www.osia.or.kr

OSIA S&TR Journal

ISSN 1738-9887 Vol. 31, No. 2, June 2018
• 발행인 : 정성호 회장/OSIA • 편집위원 : 손태식 교수/아주대학교

Editorial
02 사이버보안 기술
손태식 교수/아주대학교

Article
04 미래 환경변화와 의료보안 과제
장항배 교수/중앙대학교
10 해시함수 SHA-1에 대한 공격 그리고 그 이후
김종성 교수/국민대학교
12 디지털 포렌식 측면에서의 안드로이드 기기에 대한 데이터 수집 연구
이창훈 교수/서울과학기술대학교
18 ICS(Industrial Control System)에 적용되는 산업용 프로토콜 보안기술 현황
이건희 박사/국가보안기술연구소
23 스마트공장 사이버 위협과 보안 기술
김기현 부사장/NNSP

(사)한국컴퓨터통신연구회
Open Standards and ICT Association

사이버보안 기술



아주대학교 교수

손 태 식

현재 비트코인과 같은 블록체인 기술의 광풍이 여전한 가운데 지난 2016년 이세돌과 알파고의 대국으로 본격화된 인공지능(AI)기술을 필두로 보통 AICBM(AI, IoT, Cloud, Bigdata, Mobile)이라고 불리는 용어가 이제는 우리 삶의 한 부분처럼 일상화 되어가고 있다. 하지만 이러한 기술들이 우리 삶 깊숙이 들어오면 올수록 다양한 형태의 사이버보안 위협이 증가한다는 점은 기술의 편리한 사용에 앞서 꼭 짚고 넘어가야 할 부분이다.

본 호에서는 현재 고려되고 있는 다양한 형태의 사이버보안 이슈를 융합보안관점에서의 의료보안, ICT기술 보안에 있어 빼놓을 수 없는 기반기술인 해시함수 동향, 최근 뉴스에도 단골로 등장하는 디지털 포렌식, 전력망을 포함한 다양한 산업제어시스템에서의 보안과 마지막으로 4차 산업혁명과 함께 뜨거운 이슈가 되고 있는 스마트공장에서의 보안 기술을 소개하고자 한다.

첫 번째 논문은 “미래 환경변화와 의료보안 과제”로서 소개되는 논문으로서 공공재 비즈니스 특성을 갖고 있는 의료산업이 ICT와 밀접하게 융합함으로써 나타나는 보안 위협과 이에 대한 대응방안을 설계하고 구체적으로 의료융합산업의 실태와 의료정보의 생애주기에 따라 의료기관 외부로부터 진료, 데이터의 활용까지 시나리오를 기반으로 보안 위협과 이에 대한 기본적인 대응책을 구축할 수 있는 프레임을 제시하고 있다.

두 번째 논문은 “해시함수 SHA-1에 대한 공격 그리고 이후”로서 지난 2017년 2월 23일, 구글이 발표한 SHA-1의 충돌쌍 공격에 대한 분석과 이러한 발표로 해시함수의 취약성과 위협이IT업계 전체에 불러온 큰 파장을 설명하며 향후 해시 함수를 기본으로 사용하고 있는 대부분의 IT시스템과 보안분야에 있어서 어떠한 영향을 미칠지에 대해서 설명하고 있다.

세 번째 논문은 “디지털 포렌식 측면에서의 안드로이드 기기에 대한 데이터 수집 연구”에 대한 것으로 안드로이드 기기에 대한 디지털 포렌식 관점에서의 데이터 수집 방법, 포렌식 절차 가이드라인 등 대한 연구등 현재 활발하게 진행되고 있는 안드로이드 기기에 대한 디지털 포렌식 절차와 데이터 수집 연구들을 정리하고 향후 연구 및 한계를 소개한다.

네 번째 논문은 “ICS(Industrial Control System)에 적용되는 산업용 프로토콜 보안기술 현황”에 대한 것으로 산업제어시스템에서의 다양한 통신 프로토콜은 지금까지 주로 보안 기능이 고려되지 않고 설계되어 사용되고 있다. 이로 인해 산업제어시스템의 네트워크 트래픽을 분석하면 손쉽게 잘못된 데이터를 주입하는 것이 가능하였고, 이에 IEEE, IEC 등의 표준화 단체에서는 DNP, IEC61850, OPC UA 등의 주요 산업용 프로토콜에 대한 통신보안 규격을 개발하였으며, 본 논문에서 IEEE 1815, IEC62351, IEC62443 등에서 제시되고 있는 산업용 프로토콜에 대한 통신보안 기술의 현황에 대해서 소개하고 있다.

마지막 논문은 “스마트공장 사이버 위협과 보안기술”을 소개하고 있다. 최근 미국와 독일등 해외 주요 선진국들은 4차 산업혁명의 밑바탕으로서 제조 혁신과 경쟁력 강화를 위해 국가 차원의 전략으로 스마트공장 구축·보급 확산을 추진하고 있지만 이러한 변화의 흐름에 있어 실제 발생 가능한 사이버보안에 대한 위협들은 간과되는 경향이 있다. 본 논문에서는 스마트 공장을 포함한 다양한 산업제어시스템에 대한 사이버 위협과 전반적인 산업 보안 기술 동향을 소개한다.

바쁘신 와중에도 훌륭한 원고를 제출하여 주신 저자분들께 감사를 드리며 사이버보안 기술에 관심을 갖고 계시는 독자분들에게 관련 논문들이 도움이 되기를 기대합니다.

미래 환경변화와 의료보안 과제

김양훈[1], 장항배[2]
[1]극동대학교 산업보안학과, [2]중앙대학교 산업보안학과

요약

4차산업혁명 기반 기술이 도입된 비즈니스 환경은 새로운 융복합적인 위험요소를 발생시키고 있다. 특히, 융합된 산업의 비즈니스가 타 산업과 차별성이 강할수록 비즈니스 환경에 종속된 보안 위협들이 나타나고 있다. 실례로, 의료산업의 경우 ICT와 융합되어 다양한 보안 위험들이 나타나고 있다. 이러한 보안 위험들은 일반 PC 환경에서는 오래된 전통적인 악성코드들도 있으며, 새로운 융복합적인 위협들도 존재한다.

이에 따라 본 논문에서는 공공재 비즈니스 특성을 갖고 있는 의료산업이 ICT와 밀접하게 융합함으로써 나타나는 보안 위협과 이에 대한 대응방안을 설계하였다. 구체적으로 의료융합산업의 실태를 파악하고, 의료정보의 생애주기에 따라 의료기관 외부로부터 진료, 데이터의 활용까지 시나리오를 기반으로 보안 위협과 이에 대한 기본적인 대응책을 구축할 수 있는 프레임을 제시하였다.

1. 연구 배경

3차 산업혁명을 기반으로 한 디지털과 바이오산업, 물리학 등의 경계를 융합하는 기술 혁명인 제4차 산업혁명(Industry 4.0) 도래로 모든 사물이 연결(초연결성) 되고 보다 지능적인 사회(초지능성)로의 진화를 앞두고 있다. 이러한 진화의 과정에서 과거의 전통적인 업무환경(Legacy System)은 4차 산업혁명의 기반기술인 스마트 모빌리티(Smart Mobility), 클라우드(Cloud), 빅 데이터(Big Data), 사물인터넷(Internet of Things) 등 새로운 컴퓨팅 기술과 결합되면서 ICT 산업을 중심으로 다양한 산업들과의 융합과정이 진행되고 있으며, 새로운 가치의 융합제품 및 서비스가 산출되는 산업융합 환경으로의 변화가 예상되고 있다[14].

그러나, 4차산업혁명 기반 기술이 도입된 비즈니스 환경은 새로운 융복합적인 위험요소를 발생시키고 있다. 특히, 융합된 산업의 비즈니스가 타 산업과 차별성이 강할수록 비즈니스 환경에 종속된 보안 위협들이 나타나고 있다. 예를 들어 의료산업은 전문기기와 환경을 갖추고 있으며, 국가 공공산업의 성격을 보유함으로써 의료서비스를 중심으로 비즈니스를 수행하는 특성이 있다. 이러한 의료산업의 경우 ICT와 융합되어 병원에서 환자에게 제공한 MRI 촬영 이미지 CD에서 악성코드가 발견된 사례, 전자화된 의무기록에 대한 권한관리 미흡으로 환자의 개인정보가 유출된 사례, 오래된 운영체제를 사용하고 있으며 해당 PC에 의료기기가 연결되어 취약점에 노출된 사례 등 다양한 보안위협 사례가 나타나고 있다[9]. 이에 따라, 의료산업만의 비즈니스 환경을 고려한 융합환경에 특화된 보안기술의 필요성이 대두되고 있다[6].

이를 반영하여 의료법 시행령 제16조에 따르면, 의료인 및 의료기관에서는 전자의무기록(EMR, Electronic Medical Record)을 안전하게 관리·보존하기 위하여 전자의무기록에 대한 생성, 저장, 검증과 이력관리를 수행하고, 백업, 네트워크 및 시스템 보안 등 다양한 보안시설과 장비를 갖추도록 명시하고 있다. 그러나, 중소 의료기관 실태조사에 따르면 우리나라 중소병원 10곳 가운데 2곳은 보안 수단이 PC 백신 설치 수준에 머무른 것으로 나타났다. 전체 중소병원 10곳 가운데 2곳이 PC 백신 소프트웨어(SW) 설치 수준에 그쳤다. 데이터베이스(DB), 네트워크 보안 시스템을 구축한 비율은 각각 21.3%와 17.3%에 그쳤다. 접근 통제 권한 관리와 전자정보 암호화 시스템을 구축한 곳도 각각 31.3%, 24.6%에 불과한 것으로 나타났다[12].

본 논문에서는 공공재 비즈니스 특성을 갖고 있는 의료산업이 ICT와 밀접하게 융합함으로써 나타나는 보안 위협과 이에 대한 대응방안을 설계하고자 한다. 구체적으로 의료산업의 현황과 특성을 살펴보고, 의료융합산업 환경에서 발생가능한 시나리오 기반의 보안 위협을 도출한다. 마지막으로 이러한 보안 위협으로부터 의료융합산업을 안전하게 보호하기 위한 기존의 기술적 솔루션을 활용한 프레임워크를 제안하고자 한다.

2. 선행 연구

2.1 의료산업 현황 및 특성

의료산업은 질병방지와 건강증진을 위한 진단, 치료, 재활과정에서 사용되는 의료기술(서비스), 의료기기, 의약품, 의료조직 체계 등을 포함하는 산업을 의미하며, 최근에 발생되고 있는 사회적 환경변화에 따라 산업경계와 영역이 확대되고 있다.

이러한 의료산업은 공공재 성격을 지닌 고부가가치 산업으로써 제공되는 의료서비스 자체에 대한 "신뢰성"이 매우 중요한 가치로 여겨지고 있으며, 빠른 속도로 움직이는 사회적(고령화).경제적(산업융합) 환경변화에 따라 언제 어디서나 "지속적인" 의료 서비스를 요구하고 있다.

이러한 의료산업 변화동인은 질병(감염)관리, 의료협진, 원격의료, 의료관광 등의 주제로 나타나고 있으며, 이는 기존 "의료기관(병원) 중심의 치료 서비스 형태"에서 "환자(고객)중심의 건강관리 서비스 방향"으로 진화할 것으로 예상되고 있다. 즉, 고객중심의 상시 건강관리 지원체계로의 패러다임 변화가 나타나고 있다.

세부적으로 오진으로 인한 환자의 생명위험 가능성을 최소화하고 과잉진료 문제를 선제적으로 해결함으로써 환자(고객)중심의 맞춤형 의료서비스 제공을 위해 노력하고 있으며, 이를 위한 방법으로 다양한 분야의 업무처리를 위해 의료서비스와 IT기술 사이에 활용과 융합의 과정이 진행되고 있다. 즉, IT 활용과 융합을 통해 의료서비스에 대한 품질 고도화을 진행하고 있다.

또한, 의료기관(병원)들은 의료정보시스템(Health Information System) 도입을 통해 전자의무기록(Electronic Medical Record), 처방전달(Order Communication System), 의료영상 자료전송(Picture Archiving Communication System) 등의 기능을 포함하면서, 의료서비스 자체에 대한 고 신뢰성을 확보하여 양질의 적정한 의료서비스 제공을 추진하고 있음으로써, 가능한 범위 안에서 최신의 의학지식과 기술이 의료에 적용되는 서비스를 제공하고 있다.

그리고, 부분적인 원격협진 시스템(Telemedicine) 구축을 통하여 치료를 통한 건강 복원력을 향상시키고(의료서비스 전문성 확보) 동시에 예방적 차원의 의료서비스 지원이 가능하게 됨으로써, 의료서비스 항시성과 적시성을 확보하게 되었다. 특히, 환자(고객)중심의 체계적이고 능동적인 서비스로 대표되는 의료+IT활용(융합) 서비스는 개인화된 의료정보 수집, 의료기관(병원) 사이에 정보공유, 의료기관(병원)과 환자(고객)사이에 연결(소통) 등을 통해 혁신적인 의료 서비스로 진화하고 있다.

2.2 의료산업 보안취약 현황

의료산업과 IT활용(융합)서비스 출현에 따른 편익과 함께 의료정보 생애주기(생성~저장~활용~폐기)과정에서 다양한 정보보호 취약점(위험요소)이 발생하고 있다. 예를 들어 의료기기 오작동에 따른 의료정보 정합성 문제, 환자(고객) 개인정보 오남용, 외부로부터 의료기기에 대한 사이버 공격, 내부직원 의료정보 유출 등의 다양한 위험요소들이 지속적으로 발생하고 있다.

의료정보란 환자(고객) 이름, 성별, 연령, 사진 등의 개인 식별정보와 진료 결제내역 정보가 존재하는 통합적인 자료를 의미한다. 치료과정을 통해 수집된 개인의 의료정보는 의료기관(병원) 내 다수 부서에서 활용되며, 공적인 활용을 위해 질병관리본부, 건강보험 심사평가원, 의학 연구소 등 다양한 유관기관으로 전송되고 있다. 의료정보는 개인의 민감 정보(현재의 건강상태와 치료과정 등)로서 노출될 시에는 개인에게 정신적, 사회적, 경제적인 피해를 초래할 수 있으나, 이에 대한 의료기관(병원)의 보안수준은 매우 미흡한 상태로 나타나고 있다.

따라서 의료기관(병원)을 중심으로 의료정보에 대한 다양한 수집방법과 외부유통 경로가 존재함에 따라 의료정보 공유과정에서 "의료법"과 "개인정보 보호법" 관점의 다양한 취약점들이 발생할 수 있다. 즉, 의료정보의 안전한 처리요건을 벗어난 위법사항들이 발생가능하다는 것이다. 의료정보는 2차적 정보가공을 통해 주요 질병의 발생추이, 처방 약품 시장 현황, 진료위치 추적, 보험 상품 개발 등 다양한 목적으로 사용될 수 있기 때문에 타 산업에 비하여 의료정보 침해에 따른 사회적 비용이 매우 높은 상태이며 이에 관련된 정보보호 사고와 시장규모는 지속적으로 증가할 것으로 예상된다.

3. 의료정보 생애주기와 융합보안

3.1 의료정보 생애주기에 따른 융합보안 취약점과 보안 요구사항

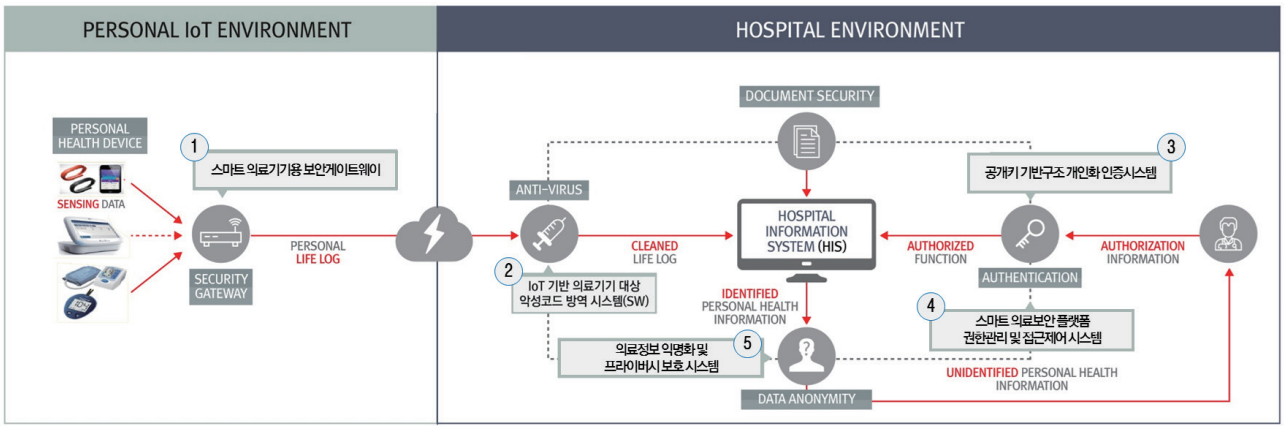
의료기관에서 활용하는 의료정보의 생성(수집)~저장~활용(내부유통과 외부제공)~폐기과정에 따른 융합보안 취약점을 분석하면 다음과 같이 나열할 수 있다. 의료정보 생성(수집)과정 보안취약점을 살펴보면, 의료정보 제공과 이용에 관하여 정보 관리자가

고의로 특정부분의 동의를 누락하거나 수집한 환자(고객)의 개인정보를 목적 이외에 용도로 사용할 수 있는 취약점이 있다. 또한 환자(고객)가 의료기관(병원) 홈페이지를 이용해 개인정보를 제공할 경우, 홈페이지 외부 공격자에 의해 시스템이 해킹당하거나 중간과정에서 개인정보가 유출당할 수 있는 문제점이 있다. 의료정보 저장과정 보안취약점을 살펴보면, 중요 정보에 대한 암호화를 누락하거나 데이터베이스에 접속한 사용자에 대한 로그기록을 놓칠 수 있는 취약점이 존재한다. 암호화되지 않은 정보는 정보 접근 권한이 없는 사람으로부터 보호될 수 없으며, 로그 파일을 기록되지 않으면 비인가 사용자에 대한 감사추적을 할 수 없는 문제점이 있다. 의료정보 활용과정(내부유통) 보안취약점은 의료기관(병원) 내부에서 각 부서로 하여금 의료정보에 대한 과도한 접근권한을 부여하거나, 접근에 대한 모니터링이 미흡하면, 직급 혹은 부서에 상관없는 내부직원(의사, 간호사, 행정직원 등)이 민감한 환자(고객) 개인정보를 열람할 수 있다는 점이다. 또한 환자(개인)정보를 저장하고 있는 의료정보시스템(홈페이지 등)에 대한 유지보수를 담당하는 외부직원(인가된 제3자)에 의한 유출 가능성이 존재한다. 의료정보 활용과정(외부제공) 보안취약점은 외부 유관기관으로 의료정보를 전송하는 과정에서 정보자체에 대한 위변조가 발생할 수 있으며(정보 암호화 누락), 의료정보 보호 범위("의료법")에 벗어나 있는 외부기관(기업) 또는 개인에게 의료정보가 불법으로 제공(저장)될 수 있다는 점이다. 의료정보 폐기과정에서는 의료정보를 수집한 의료기관(병원)과 의료정보를 제공받은 외부기관이 업무처리를 위해 정보를 사용한 후에는 의료정보를 파기해야 함에도 불구하고 파기하지 않고 저장하거나, 다른 외부기관(기업) 또는 개인에 의료정보를 제공할 수 있다.

이에 따른 의료기관의 융합보안 취약점 해결을 위한 법적, 관리적, 기술적 등의 다차원적인 융합보안 요구사항 설계하면 다음과 같다. 법적 보안요구사항으로 "의료법"은 모든 국민이 수준 높은 의료 혜택을 받을 수 있도록 국민의료에 필요한 사항을 규정함으로써 국민의 건강을 보호하고 증진하는 데에 목적을 두고 있으나, 현행 "의료법"은 과거의 종이문서 작성환경에서의 정보보호를 규정하고 있어 현재 의료IT서비스 환경에서 부적합한 상황이기 때문에, 의료정보 표준화와 함께 안전한 전자적 유통관점에서 개정될 필요가 있다. 그리고, 관리적 보안요구사항으로는 업종과 무관하게 공통적으로 적용되는 보안조직 구성, 보안교육 진행, 보안활동 규정 등에 관한 보안관리 체계와 함께, 의료기관(병원)에서 이루어지고 있는 의료행위 절차를 고려한(의료기관(병원) 내부와 함께 외부까지의 정보공유 범위가 매우 넓으며, 다양한 유형의 정보사용자가 존재) 특화된 보안관리 체계가 적용되어야 한다. 마지막으로, 기술적 보안요구사항으로는 의료정보를 다루는 의료기기와 의료정보시스템에 대한 무결성을 확보하고, 의료정보가 공유되는 환경에서 해당정보에 대한 사용자 식별과 접근통제(무단사용, 유실, 유출 등)와 함께 정보수집(생성)부터 폐기에 이르기까지 책임 있는 추적성이 확보되어야 한다.

3.2 의료기관 융합보안 체계 구축을 위한 시나리오 기반 프레임 설계

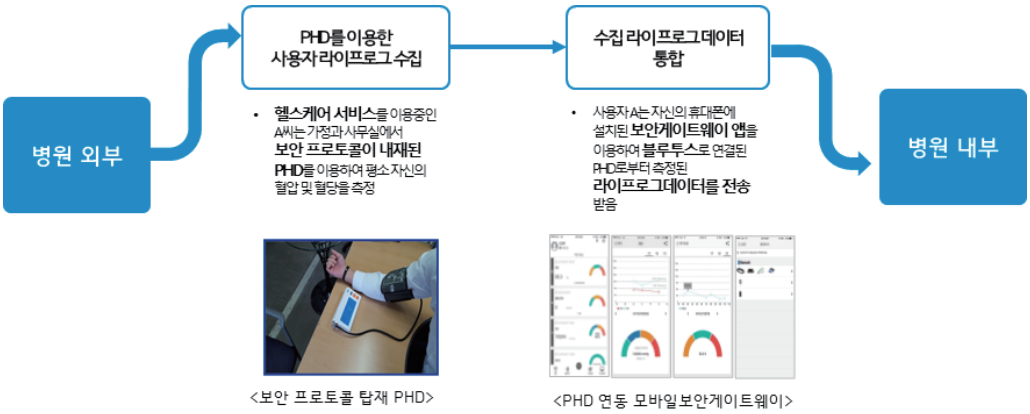
의료산업의 특성과 융합보안 취약점, 그리고 의료기관의 보안 요구사항을 분석하여 의료산업의 비즈니스를 반영한 시나리오 기반의 융합보안 프레임을 설계하면 그림 1과 같다.



〈그림 1. 시나리오 기반 의료산업 융합보안 프레임〉

위 제시한 프레임에는 기본적으로 갖추어야 할 5가지 보안기능의 시나리오는 다음과 같다.

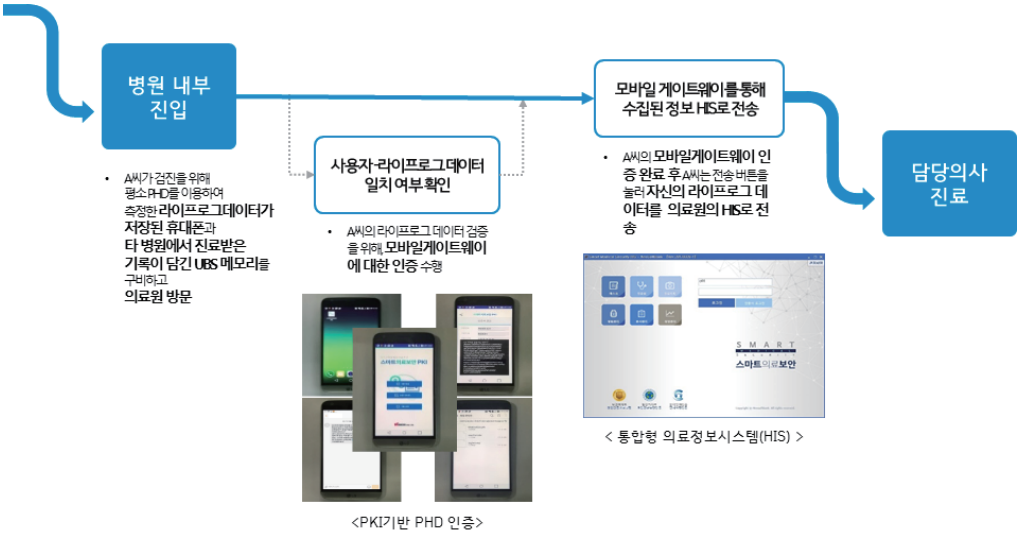
시작으로, 스마트 의료기기용 보안게이트웨이가 있다. 병원 외부에서 PHD(Personal Health Devices)를 이용하여 사용자의 라이프 로그를 수집하면, 이를 병원 내부로 전달하기 위한 게이트웨이를 거치게 된다. 이때, 사용자의 수집된 정보에 대한 위변조 오염이 발생할 수 있으므로, 최초 연결되는 기기에 대한 보안성을 강화해야 한다.



<보안 프로토콜 탑재 PHD>

<PHD 연동 모바일 보안게이트웨이>

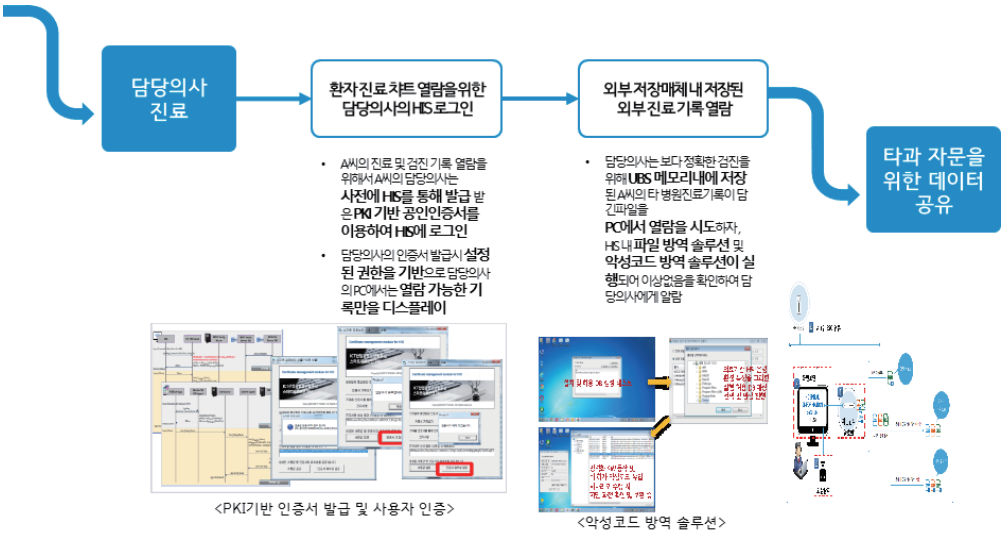
다음으로, 보안 게이트웨이를 거쳐 수집된 라이프 로그를 의료기관(병원)으로 전송할 때, 사용자와 라이프로그의 일치성을 확인할 필요가 있기 때문에 검증 기능이 필요하다. 그리고, 검증된 라이프로그는 모바일 게이트웨이를 통해 병원정보시스템으로 보내져 담당의사의 진료로 넘어가게 된다.



<PKI기반 PHD 인증>

< 통합형 의료정보시스템(HIS) >

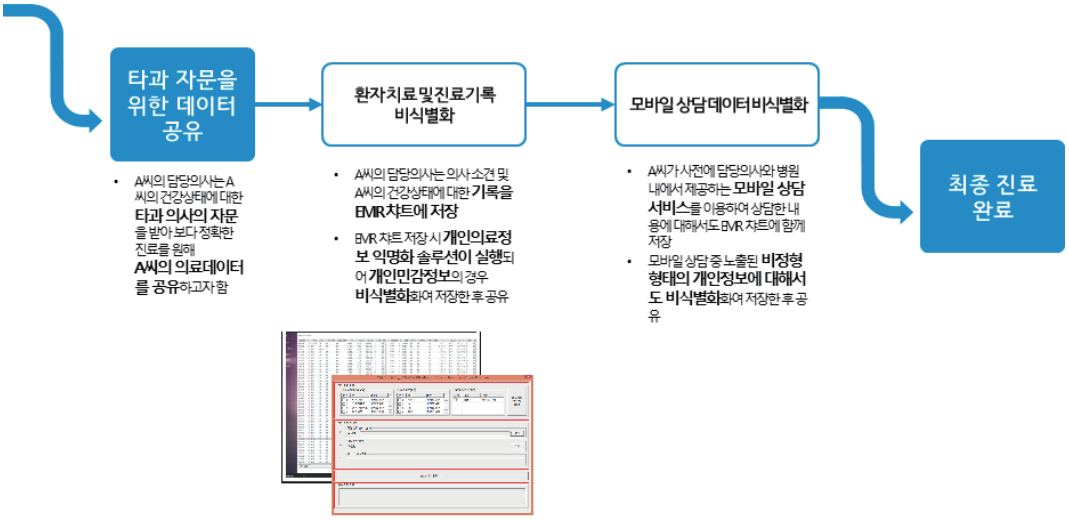
담당의사는 진료를 위하여 환자진료 챠트 열람을 위한 병원정보시스템에 로그인을 수행한다. 이때 권한관리를 위하여 인증서를 활용한 기능을 통하여 로그인을 수행한다. 그리고, 환자의 진료기록 외에 CD, USB 등 외부 저장매체를 가져온 경우 악성코드 확인을 통한 무결한 데이터만을 반입하도록 한다.



<PKI기반 인증서 발급 및 사용자 인증>

<악성코드 방역 솔루션>

마지막으로 타과의 단순 자문을 받아야 할 경우, 환자치료 및 진료기록과 라이프로그에 대한 익명화 및 비식별화를 수행함으로써 민감 의료정보에 대한 보안성을 갖춘다. 그리고, 향후 모바일 상담을 수행할 시 상담데이터에 대한 개인정보 노출을 고려하여 비정형 데이터에 대한 비식별화를 수행하는 기능을 갖춘다.



<비식별화된 의료정보 빅데이터>

4. 결론

4차산업혁명 기반 기술이 도입된 ICT 산업과 타 산업의 융합은 기존의 비즈니스를 강화하고, 새로운 비즈니스를 탄생시키고 있다. 이러한 과정에서 ICT 산업에서는 오래된 보안위협이 융합산업에서 새로운 이슈로 부각되고 있으며, 새로운 ICT 기술로 인한 융복합적 보안위협이 나타나고 있다. 융합산업의 모체산업 비즈니스 환경이 타 산업과 차별성이 강할수록 비즈니스 환경에 종속된 보안 위협들이 나타나고 있다. 실례로, 의료산업의 경우 오래된 악성코드를 통한 공격의 사례와 새로운 융합적 보안 위협들이 발생되고 있다.

이에 따라, 본 연구에서는 공공재 비즈니스 특성을 갖고 있는 의료산업이 ICT와 밀접하게 융합함으로써 나타나는 보안 위협과 이에 대한 대응방안을 설계하였다. 의료융합산업의 실태를 파악하고, 의료정보의 생애주기에 따라 의료기관 외부로부터 진료, 데이터의 활용까지 시나리오를 기반으로 보안 위협과 이에 대한 기본적인 대응책을 구축할 수 있는 프레임을 제시하였다.

본 연구의 시사점을 정리하면 다음과 같다.

1. 기존산업의 4차산업혁명 기반기술 도입은 새로운 융복합 보안위험을 발생시킨다.
2. 융복합 보안위험은 모체 비즈니스의 특성에 종속되어 ICT 산업에서는 오래된 보안이슈가 다시 나타나는 경우, 새롭게 보안위험이 나타나는 경우 등이 있다.
3. 비즈니스의 흐름을 분석하여 보안 수용성을 고려한 프레임을 구축하여야 한다.

향후 연구로는 연구된 프레임을 기반으로 현업 적합성 및 수용성을 향상시켜 비즈니스의 특성을 보존할 수 있는 시스템을 개발하고자 한다.

Acknowledgement

이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2015-0-007699, 의료정보 생애주기를 고려한 현장중심의 국제표준 스마트 의료 보안 플랫폼 개발)

참고문헌

[1] 공재근, 김윤, 장혜정, 진료정보전송 표준개발, 보건복지부 한국보건사회 진흥원, pp. 1-120, 2004.
[2] 김신효, 송지은, 정명애, 정교일, 의료정보화 및 보안기술 표준화 동향, vol. 21 No. 6, pp.190-201, 2006.
[3] 김화선, 김일곤, 조 훈 : HL7 표준 임상문서 구조를 사용한 전자퇴원요약의 생성, 저장, 관리시스템, 정보과학학회 논문지, vol. 33,

No. 2, pp.239-249, 2006.
[4] 정용식, "U-Healthcare 서비스를 위한 통합의료 정보시스템의 구축방안", 한국산업정보학회 논문지, 제15권, 제2호, pp.115-126, 2010.
[5] 김석훈 외, "의료영상저장전송 시스템 구축을 위한 병원정보시스템 연동방안 " , 한국지식정보기술학회 논문지, 제 2권 1호, pp91~98, 2007.3.
[6] 김동원, 한근희, "스마트의료 환경에서 보안위협 대응을 위한 최근 연구동향", 정보와통신, 제35권, 제2호, pp 95-99, 2018.
[7] Williams, Patricia., A practical application of CMM to medical security capability, Information Management & Computer Security, Vol. 16, No. 1, 2008; 58-73.
[8] Halperin, Daniel, Thomas S. Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. Security and privacy for implantable medical devices. IEEE pervasive computing, Vol. 7, No. 1, 2008.
[9] Gollakota, S., Hassanieh, H., Ransford, B., Katabi, D. and Fu, K.,They can hear your heartbeats: non-invasive security for implantable medical devices. ACM SIGCOMM Computer Communication Review, Vol. 41, No. 4, 2011; 2-13.
[10] Cao, F., Huang, H.K. and Zhou, X.Q., Medical image security in a HIPAA mandated PACS environment. Computerized medical imaging and graphics, Vol. 27, No. 2, 2003; 185-196.
[11] Koo, C.C. and Shyy, Y.M., iMedica Corp., 2005. Medical records data security system. U.S. Patent 6,874,085.
[12] CIOBIZ, http://m.ciobiz.co.kr/20160817120014, 2016.
[13] ISO/IEC JTC1 SC27, Information technology-security techniques - A privacy reference architecture, 2007
[14] Sangho Park, Yanghoon Kim,, Gwangmin Park, Onechul Na, Hangbae Chang, "Research on Digital Forensic Readiness Design in a Cloud Computing-Based SmartWork Environment", Sustainability, Vol. 10, No. 4,, pp. 1-24, 2018

Biographies



김양훈

2011년: 대진대학교 소프트웨어공학 (박사)
2012년 ~ 2013년: 상명대학교 박사후 연구원
2014년 ~ 현재: 극동대학교 산업보안학과 조교수
관심분야: 산업보안, 소프트웨어공학, 의료보안, 시스템 분석 및 설계
e-mail: yhkim@kdu.ac.kr



장항배

2006년: 연세대학교 정보시스템관리 (박사)
2007년 ~ 2012년: 대진대학교 경영학과 조교수
2012년 ~ 2013년: 상명대학교 경영학과 조교수
2014년 ~ 현재: 중앙대학교 산업보안학과 부교수
관심분야: 산업보안, 의료보안, 연구보안, 보안 데이터 분석
e-mail: hbchang@cau.ac.kr

해시함수 SHA-1에 대한 공격 그리고 그 이후

김한기[1], 김종성[2]
[1]국민대학교 금융정보보안학과, [2]국민대학교 정보보안암호수학과/금융정보보안학과

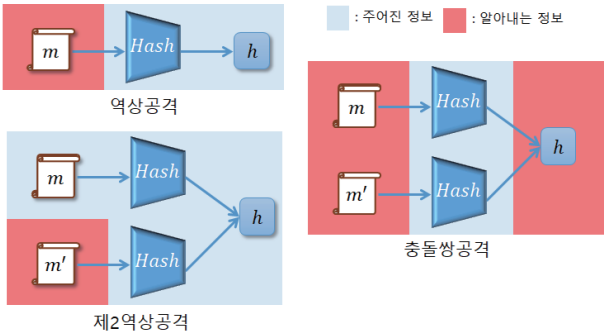
작년 2월 23일, 구글은 SHA-1의 충돌쌍 공격에 실제로 성공했음을 발표하며, shattered.io에 그 증거물인 파일 한 쌍을 업로드하였다. 제시된 두 파일은 빨간색과 파란색으로 서로 다른 배경색을 가진 그림이 저장된 PDF 파일로, 누구든 흔히 만들 수 있는 파일이었다. 하지만 이 발표는 IT업계 전체에 큰 파장을 불러왔다. 일례로, Chrome, Explorer, Firefox, Safari등의 브라우저들은 SHA-1 기반의 인증서를 두 달 만에 서둘러서 지원 중단했을 정도이다. 그렇다면 두 파일은 어떤 의미를 가지는 파일이고, 그것이 우리에게 어떤 영향을 끼치는 것일까?



〈2017년 2월 공개된 SHA-1의 충돌쌍(shattered.io)〉

해시함수는 사전에서 '임의의 길이의 데이터를 고정된 길이의 데이터로 매핑하는 함수'라고 정의되어있다. 이 정의에 따르면, 짝수 입력은 0, 홀수 입력은 1으로 매핑하는 함수도 해시함수라고 할 수 있다. 하지만 지금 이야기하고자 하는 '암호학적 해시함수'는 역상공격, 제2역상공격, 충돌쌍공격에 대하여 안전성을 가지는 해시함수이다.

역상공격은 주어진 해시값을 갖는 데이터를 찾아내는 공격이며, 제2역상 공격은 주어진 데이터와 같은 해시값을 가지는 또 다른 데이터를 찾는 공격이다. 그리고 충돌쌍공격은 같은 해시값을 가지는 서로 다른 데이터 쌍을 찾는 공격이다. 이 세 가지 공격에 내성을 가지는 해시함수를 암호학적으로 안전하다고 이야기 한다. 또한, 효율성 향상을 위해 다양한 환경에서 고정된 길이의 해시값이 원래 데이터의 고유값으로 활용된다. 이러한 성질들로 인해. 해시함수는 인터넷 브라우저의 인증서, 통신 프로토콜, 데이터 무결성 입증, 메시지 인증, 디지털 서명 등의 여러 가지 분야에서 사용된다.



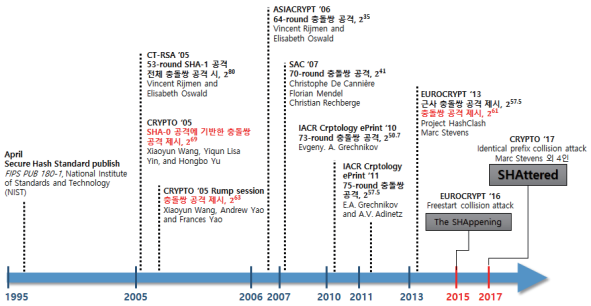
〈해시함수 공격법의 종류〉

구글과 CWI가 성공한 SHA-1 (Secure Hash Algorithm-1)에 대한 공격은 충돌쌍공격이다. 즉, shattered.io에 제시된 PDF 파일 두 개는 SHA-1의 해시값이 동일하다. 즉, 충돌쌍공격에 성공했음을 가시적인 결과로 제시한 것이다.

현재는 누구든지 SHA-1 해시값이 충돌하는 메시지 쌍을 만들어낼 수 있지만, 이는 하루아침에 이루어 진 결과가 아니다. 1995년 NIST(National Institute of Standards and Technology)에서 SHA-1을 발표한 이후, CRYPTO, EUROCRYPT, ASIACRYPT, CT-RSA 등 저명한 학회 및 논문지에 많은 공격기법이 제안된 바 있다. 충돌쌍공격에 내성을 갖기 위해서 SHA-1은 2^{80}미만의 계산복잡도로는 충돌쌍공격에 안전해야만 하지만, 2005년에 이미 2^{63}의 계산복잡도를 가지는 공격기법이 제안된 바 있다. 2010년 이후로 NIST에서는 공식적으로 SHA-1을 사용하지 않고 SHA-2 혹은 SHA-3를 사용하고 있다.

SHA-2는 NSA에서 개발되어 2001년 미연방 정보처리 표준 (FIPS, Federal Information Processing Standard)에 등록되었다. 그리고 2015년에는 공모를 통해 선정된 Keccak이 SHA-3로 선정되어 FIPS에 등록되었다. SHA-3는 독립적으로 제작된 알고리즘이기에 MD-like 구조를 가진 SHA-

0,1,2에 비해 색다른 스폰지 구조로 설계되어, 이전 버전에 대한 공격기법이 용이하게 적용되지 않는다는 장점이 있다.



〈1995년 SHA-1의 표준화 이후 발표된 주요 공격논문들〉

IT 업계는 이미 SHA-1 이전에 개발되었던 해시함수인 MD5의 취약점으로 인해 골머리를 앓은바 있다. MD5는 2006년에 1분내로 해시 충돌을 찾을 수 있는 알고리즘이 발표되었고, 2008년에는 실제 MD5기반 SSL 인증서를 변조하는 기법이 개발되어 Vulnerability Notes Database에 사용하지 말아야할 해시함수로 등록되었다. 그럼에도 불구하고 2013년 야후에서 유출된 10억 개의 사용자정보 중에는 MD5로 해싱된 패스워드가 존재하였다. 이러한 MD5 파동 이후에는 데이터베이스에 MD5 해시값을 저장하는 개발자가 많이 사라졌지만, 오래된 데이터베이스를 그대로 사용하는 사이트의 경우 업데이트가 필요하다.

이렇듯 안전성 기준을 만족하지 못하는 암호 알고리즘 사용의 피해를 겪었음에도 불구하고, SHA-1은 작년 초까지 많은 기관에서 사용되었다. 취약성이 이미 증명된 암호학적 알고리즘을 인증서로 사용하고, 실질적인 공격이 성공한 이후에야 지원 중단하는 모습은 사용자에게 불신을 줄 수 있으며, 암호학자들에게는 허탈한 일이 아닐 수 없다. 현재까지도 SHA-1은 데이터 무결성을 입증하는데 여러 기관에서 쓰이고 있다. 하지만, 보안에 민감한 영역에서는 사용을 즉시 금지해야만 한다. 또한, 하루가 다르게 컴퓨팅 성능이 발전하는 현대에서는, 암호 알고리즘의 일몰(sunsetting) 기한을 반드시 준수하여 보안사고를 미리 대비해야 할 것이다.

Acknowledgement

본 연구는 고려대 암호기술 특화연구센터(UD170109ED)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.

References

[1] “Security experts slam Yahoo management for using old crypto”, The Register, 2018년 6월 21일 접속, www.theregister.co.uk/2016/12/15/yahoos_password_hash/

[2] “5년간 공모 끝에 SHA-3 해시알고리즘 최종 선정!”, 보안뉴스, 2018년 6월 21일 접속, www.boannews.com/media/view.asp?idx=33102&kind=1

[3] “Vulnerability Note VU#83068”, Vulnerability Notes Database, 2018년 6월 21일 접속, www.kb.cert.org/vuls/id/836068

[4] “Announcing Approval of FIPS 202, SHA-3 Standard”, Federal Register, 2018년 6월 21일 접속, www.federalregister.gov/documents/2015/08/05/2015-19181/announcing-approval-of-federal-information-processing-standard-fips-202-sha-3-standard

[5] “SHATTERED”, shattered, 2018년 6월 21일 접속, shattered.io

[6] “박살난 SHA-1, 퇴출 가속화되나”, 소프트웨어정책연구소, 2018년 6월 21일 접속, https://spri.kr/posts/view/21757?code=inderstry_trend

Biographies



김한기

2016년 2월: 국민대학교 수학과 졸업
2016년 3월 ~ 2018년 2월: 국민대학교 금융정보보안학과 이학석사
2018년 3월 ~ 현재: 국민대학교 금융정보보안학과 박사과정
관심분야: 정보보호, 암호 알고리즘, 디지털 포렌식



김종성

2000년 8월 ~ 2002년 8월: 고려대학교 수학 학사/이학석사
2006년 11월: K.U.Leuven, ESAT/SCD-COSIC 정보보호 공학박사
2007년 2월: 고려대학교 정보보호대학원 공학박사
2007년 3월 ~ 2009년 8월: 고려대학교 정보보호기술연구센터 연구교수
2009년 9월 ~ 2013년 2월: 경남대학교 e-비즈니스학과 조교수
2013년 3월 ~ 현재: 국민대학교 정보보안암호수학과 부교수
2014년 3월 ~ 현재: 국민대학교 일반대학원 금융정보보안학과 부교수
관심분야: 정보보호, 암호 알고리즘, 디지털 포렌식

디지털 포렌식 측면에서의 안드로이드 디바이스에 대한 데이터 수집 연구

서승희, 박진성, 김 역, 이창훈
서울과학기술대학교 컴퓨터공학과

Abstract

안드로이드는 구글에서 개발한 모바일 운영 체제로 최근 2년간 세계적으로 가장 높은 70% 이상의 점유율을 차지하고 있다. 안드로이드 디바이스는 많은 사용자들의 생활에 밀접하게 사용됨에 따라 사용자의 다양한 데이터가 디바이스 내에 저장되고 저장된 데이터들은 디지털 포렌식적 측면에서 중요한 의미를 가진다. 이에 따라 안드로이드 디바이스에 대한 디지털 포렌식 관점에서의 데이터 수집 방법, 포렌식 절차 가이드 라인 등 대한 연구는 현재 시점까지 활발하게 진행되어 왔다. 본고는 이러한 안드로이드 디바이스에 대한 현존하는 디지털 포렌식 절차와 데이터 수집 연구들을 정리하고 향후 연구 및 한계를 제시한다.

I. 서론

스마트폰 뿐만 아니라 태블릿, 스마트 워치 등의 모바일 기기는 휴대하기 좋고 사용하기 편리하다 라는 점에서 많은 사람들에게 보편적으로 사용되고 있다. 글로벌 리서치회사 Gartner에 따르면, 지난 2017년 4분기 스마트폰의 글로벌 판매량은 약 40억을 기록했다.[1] 이는 전 인구의 약 40%에 해당하는 수로 스마트폰이 전 세계적으로 많이 사용되고 있음을 나타낸다.

모바일 기기는 전화, 메시지 전송 뿐만 아니라 사진, 음성, 동영상, 문서 등의 각종 데이터 송수신과 은행 거래, 웹 검색, 문서 작성, 일정 관리 등의 기능을 수행함으로써 사용자의 생활에 밀접한 연관성을 갖는다. 더불어 다양한 센서를 통해 심박수, 수면 패턴, 위치 정보 등을 수집하고 이를 이용하여 사용자에게 편리한 정보를 제공하기도 한다.

위와 같이 모바일 기기는 현대인의 생활을 용이하게 하는 동시에 일상 생활과 가장 밀접한 데이터들이 저장되는 정보저장 매체가 되고 있으며 [2], 이에 따라 모바일 기기에 대한 디지털 포렌식 관점에서의 연구의 중요성이 많이 대두되고 있다.

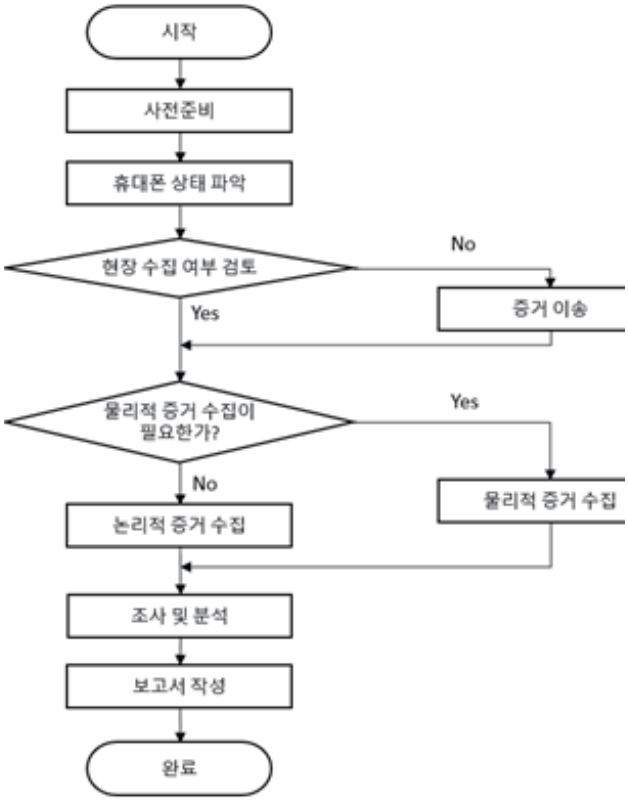
안드로이드는 구글에서 개발한 모바일 운영 체제 중 하나[3]로, 지난 몇 년 간 세계적으로 가장 높은 점유율을 차지하고 있다. 가장 최근인 2018년 3월 통계치에 따르면 안드로이드의 글로벌 시장 점유율은 80%에 육박한다. [4] 이러한 안드로이드 운영 체제에 대한 디지털 포렌식 관점의 연구가 중요해졌으며 다양한 데이터 수집 방법, 포렌식 절차 가이드 라인 등에 대한 연구가 활발하게 진행되어 왔다. [5]

본고는 이러한 안드로이드 모바일 운영 체제에 대한 데이터 수집 방법 및 포렌식 절차와 관련한 연구들의 동향을 정리하고 향후 연구 방향 및 한계에 대하여 논하고자 한다. 2장에서는 안드로이드를 비롯한 모바일 포렌식의 수행 절차와 데이터 수집에 대하여 정리하였고, 3장에서는 안드로이드 운영 체제를 사용하는 기기에 대한 논리적, 물리적 데이터 수집 방법과 최근 이슈가 되고 있는 모바일 클라우드 데이터의 수집 방안에 관한 연구 동향을 정리하였다. 이후 5장에서는 안드로이드 포렌식 연구의 한계에 대하여 논하고 6장에서 향후 연구 방향을 제시한다.

II. 모바일 포렌식의 수행 절차와 데이터 수집

안드로이드 기기에 대한 포렌식 조사 절차는 모바일 포렌식 수행 절차로 수행된다. 현재 우리나라에서는 모바일 포렌식 수행 절차에 대한 공식적인 가이드라인은 존재하지 않으며, 모바일 기기를 포함한 이동 전화 포렌식 가이드 라인인 TTAS.KO-12.0059만 존재한다. 해당 TTA 표준은 크게 그림 1과 같으며 이는 기존 디지털 포렌식 수행 절차와 유사하다. [6]

국제적으로 모바일 포렌식 수행 절차에 대한 가이드라인은 다양하나 NIST 국제 표준 문서인 NIST SP 800-101r1 “Guidelines on Mobile Device Forensics”이 가장 대표적이다. NIST SP 800-101r1은 모바일 포렌식 수행 과정을 크게 4가지 절차로 나누고 각 단계에 대한 설명을 기술하였다. 또한 모바일 디바이스의 특성, 포렌식 도구 선택 방법 등 모바일 포렌식의 전반적인 내용도 함께 기술하고 있다. [7] NIST SP 800-101r1에 기재되어 있는 4가지 포렌식 수행 단계에 대한 설명은 표 1과 같다.



〈그림 1. 모바일 포렌식 수행 절차 (TTA 가이드라인)〉

〈표 1. 국제 표준 모바일 포렌식 절차〉

단계	설명
Preservation	모바일 장치에 존재하는 데이터의 내용을 변경하거나 손상시키지 않고 안전하게 유지하는 단계. 현장에서 장치를 습득할 때 초기 대응 방안에 해당하는 단계이다.
Acquisition	습득한 모바일 장치 내부의 데이터를 이미징하거나 수집하는 단계
Examination & Analysis	수집한 데이터의 분석을 통하여 디지털 증거를 추출하는 단계. 주로 다양한 모바일 포렌식 분석 도구를 사용한다.
Reporting	모바일 포렌식의 전체적인 수행 과정과 분석의 결과를 문서화하는 단계.

그리고 NIST SP 800-101r1은 데이터의 수집 방법을 5개의 단계로 분류하였는데, 낮은 단계에서 상위 단계로 갈수록 획득 방법이 어려워지고 물리적인 성격이 강해지는 것을 알 수 있다. 데이터 획득 방법의 5 단계에 대한 설명은 표 2와 같다.

〈표 2. 5단계의 데이터 획득 방법의 분류〉

단계 수준	단계명	설명
1	Manual extraction	표준 인터페이스를 이용한 정보 획득을 의미한다. 키패드, 터치, 디스플레이 콘솔 등을 이용하여 기기 내 저장된 정보에 접근하고 화면을 캡처를 이용하여 정보를 추출한다.
2	Logical Extraction	USB, Wi-fi, Bluetooth로 조사관의 워크스테이션과 디바이스를 연결하여 데이터를 획득한다. 데이터의 접근에 대한 제한이 있을 수 있으며, 데이터가 수정될 우려가 있다.
3	Hex Dumping/ JTAG	물리적인 데이터 추출의 한 방법으로 flasher box나 기타 기술을 이용하여 flash memory를 내려 받는다. 물리적인 연결을 위한 기기의 데이터 수정이 발생할 수 있다.
4	Chip-off	물리적으로 flash memory chip을 획득하여 바이너리 이미지를 생성한다. 컴퓨터 하드 디스크에 대한 포렌식 방법과 유사하지만 기기의 물리적 손상이 반드시 야기되기 때문에 특수 경우에 사용한다.
5	Micro read	전자현미경을 이용하여 물리적인 로직 게이트를 관찰하고 이를 번역하여 read 가능한 데이터로 추출하는 방법이다. 고도의 기술력이 필요하다.

III. 안드로이드 디바이스의 데이터 수집

본고는 국제 표준 문서 NIST SP 800-101r1의 5단계의 데이터 획득 방법의 분류를 기반으로 기존 안드로이드 기기의 데이터 수집 방법을 정리하였다. 화면 캡처를 이용하여 데이터를 습득하는 Manual Extraction과 실제적인 수행이 보다 어려운 micro read를 제외하고 논리적 데이터 수집(Logical Extraction)과 물리적 데이터 수집(Hex dumping, Chip-off)에 대해 정리하였으며, 최근 이슈가 되고 있는 모바일 클라우드 데이터에 대한 수집을 추가적으로 정리하였다.

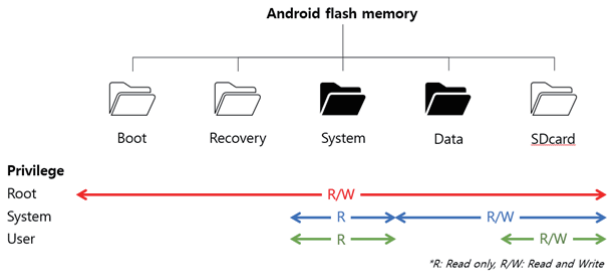
1. 논리적 데이터 수집 (Logical Extraction)

논리적 데이터 수집은 앞서 표 2 에서 설명한 바와 같이 USB, Wi-fi, Bluetooth를 이용하여 안드로이드 기기 내부 파일 시스템을 외부로 추출하여 수집하는 방법이다. 보통 논리적 데이터 수집 방법은 물리적으로 데이터를 수집하는 방법보다 빠르고 안정적이지만 비 할당 영역의 데이터 수집이 어렵고 커널 이미지의 권한에 따라 데이터에 대한 접근이 제한될 수 있다. [5]

1.1 Rooting kernel

안드로이드 기기는 펌웨어 내부의 커널 이미지의 권한에 따라서 플래시 메모리의 파티션에 대한 접근 범위가 다르다. 안드로이드는 User privilege, System privilege, Root privilege로 총 3가지 종류의 권한을 제공하고 있으며 각각에 대해 부여되는 파티션 접근 권한은 그림 2와 같이 상이하다. [8]

System 파티션은 통화 기록, 연락처, 기본 카메라 등과 같은 안드로이드 시스템에서 제공하는 어플리케이션 관련 데이



〈그림 2. 권한의 종류에 따른 파티션 접근 권한〉

터의 저장 공간으로 법적인 증거로의 잠재성이 높은 데이터들이 저장된다. 또한 Data 파티션은 시스템 어플리케이션 외에 사용자가 구글 마켓이나 기타 경로를 통해 설치한 Third-party 어플리케이션들의 데이터가 저장되며 이러한 정보들 역시 증거로써 활용 가능성이 크다. 하지만 그림 2에서 알 수 있듯 System 파티션과 Data 파티션에 대한 추출은 일반적으로 제공되는 User privilege로는 불가하며 원활한 데이터 수집을 위해서는 Root privilege가 반드시 필요하다.

Rooting kernel은 안드로이드 기기의 커널 이미지를 Root privilege를 갖도록 수정하고 이를 커널 영역 (Recovery 파티션)에 덮어씌워 부팅함으로써 Root privilege를 획득하는 방법이다.[2] 하지만 커널 영역에 수정된 이미지를 덮어씌우기 위해서는 반드시 Bootloader가 unlock되어야만 하는데, bootloader를 unlock 시키는 과정은 안드로이드 기기의 내부 데이터를 전부 손실할 위험성이 크다. [9] 이에 따라 데이터 손실의 문제를 해결하기 위해 커널 이미지를 Boot 파티션에 덮어쓰는 방법 [10], 커널 이미지를 SD 카드로 부팅하는 방법 [11], SD 카드를 Recovery 모드로 패치하는 방법 [12] 등이 제안된 바 있다.

1.2 Backup Protocol 과 Tool

안드로이드는 버전 4.0 이후부터 관리자의 권한없이 Android Debug Bridge (ADB)를 이용하여 데이터를 백업하는 프로토콜을 제공한다.[2] 이 프로토콜은 정상 부팅 후 분석 시스템을 연결하여 곧바로 데이터 수집이 가능하다. 하지만 어플리케이션 중 일부는 백업 프로토콜을 이용한 데이터 백업을 허용하지 않기 때문에 기기 내 모든 정보를 수집하는 데 어려움이 있다. 특정 어플리케이션의 백업 프로토콜을 허용하기 위한 다운그레이드 방법이 제안된 바 있으나 안드로이드의 보안 강화로 인해 어플리케이션의 임의적인 삭제가 불가하다는 한계가 있다. [13]

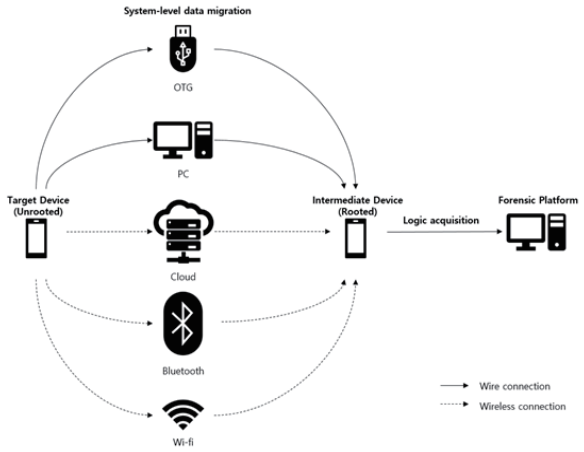
안드로이드 기기는 각 제조사별로 시스템 레벨의 데이터를 PC에 백업해주는 백업 툴을 제공하고 있다. 예를 들어 삼성은 Smart Switch, LG는 Mobile switch 라는 데이터 백업 툴을 사용자에게 제공한다. 이러한 백업 툴을 이용하면 시스템 레벨의 데이터를 조사관의 PC에 백업하여 데이터를 수집할 수 있다. [14] 하지만 백업 툴에 따라 백업 이미지를 암호화하여 저장하므로 별도의 복호화에 대한 연구가 필요하다.

1.3 Content Provider

Content Provider는 어플리케이션 데이터 공유 인터페이스로 연락처, 통화 내역, SMS, MMS, 일정, 인터넷 접속 기록 등 시스템 어플리케이션 내 저장되는 정보들을 Third-party 어플리케이션에 제공하는 역할을 한다. [15] Content Provider를 사용하여 데이터를 수집하는 어플리케이션을 개발한 후, 대상 안드로이드 기기에 설치하면 데이터 수집이 가능하나 새로운 어플리케이션의 설치는 대상 기기의 무결성을 보장하기 어려우므로 일부 해외 모바일 포렌식 도구 [16,17]만 해당 기능을 제공하고 국내에서는 사용하지 않는다. [2]

1.4 LASM

LASM은 logical Acquisition method based on System-level data Migration의 약자로 최근 Feng 외 3명이 처음 제안하였다. [8] 안드로이드 기기 제조사들의 잦은 최신 안드로이드 기기의 출시는 사용자들의 빈번한 기기 변경을 초래하였고, 이는 새로운 기기로 데이터 이전의 문제를 야기하였다. 제조사들은 데이터 이전의 불편함을 해소하기 위해 OTG, PC, 클라우드 저장소, Bluetooth, Wi-fi를 이용한 기기 간 데이터 전송 기능을 제공하기 시작했다. LASM은 이러한 기기 간 데이터 전송을 기반으로 한 제안된 포렌식 데이터 수집 방법으로 프레임워크는 그림 3과 같이 구성된다.



〈그림 3. LASM 프레임워크〉

LSAM의 절차는 다음과 같다.

Step 1. 중간 기기(Intermediate Device)를 초기화하고 Root privilege를 포함한 이미지를 덮어씌워 내부 데이터를 이미징 할 수 있도록 한다.

Step 2. 대상 기기(Target Device)와 중간 기기를 Bluetooth나 Wi-fi로 연결한다.

Step 3. 대상 기기에서 중간 기기로 필요한 모든 데이터를 전송한다.

Step 4. 대상 기기의 데이터가 모두 저장된 중간 기기를 이미징 하여 데이터를 수집한다.

LSAM은 기능을 제공하는 어플리케이션에 한해 Third-party 어플리케이션의 데이터까지 쉽게 획득이 가능하여 최근 떠오르고 있는 데이터 수집 방법이다. 하지만 이 방법은 대상 기기가 부팅이 가능해야 하고 잠금 화면이 풀릴 수 있다는 사실을 전제로 한다.

2. 물리적 데이터 수집

물리적 데이터 수집은 안드로이드 기기의 flash memory를 bit-for-bit로 복사하여 PC에 저장하는 방식[18]으로 논리적 데이터 수집과 달리 수집 방법이 까다롭고 복잡하지만 비할당 영역의 데이터까지 수집할 수 있다는 장점이 있다.

2.1 Firmware update protocol

펌웨어 업데이트 프로토콜을 사용하여 물리적인 데이터를 수집하는 방법은 2015년 양승재 외 3명[19]이 제안한 방법으로 펌웨어 업데이트 모드에서 제공되는 Bootloader의 flash memory 읽기/쓰기 명령어를 이용하여 데이터를 물리적으로 복사한다. 펌웨어 업데이트 프로토콜은 대상 안드로이드 기기의 Application Processor(AP)에 종속되고 AP마다 명령어가 상이하기 때문에 범용적인 사용이 어렵다는 한계가 있다.[2] 또한 이 방식은 선별적인 데이터 수집이 불가할 뿐 아니라, 최근 일부 제조업체에서 flash memory 읽기/쓰기 명령어를 제거하였다. [8]

2.2 JTAG

JTAG은 모바일 메인보드의 디버깅용 포트로 별도의 하드웨어 디버깅 장비를 이용하여 플래시 메모리 데이터를 이미징 할 수 있도록 한다. [2] 하지만 JTAG 포트로 데이터를 수집하기 위해서는 대상 기기의 수정이 불가피하며 심지어 최근 기기들은 JTAG 포트를 제공하지 않는다. 이에 따라 현재 이 방식의 사용은 매우 제한적이다.

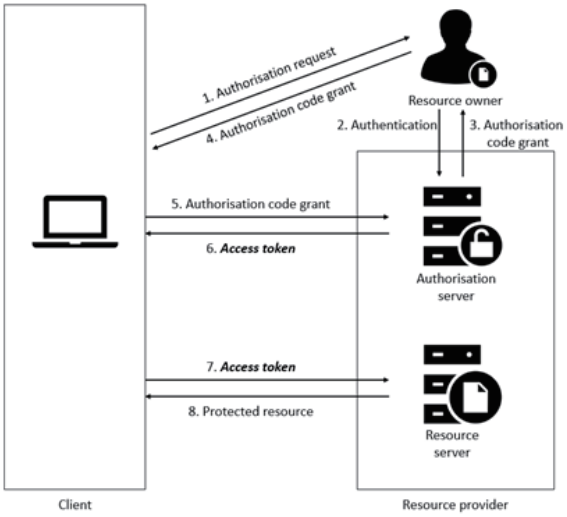
2.3 Chip-off

Chip-off는 안드로이드 기기의 flash memory chip을 물리적으로 분리하고 메모리 리더기를 이용하여 PC에 바이너리 이미지를 생성하는 방법이다.[5] 컴퓨터 하드 디스크 포렌식에 대한 수집 방식과 유사하지만 기기로부터 flash memory chip을 분리하기가 어렵고 칩이 분리된 기기는 다시 사용하기 어렵다는 점에서 차이가 있다. 메모리를 분리하는 과정 중 핀이 손상될 우려가 있으나 리볼링 과정을 통해 손상된 핀을 일부 복구할 수 있다.[2] 이 방식은 데이터 수집 후 사용자에게 돌려주어야 하는 경우 사용이 불가하고 주로 파손된 기기에서 사용한다.

3. 클라우드 데이터 수집

대부분의 데이터를 기기 내부가 아닌 클라우드에 저장하는 최근 어플리케이션의 경향은 안드로이드 기기 데이터 수집의 어려움을 가중시킴과 동시에 다양한 방향의 연구를 진행시켰다.

현재 연구 트랜드는 크게 2가지 방향으로 나누어 생각해볼 수 있는데, 첫째는 안드로이드 기기 내 크리덴셜을 이용한 클라우드 데이터 수집이다. 크리덴셜은 클라우드 데이터 접근 권한 관련 데이터로 그림 4의 Oauth protocol을 통한 인증 과정을 거친 후 획득한 Access token과 Access token의 갱신을 위한 사용자 인증 정보를 포함한다



〈그림 4. OAuth Protocol 인증 프로세스〉

Access token은 클라우드 서버에서 발급 받은 것으로 리소스 서버의 사용자 데이터에 접근할 때 사용한다. 안드로이드 기기의 경우 크리덴셜을 system 파티션에 저장하므로 앞서 말한 데이터 수집 방법을 통해 충분히 획득할 수 있다. 크리덴셜은 다른 기기에 복사하여 클라우드 데이터에 접근 및 수집이 가능하다.[20,21] 하지만 위의 방법은 장소에 구애 받지 않고 언제든 데이터에 접근할 수 있는 클라우드 저장소의 특성상 무결성 검증이 어렵고 다른 기기에 크리덴셜을 복사하여 사용하는 데 복잡한 절차를 필요로 한다.

둘째로 안드로이드 내부에 임시로 저장된 클라우드 데이터 수집 방법이 있다. 클라우드 어플리케이션들은 사용자의 데이터를 모두 클라우드에 저장하지만 사용 빈도가 높은 데이터들은 별도의 폴더에 임시로 복사하여 관리한다.[18] 이에 따라 안드로이드 flash memory 에서 클라우드 데이터의 일부를 수집할 수 있다. 각 어플리케이션마다 임시 저장 경로가 다르고 파일을 저장하는 형태가 다르기 때문에 어플리케이션 별로 분석이 필요하다.[9]

IV. 안드로이드 디바이스에서 데이터 수집의 한계

안드로이드 기기 데이터 수집의 가장 큰 한계는 안드로이드 기기의 지나친 다양성이다. 안드로이드 OS는 제조사와 기기, 버전 별로 제공 기능이 다르고 데이터 수집 방법 또한 기능에 따라 상이하다. 하지만 안드로이드 OS는 지속적으로 버전을 갱신하고 있으며 제조사는 끊임없이 새로운 기기를 출시하고 있다. 더욱이 사물 인터넷의 등장으로 그 다양성이 폭발적으로 증가하고 있다. 이에 따라 안드로이드 데이터 수집 방법의 일반화가 어렵기 때문에 데이터 수집의 연구는 가장 많이 사용되는 기기에 집중될 수 밖에 없다. 이로 인해 사용이 드문 기기가 악의적인 목적을 위한 수단이 되고 있다.[5]

또한 안드로이드 기기의 보안성 향상은 데이터의 수집에 어려움을 더하고 있다. 본고에 제시된 데이터 수집 방법 중 일부는 지속되는 안드로이드 기기의 보안 패치로 인해 사용 기기의 범위가 점차 좁아져 가고 있으며, 최근 Data 파티션 자체를 암호화하여 저장하기 시작하면서 chip-off 와 같은 물리적인 수집 방법들 마저 무색해지고 있다. 또한 보안성 향상은 데이터 수집 방법 연구를 더 복잡하게 함으로서 하드웨어 및 소프트웨어 역공학 기술, 동적 디버깅 등의 고급 기술을 필요성을 높이고 있다.[8]

V. 향후 연구

4장에서 제시한 데이터 수집의 한계를 보완하기 위해서는 지속적이고 활발한 안드로이드 기기 데이터 수집 방안 연구가 필요하다. 또한 사용자 수가 많은 기기 뿐만 아니라 사용이 드문 기기를 포함한 포괄적인 연구가 필요하다.

또한 클라우드 저장소 사용의 증가는 클라우드 데이터 수집 방안 연구의 중요성을 높이고 있다. 특히 구글 드라이브나 Dropbox와 같은 클라우드 어플리케이션은 디지털 포렌식적으로 가치를 가지는 데이터를 클라우드에 다량 저장하고 있으므로 이를 활용할 수 있도록 클라우드 데이터의 무결성 입증에 관한 연구가 필요하다.

Acknowledgement

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No. 2017-0-00344, 최신 모바일 기기에 대한 암호해독 및 포렌식 분석)

References

[1] “Gartner Says Worldwide Sales of Smartphones Recorded First Ever Decline During the Fourth Quarter of 2017”, Gatner Group, 22 February 2018; https://www.gartner.com/newsroom/id/3859963

[2] 김도현; 이상진. 모바일 포렌식 동향. 정보보호학회지, 2016, 26.5: 22-31.

[3] Google android, https://www.android.com/

[4] “Mobile Operating System Market Share Worldwide”, Statcounter GrobalStats, May 2018; http://gs.statcounter.com/os-market-share/mobile/worldwide

[5] CHERNYSHEV, Maxim, et al. Mobile Forensics: Advances, Challenges, and Research Opportunities. IEEE Security & Privacy, 2017, 15.6: 42-51.

[6] TTAS.KO-12.0059, “이동 전화 포렌식 가이드라 인”, 한국정보통신기술협회, 2007

[7] R. Ayers, S. Brothers and W. Jansen, “Guidelines on Mobile Device Forensics,” NIST Special Publication 800-101: [Online]http://dx.doi.org/10.6028/NIST.SP.800-101r1, May 2014.

[8] FENG, Peijun, et al. Logical acquisition method based on data migration for Android mobile devices. Digital Investigation, 2018.

[9] DO, Quang; MARTINI, Ben; CHOO, Kim-Kwang Raymond. A cloud-focused mobile forensics methodology. IEEE Cloud Computing, 2015, 2.4: 60-65.

[10] SON, Namheun, et al. A study of user data integrity during acquisition of Android devices. Digital Investigation, 2013, 10: S3-S11.

[11] LESSARD, Jeff; KESSLER, Gary. Android Forensics: Simplifying Cell Phone Examinations. 2010.

[12] CHEN, Sheng-Wen; YANG, Chung-Huang; LIU, Chien-Tsung. Design and implementation of live SD acquisition tool in Android smart phone. In: Genetic

and Evolutionary Computing (ICGEC), 2011 Fifth International Conference on. IEEE, 2011. p. 157-162.
[13] WU, Songyang, et al. Forensic analysis of WeChat on Android smartphones. Digital investigation, 2017, 21: 3-10.
[14] Mikhailov, I., 2017. Mobile forensic Cookbook: Data Acquisition, Extraction, Recovery Techniques, and Investigations Using Modern Forensic Tools.
[15] 이윤호; 이상진. 스마트폰 내부 정보 추출 방법. 정보보호학회논문지, 2013, 23.6: 1057-1067.
[16] Cellebrite UFED, "http://www.cellebrite.com/", 2016
[17] XRY, https://www.msab.com/, 2016.
[18] MARTINI, Ben; DO, Quang; CHOO, Kim-Kwang Raymond. Conceptual evidence collection and analysis methodology for Android devices. arXiv preprint arXiv:1506.05527, 2015.
[19] YANG, Seung Jei, et al. New acquisition method based on firmware update protocols for Android smartphones. Digital Investigation, 2015, 14: S68-S76.
[20] 남기훈, et al. 안드로이드 환경의 OAuth 프로토콜을 이용한 원격지 데이터 수집 방법 연구. 정보보호학회논문지, 2018, 28.1: 111-122.
[21] 최종원; 이정현. 안드로이드 구글 계정 앱의 개인정보 유출 취약점 분석. 디지털포렌식연구, 2014, 8.2: 65-81.

Biographies



서승희

2012년: 서울과학기술대학교 컴퓨터공학 학사
2017년: 서울과학기술대학교 컴퓨터공학 석사 과정
관심분야: 정보보호, 역공학, 디지털 포렌식, 암호학
e-mail: seunghee.seo.00@seoultech.ac.kr



박진성

2012년: 충주고등학교 졸업
2018년: 서울과학기술대학교 컴퓨터공학과 학사 재학중
관심분야: IoT 보안, 네트워크 보안
e-mail: jseongpark157@seoultech.ac.kr



김 역

1992년: 성신여자대학교 전산학과 (이학사)
2003년: 고려대학교 정보보호대학원 (공학석사)
2010년: 고려대학교 정보경영전문대학원 (공학박사)
2005년 ~ 2007년: 동양미래대학교 전임강사
2017년 ~ 현재: 서울과학기술대학교 전기정보기술연구소 연구원
관심분야: 정보보호, 디지털 포렌식, 암호모듈평가 등
e-mail: yeogkim@gmail.com



이창훈

2001년: 한양대학교 자연과학부 수학전공 학사
2003년: 고려대학교 정보보호대학원 석사
2008년: 고려대학교 정보경영전문대학원 정보보호전공 박사
2008년 4월 ~ 2008년 12월: 고려대학교 정보보호연구원 연구교수
2009년 3월 ~ 2012년 2월: 한신대학교 컴퓨터공학부 조교수
2012년 3월 ~ 2015년 3월: 서울과학기술대학교 컴퓨터공학과 조교수
2015년 4월 ~ 현재: 서울과학기술대학교 컴퓨터공학과 부교수
관심분야: 정보보호, 사이버 보안, CTI, IoT보안, 디지털 포렌식, 암호학 등
e-mail: chlee@seoultech.ac.kr

ICS(Industrial Control System)에 적용되는 산업용 프로토콜 보안기술 현황

이건희
National Security Research Institute (NSR)

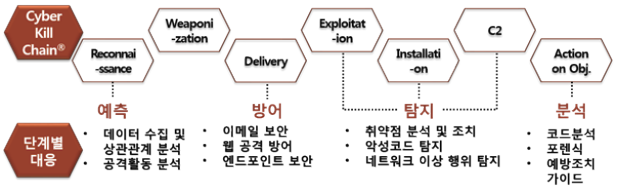
Abstract

최근 산업제어시스템을 대상으로 하는 사이버 공격 사례가 증가하고 있고, 우크라이나 정전사태와 같은 직접적 피해가 발생하기도 하였다. 이러한 상황에서 다양한 보안대책이 고려되어야 하지만 가장 기본적으로 산업제어시스템 내 통신 프로토콜의 보안 기능에 대한 검토가 필요하다. 산업제어시스템의 통신 프로토콜은 보안 기능이 고려되지 않고 설계되어 사용되고 있다. 이로 인해 산업제어시스템의 네트워크 트래픽을 분석하면 손쉽게 잘못된 데이터를 주입하는 것이 가능하다. 이에 IEEE, IEC 등의 표준화 단체에서는 DNP, IEC61850, OPC UA 등의 주요 산업용 프로토콜에 대한 통신보안 규격을 개발하였다. 본 고에서는 IEEE 1815, IEC62351, IEC62443 등에서 제시되고 있는 산업용 프로토콜에 대한 통신보안 기술의 현황에 대해서 알아보고자 한다.

I. 서론

최근 제어시스템을 대상으로 하는 사이버 공격의 늘어나면서 산업제어시스템의 사이버 보안 강화에 대한 관심이 높아지고 있다. 기존의 상용 보안 제품을 활용하여 네트워크를 안전하게 구성하고, 제어시스템 네트워크 트래픽을 분석하여 이상행위를 탐지함으로써 공격 위협을 조기에 탐지하려는 연구도 진행되고 있다.

지금까지 국내의 제어시스템 보안대책은 대부분 제어시스템과 외부 네트워크 간 연계를 최소화하는데 많은 힘을 쏟았다. 하지만 스턱스넷(stuxnet), 우크라이나 정전사태 등 최근의 제어시스템 공격 사례를 살피면 내부자를 이용해 제어시스템 네트워크에 접근한 후 지속적으로 제어시스템을 살펴보고, 그 결과를 바탕으로 제어시스템을 임의로 제어할 수 있는 공격을 감행하는 경우가 많아 지고 있다. SANS에서 제안된 사이버 킬 체인에 따르면 공격자는 시스템에 잠복하여 시스템을 정찰하는 과정을 거치게 되며[1], 이를 통해서 분석된 정보를 바탕으로 짧은 시간에 제어시스템에 피해를 입힐 수 있도록 공격을 계획한다[2].



〈그림 1. SANS Cyber Kill Chain〉

이러한 공격 전략에 대응하기 위해서는 인적 보안 및 교육을 강화해 내부에서의 위협을 최소화 하는 방법과 함께 다양한 내부자 위협 대응 방법을 적용하여 사이버 킬 체인의 각 단계를 무력화 시켜야 한다. 그 중에서도 가장 첫 번째 단계인 정찰 단계에서 공격자를 무력화 시키는 방안이 가장 우선적으로 고려되어야 한다.

공격자가 정찰에 사용하는 여러가지 기법 중 하나로 네트워크 트래픽을 모니터링하는 방법을 사용할 수 있다. 트래픽 모니터링을 통해서 시스템 간 정보흐름을 파악하고, 패킷의 내용을 살펴봄으로써 중요 시스템 및 각 시스템의 취약점을 식별하게 된다.

이러한 공격 기법은 보통은 네트워크 접근제어를 통해서 차단할 수 있다. 네트워크 접근제어는 솔루션을 이용하여 비인가 장비는 네트워크에 접속할 수 없도록 하는 방법도 있지만, 정보의 은닉이 목적이라면 통신 메시지를 암호화하거나 인증하는 것으로도 해결할 수 있다.

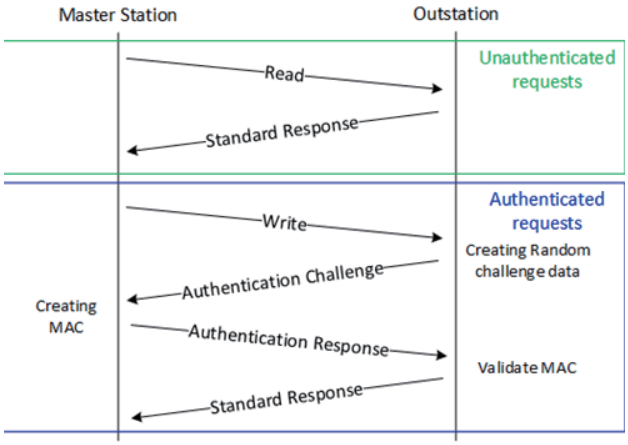
그런데 현재 Modbus, DNP, IEC61850 등 알려진 많은 산업용 제어프로토콜은 보안기능이 포함되지 않아 인증 및 암호화가 이루어지지 않고 있다. 따라서 공격자가 산업용 제어프로토콜을 수집하여 살펴볼 수 있으면, 제어시스템의 상태, 운영현황 등을 파악하는 것은 물론 나아가서는 제어를 위한 패킷 조작 마저도 이루어질 수 있다[3].

이러한 문제를 고려하여 최근에는 각 제어프로토콜에 보안기능을 추가할 수 있도록 규격이 갱신되거나 추가 규격을 만들어 활용하도록 하고 있다. 본고에서는 이러한 다양한 제어프로토콜에 적용되고 있는 보안기술 현황에 대해서 살펴본다.

II. DNP3.0 보안 규격 현황

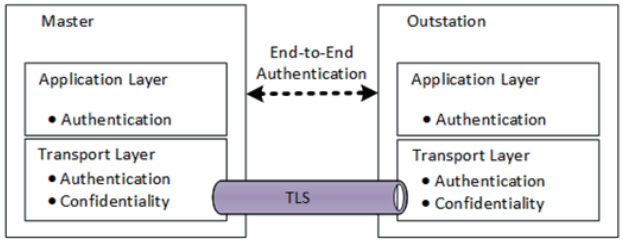
DNP3.0 프로토콜은 1993년에 개발된 기기 통신 프로토콜로 북미 지역을 중심으로 전력분야 제어시스템에서 많이 활용하고 있다. 북미 지역에서는 IEC 60870-5-104로 적용되고 있다.

DNP3.0 프로토콜의 보안은 IEEE 1815 및 IEC 60870-5-7, IEC 62351-5 등에서 다루고 있다[4-6]. 기본적으로 DNP3.0 보안은 응용계층에서의 종단간 인증 기능을 제공한다. 제어와 관련한 중요 메시지를 주고 받을 경우, 인증 요청과 응답을 통해서 제어 메시지를 전송한 단말을 인증한 후 메시지를 처리한다. 다음 그림은 일반적인 메시지를 처리하는 경우와 인증과정을 통해 중요메시지를 처리하는 경우의 각각의 절차를 설명한다.



〈그림 2. DNP3 메시지 교환 과정(무인증, 인증)〉

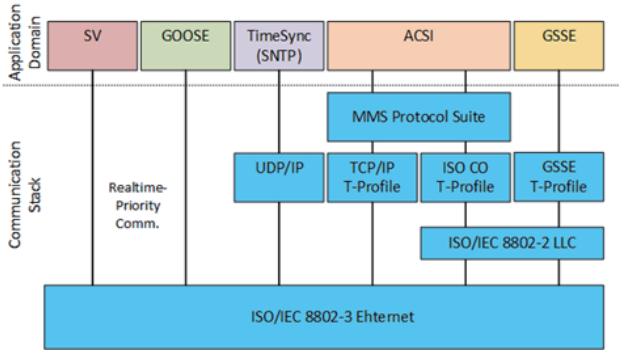
DNP3.0은 시리얼 통신과 이더넷 통신 모두에서 사용할 수 있다. 여기서 이더넷 통신 구간에서 DNP3.0을 사용할 경우는 TCP/IP를 전송계층으로 사용하는 경우가 대부분이다. 이 경우는 표준규격에서 TLS(Transport Layer Security)를 함께 사용하여 보안성을 높이도록 요구하고 있다.



〈그림 3. TLS 적용한 DNP3 전송계층 보안〉

III. IEC61850 보안 규격 현황

IEC61850 프로토콜은 전력분야 제어시스템의 제어 프로토콜로 개발된 표준프로토콜이다. IEC61850은 기기의 상태 정보를 수집하기 위한 SV(Sampled Value), 기기 간 이벤트 정보 공유를 위한 GOOSE(Generic Object Oriented Substation Events), 상위 운영시스템에서 기기 제어 및 상태 확인 등을 위한 MMS(Manufacturing Message Specification) 등의 프로토콜로 구성된다[9].



〈그림 4. IEC 61850 프로토콜 스택〉

IEC61850의 표준규격에는 보안기능에 대한 내용이 포함되지 않았다. 하지만 최근 보안 이슈가 부각되면서 IEC에서는 IEC61850 프로토콜에 보안 기능을 추가하기 위해서 IEC62351 시리즈 표준을 개발하였다. 해당 표준에서 IEC62351-4는 일반적인 MMS 프로토콜에 대한 보안 규격을 명시하고 있고, IEC62351-6은 IEC61850 전반에 걸친 보안 규격을 명시하고 있다[7-8].

IEC62351-4는 MMS 프로토콜의 안전한 통신 및 인증을 위해서 TLS를 사용하도록 규정하고 있다. IEC62351-6 표준에서는 SV, GOOSE 등을 위해서 메시지 인증 방법을 규정하고 있다. SV, GOOSE 등의 프로토콜은 상태 또는 이벤트 정보를 제공하는 프로토콜이고, 매우 짧은 응답시간이 유지되어야하는 실시간성이 요구되는 프로토콜이다. 따라서 별도의 암호화는 사용하지 않고 메시지를 전송하는 기기에 대한 인증을 효율적으로 할 수 있도록 규격을 정의하였다. IEC62351-6에서는 SHA256 기반의 HMAC 기법을 사용하도록 규정하였다.

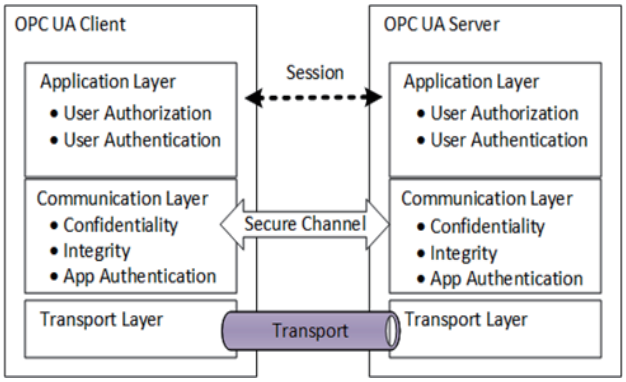
더불어 IEC61850에서 시간 동기화를 위해서 사용하도록 규정한 SNTP(Simple Network Time Protocol)에는 RFC2030의 메시지 인증 규격을 따르도록 명시되어 있다. 현재 2010년부터 RFC2030은 폐기되고 새로운 버전인 RFC5905로 대체 되었다.

Ⅳ. OPC UA 보안 규격 현황

OPC UA는 IEC 61968/61970에 근거한 CIM(Common Information Mode) 데이터를 전송하기 위해서 사용하는 산업용 M2M(Machine-to-Machine) 통신 프로토콜이다. OPC UA는 OPC 파운데이션에서 개발되었으며, 현재 IEC에서 IEC 62541로 표준화를 완료한 상황이다.

4.1. OPC UA 보안 아키텍처

OPC UA의 보안 아키텍처는 IEC 62541-2에 다음과 같이 설명되고 있다[10].



〈그림 5. OPC UA 보안 아키텍처〉

플랜트 정보, 설정값, 명령, 모니터링 정보 등을 전송하기 위해서 응용계층에서는 세션(Session)을 사용한다. 세션은 응용을 사용하는 사용자를 인증하고, 사용자의 권한을 확인한다.

OPC UA 세션은 보안채널(Secure Channel) 위에서 동작한다. 보안채널은 세션을 통해 교환하는 데이터의 무결성, 기밀성 등을 보장한다. 더불어 보안채널은 세션을 통해 통신하는 두 응용 간의 상호인증을 지원한다. 무결성을 보장하기 위해서는 전자서명을 사용하며, 기밀성을 위해서는 데이터를 암호화하고, 인증서를 이용해 응용의 상호인증 기능을 제공한다. 세션과 보안채널 등에서 X.509v3 인증서를 사용하므로, OPC UA의 보안을 위해서는 인증서 사용 인프라가 제공되어야 한다.

마지막으로 실제 데이터 전송은 전송계층의 소켓연결을 통해서 이루어진다. 전송계층에서는 OPC UA 가용성 보장을 위해서 에러 복구 및 서비스거부공격 방어 등을 제공해야 한다.

4.2. OPC UA 통신 보안

4.2.1. 연결 성립 (Connection Establishment)

OPC UA 클라이언트와 서버 간 통신연결은 총 4단계로 이루어진다.

• 1단계 : 보안설정 획득

클라이언트가 서버와 연결을 위한 설정 및 연결방법 등에 대해 파악한다. 서버 탐색 서비스를 통해서 서버에 접속하기 위해서 어떤 설정을 사용해야 하는지 파악하는 단계다. 설정정보는 보안정책(Security Policy), 보안모드, 사용자토큰정책(User Token Policy), 서버의 응용인스턴스인증서(AIC, Application Instance Certificate) 등을 포함하며, 이는 EndpointDescription이라는 객체에 명세 된다.

만약 새로운 설정정보를 획득했으면, 클라이언트는 서버의 인증서(AIC)를 검증한다. 연결과 관련된 설정이 사전에 지정되어 있으면, 이 단계는 생략 가능하다.

• 2단계 : 보안채널 생성

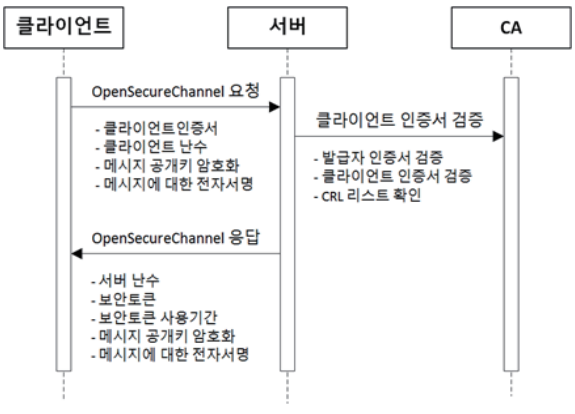
클라이언트는 OpenSecureChannel 요청을 통해서 서버와 보안채널을 생성한다. 이 요청은 보안설정에 명시된 보안정책과 보안모드를 준수하여 보호된다.

보안모드는 None, Sign, SignAndEncrypt 등의 세 가지가 있는데, 안전을 위해서 None은 사용하지 않는다. Sign은 요청메시지에 대해서 전자서명을 덧붙이며, SignAndEncrypt는 전자서명과 함께 메시지를 암호화 한다. 이 때 전자서명은 클라이언트의 개인키로 하고, 암호화는 서버의 인증서에 명시된 공개키를 사용한다. 보안정책은 어떤 알고리즘을 사용할지 명시한다.

보안채널은 정해진 기간 동안만 사용할 수 있고, 기간이 지나면 갱신되어야 한다. 이때 갱신하는 기준 및 절차는 다음과 같다.

- 클라이언트는 사용기간의 75%에 달하면 신규 보안토큰 요청
- 서버는 사용기간이 종료될 때까지 또는 새로운 보안토큰을 사용하는 메시지를 받을 때 까지 기존 보안토큰을 사용
- 클라이언트는 사용기간의 25% 해당하는 기간까지 사용기간이 만료된 보안토큰을 이용한 메시지를 수용

보안채널 생성과정에서 향후 사용될 세션키를 생성한다. 이 과정은 서버가 생성한 난수와 클라이언트가 생성한 난수를 이용해 각자 서버의 세션키와 클라이언트의 세션키를 공유하는 방식이다.



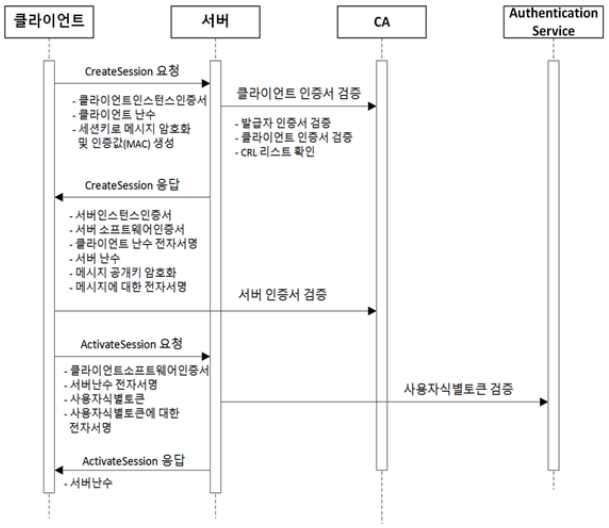
〈그림 6. OPC UA 보안채널 생성과정〉

• 3단계 : 세션 생성

보안채널 생성 시 공유한 세션키를 사용해 모든 메시지의 기밀성과 무결성을 보호한다. 보안채널 생성 시 사용한 클라이언트 응용인스턴스인증서를 서버에게 제공하여 인증을 하고, 난수를 생성하여 서버로 보낸다. 서버는 클라이언트인증서를 검증하고, 검증에 성공하면 난수를 전자서명하여 클라이언트로 보낸다. 클라이언트가 돌아온 난수를 검증함으로써 세션 생성과정이 완성된다.

• 4단계 : 세션 활성화

세션활성화는 세션을 사용하는 사용자를 인증하고 권한을 확인하기 위한 과정이다. 세션활성화 요청에서는 사용자토큰(인증서 등)과 클라이언트 소프트웨어인증서가 전송된다. 서버는 소프트웨어인증서를 검증하고, 사용자토큰을 확인한 후 세션을 활성화 한다.



〈그림 7. OPC UA 세션생성 및 활성화 과정〉

4.2.2. 사용자 변경 (Impersonation 또는 Log-over)

세션을 사용하는 사용자를 세션이 종료되기 전에 변경할 필요가 발생할 수 있으며 이를 위해서 OPC UA에서는 사용자변경 기능을 제공한다. 예를 들어, 운영자의 근무교대로 운영자가 변경되어야 할 경우가 있으며, 이 경우 새로운 세션을 맺기보다는 기존의 세션에서 사용자를 변경함으로써 시스템을 효율적으로 운영할 수 있다. 이 기능은 세션활성화 기능을 다시 호출함으로써 실행 가능하다.

4.2.3. 통신 보안 기능 구현

OPC UA를 구현함에 있어 응용계층을 SOAP을 사용하거나 XML 메시지를 사용하는 경우 WS-SecureConversation을 이용해 보안채널을 형성한다. WS-SecureConversation을 사용할 경우 RST(Reqeust Security Token) 메시지와 RSTR(Request Security Token Response) 메시지를 이용해 보안채널을 형성한다. OPC UA를 구현함에 있어 응용계층을 OPC UA 바이너리로 구현할 경우, UASC(OPC UA Secure Conversation)를 사용한다.

단 WS-SecureConversation을 사용하는 경우, 보안채널을 형성한 후 획득된 SCT(Security Context Token)을 이용하여 세션키를 유도하여 세션을 생성한다. 이때 세션키 생성 방법은 UA Secure Conversation에서와 동일하게 TLS 표준의 p_sha1을 사용한다. 생성된 세션키는 DerivedKeyToken에 저장된다.

V. 결론

이제 표준화 또는 산업표준으로 규격이 공개된 산업용 프로토콜 대부분에 대한 통신보안 기능은 규격화 되었다. DNP3, Modbus, IEC 61850, OPC UA 등 대부분의 산업제어시스템에서 사용하고 있는 프로토콜에 대해 통신보안 적용이 가능하다. 하지만 아직도 대부분의 상용 제품에는 보안기능이 배제된 채 판매가 되고 있으며, 기존에 설치된 대부분의 산업제어시스템에도 보안기능은 적용되지 않았다. 산업제어시스템에 대한 사이버 위협이 증가하면서 보안대책 적용에 대한 요구는 끊임 없이 제기되지만 아직 적용은 더디다. 이는 국내에서는 아직 공개된 사고가 없다는 안일한 생각과 높은 투자비용 때문으로 생각된다.

한편으로는 가용성과 빠른 응답 시간이 중요시 되는 산업제어시스템 운영환경 상 성능이 검증되지 않은 보안기술을 적용할 수 없기 때문이기도 하다. 실제로 국내에서는 보안이 적용된 DNP3, IEC61850, OPC UA 등의 프로토콜을 운용함으로써 발생하는 성능 저하에 대해 실증한 사례가 없다. 따라서 서둘러 산업용 통신 프로토콜의 보안기술에 대한 실용성 검증을 수행할 수 있도록 하고, 공정한 실용성 검증 결과를 바탕으로 현재 운용되는 산업제어시스템에 보안기술을 적용할 수 있도록 유도해야 할 것이다. 이를 통해서 보다 안전한 산업제어시스템 운영환경을 구축할 수 있을 것이다.

References

[1] Eric M. Hutchins, Michael J. Clopert, and Rohan M. Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin Whitepaper, Jan 2011.

[2] Cliff Wang and Zhou Lu, “Cyber Deception: Overview

and the Road Ahead," IEEE Security & Privacy, Volume 16, Issue 2, March/April 2018.
[3] Samuel East, Jonathan Butts, Mauricio Papa, and Sujeet Shenoi, "A Taxonomy of Attacks on the DNP3 Protocol," Critical Infrastructure Protection III ICCIP 2009, pp. 67-81, 2009.
[4] "IEEE Standard for Electric Power Systems Communications - Distributed Network Protocol (DNP3)," in IEEE Std. 1815-2012 (Revision of IEEE Std. 1815-2010), Oct 2012.
[5] "Telecontrol equipment and systems - Part 5-7: Transmission protocols - Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351)," IEC TS 60870-5-7:2013, 2013.
[6] "Power systems management and associated information exchange - Data and communications security - Part 5: Security for IEC 60870-5 and derivatives," IEC TS 62351-5:2013, 2013.
[7] "Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS," IEC TS 62351-4:2007, 2007.
[8] "Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850," IEC TS 62351-6:2007, 2007.
[9] R. E. Mackiewicz, "Overview of IEC 61850 and Benefits," 2006 IEEE PES Power Systems Conference and Exposition, pp.623 - 630, 2006.
[10] "OPC UA Architecture - Part 2: Security Model," IEC TR 62541-2:2010, 2010.

Biographies



이건희

2001년: 아주대학교 정보 및 컴퓨터공학부 학사
2003년: 아주대학교 정보통신전문대학원 정보통신공학 석사
2009년: 아주대학교 정보통신전문대학원 정보통신공학 박사
주요 관심분야: ICS Security, Smart grid Security, M2M authentication, Access Control
E-mail: icezzoco@nsr.re.kr

스마트공장 사이버 위협과 보안 기술

김기현
R&D Center, NNSP Co. Ltd.

Abstract

정부는 제조 혁신과 경쟁력 강화를 위해 국가 차원의 전략으로 스마트공장 구축·보급 확산을 추진하고 있으며 일부 스마트공장 구축에 따른 기술유출방지에 힘쓰고 있으나 전반적인 보안 대책은 미흡한 실정이다. 본고에서는 스마트 공장을 포함한 산업제어시스템에 대한 사이버 위협과 전반적인 산업 보안 기술 동향을 살펴볼 것이다. 우선 산업제어시스템 보안 위협과 사례를 살펴보고 스마트공장 네트워크 보안 아키텍쳐를 소개한다. 분석한다. 다음으로 스마트공장 산업용 이더넷과 IT 보안 한계를 살펴보고 산업제어시스템 보안 기술 현황을 소개한다. 마지막으로 사이버 공격으로 인한 스마트공장 운영 중단 문제를 해결하기 위한 선제적인 제조공정 이상징후 인지 과제를 소개하고 결론을 내린다.

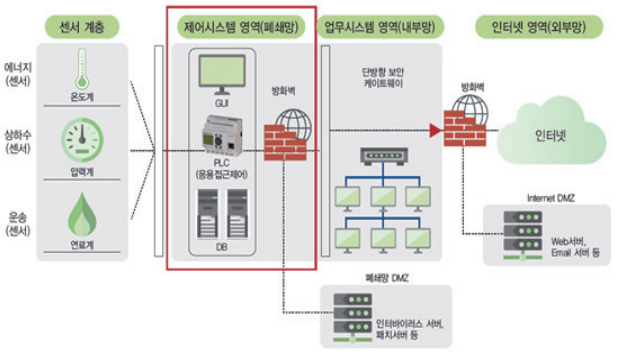
I. 서론

정부는 스마트공장을 제품의 기획, 설계, 생산, 유통, 판매 등 전과정을 IT기술로 통합, 최소비용·시간으로 고객맞춤형 제품 생산을 지향하는 공장[1]으로 정의하고 제조업의 스마트 혁신을 촉진하고 있다.

스마트공장은 생산 현장의 설비제어 자동화로부터 시작하여 공장 통합운영으로 이어지고 생산프로세스를 관리하기 위한 MES (Manufacturing Execution System), ERP (Enterprise Resource Planning), PLM (Product Lifecycle Management) 등과 연계되어 공장 제조망과 비즈니스망 간 상호 자료교환이 이루어지므로 비즈니스망 시스템이 해킹될 경우 생산 현장인 공장까지 영향을 미칠 수 있으나 보안 대책은 미비한 실정이다.

스마트공장 보안을 위한 국내 가이드는 한국인터넷진흥원(KISA) “스마트공장 중요정보 유출방지 가이드”[2]와 스마트공장추진단과 고려대학교의 “스마트공장을 위한 최소 정보보안가이드라인”[3] 정도이다.

한국인터넷진흥원(KISA) “스마트공장 중요정보 유출방지 가이드”에서는 공장제어시스템에 대한 원격 제어나 모니터링, 외부 네트워크와의 연결 등으로 인해 인해 발생하는 새로운 보안위협이 기업의 중요정보 유출로 이어지지 않도록 대비하고 있다.



〈그림 1. 산업제어시스템 네트워크 구성도(KISA)〉

그림 1에서와 같이 가이드라인에서는 수직적·수평적 통합을 유기적으로 구현하는 스마트공장 개념보다는 제어시스템 영역을 폐쇄망으로 구성하기 위한 기반시설 보호 개념이 강조되어 있다.

스마트공장추진단과 고려대학교의 “스마트공장을 위한 최소 정보보안가이드라인”에서는 스마트공장 도입을 고려하고 있는 업체에 대한 최소한의 정보보안 대응력을 마련하고 있으나 정보보호 관리체계(ISMS, Information Security Management System)에 기반한 IT 보안 대책과 유사하다.

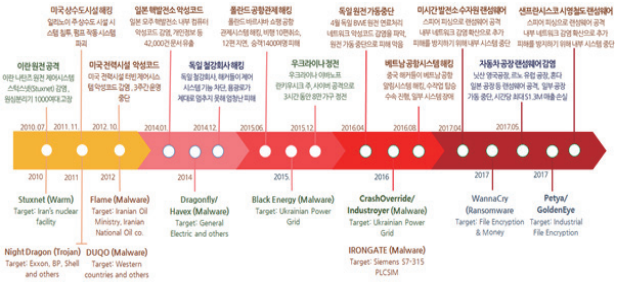
국내 스마트공장 보안은 가이드라인과 유사하게 일부 스마트공장 도입 기업을 대상으로 한 기술유출방지 시스템 구축 사업이 지원 중에 있으며 비인가 트래픽 기반의 접근제어와 같은 기존 IT보안 기술이 적용 되고 있다.

본고를 통해 스마트 공장을 포함한 산업제어시스템에 대한 보안 위협과 보안 기술 동향을 살펴볼 것이다. 본고는 다음과 같이 구성되어 있다. 2장에서는 산업제어시스템 보안 위협과 사례를 살펴보고 3장에서는 스마트공장 네트워크 보안 아키텍쳐 소개한다. 4장에서 스마트공장 산업용 이더넷과 IT 보안 한계를 살펴보고 5장에서 산업제어시스템 보안 기술 현황을 소개한다. 그리고 6장에서 결론을 내린다.

II. 산업제어시스템 보안 위협과 사례

2016 Global CEO Outlook[4]에 의하면 보안장비 도입 등 사이버 위협에 대비하고 있는 기업은 25% 수준이며, 이로 인해 사이버공격에 의한 제조설비 가동이 중단되는 사례가 계속적으로 증가하고 있다.

그림 2는 산업제어시스템 보안위협 및 사례를 나타내고 있다. 산업제어시스템에 대한 공격은 2010년 이란 원전을 공격했던 스턱스넷(Stuxnet)을 시작으로 2015년 우크라이나 정전 등 주로 기반시설이 대상으로 나타나고 있다.

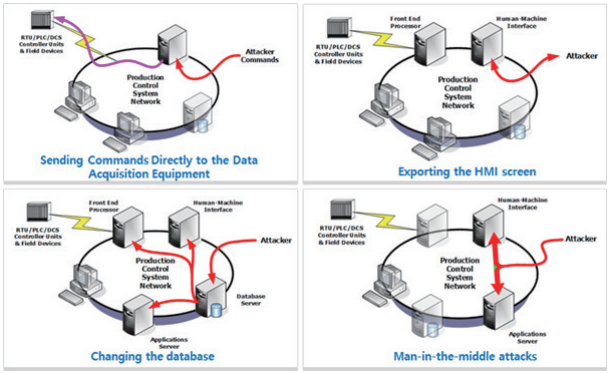


〈그림 2. 산업제어시스템 보안위협 및 사례〉

스마트공장에 대한 공격은 2014년 독일 철강회사 해킹을 시작으로 최근 랜섬웨어(RanSomeware)에 의한 공격이 증가하고 있다. 2014년 12월 독일 BSI 보고서에 의하면 독일 철강공장의 제어설비 해킹으로 용광로를 제어·차단하지 못하여 물리적으로 엄청난 피해 발생하였으며 2017년 05월 닛산 영국공장, 르노 유럽공장, 혼다 일본공장 등이 랜섬웨어 공격을 받아 일 공부 공정이 중단되었으며 시간당 최대 $1.3M 매출 손실 발생하였다. 랜섬웨어 페트야 변종 골든아이의 경우 50%이상 산업관련 기업을 공격하고 있으며 주요 감염이 보고된 곳으로 러시아 석유 회사 로즈네프트, 철강회사 에브라즈, 덴마크 선박 회사 A.P.몰러-머스크, 우크라이나 보리스필 공항, 미국 제약회사 머크, 체르노빌 방사능탐지 시스템 등이 있다.

스마트공장의 산업제어시스템에 대해 불안전한 원격 유지보수, 내부망 사용자와의 서버 공유, 불안전한 무선 시스템, 감염된 노트북, 감염된 USB, 감염된 PLC 프로젝트 파일 등 다양한 잠재적 위협 경로가 존재한다.

미국 국토안보부 ICS-CERT(Industrial Control System - Computer Emergency Response Team)는 제어시스템 공격 경로[5]를 그림 3과 같이 소개하고 있다.

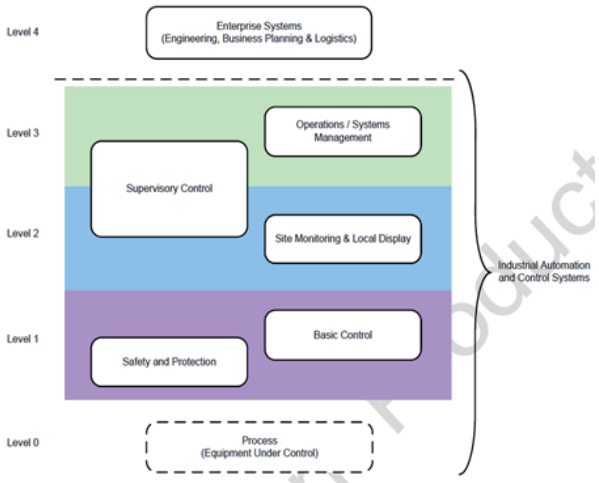


〈그림 3. 제어시스템 공격 경로〉

위 그림과 같이 산업제어시스템 공격 경로는 장치로의 직접 명령 전송, HMI(Human Machine Interface) 해킹, 데이터베이스 변경, 중간자(MITM, Man-In-The-Middle) 공격 등을 소개하고 있다. 이처럼 산업제어시스템 네트워크는 다양한 컴퓨팅과 통신 장치로 구성되어 있으며 공정 설비, 네트워크, 운영체제 및 소프트웨어 응용 등에 대한 지식이 있는 사람이 IT 기술과 OT 기술을 이용하여 여러 방법으로 접근할 수 있다.

III. 스마트공장 네트워크 보안 아키텍쳐

ISA/IEC 62443[6] (ANSI/ISA-99[7])에서는 IACS (Industrial Automation and Control System) 보안에 대한 정의, 모델 등을 포괄하고 있으며 Purdue Enterprise Reference Architecture에 기반하여 산업제어시스템 네트워크 아키텍쳐를 제시하고 있다.

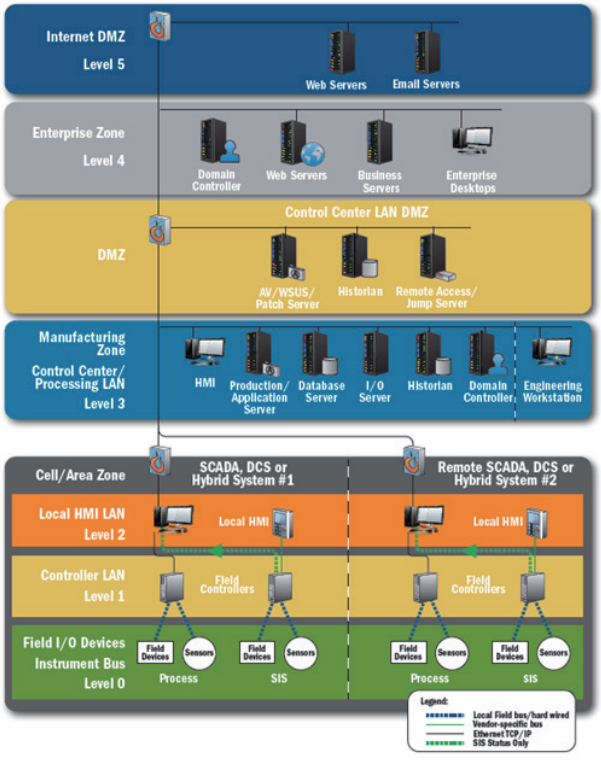


〈그림 4. ICS Reference Model〉

그림 4[6]에서 보듯 ICS 참조 모델의 Level 0는 프로세스(Process) 레벨로 센서, 디바이스, 엑추에이터 등이 있는 현장

장치 영역, Level 1은 기본 제어(Basic Control) 레벨로 PLC, RTU, IED 등이 있는 제어기기 영역, Level 2는 사이트 모니터링 및 로컬 디스플레이(Site Monitoring & Local Display) 레벨로 HMI, DCS 등이 있는 로컬 제어센터 영역, Level 3는 운영/시스템 관리(Operation/System Management) 레벨로 히스토리언(Historian), 데이터베이스 서버 등이 있는 중앙 통합운영센터 영역, Level 4는 엔트프라이즈 시스템(Enterprise System) 레벨로 MES, ERP, PLM 등이 있는 엔지니어링, 비즈니스 계획 및 로지스틱스 영역으로 구성되어 있다.

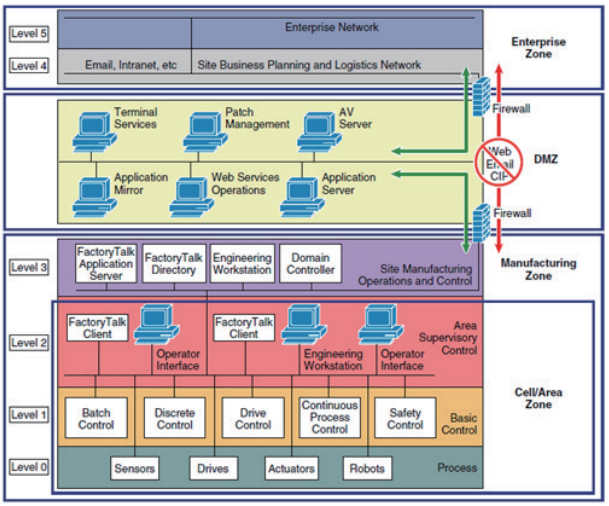
대부분 스마트공장 네트워크 아키텍쳐는 ISA/IEC 62443 (ANSI/ISA-95)에 기반하고 있으며 ICS-CERT의 ICS 심층 방어전략(Defense-in-Depth Strategies)[8]에서 ICS 보안 네트워크 아키텍처를 그림 5와 같이 권고하고 있다.



〈그림 5. Recommended secure network architecture〉

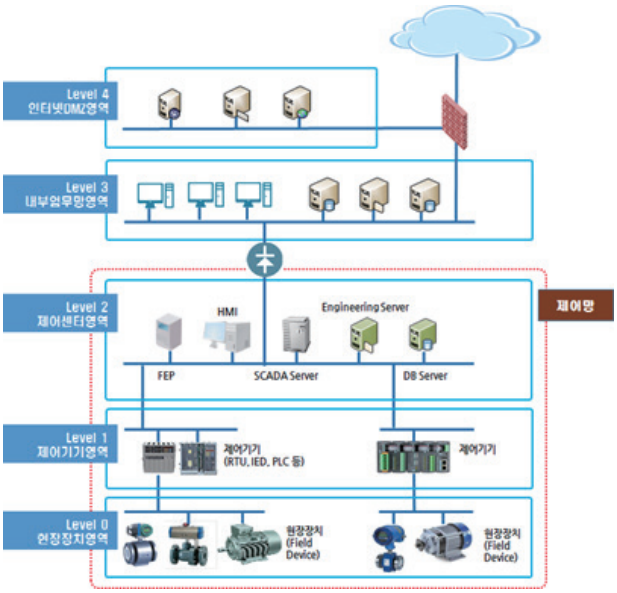
그림 5에서 보듯 ICS 보안 네트워크 아키텍처는 현장 공장 영역인 Level 0~Level 2을 Cell/Area Zone으로, 공장 통합 운영 영역인 Level 3를 Manufacturing Zone으로, MES, ERP 등의 영역인 Level 4를 Enterprise Zone으로 두고 Level 3와 Level 4 사이에 DMZ 영역을 두고 있다.

Cisco Systems와 Rockwell Automation의 CPwE(-Converged Plantwide Ethernet) Logical Framework[9]도 ISA/IEC 62443 (ANSI/ISA-95)에 기반을 두고 있으며 Level 4에 MES, ERP와 같은 Site Business Planning and Logistics Network 영역을 두고 있다.



〈그림 6. CPwE Logical Framework〉

국내의 경우 스마트공장과 같은 산업제어시스템에 대한 권고 네트워크 보안 아키텍처는 없으며 기반시설 보호를 위해 『정보통신기반보호법』에 따른 미래창조과학부 고시 "주요정보통신기반시설 취약점 분석·평가 기준", 『국가정보보안기본지침』에 따른 "국가·공공기관 제어시스템 보안 가이드라인" 등에서 안전한 제어망 연동에 대한 일방향 전송장비를 이용한 네트워크 구성 권고하고 있다. 그림 7[10]과 같이 ISA/IEC 62443의 Level 2 Cell/Area Zone과 Level 3 Manufacturing Zone을 Level 2 기반시설 제어센터 영역으로 통합하여 정의하고 있으며 Level 2(제어망)에서 Level 3(업무망)로 일방향 데이터 전송을 권고하고 있다.



〈그림 7. 산업제어시스템 운영 환경〉

Ⅳ. 스마트공장 산업용 이더넷과 IT 보안 한계

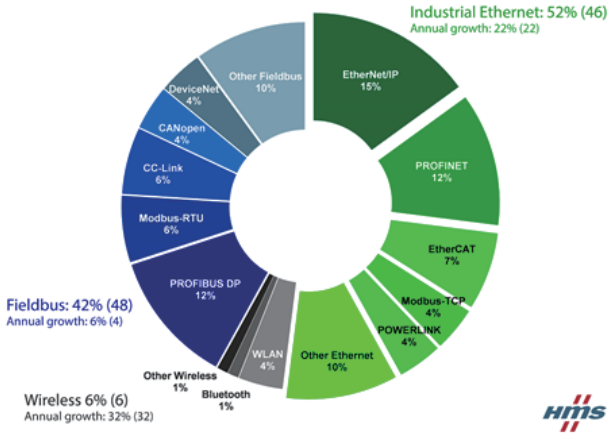
산업용 네트워크는 프로토콜 기준으로 필드버스(Field-bus), 산업용 이더넷(Industrial Ethernet) 등의 산업용 네트워크로 분류된다.

필드버스는 생산에 필요한 각종 장비/설비(Sensor, Actu-ator, Control Device 등)들의 운영 및 운전이 이루어지는 현장에서 데이터를 전송하기 위해 디지털 직렬 통신인 필드버스로 구성되어 있다.

산업용 이더넷은 산업 현장의 제어기기(PLC, Program-mable Logic Controller)의 Master & Slave 사이 통신에 인터넷 통신 개념이 도입되면서 2006년 ISO TC 184 SC5 전문위원회에서 ISO 15745 Open Systems Application Inte-gration Frameworks의 Part 4인 Ethernet-based Control System]에서 규격이 제정되어 있으며 IEC 표준으로는 IEC 61158과 IEC 61784에 정의되어 있다.

HMS Industrial Networks 시장 분석[6]에 따르면 IIoT 및 Industry 4.0에 의해 산업 기기가 점차적으로 연결되고 확대되면서 산업용 이더넷은 수년간 전통적인 필드 버스보다 빠르게 성장하여 현재 필드 버스를 따라 잡았다.

그림 8[6]에서 보듯이 사업용 이더넷은 세계 시장의 52%를 차지하고 22 %의 성장률을 보이고 있으며 이중 EtherNet/IP는 시장의 15 %를 차지하는 가장 큰 네트워크로 부상하고 있으며 PROFINET, EtherCAT, Modbus-TCP, Ethernet POWERLINK 순으로 나타나고 있다.



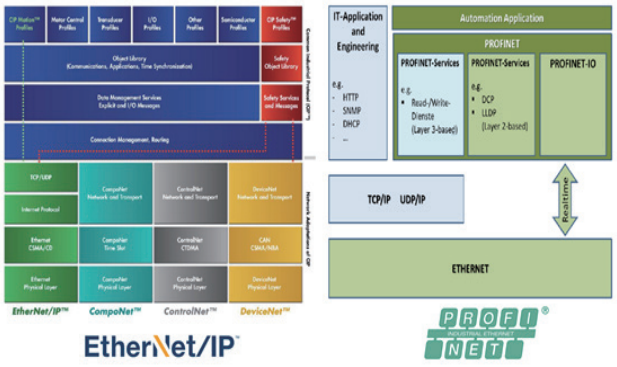
〈그림 8. 2018년 산업용 네트워크 시장 점유율〉

표 1[7]과 같이 산업용 이더넷 프로토콜들은 대부분 보안이 고려되어 있지 않으며 이더넷이 가지는 보안취약점을 안고 있다. 또한 프로토콜 특성상 멀티캐스트와 실시간 응답을 요구하는 프로토콜 특성상 암호 처리는 제한적이다.

〈표 1. ICS 프로토콜 비교〉

PROTOCOL		ENCRYPTION	AUTHENTICATION	IP / TRANSPORT LEVEL	APPLICATION LEVEL	SECURITY AND RECOMMENDATIONS
Common Industrial Protocol (CIP)	DeviceNet	NO	NO	Proprietary protocol DeviceNet™	CIP	CIP has the application level technology CIP Safety™. It is advisable to complement this with general measures for segmentation and isolation of control networks
	ControlNet	NO	NO	Proprietary protocol ControlNet™		
	CompoNet	NO	NO	Proprietary protocol CompoNet™		
	EthernetIP	NO	NO	TCP/IP		
MODBUS	Serial Modbus	NO	NO	NOT APPLICABLE (serial transmission)	Modbus (not secure)	If possible, use encryption (SSL, VPN) or traffic inspection measures like (Snort), IPS (Tofino), or similar.
	Modbus-TCP	NO	NO	TCP/IP	Modbus (not secure)	
DNP3		Only Secure DNP	Only Secure DNP	Secure DNP	Secure DNP	Implementation of secure DNP is advisable.
Profibus		NO	NO	NOT APPLICABLE (serial transmission)	Has no security measures of its own	The general recommendations for segmentation, traffic inspection and encryption should be adopted.
Profinet		NO	NO	TCP/IP UDP/IP	Has no security measures of its own	Profinet Security Guide
PowerLink Ethernet		NO	NO	Incorporates no measures of its own	Incorporates no measures of its own	PowerLink is a protocol based on Ethernet and directed towards real-time control. Segmentation measures are recommended for the architecture.
OPC		OPC UA	OPC UA	Base TCP/IP OPC UA	OPC UA	Implementation of OPC UA
EtherCAT		NO	NO	Incorporates no measures of its own	Incorporates no measures of its own	Measures for segmentation and perimeter security are recommended.

그림 9[7] EtherNet/IP와 PROFINET 프로토콜 구조에서 보듯이 산업용 이더넷 프로토콜은 TCP/IP를 사용하는 경우도 있지만 Ethernet만 사용하는 경우도 있어 방화벽(Firewall), 침입탐지/차단시스템(IDS/IPS), 가상사설망(VPN) 등 IT 보안솔루션을 그대로 적용하기는 어려우며 이들 IT 보안솔루션을 이용한 보안관제(ESM)에도 한계가 있다.



〈그림 9. EtherNet/IP와 PROFINET 프로토콜 구조〉

스마트팩공장의 현장 장치로부터 데이터를 수집하고 히스토리언(Historian) 등과 연계하기 위해 OPC(OLE for Process Control)가 많이 사용되고 있으나 Industrial 4.0에서 개별 센서와 액추에이터로부터 MES, ERP, 클라우드에 이르기까지 통신을 위하여 OPC UA(OPC Unified Architecture)가 연동 표준으로 자리잡고 있으며 IEC 62541에 정의되어 있다.

Ⅴ. 산업제어시스템 보안 기술 현황

산업제어시스템 보안 기술은 과기정통부에서 추진하고 있는 'K-ICT전략'에서 관련 산업 중 하나로 산업제어시스템 보안이 포함되어 있고, 중소벤처기업부의 중소기업 기술로드맵[13]의 정보보호분야 9개 기술개발 테마 중 하나로 스마트 산업제어시스템(ICS) 보안이 포함되어 있다.

대부분의 산업제어시스템 보안 기술들은 산업제어시스템 상의 정보를 지키기 위한 정보 보안, 적합한 권한이 없는 비인

가 접근을 막기 위한 제어기 및 제어망 부정접근방지, 주요 산업 시스템에 적용 등으로 구성되어 있으며 중소기업 기술로드맵이 그림 10과 같이 제시되고 있다.



〈그림 10. 스마트 산업제어시스템(ICS) 보안의 중소기업 기술로드맵〉

국내의 경우 산업제어시스템 보호 기술은 기반시설 보호를 위해 국가보안기술연구소, 한국전자통신연구원 등에서 화이트리스 기반 이상징후 탐지, 산업용 방화벽, 단방향 전송기술 등이 개발되었으며 한국전력공사, 한전KDN 등에서 스마트그리드 보안기술 등이 개발되고 있으나 상용화되어 보급되고 있는 솔루션은 많지 않으며 ㈜앤앤에스피, 한전KDN㈜ 등의 단방향 전송장비를, ㈜안랩, ㈜에스지에이 등의 호스트 화이트리스트 정도가 상용화되고 있는 실정이다.

해외의 경우 제어시스템 간 상호 연결과 공개된 시스템 의존성 확대로 산업 제어시스템 보안 취약성을 해소하기 위하여 산업 제어시스템 내부망 위협 방어기술 연구가 활발히 진행되고 있으며 관련 솔루션도 다양하게 출시되고 있으며 최근 인공지능 기술을 이용한 위협분석 기술이 많이 연구되고 있다.

스마트공장을 포함한 산업제어시스템에 대한 보안 기술과 솔루션은 표 3과 같이 일방향 전송장비, 산업용 방화벽, 산업용 침입탐지시스템, 시스템 화이트리스트 제품, 통합보안관리 시스템 등 다양한 솔루션 기술들이 있다.

〈표 2. 산업제어시스템 보안 기술〉

분류	기술명	레벨	적용범위	IT 보안 기술	제어 보안 기술	비고
단방향 전송 (연계/ 예방)	NNSP nNetTrust	L2,3	OPC, DB, File 등	O	O	
	Waterfall USG	L2,3	OPC, DB, File 등	O	O	
	OWL DualDiode	L2,3	OPC, DB, File 등	O	O	
산업용 방화벽 (연계/ 예방)	BELDEN Tofino	L2,1	CIP, DNP3, Modbus등	X	O	
	ETRI IndusCAP	L2	DNP3, Modbus등	X	O	
	NSR F.Switch	L2	Ethernet 기반	X	O	
	NNSP nNetGuard	L2,1	CIP, DNP3, Modbus등	X	O	
산업용 IDS/ IPS (탐지)	DigitalBond Quickdraw	L2,1	DNP3, Modbus 등	O	O	snort
	NSR W/L	L2	Ethernet 기반	X	O	
	Radiflow iSID	L2,1	DNP3, Modbus 등	X	O	
	GE Opshield	L2	DNP3, Modbus 등	X	O	
Host W/L (예방)	McAfee Application Control	L2	Whitelist	X	△	
	AhnLab TrusLine	L2	Whitelist	X	△	
통합보안 분석기술 (분석/ 대응)	GE SecurityST	L2,1	GE	X	O	
	Emerson Ovation	L2,1	Emerson	X	O	
	RAPAEL SCADA Dome	L2,1	CIP, Profinet, Modbus등	X	O	
	Cyberbit Claroty	L2,1	CIP, Profinet, Modbus등	X	O	
	Darktrace Industrial	L2,1	CIP, Profinet, Modbus등	X	O	

먼저 단방향 전송 기술은 국내에서 가장 많이 발달된 기술로 제어망(OT) 영역의 데이터를 수집하여 업무망(IT)에서 원격 모니터링할 수 있도록 데이터를 단방향으로 전달하는 기술로 OT/IT 기술과 보안기술이 모두 필요하다. 국외 제품으로 Waterfall社 USG (Unidirectional Security Gateway) 등이 있지만 국내 기술도 이와 동등한 수준으로 발달되어 있다.

민간에서 독자적으로 개발하여 상용화하고 국내용 CC인증을 획득하여 국내 주요 발전소, 정수장, 교통, 국방 등에 활발히 보급되고 있는 ㈜앤앤에스피의 nNetDiode가 있으며 국가보안기술연구소에서 한국전력공사와 단방향 전송장치를 개발하여 한전KDN으로 기술이전한 NIMA-10000이 한전을 중심으로 일부 보급되고 있으며 한국전자통신연구원에서도 사이버물리시스템에서의 물리적 단방향 보안 게이트웨이를 개발하였다.

산업용 방화벽 기술은 IT 방화벽과 달리 산업용 이더넷 프로토콜에 대한 통제 기능을 제공한다. 국외 Tofino와 같은 제품은 산업용 방화벽 제품으로 EtherNet/IP, Modbus, DNP3 등과 같은 다양한 산업용 이더넷 프로토콜을 통제한다. 국내의 경우 기반시설에서 사용되는 DNP3와 Modbus를 대상으로 한국전자통신연구원에서 IndusCAP을 개발하였으나 프로토콜이 제한적이며 국가보안기술연구소에서는 이더넷 기반의 보안스위치 F.Switch를 개발하여 기술이전되었다. ㈜앤앤에스피에서 EtherNet/IP, PROFINET, DNP3, Modbus 등 다양한 산업용 이더넷을 통제할 수 있도록 산업용 방화벽 nNetGuard를 개발하고 있으나 국내 산업용 방화벽 시장이 활성화되지 않아 판로에 어려움을 겪고 있다.

산업용 침입탐지/방지시스템은 화이트리스트와 시그너처 기반으로 이상징후를 탐지한다. DigitalBond의 Quickdraw

와 같이 오픈소스 침입탐지시스템인 snort에 add-on 방식으로 DNP3, Modbus 등에 대한 시그너쳐 기반 침입탐지시스템에서 Radiflow iSID, GE Opshield 등과 같이 화이트리스트와 시그너처 기반 이상징후 탐지와 방화벽 기능과 결합된 산업용 침입방지시스템이 주를 이루고 있다. 국내의 경우 국가보안기술연구소, 한전KDN 등에서 화이트리스트 기반 이상징후 탐지가 활발히 진행되고 있으나 별도의 독자적인 솔루션 형태보다는 통합보안분석을 위한 이상징후 센서로 개발되고 있다.

호스트 화이트리스트 기술은 HMI 등 시스템에서 인가된 프로세스와 자원, 네트워크 서비스를 화이트리스트로 구성하는 기술로 제어보안 기술이라기 보다는 IT보안 기술에 속하지만 기술 특성으로 인하여 산업제어시스템에서 사용된다. 호스트 화이트리스트는 McAfee社 Application Control, 안랩社 TrustLine 등이 있으나 제어시스템 공급 업체에서 자사 솔루션에 설치를 허용하지 않아 공급에 어려움을 겪고 있다.

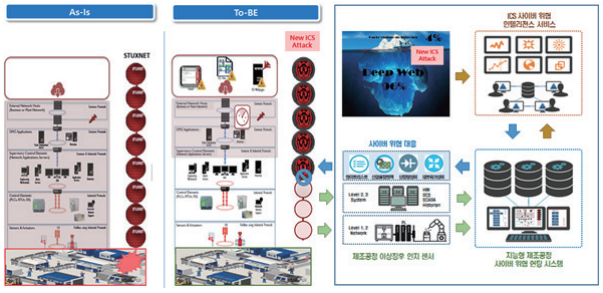
통합보안분석기술은 산업제어망에 대한 통합보안관제기술로 볼 수 있다. IT 영역에서 통합보안관제는 방화벽, 침입탐지시스템, 가상사설망 등 보안솔루션들의 이벤트를 수집하여 통합분석하지만 ICS 통합보안분석은 제어네트워크나 시스템에서 이벤트를 직접 수집하여 분석하는 경우가 많고 대부분 산업용 침입탐지시스템을 이상징후 탐지 센서로 포함하는 경우가 많다. GE SecurityST, Emerson Ovation 등과 같이 자사 제어시스템에 대한 통합분석 기능을 제공하는 솔루션에서 RAPAEL SCADA Dome, Cyberbit Claroty, Darktrace Industrial 등과 같이 산업제어시스템 네트워크에 대한 이상징후 탐지 및 위협분석 기능을 독자적으로 제공하는 형태의 솔루션들이 나오고 있으며 대부분 인공지능 기술을 사용한다.

국내의 경우 산업제어망에 대한 통합보안분석기술은 초기 단계이며 화이트리스트 기반의 이상징후 탐지를 통합보안관제로 연결시키는 수준으로 일부 인공지능 기술이 적용되고 있다.

VI. 결론

스마트공장은 4차산업혁명과 더불어 산업제어시스템 보안 시장의 중요한 영역으로 부상하고 있다. 스마트공장에 대한 해킹은 실제 물리공간으로 확대되어 제조설비 안전은 물론 인명피해까지 이어질 수 있으며 스마트공장의 제조공정 마비는 기업 매출에 큰 타격을 입을 수 있다.

과학기술정보통신부와 정보통신기술진흥센터는 6대 공공분야(도시, 교통, 복지, 환경, 안전, 국방) 관련 사회문제를 발굴하여 ICT R&D를 활용한 해법 모색하고 있으며 스마트공장 보안과 관련하여 “사이버공격으로 인한 스마트공장 운영중단 문제해결을 위한 선제적인 제조공정 이상징후 인지” 과제를 도출하였으며 ㈜앤앤에스피, ㈜앤에스에이치씨, 아주대학교에서 개발을 진행하고 있다. 본 과제에서는 사이버 공격에 취약한 제조설비의 가동중단을 미연에 방지하기 위하여 제조공정 네트워크와 시스템에 대한 이상징후를 탐지하고 사이버 킬체인(Cyber Kill-Chain) 분석과 인공지능 기법을 이용하여 ICS 보안 위협 헌팅하고 사이버 위협에 대응함으로써 갑작스런 제조 설비의 가동중단을 예방하고자 한다. 또한 다크웹 등의 오픈정보를 이용하여 ICS(Industrial Control System) 사이버 위협 정보를 수집하고 ICS에 특화된 악성코드를 분석하여 인텔리전스 서비스로 제공함으로써 최신 ICS 사이버 공격에 선제적으로 대응하고 스마트공장에 대한 보안 위협을 획기적으로 감소시키고자 한다. 본 과제의 진행에 있어 기술개발부터 지속적으로 수요기관 의견을 반영하는 ICT 리빙랩 방식 도입하고 있으며 사이버 위협으로 인한 스마트공장 운영 중단 문제를 실질적으로 해결할 수 있는 기술개발이 되도록 힘쓰고 있다.



〈그림 11. 스마트공장 운영중단 문제해결 개념도〉

마지막으로 스마트 산업제어시스템 보안 시장은 제품 관련된 직접적인 시장 외에도 서비스 시장을 포함한 지속적인 성장이 전망되며, 2017년 90억달러 규모에서 2021년 126억달러 규모로 연평균 성장률 7%의 산업 발전 가능성이 높은 분야[14]로 국내 산업제어시스템 보안 기술을 활성화하고 국제 경쟁력있는 제품으로 수출과 연계함으로써 향후 전략적 먹거리 산업으로 육성할 필요가 있다.

Acknowledgement

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행하고 있는 연구임 (No. 2018-0-00336, 사이버공격으로 인한 스마트공장 운영중단 문제해결을 위한 선제적인 제조공정 이상징후 인지)

References

[1] 관계부처 합동, 「제조업 혁신 3.0 전략」 실행대책, 2015. 03.

[2] 한국인터넷진흥원, 스마트공장 중요정보 유출방지 가이드, 2017. 03.
[3] 스마트공장추진단, 고려대학교, 스마트공장을 위한 최소 정보보안 가이드라인, 2016. 09.
[4] KPMG International, Global CEO Outlook, 2016. 08.
[5] ICS-CERT, https://ics-cert.us-cert.gov/Introduction-Recommended-Practices
[6] IEC TS 62443-1-1:2009, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models, Jul. 2009.
[7] ISA-95.00.01-CDV3, Enterprise-Control System Interation, Part 1: Models and Terminology, 2008.
[8] ICS-CERT, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, 2016. 09.
[9] Cisco Systems, Rockwell Automation, Converged Plantwide Ethernet(CPwE) Design and Implementation Guide, 2011. 09.
[10] 국가보안기술연구소, 산업제어시스템 보안요구사항, 2017. 11.
[11] HMS Industrial Networks, Industrial Ethernet is now bigger than fieldbuses, 2018. 02..
[12] INCIBE(Spanish National Cyber-security Institute), Protocols and Network Security in ICS Infrastructures, 2015. 05.
[13] 중소벤처기업부, 중소기업기술정보진흥원, 기술기업 기술로드맵 - 정보보호, 2018.
[14] MarketsandMarkets, Industrial Control Systems Security Market by Solution, Service, Security Type, Vertical, and Region - Global Forecast to 2022, 2017.06.

Biographies



김기현

1993년: 경북대학교 전자공학과 학사
1995년: 경북대학교 전자공학과 석사
2011년: 충북대학교 컴퓨터공학과 박사
관심분야: 산업제어시스템 보안, 네트워크 보안, 보안관리
e-mail: khkim@nnsp.co.kr

ETRI
한국전자통신연구원
Electronics and Telecommunications Research Institute



제4차 산업혁명을 선도하는

ICT Innovator

ICT Innovator leading the 4th Industrial Revolution

ETRI의 최첨단 기술은
새로운 영역과 새로운 가치를 만들어내고 있습니다.
꿈꾸는 모든 것을 현실로 구현하는 기술,

ETRI의 첨단 ICT기술은
세상을 더욱 풍요롭게 만들어갑니다.