Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.5, Oct. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.5.1001

디지털트윈 기반의 스마트공장에서 랜섬웨어 공격과 피해 분석을 위한 정보보안 실습콘텐츠 시나리오 개발*

남 수 만,[1†] 이 승 민,[1] 박 영 선[2‡]
[1,2]두두아이티 (연구원, 대표이사)

Development of Information Security Practice Contents for Ransomware Attacks in Digital Twin-Based Smart Factories*

Su Man Nam,[1†] Seung Min Lee,[1] Young Sun Park[2‡]
[1,2]DUDU Information Technologies Inc. (Researcher, President)

요 약

스마트공장은 운영 기술에 최신 정보 기술이 융합된 복합 체계이다. 스마트공장은 복합 기술의 융합으로 기존 공장에 비해 제조 능력 향상, 맞춤형 생산, 자원 절감 등을 목표로 두고 있다. 이처럼 스마트공장은 개방된 환경으로 공장의 효율성을 증가시킬 수 있음에도, 기존 정보 기술의 취약점이 그대로 전이되어 공장의 보안 수준은 낮다. 게다가 스마트공장의 보안 전문가의 부재로 피해 발생 시 업무연속성계획의 대응 및 복구가 미흡한 실정이다. 상기 문제에 대응하기 위해, 우리는 실제와 유사한 디지털트윈 기반의 스마트공장에서 랜섬웨어 공격을 발생 시켜 피해를 분석하는 정보보안 실습 콘텐츠를 제안한다. 우리의 정보보안 콘텐츠에서는 디지털트윈의 실습 환경 구축을 위해 물리적 기기들을 가상 머신 또는 시뮬레이션 모델로 전환하는 기술을 소개한다. 이 콘텐츠는 구현된 디지털트윈에서 정해진 시나리오에 따라 두 가지 유형의 랜섬웨어 공격을 발생한다. 이 발생된 공격이 성공적으로 완료될 경우 23대의 가상 요소 중 최소 8대와 5대에서 각각 피해를 본다. 그리하여 우리의 제안 콘텐츠는 가상세계의 스마트공장에서 두 가지 유형의 랜섬웨어를 발생시켜 이의 피해를 직접 확인한다.

ABSTRACT

Smart factories are complex systems which combine latest information technology (IT) with operation technology (OT). A smart factory aims to provide manufacturing capacity improvement, customized production, and resource reduction with these complex technologies. Although the smart factory is able to increase the efficiency through the technologies, the security level of the whole factory is low due to the vulnerability transfer from IT. In addition, the response and restoration of the business continuity plan are insufficient in case of damage due to the absence of factory security experts. The cope with the such problems, we propose an information security practice content for analyzing the damage by generating ransomware attacks in a digital twin-based smart factory similar to the real world. In our information security content, we introduce our conversion technique of physical devices into virtual machines or simulation models to build a practical environment for the digital twin. This content generates two types of the ransomware attacks according to a defined scenario in the digital twin. When the two generated attacks are successfully completed, at least 8 and 5 of the 23 virtual elements are take damage, respectively. Thus, our proposed content directly identifies the damage caused by the generation of two types of ransomware in the virtual world' smart factory.

Keywords: Information Security Contents, Ransomware, Smart Factories, Digital Twin, Conversion Technology

Received(08. 17. 2021), Modified(09. 13. 2021), Accepted(09. 13. 2021)
* 본 연구는 2020년도 중소벤처기업부의 기술개발사업 지원에 의한 연구임[S2966549]
† 주저자, sumannam@gmail.com
‡ 교신저자, ohipark@duduit.co.kr(Corresponding author)

I. 서 론

최근에 보안이 취약한 스마트공장에서 금전 확보를 목적으로 하는 랜섬웨어 공격이 늘어나고 있으며, 이를 위한 사이버 보안 관심이 높아지고 있다. 그럼에도 랜섬웨어 공격을 효율적으로 대응할 수 있는 전담인력이 부족할 뿐만 아니라, 무선통신, 사물 인터넷(Internet of things; IoT) 등과 같은 신기술들의 등장으로 융합 기술이 늘고 있어 이로 인한 사이버 공격이 꾸준히 증가하고 있다[1-3].

스마트공장(Smart Factory)은 신기술을 기반으로 운영 기술(Operation Technology; OT), 정보 기술(Information Technology; IT), 디지털 변환(Digital Transformation; DT)의 융합으로 제조업 분야 발전을 가속화시키고 있다[4-8]. 이 스마트공장은 맞춤형 생산 공장 구현으로 제조 경쟁력을 확보하기 위해 원가 절감, 생산성 향상, 품질 향상, 설비 가동률 향상, 에너지 절감 등이 가능하다.

스마트공장은 기존 자동화 공장 시스템과 달리 실시간 자율화에 의한 생산인 설비, 재료, 환경 등의 상태에 따라 최신 통신 기술을 적용하여 자율 판단 및 수행이 가능하다[4, 5]. 또한, IoT로 초연결 기술을 통해 수직 및 수평적 통합 연결이 가능하다[9].

스마트공장의 대표적인 특징은 지능화(Intelligence), 연결화(Connectivity), 그리고 가상화(Virtualization)이다[4]. 지능화는 IoT로부터 데이터 및 정보 수집, 저장, 분석한 후 인공지능(Artificial Intelligence; AI)을 활용하여 자율 제어하는 기술이다. 연결화는 최신 통신 기술을 활용하여 공장 안에 존재하는 모든 구성 요소(사람, 설비, 부품, 재료 등)를 연결하는 기술이다. 마지막으로, 가상화는 디지털트윈(Digital Twin)[10, 11] 기술을 기반으로 실제 공장과 가상 공장을 서로 연계하여, 실제 데이터를 통해 다양한 시뮬레이션을 수행함으로써 최적인 운영 환경을 예측 및 제공하는 융합 기술이다.

이처럼 스마트공장은 다양한 특징들을 보유하고 있음에도 불구하고 OT 영역에 최신 통신 기술(5G, WiFi 등)과 IT의 융합으로 개방된 구조를 갖게 되어 기존 IT 영역에서 발생 가능한 보안 위협이 그대로 OT로 전이되고 있다. 뿐만 아니라, 스마트공장의 공격 접점 증가[7-9]는 위협의 규모와 이에 따른 피해를 더 증가시키고 있다. 스마트공장에서는 사이버 공격, 정전 등과 같이 잠깐의 운행 중단에도 엄청난 피해가 야기된다. 특히, 스마트공장의 보안 전문가의 부재로 사이버 공격 피해[12, 13] 발생 시 업무연속성계획의 대응 및 복구가 미흡한 실정이므로 기존 IT 인력을 활용한 체계적인 정보보안 교육이 중요하다.

본 논문은 스마트공장에서 발생하는 랜섬웨어 공격에 대응하기 위해 공장의 구성요소를 디지털트윈으로 변환하고, 변환된 디지털트윈에서 실제와 유사한 랜섬웨어 공격을 시도하여, 그 피해를 분석하는 정보보안 콘텐츠를 제안한다. 제안 콘텐츠를 개발하기 위해 목표 공장을 디지털트윈으로 변환하는 기술이 필요한데, 이를 위해 가상화 가능 요소와 불가능 요소로 구분한다. 가상화 가능 요소(예: 개인용 컴퓨터, 서버 등)는 물리적 머신을 가상 머신으로 변환(Physical-to-Virtuall 이하 P2V)하는 기술[14-16]을 활용하고, 가상화 불가능 요소(예: 센서, 로봇 등)는 모델링 및 시뮬레이션(Modeling and Simulation; M&S) 기술[8, 15]을 활용하여 시뮬레이션 모델로 구현한다. 목표 스마트공장을 디지털트윈으로 변환 완료 후에는 두 가지 유형의 랜섬웨어 공격을 발생시켜 스마트공장의 피해를 분석한다. 분석 결과, 총 23개의 가상머신 또는 시뮬레이션 모델로 구현된 디지털트윈에서 8대와 5대에서 각각 랜섬웨어 피해가 발생하였다. 그러므로 본 논문의 기여는 다음과 같다.

- 스마트공장 기반의 정보보안 콘텐츠 설계 및 개발
- 스마트공장을 디지털트윈으로 변환
- 개발 정보보안 콘텐츠에서 랜섬웨어 공격 시도 및 피해 분석

본 논문의 구성은 2장에서는 기존 연구들을 보여주고, 3장에서는 스마트공장의 개념 및 보안위협과 디지털트윈에 대해 소개한다. 4장에서는 제안 콘텐츠를 설명하고, 마지막으로 5장에서는 전반적인 결론을 요약한다.

II. 관련연구

사이버보안 훈련 시스템의 대표적인 시스템은 SecGen[17], MetaCTF[18], 자동화 문제 생성[19], 사이버 해킹 대응 시스템[20-21] 등이 있다. SecGen는 임의의 시나리오를 기반으로 가상머신을 사용하여 자동으로 생성하는 보안 시나리오를 생성한

후 모의 해킹, 보안 교육, CTF(capture-the-flag) 등에 활용한다. MetaCTF는 바이너리 역공학(binary reverse engineering) 중심의 CTF 문제를 자동 생성하고, 매개변수를 활용하여 사용자들에게 서로 다른 문제들을 제공한다. 두두아이티의 사이버이지스는 사이버 침해대응에 관한 이론과 실제 정보시스템과 유사한 상황 하에서 대응 능력을 숙달시키는 모의훈련 시스템이다. 그러나 이들은 사전에 정의된 콘텐츠를 통해 문제 풀이 방식으로 진행하고, 스마트공장에 특화된 정보보안 콘텐츠 보다는 일반 정보시스템의 보안 콘텐츠에 가깝다.

스마트공장을 위한 정보보안 콘텐츠를 설계 및 개발하기 위해서는 다양한 방법들이 있다. 최근에는 디지털트윈 기반의 스마트공장에서 보안성을 평가한 연구들이 나오고 있다. [12]에서는 스마트공장에서 사이버 보안 향상을 위해 디지털트윈 활용한 프레임워크를 제안한다. 이 프레임워크의 디지털트윈은 지속적인 모니터링 및 제어를 제공하기 위해 물리적 시스템과 지속적으로 연동한다. 이 디지털트윈은 시뮬레이션과 물리적 시스템 사이의 실시간 양방향 커플링 기술을 사용하여 시스템 구성 요소 고장과 사이버 공격을 진단한다. 다만 기존 디지털트윈은 제안 콘텐츠의 디지털트윈과 달리 물리적 시스템과의 지속적인 데이터 전달이 필요하여 부하가 클 수 있다.

[13]에서는 보안 강화를 위한 디지털트윈 기반 보안 프레임워크를 제안한다. 이 프레임워크는 구축된 디지털트윈에서 공격자 모델을 도입하고, 기본적인 보안 정의를 만들어 기본적인 보안 요구사항(침입자 탐지, 접근 제어 등)을 평가한다. 더불어 제시된 프레임워크는 개념 증명과 성능 평가와 함께 실제적인 제작 사례가 잘 동작한다는 것을 보여주었다. 다만 제안 콘텐츠과 달리 구성 요소들을 모두 시뮬레이션 모델로만 구현하여, 물리 시스템을 그대로 재현하지는 못했다.

그러므로 본 논문은 상기 연구들과 달리 P2V와 시뮬레이션 모델을 활용하여 스마트공장의 구성요소들을 그대로 디지털트윈으로 구현하고, 거기서 두 유형의 랜섬웨어 공격을 시도하여 그 피해를 분석하는 정보보안 콘텐츠를 설계하고 개발하였다.

III. 배 경

본 장에서는 최신 기술인 스마트공장과 디지털트윈에 대해 각각 소개한다.

3.1 스마트공장

본 절에서는 스마트공장의 개념과 이의 사이버보안 위협에 대해 소개한다.

3.1.1 개념

스마트공장은 자동화 수준을 넘어 복합적인 IT 기술이 융합된 생산체계를 갖춘 지능화된 공장이다[9]. 스마트공장의 장점은 생산 비용 및 시간 감소, 고객 맞춤형 생산, 생산 효율성 극대화 등이 있다[8]. 스마트공장은 사물인터넷(IoT), 빅데이터, 인공지능, 5세대 이동통신 기술 등의 4차 산업혁명 핵심 기술들이 포함된 복합 시스템이다.

Fig. 1은 [8]에 근거한 스마트공장 시스템의 구성요소를 보여준다. 이 복합 시스템의 구성요소는 크게 현장 자동화, 제어 자동화, 응용 시스템으로 구성된다. 현장 자동화는 스마트공장의 최하위 영역으로 상황 감지 및 자동 수행하는 로봇, 공작기계, 컨베이어 벨트 등이 있으며, 제어 자동화는 응용 시스템과 현장 자동화 기기 간 연동하는 PLC(

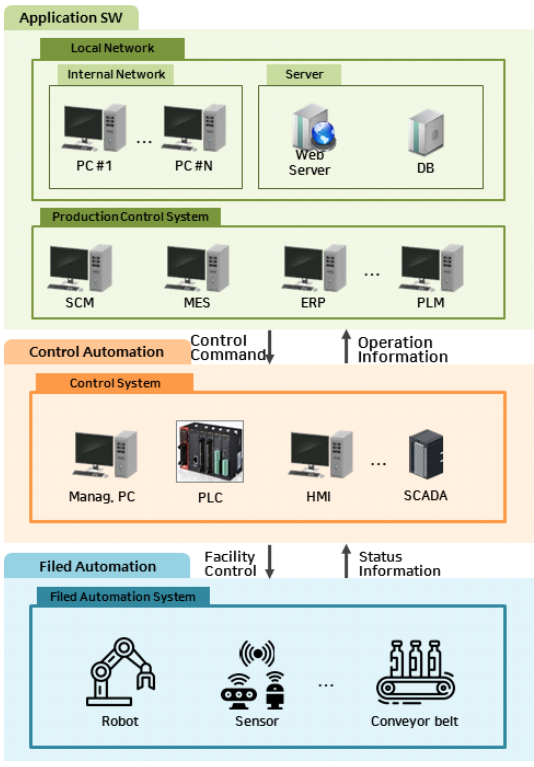

Fig. 1. Smart Factory Architecture

Programmable Logic Controller), HMI (Human Machine Interface), 산업 센서 등을 포함한다. 응용 시스템은 기존 공정관리시스템인 PLM(Product Lifecycle Management), SCM (Supply Chain Management), MES(Manufacturing Execution System), ERP(Enterprise Resource Planning) 등이 있으며, 이들은 제어 자동화와 다양한 서버에 연결되어 있다.

3.1.2 사이버보안 보안 위협

[6]에서는 스마트공장이 기존 OT 영역에 IT 기술이 융합되면서 개방형 구조의 위협을 소개한다. 현재 스마트공장은 개방형 네트워크를 위해 5세대 이동통신을 활용하여 모든 기기를 인터넷에 연결한다. 이 개방된 구조는 편리성과 함께 지능화 서비스가 가능함에도 불구하고, 보안 관리대상이 확대되어 보안 위협의 규모도 함께 커졌다. 또한, 모든 기기의 인터넷 연결은 실시간 자동 제어 및 정보 공유의 편리함이 있음에도 불구하고 보안 위협에 취약하다.

스마트공장의 보안 위협은 아래와 같이 크게 6가지로 분류할 수 있다[8, 9, 25].

- 악의적인 활동: 랜섬웨어, DDOS 공격, 멀웨어, 무작위 공격, 개인정보 유출 등
- 도청: 중간자 공격, IoT 통신 프로토콜 하이재킹, 네트워크 정보 유출 등
- 물리적인 공격: 기기 손상, 시설 파괴 등
- 고장 및 오작동: 센서 및 액추에이터 고장 또는 오작동, SW 취약점 악용, 서비스 제공 업체 실등
- 사고: 의도하지 않은 데이터 또는 구성 변경, 장치 및 시스템 오용 등
- 기타: 정전(네트워크 중단 등), 위법(개인정보보호 위반 등), 재해(자연 및 환경 재해)

최근에 스마트공장에 주로 발생하는 악의적인 활동의 랜섬웨어는 몸값(Ransom)과 소프트웨어(Software)의 합성어로, 컴퓨터 파일을 인질로 잡고 돈을 요구하는 최근 공격 패턴 중 하나이다. 랜섬웨어 유형 중 소디노키비[26]는 이메일 첨부파일로 위장하여 실행 파일을 숨긴 다음, 주요 파일들을 암호화하고, 공격자가 원하는 바탕화면으로 변경시킨다. 이 공격의 특징은 복구할 수 없는 랜섬웨어로 구분되어 있다[26]. 소디노키비와 같은 랜섬웨어 공격이 스마트공장에 발생하게 되면 제어와 현지 자동화는 그대로 멈추게 되어 큰 피해를 보게 된다. 뿐만 아니라 가동이 중단된 공장을 다시 재가동시키는 데도 큰 비용이 소모된다.

3.2 Digital Twin

디지털트윈[13, 27, 28]은 물리적 환경인 현실세계와 디지털 환경인 가상 세계를 융합한 4차 산업혁명의 디지털 기술 중 하나이다. 이 기술은 목표 시스템의 모든 기록을 데이터로 저장하고, 전체적인 흐름을 관리하면서 실시간 피드백을 진행한다. 현실 세계를 가상화로 구축하기 위해서는 물리적 환경 고도화, 시뮬레이션, 예측 기술 등이 필요하다.

Fig. 2는 현실 세계를 가상 세계로 변환하는 디지털트윈의 구축 기술들을 보여준다. 다양한 IoT 기기로 구성된 스마트공장, 스마트시티와 같은 지능형 시스템들은 가상세계를 구축하기 위해 가상화가 가능한 요소와 불가능한 요소로 구분하여야 한다. 가상화가 가능 요소(PC와 서버 등 IT 장비들)는 P2V 기술로 적용하고, 불가능 요소(로봇 등 OT 장비들)는 M&S 기술로 활용한다. 이 두 기술을 모의하기 위해서는 가상머신 및 모델의 연동(V-C) 시뮬레이션 기술을 사용한다.

이처럼 가상으로 변환된 디지털트윈에서는 현실의 직접적인 문제를 가상 세계에 발생시켜 피해 규모들을 예측하거나 최적의 의사결정을 하도록 돕는다. 예를 들어, 복잡한 지능형 시스템 중 하나인 스마트공장은 실제 운영 기기에 고도화된 사이버 위협(랜섬웨어 공격 등)을 가해 그 공격의 피해 및 규모를 예측하기 매우 어렵다[12, 13]. 하지만, 디지털트윈에서는 실제 기기들이 가상으로 변환되기 때문에 고도화

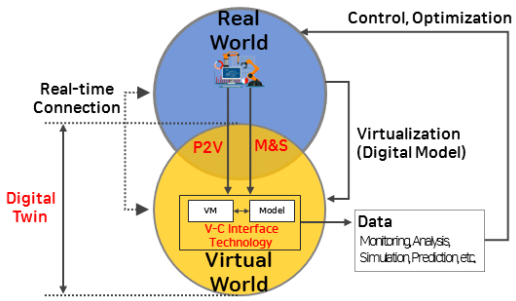

Fig. 2. Technologies of Digital Twin using P2V and M&S.

된 다양한 사이버 위협을 발생시켜 그 피해 및 규모를 예측하기 용이하다.

IV. 스마트공장을 위한 제안 콘텐츠

본 장에서는 디지털트윈 기반의 스마트공장에서 정보보안을 위한 한 실습콘텐츠를 제안한다.

4.1 개요

스마트공장은 OT와 IT 기술을 서로 융합하여 개방된 네트워크 구조를 갖는 융합 기술임에도 공장 사이버보안 전담인력 부족으로 랜섬웨어 공격을 통한 큰 피해를 볼 수 있다. 게다가 스마트공장의 모든 기기가 네트워크에 연결되어 접점 확대로 보안 취약성이 증가하고 있다. 우리의 콘텐츠는 목표 공장을 디지털트윈으로 전환하여 랜섬웨어 공격에 따른 피해를 분석하는 정보보안 콘텐츠를 제안한다. 본 제안에서 디지털트윈으로 변환하기 위해서는 가상화 가능 요소와 불가능 요소로 구분하고, 가능한 요소는 P2V을 활용하고 불가능한 요소는 모델링 및 시뮬레이션을 활용한다. 그러므로 본 정보보안 콘텐츠는 디지털트윈 기반의 스마트공장에서 취약한 서버들을 통해 배포되는 랜섬웨어를 시도하고 그 피해를 분석한다.

4.2 디지털트윈 변환 기술

본 제안 콘텐츠에서는 [8]에 근거한 스마트공장 시스템을 디지털트윈으로 구축하기 위한 변환 기술을 사용한다. 이를 전환하기 위해 각 구성요소는 가상화 가능 요소와 불가능 요소로 분류한다. 가상화 가능 요소는 P2V를 위해 VMware의 vCenter 변환기[22]을 사용하고, 가상화 불가능 요소는 M&S를 위해 DEVS 기반의 시뮬레이션 모델[18, 29-31]로 구현한다. Fig. 3은 우리의 제안 콘텐츠의 전체 아키텍처를 보여주며 가상화 가능 영역과 불가능 영역을 보여준다.

제안 콘텐츠에서 현장자동화(Machine Automation) 영역은 가상화 소프트웨어(Software)의 지원 운영체제(Operating System; OS)가 없어 가상화가 불가능하고, 제어자동화와 응용시스템 영역은 가상화가 가능하다(제안 자동화의 PLC-PC (Programmable Logic Controller)는 PC에 PLC가 바로 연결되어 있는 컴퓨터를 의미한다). 각 영역별 구성요소 및 운영체제는 Table 1과 같다.

Fig. 4는 제안 콘텐츠에서 현실 세계의 스마트공장은 가상세계의 디지털트윈 변환 기술을 보여준다. 스마트공장의 대부분 장비는 서버로부터 명령을 받은 한 개인용 컴퓨터(PC)에서 여러 PLC와 자동화 기기가 함께 동작한다. 자체 현장 조사 결과, 거의 대

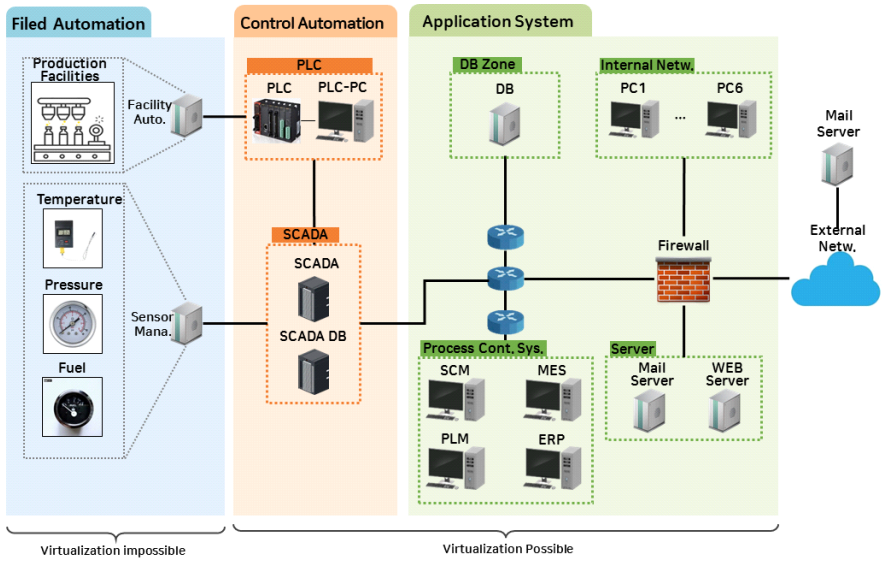

Fig. 3. A Digital Twin-based The Smart Factory Architecture

Table 1. Components of Proposed Digital Twin

Level	Type	OS	Num	Conversion
Application System	PC	Windows 7	6	VM
	Firewall	CentOS7	1	VM
	DB	CentOS7	1	VM
	Web Server	CentOS7	1	VM
Control Automation	Router	dd.wrt	3	VM
	ScadaBR	CentOS7	1	VM
	ScadaDB	CentOS7	1	VM
	PLC-PC	Windows 7	1	VM
Machine Automation	Sensor Management	-	1	Model
	Thermometer	-	1	Model
	Manometer	-	1	Model
	Fuel Gauge	-	1	Model
	Robot	-	1	Model
	Production Facility	-	1	Model
External Network	Mail Server	Ubuntu12	2	VM

VM: Virtual Machine / Model: DEVS Model

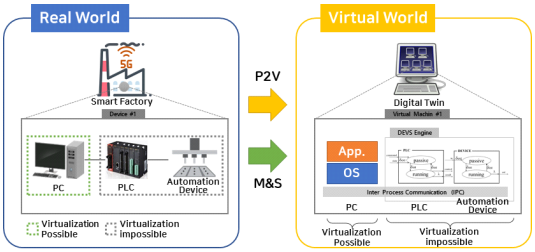

Fig. 4. Our Digital Twin Conversion Technology

부분 PC의 운영체제는 윈도우 계열을 사용하고 있었고, PC와 PLC 및 자동화 기기는 이더넷(Ethernet) 통신을 통해 동작하였다. 제안 콘텐츠에서 가상화 가능 요소인 PC는 vCenter 변환기를 통해 가상머신으로, 가상화 불가능 요소인 PLC와 자동화 기기는 DEVS 기반의 시뮬레이션 모델로 구현한다. 각 시뮬레이션 모델들은 가상머신 내에서 동작하며, 내부 프로세스 통신(Inter Process Communication; IPC)[32]을 활용하여 가상머신과 모델 간 메시지를 공유한다.

4.3 제안 콘텐츠 시나리오

제안하는 정보보안 콘텐츠는 목표 공장을 디지털 트윈으로 변환한 다음, [26]의 공격 콘텐츠 시나리오를 근거하여 MITRE ATT&CK을 활용한 소디노키비의 두 가지 공격 유형을 도출했다.

Fig. 5는 제안 콘텐츠의 디지털트윈에서 메일 서버를 통해 랜섬웨어를 시도한 첫 번째 콘텐츠 시나리오를 보여준다. 공격자(Kali)는 외부 상용 메일서버(네이버 메일서버)를 이용하여 관리자로 위장한 계정으로 패치 파일로 위장한 악성파일(백도어)을 한 직원에게 메일을 보낸다(①). PC1의 직원은 그 실행파일을 다운로드한 후 실행한다(②). 연결 세션 대기 중이던 공격자는 PC1과 세션 연결한 후 그 컴퓨터를 장악한다(③). 연결된 세션을 통해 윈도우용 랜섬웨어를 몰래 업로드시킨다. 공격자에게 장악된 컴퓨터에서는 공유 폴더를 통해 측면 이동한 후 랜섬웨어를 다시 업로드하고 실행시킨다(④). 그 PC는 SSH로 SCADA를 접속한 후 Linux용 랜섬웨어를 업로

Table 2. Tactics and Techniques

	Scenario #1	Scenario #2
Initial Access	[T1566.001] Phishing	
Execution	[T1204] User Execution	
Command and Control	[TA0011] Command and Control	
Impact	[T1486] Data Encrypted for Impact	
Lateral Movement	[T1021.002] SMB Admin Share	
Execution	[T1204] User Execution	
Impact	[T1486] Data Encrypted for Impact	
Execution	[T1204] User Execution	[T1021.004] Remote Services
Lateral Movement	[T1021.004] Remote Services	[T1486] Data Encrypted for Impact
Impact	[T1486] Data Encrypted for Impact	N/A
Execution	[T1204] User Execution	N/A
Lateral Movement	[T1021.004] Remote Services	N/A
Execution	[T1204] User Execution	N/A
Impact	[T1486] Data Encrypted for Impact	N/A

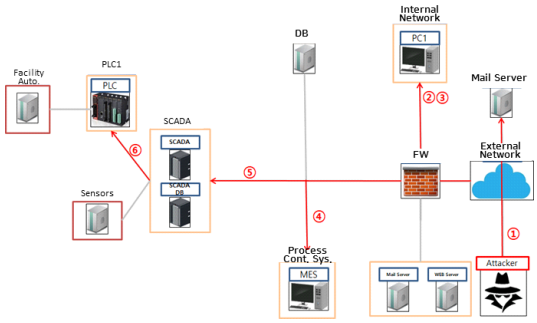

Fig. 5. Ransomware Content Scenario #1

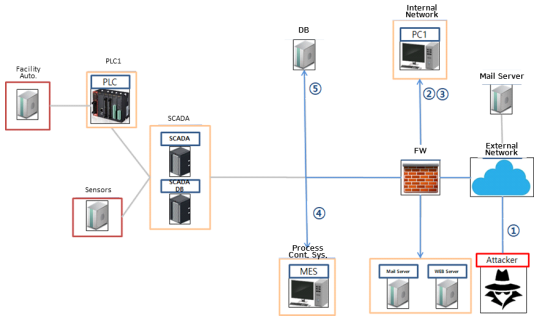

Fig. 6. Ransomware Content Scenario #2

드하고 실행한다(⑤). 다시 PLC로 랜섬웨어를 업로드한 후 실행시킨다(⑥). 마지막으로 공격자는 최초 감염된 PC에 블루키 공격을 이용하여 블루스크린을 공장 설비 작동을 마비시킨다.

Fig. 6은 가상 스마트공장 환경에서 웹 서버를 통해 랜섬웨어를 시도한 두 번째 콘텐츠 시나리오를 보여준다. 공격자는 내부망에 잠입하여 내부 홈페이지 게시판을 이용하여 악성파일을 배포한다(①). PC1의 직원은 첨부파일을 다운로드한 후(②) 그 파일을 실행한다. 실행과 동시에 공격자에 세션이 연결되고(③) 그 PC에 랜섬웨어 파일이 업로드된다. 악의적인 공격자는 내부망의 SSH를 이용하여 MES(Manufacturing Execution System)로 파일을 전달하고 실행시킨다(④). 공격자는 장악한 MES를 통해 DB에 접근하고 랜섬웨어 공격을 시도한다(⑤).

4.4 랜섬웨어 공격의 피해 분석

우리는 디지털트윈 기반 스마트공장에서 두 가지 유형의 랜섬웨어 공격하는 콘텐츠를 설계 및 개발하였다. 첫 번째에서는 외부 메일서비스의 첨부파일을 통한 공격이며, 두 번째에서는 내부 홈페이지에 게시된 악성파일을 통한 공격이다.

Table 3. Analysis Result of Damage

Level		Content Scenario #1	Content Scenario #2
Damage	Application System	2 (Employee PC, MES)	2 (Employee PC, MES)
	Control Automation	2 (ScadaBR, PLC-PC)	1 (DB)
	Sensor Level	4 (Sensor Management/Sensors)	2 (Robot, Production Facility)
Total Damage		8	5

Table 2는 두 유형의 시나리오에 대한 공격 피해 결과를 보여준다. 두 시나리오의 콘텐츠 모두 모든 계층에서 랜섬웨어 피해가 발생하였다. 주요 피해를 보면 1번 시나리오는 PLC가 연결된 PC에 감염되어 관련된 센서와 기기들은 사용 불가하며, 2번 시나리오는 로봇과 연결된 DB가 랜섬웨어에 감염되었다. 따라서, 두 시나리오 모두 랜섬웨어를 통한 스마트공장의 일부분을 사용하지 못한다. 랜섬웨어 공격을 대응하기 위해서는 평소 주기적인 백업이 중요할 뿐만 아니라 OS 및 백신 프로그램 업데이트 등도 필요하다[26].

V. 결 론

본 논문의 제안은 한 스마트공장을 디지털트윈으로 전환하여 두 가지 유형의 랜섬웨어 공격을 시도하는 정보보안 콘텐츠를 설계하고 개발한다. 스마트공장을 디지털트윈으로 변환하기 위해서는 디지털트윈 변환 기술을 제안하였다. 변환 기술에서는 스마트공장의 구성요소 중 가상화가 가능한 요소들은 P2V를 사용하여 가상머신을 생성하고, 가상화가 불가능한 요소들은 DEVS 형식론으로 시뮬레이션 모델을 구현한다. 제안 콘텐츠는 변환된 디지털트윈에서 메일서버와 웹서버를 이용하여 랜섬웨어가 네트워크 내부에 주입된다. 주입된 랜섬웨어는 응용시스템, 제어자동화, 현장자동화의 구성요소들에 침입하여 시스템을 파괴한다. 그 결과 첫 번째 시나리오는 8개의 기기에서 피해가 있었고, 두 번째 시나리오는 5개의 기

기에서 피해가 있었다. 그리므로, 제안 콘텐츠는 한 스마트공장을 디지털트윈으로 변환한 후 그 디지털트윈에서 랜섬웨어 공격을 시도하여 그 피해를 분석하는 콘텐츠이다. 향후 연구에서는 본 논문에서 제시한 랜섬웨어의 효율적인 방어 기법과 산업 제어 시스템을 위한 공격 프레임워크(칼데라 프레임워크)[33]를 사용하여 정보보안 콘텐츠를 확장할 것이다.

References

[1] Whitehouse, "The National Cyber Range,"https://obamawhitehouse.archives.gov/files/documents/cyber/DARPA - NationalCyberRange_FactSheet.pdf, Aug. 2021.

[2] D. Kim and Y. Kim, "A Study of Administration of Cyber Range," J. Internet Comput. Serv., vol. 18, no. 5, pp. 9-15, 2017.

[3] Y. G. Kang, J. D. Yoo, E. Park, D. H. Kim, and H. K. Kim, "Design and Implementation of Cyber Attack Simulator based on Attack Techniques Modeling," Journal of The Korea Society of Computer and Information, vol. 25, no. 3, pp. 65-72, Mar. 2020.

[4] B. Chen, J. Wan, L. Shu, P. Li, M. Mukherjee, and B. J. I. A. Yin, "Smart factory of industry 4.0: Key technologies, application case, and challenges," Ieee Access, vol. 6, pp. 6505-6519, Dec. 2017.

[5] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," Journal of Manufacturing Systems, vol. 47, pp. 93-106, Apr. 2018.

[6] S. Wang, J. Wan, D. Li, and C. Zhang, "Implementing Smart Factory of Industrie 4.0: An Outlook," International journal of distributed sensor networks, vol. 12, no. 1, pp. 1-10, Jan. 2016.

[7] B. H. Bae "Analysis and Implications of Security Trends in Smart Factories in Major Countries" ITFIND Magazine, Oct. 2019.

[8] Korea Internet & Security Agency, "Smart Factory Cyber Security Guide" KISA Report, 2019.

[9] S. Kwon, J. Kim, J. Lim, I. Yu, "5G-based Smart Factory Security Trend Analysis," Korea Institute Of Information Security And Cryptology, 30(6), pp. 39-46, Dec. 2020.

[10] T. H.-J. Uhlemann, C. Lehmann, R. J. P. C. Steinhilper, "The digital twin: Realizing the cyber-physical production system for industry 4.0," Procedia Cirp, vol. 61, pp. 335-340, Jan. 2017.

[11] Seon Han Choi, Piljoo Choi, Won-Du Chang, Jihwan Lee, "A Digital Twin Simulation Model for Reducing Congestion of Urban Railways in Busan," Journal of Korea Multimedia Society 23(10), pp. 1270-1285, Oct. 2020.

[12] W. Danilczyk, Y. Sun, and H. He, "ANGEL: An Intelligent Digital Twin Framework for Microgrid Security," in 2019 North American Power Symposium (NAPS), pp. 1-6, Oct. 2019.

[13] C. Gehrmann and M. J. I. T. o. I. I. Gunnarsson, "A digital twin based industrial automation and control system security architecture," IEEE Transactions on Industrial Informatics, vol. 16, no. 1, pp. 669-680, Sep. 2019.

[14] D. Y. Jung, S. T. Kim, Y. B. Kim, "Technical Definition and Detailed Development 5-level Model of Digital Twin," OSIA Standards & Technology Review, 34, pp. 10-16, Mar. 2021.

[15] Y. Kim, S. Yoo, H. Lee, S. Han, "Characterization of Digital Twin," ETRI Insight, pp. 1-112, Dec. 2020.

[16] K. Han, "Smart Factory Security and Standards," The Journal of The Korean Institute of Communication Sciences 36(6), pp. 41-46, May 2019.
[17] Z. C. Schreuders, T. Shaw, M. Shan-A-Khuda, G. Ravichandran, J. Keighley, and M. Ordean, "Security Scenario Generator (SecGen): A Framework for Generating Randomly Vulnerable Rich-scenario VMs for Learning Computer Security and Hosting CTF Events," in 2017 USENIX$ Workshop on Advances in Security Education (ASE), 2017.
[18] W. Feng, "A Scaffolded, Metamorphic CTF for Reverse Engineering," in 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE), 2015.
[19] J. Burket, P. Chapman, T. Becker, C. Ganas, and D. Brumley, "Automatic problem generation for capture-the-flag competitions," in 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE), 2015.
[20] DuDuIT, "Cyber-hacking response training system." http://duduit.co.kr/.
[21] Y. S. Park, J. M. Ryoo, H. Y. Lee, "Virtualization-based training content delivery system". Kor. Patent No. 10-2107374, Apr. 2020.
[22] VMware vCenter Converter, https://www.vmware.com/, Aug. 2021.
[23] S. M. Nam and H.-J. Kim, "WSN-SES/MB: System Entity Structure and Model Base Framework for Large-Scale Wireless Sensor Networks," Sensors, vol. 21, no. 2, p. 430, Jan. 2021.
[24] T. G. Kim, C. H. Sung, S. H, J. H. Hong, C. B. Choi, J. H. Kim, K. M. and Seo, J. W. Bae, "DEVSim++ Toolset for Defense Modeling and Simulation and Interoperation," The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 8(3), pp. 129-142, Jul. 2010.
[25] K. K. Kim, "Smart Factory Security," KISA Report, pp. 1-107, 2019.
[26] E. Park, S. Kim, S. Lee, and J. Kim, "2019 Analysis of Major and New Ransomware Trends in Korea and Foreign countries," Korea Institute Of Information Security And Cryptology, 29(6), pp. 39-48, Dec. 2019.
[27] S. Y. You, M. H. Kim, "Digital Twin Technology Trends and Application of Postal Logistics," Korea Post Information, 120, pp. 1-17, Mar. 2020.
[28] Y. J. Jang, "The Key to Digital Transition, Digital Twin," IITP ICT Sport Issue, 2019-26, pp. 1-30, Dec. 2019.
[29] T. G. Kim and B. P. Zeigler, "The devs formalism: hierarchical, modular systems specification in an object oriented framework," Institute of Electrical and Electronics Engineers (IEEE), 1987.
[30] A. I. Concepcion and B. P. J. I. T. o. S. E. Zeigler, "DEVS formalism: A framework for hierarchical model development," vol. 14, no. 2, pp. 228-241, Feb. 1988.
[31] S. M. Nam and T. H. Cho, "Context-Aware Architecture for Probabilistic Voting-based Filtering Scheme in Sensor Networks," IEEE Transactions on Mobile Computing, vol. 16, no. 10, pp. 2751-2763, Oct. 2017.
[32] L. J. D. c. Lamport, "On interprocess communication," Distributed computing, vol. 1, no. 2, pp. 86-101, Jun. 1986.

[33] MITRE ATT&CK for ICS, https://collaborate.mitre.org/attackics/index.php/Main_Page, Aug. 2021

〈저자소개〉

남 수 만 (Su Man Nam) 정회원
2011년 3월~2013년 2월: 성균관대학교 전자전기컴퓨터학과 석사
2013년 3월~2017년 8월: 성균관대학교 전자전기컴퓨터학과 박사
2017년 10월~2018년 9월: 아주대학교의료원 의료정보연구센터 연구원
2018년 10월~현재: ㈜두두아이티 책임연구원
〈관심분야〉 정보보호, 디지털트윈, M&S, 스마트팩토리

이 승 민 (Seung Min Lee) 정회원
2010년 3월~2017년 2월: 목포대학교 조선공학과 학사
2018년 10월~현재: ㈜두두아이티 연구원
〈관심분야〉 정보보호교육, 포렌식, 정보보안, 사이버해킹

박 영 선 (Young Sun Park) 정회원
1990년 3월~1994년 2월: 경북대학교 전자공학 석사
1997년 3월~2000년 2월: 충남대학교 컴퓨터과학 박사수료
2015년 2월~현재: ㈜두두아이티 대표이사
〈관심분야〉 정보보호, M&S, 워게임, 정보보호교육