한국컴퓨터정보학회 하계학술대회 논문집 제26권 제2호 (2018. 7)

스마트 팩토리 보안 사고 유형 분석 및 대안 프레임 제시

김현진*, 김진영°, 백주련*
°*평택대학교 데이터정보학과
e-mail: jlkh618@naver.com*, wlsdud1517@naver.com°, jrpaik@ptu.ac.kr*

Analysis of Security Attacks and Design of Defense Strategies Found in Smart Factory

Hyeonjin Kim*, Jinyeong Kim°, Juryon Paik*
°*Dept. of Digital Information & Statistics, Pyeongtaek University

● 요 약 ●

최근 제조업의 근로 시간 단축 및 전문 노동력의 감소로 인하여 발생할 수 있는 문제를 개선할 수 있는 스마트 팩토리(Smart Factory)가 주목받고 있다. 스마트 팩토리는 생산품의 불량률을 줄이고, 숙련공 없이 비숙련공만으로 현장 가동이 가능하다는 점 등의 긍정적 효과를 기대할 수 있다. 그러나 스마트 팩토리는 높은 설비 도입 비용, 업무 시스템 재설계 등의 문제점이 등이 있으며, 특히 보안의 취약성이 심각하다. 그렇기 때문에 많은 기업이 현실에서 스마트 팩토리를 도입하는 어려움을 겪고 있다. 본 논문에서는 스마트 팩토리의 다양한 보안 사고를 유형 및 정형화시키고 여러 보안 사고를 유발하는 취약한 부분을 구체화하여 스마트 팩토리의 보안 연구의 방향성을 제시하고자 한다.

키워드: 스마트 팩토리(Smart Factory), 보안 사고(Security Attacks), 센서 데이터(Sensor data)

Ⅰ. 서론

스마트 팩토리(Smart Factory)는 센서 데이터를 제조업 환경에서 활용하는 것으로 센서를 이용해 공장 안 모든 요소를 유기적으로 연결하여 데이터를 수집 및 분석한다. 예를 들어, 불량 원인을 예측하여 불량률을 줄이며, 숙련공의 경험을 데이터화하여 비숙련공에게 제공한다. 또한, 고객 맞춤형 상품을 제작하는 등 업무의 효율성을 증대시킨다.

민감한 정보를 담고 있는 만큼 스마트 팩토리의 가장 중요한 요소는 보안이지만 외부 악성코드의 침입, 직원의 관리 소홀, 시스템의 부실 등 아직은 보안에 취약한 것이 사실이다. 스마트 팩토리의 보안 기술은 연구 및 개발 중으로 스마트 팩토리의 상용화는 얼마나 강력한 보안 기술이 적용되느냐에 따라 그 시기가 결정된다고 볼 수 있다.

본 논문은 스마트 팩토리의 보안 사고의 개념과 유형에 관해 설명하고 다양한 유형의 보안 사고를 유발시키는 취약한 부분을 구체화하여 스마트 팩토리 보안 연구의 방향성을 제시하고자 한다.

Ⅱ. 본론

1. 보안 사고의 유형

보안 사고란 조직의 업무에 영향을 미치는 승인되지 않은 정보 자산에 대한 접근, 변경, 유출 등의 사건을 말한다[1]. 바이러스나 악성코드 감염으로 인한 피해, 또는 허락되지 않은 기기의 접속으로 인한 유출 등 그 사례가 매우 다양하며 사물인터넷(Iot, Internet Of Things)에 기반을 둔 기술로 스마트 팩토리 분야에서도 보안 사고를 막기 위해 다양한 노력을 기울이고 있다.

보안 사고는 일반적으로 14개의 공격 유형과 5개의 대상 분야로 분류된다[2]. 대표적으로 '웜과 바이러스'와 'Dos 및 분산 Dos(DDoS)', '방화벽의 부적절한 사용', '비인가 된 접근'이 자주 발생 된다. '웜과 바이러스'에서 웜은 기기 안에서 무한정 증식하며 자원을 낭비시켜 기기의 성능을 저하시키거나 데이터를 직접 파괴하기도 한다. 바이러스는 데이터를 직접 파괴할 뿐 스스로 증식하지는 않는다. 'Dos 및 분산 Dos (DDoS)'는 대량의 데이터를 지속적으로 송신하여 네트워크에 부하를 발생시키는 공격 유형이다. '방화벽의 부적절한 사용'의 경우 방화벽이 적절하게 설계되지 않아 생긴 보안 취약점이다. '비인가 된 접근'은 공격자가 기기에 비인가 된 접근을 시도한 후 접근 권한을 탈취하여 조작함으로써 물리적 손상 등을 입히게 할 수 있다[3]. [그림1]을 통하여 위에서 설명한 공격 유형과 대상의 연결성을 알 수 있다.

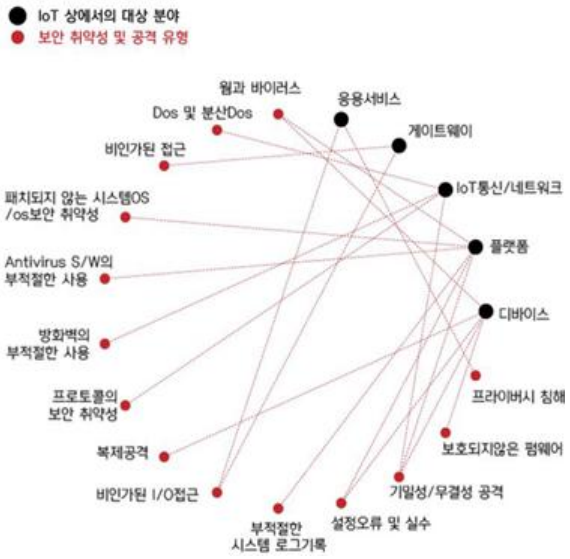

Fig. 1. 스마트 팩토리 보안 취약성 및 공격 유형[2]

2. 보안 사고의 사례

Table 1. 산업 제어 시스템 공격 사례

시기	국가	공격 대상과 형태 및 피해
2001년	호주 퀸즈랜드	폐수처리 제어시스템 외부 원격접속을 이용한 시스템 조작, 오작동 유발하여 폐수 무단 방출
2003년	미국 플로리다	CSX 철도회, 멀웨어 'sobig'에 감염되어 철도 신호체계 정지. 복구 과정 동안 열차 운행 중단
2009년	미국	병원 냉난방공조(Heating, Ventilation, Air Conditioning; HVAC) 시스템 침입
2010년	이란	나탄즈(Natanz) 우라늄 농축시설 유지보수를 위한 데스크톱에 악성코드 'Stuxnet' 감염, 1,000여 개의 부품 고장 및 교체
2012년	사우디 아라비아	국영정유회사 사우디 아람코(Aramco) 악성코드 'Shamoon' 감염, 네트워크 및 사내 컴퓨터 마비 일시적인 석유 판매 중단 조치.
2014년	한국	한국수력원자력(KHNP) 이메일 피싱에 의한 원자력 발전소 도면 유출.
2015년	우크라이나	전력제어시스템 악성코드 'Black Energy'에 감염, 전력망이 마비되어 6시간에 걸친 광범위한 정전 발생
2016년	한국	한국철도공사(Korail) 피싱 메일, 직원을 대상으로 계정과 비밀번호를 탈취하려는 메일이 유포
2016년	미국 미시건	미시건 주의 전기와 물을 공급하는 랜싱보드(The Lansing Board) 랜섬웨어를 통한 스피어 피싱. 내부 네트워크까지 감염이 확산, 추가 피해 발생을 막기 위해 시스템 일시 중단.
2016년	미국 샌프란시스코	시영철도시스템(MUNI) 결제 시스템 등 도시철도 시스템이 랜섬웨어 'Mamba'에 감염, 무인발급기가 마비.
2017년	일본 사야마	혼다자동차 사야마 공장 랜섬웨어 'WannaCry'에 감염되어, 8시간에 걸쳐 공장가동 중단

[표1]은 최근의 주요 산업 제어 시스템 공격 사례이다[3][4][5][6][7]. 보안 사고의 사례로 대표적인 예시는 바로 '스턱스넷(Stuxnet)'으로 스턱스넷은 'Stuxnet'이라는 코드가 반복되어 이름 붙여졌다고 한다. 2010년 이란 나탄즈 핵시설을 공격하며 바이러스의 존재가 널리 알려지게 되었다. 웜 바이러스에 의한 악성코드 감염사례로 네트워크의 보안 취약을 주원인으로 꼽을 수 있다. 국가적인 규모로 행한 바이러스인 만큼 피해도 컸는데, 행정 안전부의 발표에 의하면 나탄즈 핵시설에서는 우라늄 농축시설이 수차례 오작동하였고, 중국 600만 PC가 스턱스넷에 감염되었다고 한다[6][7]. 또한, 2016년 12월에 발견된 미라이 봇넷의 IoT 기기 겨냥 대규모 분산서비스거부 공격 이후로 랜섬웨어까지 진화한 사례가 있다.

단순한 IoT 기기 해킹에서 '좀비PC'처럼 전체 네트워크를 마비시키는 악성 바이러스까지 출현하고 있다. 이러한 디바이스 바이러스 중 가장 큰 문제는 IoT 기기의 특성에 기반한다. 일반 디바이스와 다르게 IoT 기기는 좀비화되는 확인이 불가능할 뿐만 아니라, 공격자들의 목표는 단순 금전 목적이 아닌 네트워크 마비 목적이 강하다. 따라서 IoT 환경은 네트워크 보안에 대한 중요성이 더욱 필요한 상황이다.

IoT의 비슷한 기술을 사용하는 스마트 팩토리도 안전하다고 할 수 없다. 대부분은 제조업체가 취약점에 대응하지 못하고 있고, 정부도 침해 대응 가이드라인 제정과 권고 수준에 그치기 때문에 공격을 실질적으로 방어할 수 있는 보안의 필요성이 보다 요구된다.

III. 이상적인 센서 네트워크의 보안 방법

일반적인 측면에서 방화벽 시스템의 주요 목적은 내부 네트워크의 보호이다. 스마트 팩토리는 센서 데이터들이 내부 네트워크에서 교환되기 때문에 방화벽이 가장 적합한 모델의 센서 네트워크 보안 방법이라고 판단된다. 하지만 구현과 설치에 있어서 보안성과 편리성, 유지보수를 고려할 수밖에 없다. 이에 따라 그 비용 역시 설계에 따라 차이가 발생하여 기술적으로나 비용 면에서 도입에 어려움이 있을 수 있다. 그러므로 필요한 부분과 불필요한 부분을 구별하여 구현하기 위해서는 비용과 노동이 요구되기 때문에 이런 비용적인 부분을 최소화하는 노력이 수반되어야 한다.

내부 네트워크 보호 전에 중요하게 다루어져야 할 단계가 있다. 특정 권한을 획득할 수 있는 인증 단계이다. 보편적으로 특정한 권한의 획득은 사용자를 인증하는 절차를 거쳐 이루어지게 되는데, 이때 사용자 확인을 위한 방법은 분실이나 복사, 유출의 우려가 있는 패스워드 방식보다는 물리적 장치와 신체정보를 결합한 지문 인식 시스템과 홍채 인식 시스템 등이 보안에 더 도움이 된다. 보안을 위한 각각의 인증 방법은 저마다의 장·단점이 있기에 독립적으로 적용하기에는 운영 및 효율성에서 한계가 발생한다. 따라서 두 가지 이상의 보안 요소를 결합하여 네트워크 침투를 어렵게 만들어 보안 기능을 강화하는 것이 바람직한 방법이다. 생체 인식 시스템과 방화벽 두 가지 보안 요소를 결합한 방법이 [그림2]이다.

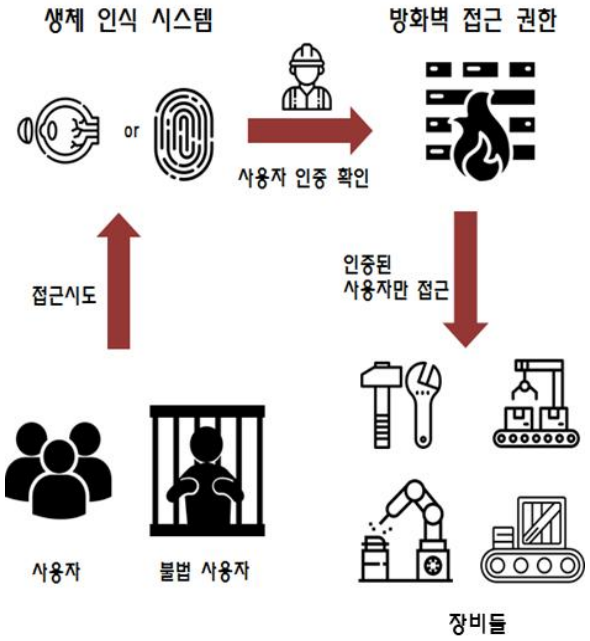

Fig. 2. 이상적인 보안 방법 제안

접근을 시도한 사용자의 지문 및 홍채 인식을 통하여 불법 사용자가 아니라는 것을 확인하면 방화벽의 접근 권한을 준다. 인증된 사용자만 이 장비에 대한 접근을 허락받는다.

미국 및 유럽의 산업 IoT에서 의미 있는 보안 수준에 도달하는 데는 5년 이상 소요될 가능성이 크다고 예측한다. CyberX가 미국과 유럽의 산업 현장 375개를 대상으로 조사한 2017년도 보고서를 보면 관련 산업 일선에 있는 공장의 보안 실태는 다음과 같다[8][9].

Table 2. 미국과 유럽의 산업 현장 보안 실태

번 호	내 용
1	산업 조직의 60%는 암호가 OT 네트워크에서 암호화되지 않은 상태로 통과하는 것을 허용하고 있다.
2	산업 조직의 50%가 백신 소프트웨어를 가동하지 않는다.
3	산업 조직의 82%는 디지털 정찰에 취약한 원격 관리 프로토콜을 사용하고 있다.
4	산업 조직의 75%는 적어도 하나 이상의 제어장치가 마이크로소프트에서 더이상 추가적인 보안 패치를 제공하지 않는 구형 윈도우에서 실행되고 있다.

그것들보다 더 큰 문제점은 스마트 팩토리에서 사용하는 센서의 특수 칩의 표준 규격이 생산하는 업체마다 다르므로 표준화된 보안을 만드는 데 어려움이 있다. 따라서 칩 내부의 보안을 통합하는 방법을 추진하고 있다고 한다.

IV. 결론

스마트 팩토리는 국내에서 전문 노동력의 감소와 근로 시간 단축 등의 원인으로 한계에 부딪힌 제조업을 발전시킬 중요한 방안이다. 하지만 비인가 된 기기의 접근, 악성코드의 침입 등으로 인한 보안의 문제 대두되고 있다. 실제 전 세계에서 다양한 보안 사고의 사례가 있었으며, 이것을 통해 네트워크에서 보안의 취약점이 가장 크게 드러난다는 것을 알 수 있었다. 따라서 지문 인식 및 홍채 인식과 더불어 방화벽 기술을 함께 사용하여, 보다 보안을 강화하였다.

미국과 유럽에서는 센서에 들어가는 특수 칩을 표준화하여 보안을 강화하는 방안을 노력해 보고 있다.

따라서 비교적 개방이 쉬운 센서 네트워크의 공격 위협을 조기에 찾아내고 방지할 수 있는 보안 방법에 관한 연구가 추후 필요할 것으로 보인다.

ACKNOWLEDGEMENT

이 논문은 2018년도 정부 (과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (NRF-2017R1A2B1007015).

REFERENCES

[1] KISA and CONCERT(Consortium of CERTs), *"CERT Deployment and Operations,"* pp.1-150, 2010.

[2] S.H.Hong, *"A Study on the Development Strategy and Enhancement of Smart Factory,"* MOTIE(Ministry of Trade and Industry), pp.138-140, 2015.

[3] M.G.Kang, *"Status and difference in security perspectives on IT, IoT, and ICS,"* IITP(Institute for Information & communications Technology Promotion) Weekly Technology Trends, pp.2-14, 2017.

[4] MSS(Ministry of SMEs and Startups), *"Technology Roadmap for SME - Data Protection,"* MSS, pp.253, 2017.

[5] Security Attacks, *http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=24472*

[6] J.J.Heo and S.C.Lee, "A Study on the infection route and Countermeasures of 'Stuxnet,'" Review of KIISC, Vol. 21, No. 7, pp.23-29, Nov. 2011.

[7] Ministry of the Interior and Safety, *"A Study on the Emergency Measures to Stop the Infection of Stuxnet in main information and communication facilities,"* Ministry of the Interior and Safety, pp.1-6, 2010.

[8] CyberX, *"Global ICS & IIoT Risk Report,"* CyberX, pp.3-4, 2017.

[9] IIoT Security, *https://semiengineering.com/why-iiot-security-is-so-difficult/*.
[10] Zombi IoT, *http://www.etnews.com/20180614000119*
[11] Zombi IoT case, *http://www.etnews.com/20180613000124*