므로 PLC를 감시하고 PLC와 연결된 모터, 펌프, 밸브, 컨베이어 벨트 등의 장비를 제어하는 것이 가능하였다[10,-12,16,18,20-22].

국내의 공격사례를 살펴보면, 제어 시스템에 대한 침해사고는 공식적으로 확인된 바가 없다. 하지만 지식경제 사이버안전센터에서 시행하였던 취약점 분석 및 평가 결과를 살펴보면, 제어서버 및 운전조작부 서버와 같은 윈도우즈 운영체제를 사용하는 일부 서버에서 바이러스의 감염흔적이 발견되었으며, 단위 기기를 제어하는 보조 제어서버에 악성코드가 침입하여 대량의 트래픽을 네트워크에 발생시키는 DoS 공격이 시도된 사례가 있다. 또한, 모의해킹 결과를 살펴보면, 인터넷에 유출된 기관 직원들의 개인정보와 업무정보를 활용하여 업무망까지 침투한 후, 업무망과 제어망 사이에 연결된 통로를 찾아 제어 시스템의 운전자 조작 콘솔 (HMI, Human Machine Interface) 장비에 대한 침투 가능성이 확인되었다[6].

Ⅲ. 기반시설에서의 보안위협

원전과 같은 기반시설의 경우에는 외부와 분리된 폐쇄적인 성격의 네트워크로 구성되어 타 시스템보다 비교적 안전한 실정이지만, 상기와 같이 기반시설에 대한 침해사고가 발생하게 되었고, 이러한 사고가 발생한 원인은 다음과 같은 보안위협이 존재하기 때문이다[16,23-25].

기반시설에서 발생하는 보안위협은 크게 오프라인 위협과 온라인 위협으로 분류된다. 오프라인 위협은 네트워크와 같이 외부 및 원격에서 접근하는 방식이 아닌, 장비 및 시스템에 직접적으로 접근함으로써 발생하는 위협이며, 자연재해에 의한 위협, 정전에 의한 위협, 물리적 위협, 조작 미숙에 의한 위협, 조작 실수에 의한 위협으로 분류된다. 자연재해에 의한 위협은 자연적인 수력, 풍력, 화력 등으로부터 발생하는 태풍, 호우, 화재 등에 의하여 시스템의 고장이 발생하거나 파괴됨으로써 운영이 중지되는 위협이다. 정전에 의한 위협은 자연재해, 혹은 악의적으로 전원의 공급을 차단하는 것과 같이 기반시설에 전력이 공급되지 못함으로써 발생하는 위협으로, 전력이 공급되지 못하여 데이터가 파괴되거나 실시간으로 처리되지 못하여 에러 및 지연이 발생하는 위협이다. 물리적 위협은 기반시설 및 장비에서의 물리적인 문제점으로 인하여 발생하는 위협으로, 전자장비가 오염되어 사용이 불가능하거나 전자기파로 인한 사용 불능, 시스템에서 활용하는 하드웨어에 고장이 발생하거나 파괴됨으로써 발생하는 위협, 그리고 내/외부자가 시스템과 관련된 하드웨어를 절도함으로써 발생하는 위협이 있다. 조작 미숙에 의한 위협은 기반시설을 담당하는 사람의 잘못된 조작으로 인하여 입력에 오류가 발생하는 위협이며, 조작 실수에 의한 위협은 기반시설을 담당하는 사람의 실수로 인하여 잘못된 정보를 입력하거나 잘못된 절차로 운영하면서 발생하는 위협이다. 온라인 위협은 크게 내부 위협과 외부 위협으로 분류되며, 내부 위협은 내부 관리자 및 협력업체 직원 등의 내부자에 의한 위협, 외부 위협은 사회공학적 기법에 의한 위협, 내부 탐색에 의한 위협, 위장에 의한 위협, 권한 획득에 의한 위협, 비인가 접근에 의한 위협, 데이터

유출에 의한 위협, 과부하 유발에 의한 위협, 시스템 결함에 의한 위협, 위/변조에 의한 위협, 악성코드에 의한 위협으로 분류된다. 내부자에 의한 위협은 기반시설의 권한을 가진 내부 관리자 및 협력업체 직원에 의하여 의도적으로 기밀정보를 유출하거나 시스템의 운영 중지 및 파괴하는 위협이며, 사회공학적 기법에 의한 위협은 악성코드가 포함된 스팸 메일 및 스피어 피싱 메일을 발송하여 시스템 내부에 침투하는 위협, 내부 탐색에 의한 위협은 미디어 탐색, 트래픽 분석, 도/감청 및 스니핑을 통하여 인증정보 및 기밀정보와 같은 침입에 필요한 정보를 수집하는 위협, 위장에 의한 위협은 공격자가 정상적인 기기 및 시스템으로 위장하여 전달되는 정보 및 침투에 필요한 정보를 수집하여 접근 우회 및 인증을 우회함으로써 발생하는 위협, 권한 획득에 의한 위협은 리소스 및 시스템에 권한이 없는 공격자가 권한을 획득하기 위하여 우회 제

표 1. 기반시설에서의 보안위협
Table 1. Security threats in the infrastructure

Category	Cause		Security threat
Offline	Natural disasters		• System outage and destruction
	Blackout		• Data destruction • Processing error • Processing delay
	Physical threat		• Pollution and threat to electronic equipment • Electromagnetic wave threat • Hardware destruction • Hardware failure • Theft
	Immature operation		• Input error
	Operation mistake		• Input mistake • Mistake and error in personnel and procedure to operate
Online	Inside	Insider threat	• Information leakage • System outage and destruction
	Outside	Social engineering attack	• Spam mail • Spear phishing
		Collecting internal information	• Media explorer • Traffic analysis • Eavesdropping and sniffing
		Camouflage	• Disguising as a normal device or a system
		Acquiring privilege	• Bypassing control • Exploiting privilege
		Unauthorized access	• Unauthorized manipulation
		Data leakage	• Password leakage • Hardware and software information leakage • Leakage of processing information • Leakage of asset information by external parties
		Overload induction	• DoS and DDoS • Attacks based on system throughput
		System fault	• Operating system vulnerability • Program vulnerability
		Falsification	• Unauthorized access and falsification
		Malicious code	• Spoofing attack • MITM (Man-In-The-Middle) attack • Trojan horse • Backdoor • Trapdoor • Replay attack

어 및 권한을 위조함으로써 악의적인 행위를 수행하는 위협, 비인가 접근에 의한 위협은 인가되지 않은 공격자가 시스템으로부터 인가받기 위하여 시스템에 대한 비인가 조작을 시도하는 위협, 데이터 유출에 의한 위협은 시스템의 접근 및 권한, 그리고 기밀정보와 관련된 비밀번호, 하드웨어 및 소프트웨어 정보, 공정 처리 정보, 자산정보가 외부자에 의하여 유출되는 위협, 과부하 유발에 의한 위협은 시스템의 구동을 방해할 목적으로 DoS 및 DDoS 공격, 시스템이 처리하는 능력을 넘어서는 운영을 시도하는 공격에 의한 위협, 시스템 결함에 의한 위협은 시스템을 구동하기 위하여 설치된 운영체제 및 프로그램에 존재하는 취약점

표 2. 기반시설에서의 보안 취약점
Table 2. Vulnerabilities in the infrastructure

Category	Vulnerability
Policy and procedure	Inappropriate cyber security policy and procedure
	Absence of systematic cyber security training and awareness education program
	Inadequate cyber security structure
	Insufficient cyber security requirement and implementation
	Absence of cyber security monitoring
	Using standardization technique having known vulnerability
	Absence of security document with policy and implementation guides
Platform configuration	Inadequate proactive response of cyber threat
	Absence or difficult of cyber security patch
	Absence of cyber security evaluation and test
	Absence of proper cryptography policy
	Inproper access control
	Improper remote access
	Unauthorized personnel having physical access privilege
	Technical and information attacks on known infrastructure
	Communication protocol vulnerability based on Modbus
	Erroneous configuration and error in hardware, operating system, and application
	Incorrect management of the platform
Malicious code	Absence of malicious protection software
	Unused malicious protection software
Software	Buffer overflow
	Unavailable default security features installed
	Denial of service attack
	Use of unsafe communication protocol
	Absence of intrusion detection/intrusion prevention software
	Usage restriction of existing security product
	Transmission of unauthenticated command and authentication data
Network	Data flow control
	Transmission of unencrypted data
	Inproper access control
	Absence or insufficient management of firewall at network edge
	Absence of network monitoring
	Insufficient integrity check of communication
	Insecure connection

에 의하여 발생하는 위협, 위/변조에 의한 위협은 인증과 관련된 정보를 위/변조하여 비인가된 공격자가 접근을 시도하거나 악의적인 시도를 위한 데이터를 변조하는 위협, 악성코드에 의한 위협은 시스템에 침투하기 위하여 스푸핑, 중간자 공격, 트로이 목마, 백도어, 트랩도어, 재생공격 등을 시도하는 위협이다.

상기 분류된 보안위협은 발생하는 원인에 따라 크게 사고에 의한 발생과 악의적인 공격에 의한 발생으로 분류된다. 사고에 의한 발생은 오프라인의 자연재해, 정전, 조작 미숙, 조작 실수와 같이 사고의 발생이 특정인에 의하여 의도적으로 발생하는 것이 아닌 사람에 의한 실수나 미숙한 조작, 정전 및 지진 등과 같은 자연재해로 인하여 발생하는 것을 의미한다. 이와는 반대로 악의적인 공격에 의한 발생은 특정인 및 특정 단체 등이 정보 유출부터 시스템 중지, 더 나아가 시스템을 파괴하기 위한 목적으로 내부 및 외부로부터의 공격에 의하여 발생하는 것을 의미한다.

Ⅳ. 기반시설에서의 보안 취약점

기반시설에서의 보안위협은 사람의 실수에 의하여 발생하는 사고도 있지만, 악의적인 공격에 의하여 발생하기도 하며, 이러한 공격은 기반시설에 존재하는 보안 취약점으로부터 기인한다. 보안 취약점은 크게 정책 및 절차에 의한 취약점, 플랫폼 설정 취약점, 악성코드 취약점, 소프트웨어 취약점, 네트워크 취약점으로 분류되며, 표 2와 같은 취약점을 가진다[5,6,10,16,26].

상기와 같은 취약점을 토대로 공격자가 기반시설에 침투하는 시나리오를 살펴보면, 다음과 같다. ① 공격자는 목표 대상의 시스템과 네트워크 구조를 분석한 후, 상기와 같은 취약점을 도출한다. ②이러한 취약점을 활용하여 기반시설 내부로 침투를 시도하며, 침투를 위하여 기반시설에서 제공하는 서비스인 FTP, Telnet, 제어 서비스 등을 대상으로 guest, anonymous 계정, 비밀번호가 없는 계정, 추측한 ID, 디폴트 계정 등을 이용하여 접근한다. ③시스템에 접근이 가능한 공격자는 권한을 탈취하기 위하여 버퍼오버플로우 공격 등을 시도하여 root 권한을 확보하며, ④권한을 확보한 공격자는 시스템 내부를 스캐닝하기 위하여 스니퍼를 설치하고 설치된 스니퍼를 통하여 네트워크로 전송되는 데이터를 감청하여 사용자의 아이디 및 비밀번호 등의 중요정보를 탈취한다. ⑤인증정보를 탈취한 공격자는 이후의 접근을 위하여 백도어 및 트로이 목마 등을 설치하며, 이를 통하여 관리자 권한으로 우회 접근을 시도하고 로그 기록을 삭제하거나 은폐를 위한 루트킷 등의 추가적인 프로그램을 설치한다. ⑥침입에 성공한 공격자는 실질적으로 악의적인 행위를 수행하며, 데이터 삭제, 위/변조, 데이터 유출 및 악성코드 등을 설치하며, ⑦침입의 흔적을 삭제하기 위하여 로그 기록을 삭제한다. ⑧더욱 심각하게는 시스템의 동작을 중지시키거나 파괴하는 공격을 수행한다[23].

Ⅴ. 결 론

본 논문에서는 기반시설에서의 대응체계 구축을 위하여 발생 가능한 보안위협을 조사하고, 이를 그 특징에 따라 분류하며, 위협을 유발할 수 있는 취약점에 대하여 분석하였다. 기반시설에서 발생하는 보안위협은 크게 오프라인 위협과 온라인 위협으로 분류되며, 기반시설에서의 보안 취약점은 크게 정책 및 절차에 의한 취약점, 플랫폼 설정 취약점, 악성코드 취약점, 소프트웨어 취약점, 네트워크 취약점으로 분류된다.

기반시설은 취약점에 의하여 위협에 노출되는 원인도 있지만, IT 영역에서 룰 (Rules) 기반, 시그니처 기반, 행위기반 모니터링, 이상행위 분석 기반의 보안 솔루션을 통하여 탐지하는 악성코드를 기반시설에서는 프로토콜 및 실시간성이 가지는 특성으로 인하여 기존의 IT 영역에 적용된 보안 솔루션을 그대로 적용하지 못함으로써 발생하는 문제점도 존재한다. 뿐만 아니라, 근본적인 원인의 일례로, 가동원전의 계측제어 시스템이 과거에 도입할 당시에는 보안성을 고려하지 않았으며, 다양한 이기종의 시스템으로 구성되었기 때문에 IT 영역에서와 같이 동일한 보안체계를 적용하는 것은 현실적으로 불가능에 가까우며, 기술적으로 보안조치를 적용하기에는 한계가 존재한다. 이러한 이유로 현재 원전에 설치된 이기종의 제어 시스템에 공통적으로 적용하기 위한 APT 등의 악성코드를 탐지하는 기술을 마련하는 것이 시급한 실정이다[27]. 또한 원전 제어시스템에 오동작이 발생하는 경우가 존재하는데, 그 원인은 악성코드에 의하여 발생하는 경우도 있으며, 제어 시스템 자체적으로 발생하는 고장에 의한 경우도 존재한다. 이러한 경우에는 오동작이 발생하는 원인을 파악하여야 하지만, 실질적인 원인을 판단하기는 매우 어려운 실정이므로 그 원인을 판단하기 위한 방안이 요구된다. 더욱 심각한 문제점은 제어 시스템의 리소스를 사용하는 보안 기술을 기반으로 악성코드를 탐지할 경우에는 사용되는 리소스가 기존 원전 제어시스템의 안전성을 침해할 가능성이

존재하기 때문에, 기존의 기능에 영향을 미치지 않는 방안도 필요하다. 따라서 상기의 모든 배경을 종합적으로 판단하면, 국내 기반시설에서 APT 등의 악성코드 탐지기술을 적용하기 위하여 기반시설의 특성에 따라 적용 가능성이 높은 탐지기술을 선정하여 적용성 평가를 통하여 적용 방법론으로 국한하여 기반시설에서 공통적으로 적용할 수 있는 특화된 APT 등의 악성코드 탐지기술을 개발하여야 한다.

References

[1] The National Law Information Center, *Act on Measures for the Protection of Nuclear Facilities, etc. And Prevention of Radiation Disasters*, Retrieved Jan. 22, 2018, from http://www.law.go.kr

[2] KEPCO E&C, *Introduction of Regulatory Standard on Cyber Security for Nuclear Power Plants, Research report, 2018.* Retrieved Jan. 22, 2018, from https://www.kepco-enc.com

[3] Nuclear Safety and Security Commission, *8. 13 Using a safety system with a digital computer*, Retrieved Jan. 22, 2018, from http://www.nssc.go.kr/_custom/nssc/_common/board/download.jsp?attach_no=11761

[4] The National Law Information Center, *Enforcement Decree of the Information Communication Infrastructure Protection Act*, Retrieved Jan. 22, 2018, from http://www.law.go.kr

[5] K. S. Han, "Design of instrumentation and control system nuclear protection profile (NPP-ICS) based on nuclear cyber security guidenline," M.S. Thesis, Dept. of Computer Sci., Hannam Universiry, Feb. 2013.

[6] S. H. You, "A study on security indicator based on vulnerability analysis of major ICS," M.S. Thesis, Korea University, Jun. 2012.

[7] G. H. Yim, "Control system security vulnerabilities and countermeasures," M.S. Thesis, Dept. of Cyber Secur., Korea University, Jun. 2011.

[8] Korea Customs Service, *Security guideline for national infrastructure electronic control system*, Retrieved Jan. 22, 2018, from http://www.customs.go.kr

[9] ASEC (AhnLab Security Emergency response Center), *Report of the analysis of infrastructure attacks*, Retrieved Jan. 22, 2018, from http://download.ahnlab.com/kr/site/library/%5BAnalysis%20Report%5DCritical%20Infrastructure%20Threats.pdf

[10] H. J. Go, "Analysis of vulnerability through penetration testing of power generation system and countermeasure of intrusion," Master's thesis, Korea University, Jun. 2013.

[11] S. G. Han, "A study on cyber threats in control system linkage section," M.S. Thesis, Korea University, Jun. 2011.

[12] H. G. Kwon, "The efficient analysis of the security situation through visualization of the control system," M.S. Thesis, Dept. of Cyber Secur., Korea University, Jun. 2012.

[13] S. Lim, A. Kim, and I. Shin, "Trends of cyber security regulatory of overseas nuclear power plant digital asses supply chain," *R. KIISC*, vol. 26, no. 1, pp. 54-60, Feb. 2016.

[14] Department of justice, *Departments of Justice and Homeland Security Announce International Initiative Against Traffickers in Counterfeit Network Hardware*, Retrieved Jan. 22, 2018, from https://www.justice.gov/archive/criminal/cybercrime/press-releases/2008/Intl-Initiative.pdf

[15] Daily mail online, *Man pleads guilty in counterfeit sub parts case*, Retrieved Jan., 22, 2018,from http://www.dailymail.co.uk/wires/ap/article-2647551/Man-pleads-guilty-counterfeit-sub-parts-case.html

[16] Y. D. Kang, "A study on cyber security assessment methodology of instrumentation & control systems for nuclear power plants," Ph. D. dissertation, Chonbuk National University, Feb. 2011.

[17] Z. Kim, J. Kim, Y. Kang, K. Kim, D. Kim, and C. Jeong, *Guideline of cyber security policy for digital I&C systems in nuclear power plant*, Retrieved Jan. 22, 2018, from https://www.kns.org/kns_files/kns/file/306%B1

%E8%C1%F8.pdf
[18] D. Kim, “Security criteria for design and evaluation of secure plant data network on nuclear power plants,” *J. KIECS*, vol. 9, no. 2, pp. 267-271, 2014.
[19] NRC Information Notice 2003-14, *Potential vulnerability of plant computer network to worm infection*, *Nuclear regulatory commission*, Retrieved Jan. 22, 2018, from https://www.nrc.gov/docs/ML0324/ML032410430.pdf
[20] N. Falliere, et. al, *W32.Stuxnet Dossier*, Retrieved Jan. 22, 2018, from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
[21] J. Moon and I. Lee, “Cyber terrorism trends and countermeasures,” *R. KIISC*, vol. 20, no. 4, pp. 21-27, Aug. 2010.
[22] K. Lee and K. Yim, “Analysing and neutralizing the stuxnet’s stealthing techniques,” *J. KONI*, vol. 14, no. 6, pp. 838-844, Dec. 2010.
[23] J. S. Kim, “A study on the implementation of intrusion detection system based on whitelist for substation automation system,” M.S. Thesis, Korea University, Jun. 2015.
[24] T. Kim and D. Kang, “A study on identification and classification of cyber security threats on electric power system,” *J. SE*, vol. 9, no. 1, pp. 53-65, Feb. 2012.
[25] K. Chung, H. Park, B. Jung, J. Jang, and M. Chung, “Safety and security issues in smart grid,” *R. KIISC*, vol. 22, no. 5, pp. 54-61, Aug. 2012.
[26] Intea, *Introduction to MODBUS*, Technical Tutorial, Retrieved Jan. 22, 2018, from http://www.intea.hr/downloads/introduction_to_modbus.pdf
[27] Y. Jung and M. Park, “Network defense mechanism based on isolated networks,” *J. KICS*, vol. 41, no. 9, pp. 1103-1107, Sept. 2016.

이 경 룰 (Kyungroul Lee)

2008년 8월 : 순천향대학교 정보보호학과(공학사)
2010년 8월 : 순천향대학교 정보보호학과(공학석사)
2015년 2월 : 순천향대학교 정보보호학과(공학박사)
2011년 5월~2011년 12월 : (미) 퍼듀대학교 방문연구원
2015년 6월~2016년 2월 : 순천향대학교 박사후연구원
2016년 3월~현재 : 순천향대학교 연구조교수
<관심분야> 취약점 분석, 시스템 보안, 하드웨어 보안, 인터넷 뱅킹, 사용자 인증, 디바이스 인증

이 선 영 (Sun-Young Lee)

1993년 2월 : 부경대학교 전자계산학과(이학사)
1995년 2월 : 부경대학교 전자계산학과(이학석사)
2001년 3월 : 일본동경대학 전자정보공학(공학박사)
2004년 3월~현재 : 순천향대학교 정보보호학과 교수
<관심분야> 콘텐츠 보안, 암호이론, 정보이론, 정보보안

임 강 빈 (Kangbin Yim)

1992년 2월 : 아주대학교 전자공학과(공학사)
1994년 2월 : 아주대학교 전자공학과(공학석사)
2001년 2월 : 아주대학교 전자공학과(공학박사)
1999년 3월~2000년 2월 : (미) 아리조나주립대학교 연구원
2003년 3월~현재 : 순천향대학교 정보보호학과 교수
2005년 3월~현재 : 한국정보보호학회 이사
2009년 3월~현재 : 한국인터넷정보학회 이사
2010년 12월~2012년 2월 : (미)퍼듀대학교 객원교수
<관심분야> 시스템보안, 접근제어, 보안구조설계, 취약점분석, 개념증명도구개발