JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 19, No. 2, pp. 293-300, Feb. 2018

4차 산업 시대의 ICT 보안 변화와 CPS 보안 시스템에 관한 연구

주 헌 식
삼육대학교 컴퓨터·메카트로닉스공학부

A Study on ICT Security Change and CPS Security System in the 4th Industry Age

Heon-Sik Joo
Sahmyook University, 815, Hwarang-ro, Nowon-gu, Seoul, Korea

[요 약]

본 연구에서 4차 산업 시대에서의 보안의 트랜드 변화와 보안위협, 4차 산업 시대의 보안 시스템 등 4차 산업 시대의 보안 시스템에 대해서 나타내었다. 4차 산업 시대는 ICT에서 IoT로 CPS보안으로 위협요소가 변화되며, 이에 따른 보안 패러다임 변화와 보안 시스템도 변화하여야 한다. 특히 CPS 보안을 해결하기 위해서는 환경적 보안과 관리적 보안이 더 중요하다. 4차 산업 시대 보안은 개별시스템에 대한 맞춤형 보안으로 변화하여야 제품 생산 설계에서 하드웨어와 소프트웨어가 융합된 보안 기술이 개발 초기부터 변화하여야 한다고 제안한다. 4차 산업의 보안 시스템은 네트워크와 같은 단일 시스템에서의 보안 시스템에서 개별시스템으로 다양한 기기들과 플랫폼들을 수용할 수 있는 보안 시스템으로 CPS 보안 시스템으로 설계 및 구현을 제안한다.

[Abstract]

This study explored the security of Industry 4.0 such as security trends and security threats in Industry 4.0, and security system in Industry 4.0. The threat elements in Industry 4.0 are changing from ICT to IoT and to CPS security, so security paradigm and security System should change accordingly. In particular, environmental and administrative security are more important to solve CPS security. The fourth industry-age security should change to customized security for individual systems, suggesting that the security technology that combines hardware and software in product production design should change from the beginning of development. The security system of the fourth industry proposes design and implementation as a CPS security system as a security system that can accommodate various devices and platforms from a security system in a single system such as a network to an individual system.

색인어 : 4차 산업 , 보안, 사물인터넷, 정보통신 기술, 사이버-물리시스템

Key word : Industry 4.0, Security, Internet of Things, Information Communication Technology, Cyber Physical System

http://dx.doi.org/10.9728/dcs.2018.19.2.293

Received 22 November 2017;**Revised** 13 February 2018
Accepted 26 February 2018

***Corresponding Author; Heon Sik Joo**

Tel: +82-2-3399-1788
E-mail: hsjoo@syu.ac.kr

Ⅰ. 서 론

4차 산업 시대는 3차 산업혁명(ICT)을 기반으로 한 디지털과 바이오산업, 물리학 등의 경계를 융합하는 기술혁명이다. 4차 산업 시대는 3차 산업의 기반에 인공지능(AI), 로봇 등 실제와 가상이 통합되어 사물을 자동적, 지능적으로 제어할 수 있는 가상 물리 시스템 구축이 기대되는 산업이다[1, 2]. 즉, 제조업과 정보통신기술을 융합해 사물인터넷(IoT; Internet of Things)[3], 인공지능, 빅 데이터, 클라우드, 무선통신 등이 4차 산업 시대의 주요 기술이다[4]. 4차 산업 시대는 인간과 사물간의 연결성이 확대되고 인공지능과 빅 데이터의 연계 및 융합으로 지능화될 것으로 전망한다. 4차 산업 시대는 인간의 삶의 질 향상, 새로운 형태의 일자리 창출, 노동생산성 향상 등의 많은 긍정적인 효과 나타낸다고 볼 수 있다. 이러한 4차 산업 시대 산업은 3.0 기반의 ICT의 기술을 기반으로 발전하여 CPS(Cyber-Physical System)으로 발전하였고, 인터넷기술과 네트워크 기술, 그리고 모바일 기술을 사용하여 편리성과 산업적 효과가 크게 상승한다. 이러한 편리성과 산업적 혁명에 함께 보안 위협 측면도 고려하여야 한다[5]. 과거 보안에 대한 서베이로 3차시대 보안이 ICT 보안으로 일반적인 보안 특성을 가지고 있다면 4차 산업 시대의 보안은 CPS 보안으로 개별 보안 시스템을 제안한다. 따라서 본 연구에서는 4차 산업 시대의 보안 변화와 보안 위협 그리고 새로운 4차 산업 보안은 CPS 보안 시스템을 제안 한다.

Ⅱ. 3차 산업 시대의 ICT 보안 트랜드

2-1 3차 산업 시대의 ICT 보안 변화

4차 산업 시대는 제 3차 산업혁명인 ICT 기반에서 발전하였다. ICT의 발전은 디지털 혁명으로 디지털, 바이오, 물리학 등 산업융합기술과 로봇, 인공지능(AI), 가상현실 등과 같은 통합과 사물을 자동적이고 지능적으로 제어하는 가상 물리시스템을 구축하였고, 기업들이 제조업과 정보통신 기술을 융합하여 작업 경쟁력을 갖게 한다[6]. 제 3차 산업 혁명은 전자, IT를 중심으로 정보화와 데이터를 중심으로 발전하였다. 이러한 배경에서 4차 산업 혁명은 사물인터넷, 인공지능, 빅 데이터, 클라우드, 무선 통신 등 3차 산업과 공존하면서 4차 산업혁명의 주요 기술로 발전하였다[7]. 각 산업별 발전을 이룩하였는데 그 산업의 중심을 그림 1과 같이 각 산업의 중심 변화로 나타내었다.

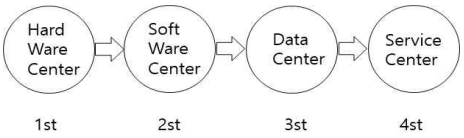

그림 1. 산업 발전에서 중심 변화
Fig. 1. Central change in industrial development

이렇게 중심 변화로 발전하였으며 좀 더 구체적으로 산업적 발전을 1차 산업으로부터 4차 산업 발전까지 그 특성들을 분류하여 나타내면 표 1과 같다. 4차 산업은 인간과 사물간의 연결성을 확대하고, 인공지능과 빅 데이터를 융합하여 지능화로 산업구조가 발전하고 있다.

표 1. 산업 발전의 특성 분류
Table. 1. Classification of characteristics of industrial development

Classify	1st	2st	3st	4st
Motive	Steam	Electricity	Electronics IT	CPS
Core Keyword	Mechanization	Industrialization	Informationization	Intelligent Hyper Connected
Core Success	Resource	Capital	Data	Knowledge
Labour Viewpoint	Simple Physical Work Labour Replacement	Main Physical Work Labour Replacement	Simple Knowledge Labour Replacement	High Class Knowledge Labour Replacement
Source Character	Possession	Possession	Open	Sharing

2-2 3차 산업 시대의 보안

3차 산업은 정보혁명으로 데이터를 핵심 요소로 하여 지식발전을 도모하였고, 기술력과 프로그램들을 공개적으로 사용할 수 있도록 하여 보다 크나큰 발전을 이룩하였다. 이러한 발전과 더불어 보안 위협도 그 만큼 더 커졌다. 3차 산업혁명 보안은 ICT 보안이다. ICT 보안은 크게 모바일 보안, 클라우드 보안, 빅 데이터 보안, 사물인터넷 보안으로 분류할 수 있다[8]. 무선과 유선으로 네트워크 보안으로 구분 할 수 있다.

1) 모바일 보안

모바일 보안에서 가장 대표적인 것은 스마트보안이다. 스마트 기기를 대상으로 한 해킹이나 악성코드 감염 등 위협이 증가하고 있다. 모바일 악성코드의 주요 특징은 통화 기록이나 전화번호, 사진 등의 개인 정보 탈취나 비정상적인 트랙픽을 유발하여 과다 요금을 유도하거나 배터리를 소진하게 한다. 휴대용 단말이 가지는 특성에 따른 몇 가지 보안 위협이 있다.

스마트 단말기의 보안 위협은 스마트폰 단말기의 도난 분실로 인한 개인정보 또는 업무 정보의 유출, 불법 과금 발생, 업무용 서버에 불법 접속하여 업무정보 유출, 스마트폰 소유자가 악의적으로 업무 정보의 외부유출 가능성이다.

네트워크 보안 위협은 스마트폰을 와이파이 등의 무선 인터넷에 접속하여 사용함에 따라 무선 구간에서 패스 스피닝, 상용인터넷망을 통한 해킹, 스마트폰을 경유하여 인트라넷 서버에 접속, 모바일DDoS 등의 보안 위협 발생이 있다[9].

응용서비스 보안 위협은 모바일 SMS, 뱅킹, VOIP 등 이용으로 해킹, 서비스중단, 사회공학적 공경이 증가할 수 있다.

또한 악성코드 감염이나 악의적 목적으로 앱으로 인해 위치, 개인정보유출 등의 사생활 침해가 발생할 수 있다.

모바일 콘텐츠 위협은 뉴스, 방송, 음악, 라디오, 영화 등 콘텐츠 DRM해킹, 모바일 스팸, 불법 유행 콘텐츠 유통 등의 위협이 있다.

2) 클라우드 보안

클라우드 서비스는 기존 IT 환경의 보안 위협과 클라우드 특성에 따른 가상화, 다중 임차, 원격지에 정보 위탁, 사업자 종속, 모바일 기기 접속, 데이터 국외이전, 침해사고 대형화, 데이터센터 안정성 등 신규 공격 위협이 존재한다. 또한 가상화의 구조적 특성 인식 한계, 하이퍼바이저 루트키트 등 진화하는 악성코드 탐지한계, 빈번한 자원변동 및 물리적 자유 공유 특성으로 인한 가상머신 보안관리 어려움이 존재한다. 클라우드 환경에서는 가상화 플랫폼의 하이퍼바이저를 통해 가상서버가 상호 연결된 구조적 특성에 따라 신규 공격 경로가 존재할 수 있으며 특권을 가진 사용자의 접근 제어, 데이터 무결성, 데이터 분산관리, 서비스의 가용성 보장 등이 중요한 보안 요소이다.

3) 빅 데이터 보안

다양한 IT서비스와 플랫폼이 등장하면서 엄청난 양의 데이터가 생산되고 있다[10]. 이른바 빅 데이터 시대가 도래 했다. 모바일 기기의 진화와 트위터, 페이스북 등과 같은 소셜 네트워크 서비스의 출현으로 기업들의 기업 내 데이터가 폭발적으로 증가하고 있다. 이러한 데이터의 생성에서 장시간에 걸쳐 목적을 가지고 공격하는 지능형지속위협이 발생 할 수 있다. 빅 데이터의 생성 및 수집 과정에서 신뢰성 및 무결성의 우려가 있다. 빅 데이터들은 개인 IT 단말기를 통해 생성되고 수집되는 과정에서 의도하지 않게 개인정보가 노출되거나 개인 데이터가 무분별하게 사업적으로 이용될 수 있고[11], 사용자 인증, 접근 제어, 데이터 기밀성, 무결성, 프라이버시 침해, 물리적 침입, 네트워크 보안 등의 문제가 발생할 수 있다.

4) 사물인터넷 보안

스마트 홈, 스마트 의료, 스마트 카 등 IoT 서비스가 일상생활로 되면서 기존 사이버세계의 위험이 현실세계로 전이 확대 되었다. 기존 PC, 모바일기기 중심의 사이버 환경과 달리 IoT 환경은 보호대상, 주체, 방법 등에 있어 새로운 정보보호 패러다임으로 접근이 필요하다. 사물인터넷은 여러 가지 요소기술들이 통합되어 특정 서비스를 구성하기 때문에 각 요소기술 자체의 보안 취약점과 연동시 새로운 보안 취약점이 발생할 가능성이 매우 크다. 그림 2는 IoT의 응용분야를 나타낸다.

사물인터넷 보안은 센서/디바이스 영역, 네트워크 영역, 플랫폼/서비스 영역으로 분류할 수 있는데 이에 따른 각각의 보안 위협을 나타낸다.

센서/디바이스 영역 보안은 저 사양 기기 사용이 늘어나면서 저 사양 기기에 보안 기능을 적용하기 고난하다. 또한 디바이스 관리 취약으로 디바이스 수가 증가하여 보안 패치가 곤란하고 모니터링에 어려움이 있다.

네트워크 영역 보안 위협은 이종무선 네트워크 간 상호 연동이 되면서 일정한 보안 수준을 유지하기 어렵고 디바이스 간 통신이 지연되면서 디바이스 인증이 제한적으로 지원된다.

네트워크 트래픽 공격량 급증인데 클라우드 가상화 서비스를 통한 감염PC 대량 생산, 냉장고, 청소로봇 등 대규모 디바이스에 악성코드를 감염시켜 트래픽을 폭증시키는 공격 발생이 일어난다.

플랫폼/서비스 영역보안 위협은 공개 플랫폼을 통한 기기, 서비스 간 허위 데이터 전송 및 오작동 등의 공격이 발생할 수 있다. 또한 사용자 신원정보유출/추적인데 이는 IoT 디바이스가 수집한 단편 정보의 중앙 집중 및 조합으로 사용자 신원정보가 유출 우려가 있다.

새로운 ICT 기술이 등장하면 이에 대한 신종 위협이 나타나고, 이에 대응하기 위한 보안 기술이 개발된다. 문제는 ICT 기술이 급속도로 발전하는데 비해 보안 제품과 방법론이 새로운 ICT 환경 변화에 못 미친다는 것이다. 따라서 보안 위협과 이에 맞서는 대응 기술과 보안 전략이 점점 더 벌어지고 있다. 그래서 새로운 시대에는 신종 보안 위협에 대응하기 위한 보안 모델부터 다시 재고하여야 한다. 이를 위해서는 보안의 대상과 목적의 보안 패러다임의 변화이다. 또한 보안 아키텍처의 변화이며 보안 기술의 변화 등이 필요하다.

그림 2. 사물인터넷 응용분야
Fig. 2. Things Internet Applications

Ⅲ. 3차 산업시대의 보안 및 대응 전략

3-1 3차 산업 시대의 보안 변화

새로운 ICT 기술이 등장하면 이에 대한 신종 위협이 나타나

고, 이에 대응하기 위한 보안 기술이 개발된다. 문제는 ICT 기술이 급속도로 발전하는데 비해 보안 제품과 방법론이 새로운 ICT 환경 변화에 못 미친다는 것이다. 따라서 보안 위협과 이에 맞서는 대응 기술과 보안 전략이 점점 더 벌어지고 있다. 그래서 새로운 시대에는 신종 보안 위협에 대응하기 위한 보안 모델부터 다시 재고하여야 한다. 이를 위해서는 보안의 대상과 목적의 보안 패러다임의 변화이다. 또한 보안 아키텍처의 변화이며 보안 기술의 변화 등이 필요하다.

3-2 3차 산업 사회의 보안 위협과 대응

인터넷을 사용하기 위해서는 네트워크 장비들을 사용하는데 라우터는 송신 정보를 패킷을 사용하여 위치를 추출하고 그 위치에 대한 최적의 경로를 지정하여 패킷을 전송한다. 스위치는 네트워크 단위들을 연결하는 통신장비로서 데이터가 컴퓨터에 잘 전송될 수 있도록 한다. 라우터나 스위치도 보안 장비로서 보안 기능을 적용 한다. 이보다 더 강하된 보안을 적용하기 위해서는 방어벽(Firewall)을 사용 한단. 방어벽은 외부 네트워크로부터 내부 네트워크를 보호하는 보안 장치로 외부 네트워크와 내부 네트워크 사이의 불법적인 접근이나 내부 사용자의 외부 네트워크에 대한 접근을 통제하기 위해 사용한다. 또 다른 보안 장비로 침입차단시스템을 사용하여 침입을 탐지 하는 방법으로 특정한 종류의 공격을 탐지하거나 비정상적인 트래픽을 찾아내고, 기밀성, 무결성, 가용성을 저해하는 일련의 행위들의 집합과 정보시스템의 보안정책을 파괴하는 행위들을 탐지하여 정보시스템을 보호한다[12]. 따라서 침입탐지 시스템과 함께 침입방지시스템을 설치하여 보다 안정적인 보안시스템을 구축하고 보안 솔루션을 적용하여 네트워크 보안을 구성하는데 그림 3과 같이 네트워크 보안 시스템을 전략적으로 대응하여 운영한다.

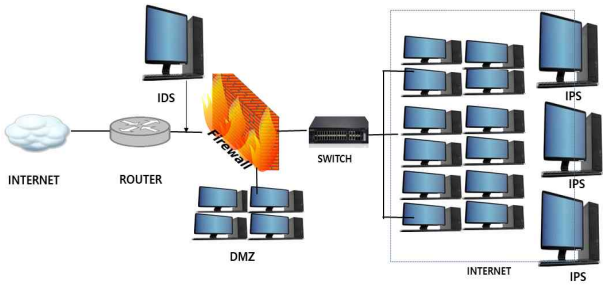

그림 3. 3.0 네트워크 보안 시스템
Fig. 3. 3.0 Network Security System

Ⅳ. 4차 산업 시대의 CPS 보안 시스템

4-1 4차 산업 혁명 시대의 CPS 이해

CPS는 사이버 상에서 물리적 환경 정보(데이터) 처리 결과를 현실의 시스템 혹은 프로세스를 제어하는 고신뢰 시스템(Dependable Systems)개념이다. 그림 4와 같이 융합 및 환경 변화로 모든 사람의 지식, 모든 사물데이터, 모든 프로세스를 인터넷 기반으로 사람과 사물, 공간, 사건들을 초 연결하여 지능적으로 물리적 시스템과 사이버 시스템을 통합 하여 제조 형태 및 인류 생활에 가치를 창출한다. CPS는 Iot, 5G, AM, Robot, AI를 처리 가공하여 빅 데이터를 처리하며, 다양한 임베디드 기기와 물리시스템의 정보를 연산 후 다시 연산결과를 물리시스템에 영향을 미치는 피드백 시스템(feedback system)기능을 갖는다.

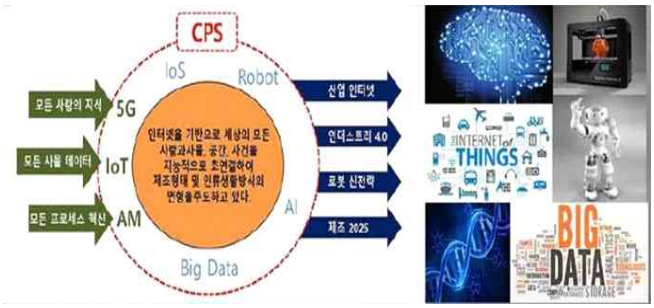

그림 4. CPS 융합 및 환경 변화
Fig. 4. CPS convergence and environmental change

4-2 CPS 시스템 구성

CPS 시스템을 그림 5와 같이 5가지 레벨 단계로 기능적 구성을 갖는다. 맨 하단 스마트 연결 레벨에서는 플러그앤 플레이로 센서 네트워크로 연결한다. 데이터 정보 변환레벨은 스마트 분석, 다중 차원 데이터 정합, 네트워크로 연결된 데이터 추출, 추출된 데이터 조작한다. 사이버레벨에서는 데이터 마이닝, 메모리 식별한다. 인식레벨에서는 시뮬레이션과 통합, 시각화, 의사결정을 진단하고 협업한다. 환경 설정 레벨에서는 탄력적으로 환경 설정하고, 변화, 장애 최적화를 한다. 따라서 사이버 시스템과 물리시스템의 유연한 연결, 물리시스템 제어 및 모니터링, 안전성 확보 등의 기능 들이 원활하도록 한다.

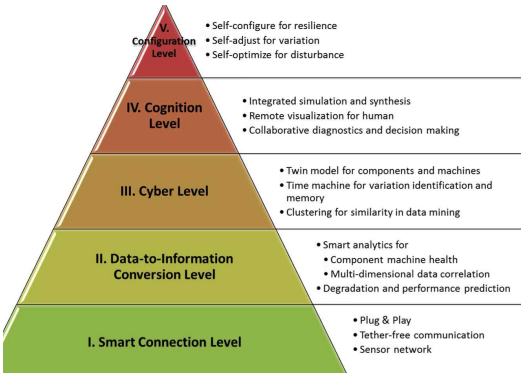

그림 5. 사이버-물리적 시스템 구조
Fig. 5. CPS System Architecture

4-3 4차 산업 혁명 시대의 CPS 보안

4차 산업 시대 보안은 단일 시스템에서 균등한 데이터가 생산되는 것과 다른 사이버 세상과 물리적 세상을 연결하는 사이버 시스템, 데이터, 시설들로 사회기반 시설뿐만 아니라, 인터넷에 연결된 기기, 사람들까지 보호해야 할 대상으로 확대된다. 단순한 데이터 보호(Protection)가 아니라 사람과 환경에 대한 안전(Safety)까지 고려하는, 전체적인 보안 패러다임변화로 확대 된다[13]. 따라서 사이버와 물리적 시스템에서 다양한 보안 위협 발생 요인을 그림 6과 같이 갖고 있다.

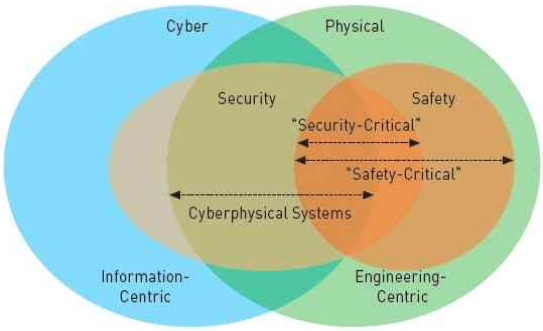

그림 6. 사이버-물리적 보안 위험
Fig. 6. CPS System Security risk

4차 산업 시대는 인공지능, 사물 인터넷 등이 중요 이슈인데 사이버 보안 위협 대한 충분한 인지가 되지 않고 있다. 4차 산업 시대 시대의 보안은 보안 관점의 변화이다. 현재의 보안은 ICT 시스템 중심으로 시스템과 데이터로 기술적 위협요소로서 하드웨어, 소프트웨어, 매체, 통신, 전자파 중심의 보안이다. 4차 산업 시대 보안은 인터넷과 디지털이 물리적 영역으로 융합되는 물리적 위협이 더 비중이 높다[14]. CPS 보안은 사이버 영역과 물리적 영역의 보안으로 현실 세계와 가상의 보안 문제라고 볼 수 있다. 따라서 보안 인증과 위협 탐지 등의 조치가 필요하다.

4-4 4차 산업 시대의 IoT 보안 위협

4차 산업 시대에서의 보안은 보안 위협의 경계가 모호해지고 있다고 볼 수 있다. ICT 기술들을 하나하나 떼어놓고 보기 어려울 정도로 유기적으로 관계로 되어 있다. IoT 기기를 이용해 DDoS 공격을 감행하는 등 복합적인 사이버 공격이 발생하고, 기밀 정보 유출에서 사회기반시설 파괴, 사람의 생명 위협까지 보안 위협이 확장될 수 있다. 4차 산업 시대 혁명 시대의 보안 위협을 몇 가지 살펴본다.

1) IoT 보안 위협

사물인터넷(IoT) 기기를 사용하여 사이버 공격으로 보안 위협을 한다. IoT 기기는 경량으로 운영체제(OS)와 인증 방식에 취약함을 가지고 있다. 보안이 취약한 사물 인터넷 기기를 좀비로 만들어 네트워크를 통한 봇넷(BotNet) 공격을 실시한다. IoT 보안 취약점은 관리자 계정에 설정된 단말을 초기 패스워드로 로그인을 시도 및 접속하여 악성코드를 유포하고, 악성코드에 감염된 IoT 기기는 해커의 명령에 따라 그림 7과 같이 DDoS 공격을 수행하도록 한다[15]. IoT 기기의 보급은 더욱 가속화되고 있으며, 스마트 생산, 물류, 서비스 핵심 요소로 보안 위협이 빠르게 증가 하고 있다.

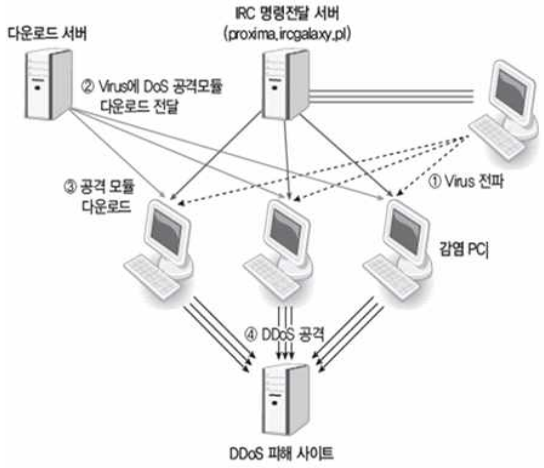

그림 7. 분사 서비스 공격 개요도
Fig. 7. DDoS Service Attack Overview Diagram

2) 가전제품 해킹 위협

가전제품에 대한 해킹 공격이다. 국내 대기업에서 생산한 스마트 냉장고가 해킹 사고를 나타냈다. 해커들은 암호화 시스템을 뚫고 기기와 인터넷망의 통신 정보를 탈취하여 공격을 하였다. 스마트 냉장고가 설치된 집 근처에서 제품에 등록된 사용자의 구글 계정에 대한 정보화 권한을 획득할 수 있는데 이러한 공격으로 인해 사생활 침해는 물론 개인정보와 금융정보까지 탈취할 수도 있다.

3) 자동차 해킹 위협

미국의 보안기술연구원 2명이 고속도로에서 달리는 자동차를 16km 떨어진 집에서 컴퓨터로 해킹하여 원격으로 조정하는 것을 시연해 보였다. 인터넷에 연결된 자동차가 해킹을 당하게 되면 주행 중인 운전자가 인지하지 못한 상태에서 시동, 속도, 방향 등이 원격 조정될 수 있다는 것을 나타낸다[16]. 달리는 자동차가 해커에 의해 마음대로 원격조정이 가능해진다면 탑승객의 안전 위협은 물론 자동차를 무기로 이용하여 피해를 초래할 수 있다.

4) GPS 해킹 위협

네 번째는 GPS 해킹 위협이다. 스마트카가 인공위성과 연

결되어 교통정보센터의 정보를 활용하여 목적지까지 자율적으로 도달할 수 있게 되는데 이러한 통신 과정에서도 해킹 공격이 발생할 수 있다. 인공위성은 GPS 통신을 이용하게 되는데 GPS는 일반 네트워크에 비해 보안이 매우 취약하기 때문이다. 그림 8은 GPS 보안 위협을 나타내는데 GIS와 GPS를 이용하여 해커는 GPS 통신을 해킹하여 정보를 탈취할 수 있는데 이로 인해 개인의 이동경로가 유출되어 사생활을 침해할 수 있다.

그림 8. GPS 보안 위협
Fig. 8. GPS Security Threat

4-5 제안하는 4차 산업 시대의 보안 시스템

4차 산업 시대의 보안 시스템은 3차 산업 보안 시스템과는 다른 양상이다. 다양한 디지털 비즈니스 시대로 사용자의 니즈와 각 산업영역에서 요구하는 스마트기기, 스마트제품, 스마트서비스, 스마트 플랫폼[17] 에 적용한다.

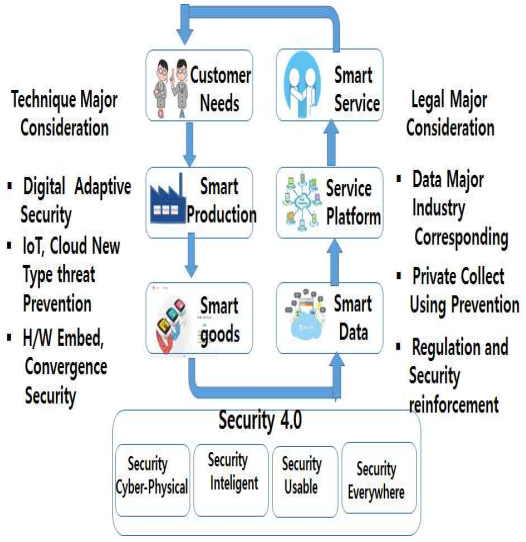

그림 9. 제안하는 CPS 보안 시스템
Fig. 9. Proposed CPS security system

사이버-물리적 보안, 지능형보안 등 기존의 ICT를 기반으로 보안은 획일화 된 보안에서 4차 산업 시대 보안은 다양한 제품 생산에 대한 개별 솔루션 중심의 맞춤형 보안으로 변화해야 한다[18]. 그림 9은 제안하는 CPS보안 시스템을 나타낸다.

그림 9는 제안하는 CPS 보안 시스템으로 사용자의 니즈와 스마트한 서비스를 제공하여야 하며 다음과 같은 고려사항을 적용하여 설계 한다.

1) 기술적 고려 사항

기술적 고려사항으로 디지털, 적응형 보안, 사물인터넷, 클라우드의 신종 위협 등이다[18, 19]. 보안 측면에서 보면 이러한 것을 수용하기 위해서는 하드웨어를 내장한 융합 보안 기술이 필요 된다. 따라서 이 고려사항은 보안의 기술이 융합적인 보안 기술이 필요 된다.

2) 법제도적 고려 사항

법제도적 고려사항은 데이터 중심 산업 변화 대응에 대한 폭 넓은 매뉴얼들이 있어서 법제도적으로 충돌이 발생하지 않아야 한다. 개인정보 수집 및 활용 보호이다. 개인 정보 보호의 중요성이 법적, 제도적으로 잘 되어 있어 문제가 발생되지 않도록 하는 것이다.

4차 산업 시대의 범위는 굉장히 넓고, 특정 산업 또는 기업에서만 사용하는 특화된 컴포넌트들이 존재한다. 따라서 기존 보안 기술에 의존하기 보다는 컴포넌트 자체에 보안 기능을 내제화하여 결과적으로 기존의 정적인 경계 보안 대신 디바이스 레벨의 마이크로한 경계 보안이 필요 하다. 특히 기존과 같은 내/외부망의 이분법적인 규정은 더 이상 유효하지 않기 때문에 보다 초미세한 구분을 통해 각각에 적합한 보안 기술과 정책을 수립해야 한다. 또한 산업 목적의 변화에 따라 새로운 시스템이 등장할 것이고, 그에 따른 새로운 보안 위협에 대한 분석과 대응 방안 마련이 중요하다. 4차 산업 보안은 다변화된 환경에서 기업과 보안 업체, 또는 보안업체와 보안업체 간에도 위협 정보를 공유하는 보안시스템 설계 등 전반적인 재설계가 필요 된다.

2) 제안하는 CPS 보안 시스템 기능

제안하는 그림 9의 CPS 보안 시스템은 Security 4.0 보안 시스템으로 사이버와 물리적 영역에 결합된 보안 기능을 수용하여야 설계한다. 제안하는 그림 9 CPS 보안 시스템은 그림 5의 CPS 시스템과 다르다. 또한 그림 3의 네트워크 보안 시스템과 다르다. 그림 9의 CPS 보안 시스템은 맨 하단 부에 사이버와 물리적 보안에 대비하기 위한 여러 보안 기능들을 가지고 있다. 따라서 네트워크 보안에서와 같은 보안시스템을 적용시킬 수 없다. 왜야 하면 CPS보안은 작은 규모의 IoT나 임베디드 기기와 같은 소형 디바이스들을 사용함으로 방화벽이나 침입탐지, 침입방지시스템을 적용하기가 어렵다.

따라서 사이버와 물리적 시스템에 지능적인 높은 수준의 안전한 보안 시스템을 구축하여야 하며, 보다 편리한 보안을 실현 하여야만 한다. 또한 어디에서나 모든 것에 보안이 가능하도록 보안 시스템을 설계한다.

CPS 보안 시스템은 스마트 데이터를 사용함으로 물리적 보안, 정보 획득 보안, 정보 전송 보안, 정보 처리 보안을 등 모든 데이터들을 수용하고 변환하면서 보안 처리를 하여야 한다. 물리적 보안의 경우, 악의적인 사용자가 환경 속에 설치된 저가의 태그와 센서에 접근하여 데이터 정보를 파악하거나 불법적인 인가작업이 할 수 없도록 안전한 암호화와 프로토콜이 사용되어야 한다. 정보 접근 및 획득에 대한 보안에서는 이기종의 기기들 간의 다중 미디어 스윙칭 기술과 위치 관리 기술로 인해 발생하는 다중 정보 접근에 대한 보안 취약성을 제거하여야한다.

서비스 플랫폼은 IoT 기기 뿐만 아니라 다양한 기기에 서비스 플랫폼을 탑재하여 다양한 플랫폼을 수용하여야 한다. IoT 기기를 사용하여 시스템의 상단부터 하단까지 발생하는 모든 문제점들을 해결하기 위해 Security 4.0과 플랫폼과 보안을 체크하도록 한다.

스마트 서비스는 사용자가 니즈한 다양한 목적에 따라 필요한 서비스를 제공한다. 따라서 고객의 니스가 요청되었을 때 스마트 생산을 하고, 스마트한 상품을 만들어 사용자의 요구에 부흥한다. 그러면서 디지털 적용 보안, IoT, 클라우드 등 새로운 타입의 보안 위협과 하드웨어 등 융합적인 보안 기술을 적용하여 CPS 보안 시스템을 구현한다.

Ⅴ. 결 론

4차 산업 시대는 기존의 ICT 산업의 보안에서 CPS 보안 형태로 변화되고 3차원 보안과 다른 패러다임 변화와 전략이 요구된다. 따라서 기존의 일괄적인 보안에서 특성에 따른 보안으로 변화하면서 보안 대상과 보안 패러다임, 아키텍처 등의 보안 기술 변화가 필요 된다. 인증, 암호화, 빅데이터 분석, 위험 평가, 탐지 등의 기술 등 현재도 존재하고 있는 기술이지만 4차 산업 시대에서는 하드웨어 또는 소프트웨어 제품의 설계 시점부터 보안 조치가 동반되어야 한다. 기존의 단순 보안 구축 및 운영, 관리가 아닌 설계, 개발, 운영에 이르는 전 과정에 보안 기술과 프로세스가 반영되는 관점으로 변화가 필요 된다. 따라서 새로운 CPS 보안 시스템을 4차 산업의 보안 대응 전략으로 제안한다. 차후 연구 과제는 실제적인 CPS보안 시스템을 구현하여 보안 위협과 안전성을 실험하는 것으로 한다.

참고문헌

[1] Jeong Hey un,"The Strategic Initiative INDUSTRIE 4.0 and IT-based ship production systems research trends", *Society for Computational Design and Engineering*, pp.333-342, 2014.

[2] Hea-Jo Kang, "A Study on Disaster Safety Management Policy Using the 4th Industrial Revolution and ICBMS", *Journal of DCS*, Vol. 18, No. 6, pp.1213-1216, 2017.

[3] Hyo-Nam Kim, "A Study on Obfuscation of the InGame Data for the Mobile Game Security", *Proceedings of the Korean Society of Computer Information Conference*, Vol. 25, No. 1, pp.179-180, 2017.

[4] Byung-Woon Kim, "The Forth Industrial Revolution", Industrial Internet of Things, *Journal of Law & Economic Ragulation* ,Vol. 9, No. 1, pp.215-232, 2016.

[5] Gu-Man Kang, Bum-Gu Lim, Joung-Han Lee, "Implementation of Palnt Object Model for the Application of Industry 4.0", *THE INSTITUTE OF ELECTRONICS ENGINEERS OF KOREA*, pp.1610-1612, 2014.

[6] Sang-Hoon Kim, Sun-Young Park, "Influencing Factors for Compliance Intention of Information Security Policy", *The Journal of Society for e-Business Studies* , Vol. 16, No. 4, pp.33-51, 2011.

[7] Cheoi yeoung su, "Information Protection and Security", *The Institute of Electronics Engineers of Korea －Computer and Information*, Vol. 47, No. 6, pp.139-139, 2010

[8] Ho-Chul Park, Ki-Hyung Kim, Joo-Yoen Lee, Gi-Nam Wang, Kang-Seok Kim, Tae-Shik Shon, "Design & Implementation of CPPS (Cyber Physical Production System) for Smart Factory, *KOREA INFORMATION SCIENCE SOCIETY*, Vol. 12, pp.838-840, 2014.

[9] Donghwi Shin, Chaetae Im, HyunChul Jung, Dongho Won, "A study on automatic static analysis method for malware analysis", *KOREA INFORMATION SCIENCE SOCIETY*, pp.84-89, 2010.

[10] Jeong-Rae Cho, Hye-Suk Kim, Doo-Keol Chae, Suk-Ja Lim, "Smart CCTV Security Service in IoT(Internet of Things) Environment", *Journal of Digital Contents Society*, Vol. 18, No. 6, pp.1135-1142, 2017.

[11] Seon-hyeok Lee, Jin-sul Kim, Jae-hyung Park, "An Efficient Protection Scheme against Distributed DoS Attacks in VANET using Bloom Filter", *Journal of Digital Contents Society*, Vol. 18, No. 6, pp.1157-1163, 2017.

[12] Heon-Sik Joo, Jong-Wan Kim, "An Efficient Management Model of Security Policy in the Unified Threat Management System", *Journal of the Korea Society of Computer and Information*, Vol. 15, No. 9, pp.99-107, 2010.

[13] Hong-Je Lee, Hyeong-Seog Kho, Eun-Hee Roh, "Kyeong-Seok Han, A Study on the Factors of Experience

and Habit on Information Security Behavior of New Services", *Journal of Digital Contents Society*, Vol. 19, No. 1, pp.93-102, 2018.

[13] Seon-Hui Bak, Jong-Ho Kim, Hyun-Bea You, "Implementation of Public data contents using Big data Visualization technology" *Journal of Digital Contents Society,* Vol. 18, No. 7, pp.1427-1434, 2017.

[14] Yongsoon Eun, Kyung-Joon Park, Myounggyu Won, Taejoon Park, Sang Hyuk Son,"Recent Trends in Cyber-Physical Systems Research", *Communications of the Korean Institute of Information Scientists and Engineers*, Vol. 31, No. 12, pp.8-15, 2013

[15] Duck-Yong Kim, "A Study on Voice Phishing Countermeasures of the Police", *Journal of Digital Contents Society*, Vol. 19, No. 1, pp.193-198, 2018.

[16] Kwon-Taeg Choi, "Neural networks optimization for multi-dimensional digital signal processing in IoT", *Journal of Digital Contents Society*, Vol. 18, No. 6, pp.1157-1163, 2017.

[17] Min-Suk Chang, Hyoung-Joong Kim, "A Customer Segmentation Scheme Base on Big Data in Bank", *Journal of Digital Contents Society,* Vol. 19, No. 1, pp.86-92, 2018.

[18] Kwang-Young Kim, Seok-Hyoung Lee, Hye-Jin Lee, Jung-Hoon Park, Jae-Wook Seol, Jin-Young Kim, Heung-Seon Oh, Jung-Sun Yoon, Seo-Young Jeong, " A Study on Knowledge Open Platform for Science and Technology Information Service:With a Focus on Data, Technology Software and Utilization-Case", *Journal of Digital Contents Society*, Vol. 18, No. 6, pp.1183-1192, 2017.

[19] Dae-Jin Kim, "Implementation of Parking Management System using Cloud based License Plate Recognition Service", *Journal of Digital Contents Society*, Vol. 19, No. 1, pp.173-180, 2018.

주헌식(Heon-Sik Joo)

1994년 : 호서대학교 대학원 (이학석사)
2005년 : 아주대학교 대학원 (공학박사-컴퓨터그래픽)

2012년～2014년: 삼육대학교 정보전산원장
1997년～현 재: 삼육대학교 컴퓨터학부 교수
※관심분야 : 모바일 콘텐츠, 정보보호 및 보안, 모바일 보안 등