Journal of Digital Convergence
Vol. 16. No. 9, pp. 179-185, 2018

ISSN 1738-1916
https://doi.org/10.14400/JDC.2018.16.9.179

해시를 활용한 사이버킬체인 기반의 사물인터넷 보안 정책

정소원[1], 최유림[1], 이일구[2*]
[1]성신여자대학교 융합보안학과 학사과정
[2]성신여자대학교 융합보안공학과 조교수

Cyber KillChain Based Security Policy Utilizing Hash for Internet of Things

So-Won Jeong[1], Yu-Rim Choi[1], Il-Gu Lee[2*]
[1]Student, Department of Convergence Security, Sungshin University
[2]Assistant Professor, Department of Convergence Security Engineering, Sungshin University

요 약 4차 산업 혁명의 정보통신기술 산업 분야의 새로운 성장 동력으로 주목받는 사물인터넷 기술은 단순한 보안 기술을 넘어 신뢰성이 필요하다. 이러한 신뢰성은 IoT 제품의 기획 및 설계 단계부터 고려되어 제품을 개발하고 평가하며 사용하는 모두가 보안성을 측정하고 신뢰할 수 있는 시스템이 구축되어야 한다. 사용되는 IoT 기기 수의 급격한 증가와 사용 생명주기의 증가는 소프트웨어 패치와 업데이트 및 관리의 어려움으로 인한 보안 취약성 증가로 이어진다. 본 논문에서는 IoT 산업 분야의 기술적·정책적 동향을 분석하고 이를 통해 IoT 기기의 보안성과 확장성의 한계점을 분석한다. 이러한 한계점을 보완하기 위해 블록체인의 요소 기술인 해시를 활용해 소프트웨어의 무결성을 자동 검증하는 방법을 제안한다. 해시를 활용한 소프트웨어 무결성 자동 검증 방법으로 사물인터넷의 보안성과 확장성을 강화하고, 제안하는 보안 기술 적용을 위한 정책적 솔루션을 제시한다.

주제어 : 사물인터넷, 사이버킬체인, 블록체인, 무결성, 소프트웨어

Abstract Technology of Internet of Things (IoT) which is receiving the spotlight recently as a new growth engine of Information Communications Technology (ICT) industry in the 4th Industrial Revolution needs trustworthiness beyond simple technology of security. IoT devices should consider trustworthiness from planning and design of IoTs so that everyone who develop, evaluate and use the device can measure and trust its security. Increased number of IoTs and long lifetime result in the increased securituy vulnerability due to the difficulty of software patch and update. In this paper, we investigated security and scalability issues of current IoT devices through research of the technical, political and industrial trend of IoT. In order to overcome the limitations, we propose an automatic verification of software integrity utilizing and a political solution to apply cyber killchain based security mechanism using hash which is an element technology of blockchain to solve these problems.

Key Words : Internet of Things, Cyber KillChain, Blockchain, Integrity, Software

*This work was supported by the Sungshin Women's University Research Grant of 2018-1-11-050/1
(본 연구는 성신여자대학교 연구과제 (2018-1-11-050/1) 지원으로 수행하였음.)
*Corresponding Author : Il-Gu Lee (iglee@sungshin.ac.kr)
Received July 20, 2018 Revised August 27, 2018
Accepted September 20, 2018 Published September 28, 2018

1. 서론

사물인터넷 (Internet of Things, IoT) 기술은 4차 산업혁명의 정보통신기술 (Information Communication Technology, ICT) 산업 분야의 새로운 성장 동력으로 주목받고 있다[1-3]. 시스코에 따르면 인터넷에 연결되는 IoT 장치 수가 2018년에는 350억 개이고 2020년에는 500억 개에 달할 것으로 전망하고 있다[4]. 언제 어디서든 인터넷에 연결되어 서비스를 제공하는 IoT 기기는 사용자에게 향상된 편의성을 제공하고 업무의 효율성을 증진시키는 장점이 있지만 부작용도 있다. IoT 기기는 신뢰할 수 없는 불특정 다수의 사물들과 연결되어 데이터를 공유해야 하고, 보안 위협의 파급효과가 크며 인간의 생명, 사회 안전, 금융 자산 등 신체적, 물질적 피해로 이어질 수 있다[5-8]. 실제로 IoT 기기로 구성된 봇넷(Botnet)으로 최대 규모의 분산 서비스 거부 공격 (Distributed Denial of Service, DDoS) 공격이 있었으며 미국 전역과 서유럽에 막대한 네트워크 중단 상태를 야기한 사례도 있었다[9].

이러한 배경 속에서 IoT를 상용화하기 전에 보안 내재화를 제품과 서비스의 기획, 설계의 필수 요건이 되고 있다. 그러나 4차 산업혁명 시대에는 보안의 3대 요소인 무결성, 가용성, 기밀성이 뛰어나다고 보안성을 인정하지 않는다. 단순한 보안 (security)을 뛰어넘는 측정·평가·보증 가능한 신뢰성 (Trustworthiness)이 요구된다. 그러므로 IoT 제품의 기획 및 설계 단계부터 필수 보안 요소가 고려되어 보안 내재화가 이루어져야 한다. 즉, 보안성을 측정하고 평가할 수 있는 기술적·관리적 체계가 제품과 서비스에 내재되어야 한다는 것이다. 또한 제품의 모든 라이프 사이클에서 사용자, 개발자와 평가자 모두가 보안성을 측정하고 관리할 수 있어야 한다.

본 연구는 IoT 기기의 동향과 분석을 통해 미래의 IoT 보안 기술 방향을 제시하고 블록체인의 요소 기술인 해시를 이용한 사이버킬체인 기반의 보안 기술과 정책적 솔루션을 제시하는 것을 목적으로 한다.

연구 논문의 2장에서는 사물인터넷 동향을 분석하고, 3장에서 사물인터넷을 위한 블록체인과 사이버킬체인 기술을 소개한 후, 4장에서 사이버킬체인 기반의 사물인터넷 보안 기술과 정책을 제안한다. 그리고 5장에서 마무리 짓는다.

2. 종래의 사물 인터넷 보안성 분석

2.1 사물인터넷 보안성 한계의 기술적 분석

IoT는 인간의 개입 없이 사물 간에 협력하여 센싱, 네트워킹, 정보 처리 과정을 거쳐 사람에게 서비스하는 사물 네트워크이다[10]. IoT의 개념은 만물이 현실과 가상세계 간 상호작용하며 정보를 공유하는 개념으로 진화하고 있으며, 제4차 산업 혁명 시대에 인간의 삶을 윤택하게 만들어줄 필수 기술로 인정받고 있다.

그러나 미래의 4차 산업혁명 시대에 대한 전망이 긍정적인 것만은 아니다. 종래의 IoT 기술은 중앙 서버에서 데이터를 처리하는 중앙 집중형 시스템으로 비용, 안전성, 보안성 등의 단점이 존재한다. 시만텍 인터넷 보안 위협 보고서에 따르면 2016년도 대비 2017년도에는 IoT 공격 증가 추이가 8.5배 증가했다[11]. IoT는 신뢰할 수 없는 불특정 다수의 사물들과 연결되어 있다는 점에서 사이버 공격에 대한 노출이 증가하고, 취약성이 증가할 수밖에 없는 약점을 갖고 있다.

IoT 보안사고가 발생하는 주요 원인은 빠른 시장에 대응하기 위해 저가의 하드웨어가 충분한 보안성 검증 없이 경쟁적으로 출시된다는 것에 있다. 그리고 다양한 기기가 출시되면서 수많은 공격 시나리오가 만들어져 이에 대해 일일이 대응하기 어려워졌다.

사물들이 스스로 알아서 정보를 주고받는 IoT는 통신 대상과 데이터에 대한 신뢰가 필수다. 그러나 IoT 장치는 저전력, 저가로 구현되어야 하므로 PC 또는 모바일 기기에서 사용하던 전통적 보안기술을 IoT 기기에 적용하는 건 불가능하다. 기존보다 최소 10배에서 수백배 길어진 라이프 타임도 보안 취약성을 높이는데 일조하고 있다. 스마트폰은 사용자의 사용 목적에 따라 애플리케이션을 선택하는 반면에 IoT 기기는 특정 목적을 위해 제작되고 그 목적으로만 사용된다. 만약 이러한 목적이 인간의 생명과 관련되어 있다면 안전 문제에 치명적이다.

IoT 환경에서 보호대상은 PC, 모바일 기기 중심이 아닌 의료기기, 자동차, 가전 등의 사물들이다. IoT 장치는 아주 작은 마이크로 컴퓨터들로 구성되어 있어, 전통적인 IT 보안 솔루션들로는 안전을 보장할 수 없다. 서비스 요구사항 분석 및 설계 단계에서부터 꼭 필요한 기능들만 선별해 제품에 내재화하는 '보안 내재화 (Security by Design)'가 요구된다. 이 보안 내재화는 IoT 장치의 소프트웨어 업데이트 및 패치가 쉽지 않고, 인접한 사물들과

언제 어디에서든 연결될 수 있는 환경적인 특수성을 고려해 수행되어야 한다.

2.2 사물인터넷 정책 동향 분석

선진국들은 안전한 IoT 보안 환경을 위한 법제화를 추진하기 위해 지속적이고 범국가적인 연구를 진행하고 있다. 미국과 유럽, 일본의 경우를 살펴보면 다음과 같다.

미국에서는 2016년에 IoT 보안 위협에 대처하기 위해 미국의 표준기술연구소가 IoT 디바이스에 대한 사이버 보안 가이드라인을 발표했다[12]. 또한 2017년에 미국 민주당 의원들을 주축으로 벤치마크 테스트에 기반한 IoT 기기 보안 성능 인증 프로그램 도입을 위한 '사이버 쉴드 법안'을 발의하기도 하였다.

유럽의 경우 IoT 보안에 특화된 법률은 별도로 제정되어 있지 않지만 유럽 개인정보보호법에 IoT와 관련된 '프라이버시 중심 설계'라는 규정을 통해 IoT 보안에 대비하고 있다[13]. 이 규정은 시스템 구축 단계에서부터 데이터를 보호하기 위하여 생산 업체들이 IoT 기기를 판매하기 위해서는 정해진 보안 가이드라인을 준수해야 한다는 것이다.

일본은 IoT 보안 인증제 도입을 준비 중이다[14]. 일본 총무성은 2017년에 IoT 관련 사이버보안 위기 확산에 대응하기 위해 IoT 보안 종합 대책을 발표했으며, 2018년 안에 정보보안정책국 설립을 생각하고 있다. 또한, 바이러스 방어 체제를 갖춘 IoT 기기에 대해서 공적인 인증제도를 2020년까지 도입할 예정이다. 이미 일본은 IoT 보안 환경 구축을 위해 2016년 경제 산업성 산하의 정보처리추진기구(IPA)를 통해 IoT 보안 가이드인 연결세계의 개발 지침과 IoT 개발의 보안 설계 가이드를 발표한 바 있다.

우리나라도 이와 같은 선진국의 행보에 발맞추어 IoT 보안위협에 대응하기 위해 법안 발의와 IoT 보안 가이드를 발표하였고 국가기관 처음으로 한국인터넷진흥원(KISA)에서 'IoT 보안 인증제'를 시행했다[15]. 그러나 이는 필수가 아닌 민간 자율 인증제로, 국내에서 IoT 인증을 받지 않더라도 판매하는데 제지를 당하거나 불이익이 없어 인증에 대한 실효성이 부족한 현실이다.

IoT의 수가 늘어날수록 기기의 보안성은 점점 더 중요해지는 추세지만, 법이나 정책적으로 그 중요성이 제대로 반영되지 않고 있는 실정이다. 더욱이 최소한의 가이드라인에 강제성이 없어서 실효성이 결여되어 있다. 따라서 이번 논문에서는 이러한 문제점을 해결하고자 관련된 기술 및 이를 실현하기 위한 정책을 제시하고자 한다.

3. 블록체인과 사이버킬체인 기술

3.1 블록체인과 사물인터넷

블록체인 기술은 기존 IoT 시스템의 한계를 개선하는데 활용될 수 있다. 운용 효율성 측면에서 별도의 중앙처리 시스템을 필요로 하지 않고 분산 방식으로 전체 시스템을 구축 비용, 중개비, 운영비용을 절감할 수 있고, 분산되어 저장되므로 디도스 공격에 강하며, 위변조가 어렵다.

IoT에 블록체인이 도입될 경우 블록체인 고유의 분산화된 보안 기능을 IoT 장치에 내장할 수 있고, 비인가 디바이스 및 데이터 위변조 문제도 해결 가능해 소프트웨어 이력과 감사 기록을 안전하게 관리할 수 있다. 스마트홈, 스마트공장, 스마트팜 등에서 IoT 장치 인증을 위해 지문 등 생체인식 정보를 블록체인에 보관하여 보안성을 강화할 수 있다.

정부와 기업체는 IoT의 보안성 강화를 위해 IoT 기술에 블록체인 기술을 접목하는 기술과 정책을 다각도로 연구하고 있다[16]. 이것은 블록체인의 분권화된 통제 기능이 사물 인터넷의 중앙서버 데이터 관리의 보안 문제를 보완하고, 데이터를 안전하게 등록하고 추적하며, 스마트 계약 기능은 안전하고 신뢰할 만한 응답 확인 방식을 실현하여 IoT 장치끼리 데이터, 정보, 전자화폐 등 자산을 전달하거나 공유할 수 있는 인프라를 제공하기 때문이다.

3.2 사이버킬체인과 사물인터넷

킬체인은 군사 전쟁 용어로서 적군이 계획하고 있는 공격 절차를 선제 타격해 공격을 무력화시키는 개념이다[17]. 록히드마틴은 사이버 공격과 대응에 킬체인 개념을 도입해 최근 이슈가 되는 지능형 지속 공격의 대응으로 사이버킬체인 기반의 대응 기법을 제시했다[18].

사이버킬체인 기반 대응의 정수는 사이버 공격과 대응은 게임이론에 근거해 방어자의 최선은 공격자의 성공확률을 낮추고 기회비용을 높이는데 있다. Fig. 1은 사이버킬체인 기반의 공격 및 방어 모델을 보여준다. 지능형 지속 공격의 특성상 장시간 공격 대상에 대해 정보를 수집한 후 (정찰단계, Reconnaissance), 공격에 가장 경제

적이고 효율적인 사이버 무기인 악성코드를 만들고 (무기화 단계, Weaponization), 악성코드를 공격 대상에게 전달한다 (유포 단계, Delivery). 공격 대상 시스템의 취약점을 이용해 제작된 악성코드가 공격 대상 시스템 사용자에 의해 실행되면 (악용 단계, Exploitation), 공격자가 지속적으로 공격 대상 시스템에서 활동할 수 있도록 트로이목마나 백도어 등의 추가적인 악성 프로그램을 설치한다 (설치 단계, Installation). 그리고 공격 대상 시스템을 원격 제어하는 환경을 구축하고 (명령 및 제어 단계, Command and Control), 원격 통제 권한 획득 후 목적을 달성하면 흔적을 은닉하거나 시스템을 파괴한다 (목적 달성 단계, Actions on Objects).

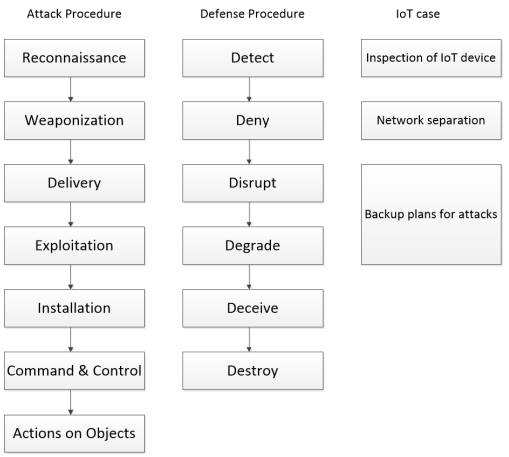

Fig. 1. Cyber killchain based attack and defense procedures for IoT security

이러한 사이버 공격 체인에 대한 대응 방법은 공격자의 공격 행위를 사전에 발견하는 탐지 단계 (Detect), 공격자의 접근시도를 차단하는 거부 단계 (Deny), 공격 흐름을 방해하는 방해 단계 (Disrupt), 공격을 위한 시간을 지연시키거나 공격 효과를 감소시키는 저하 단계 (Degrade), 공격자를 속이는 기만 단계 (Deceive), 공격자 시스템 및 공격 도구를 손상시키는 파괴 단계 (Destroy)로 구성된다.

사이버킬체인 기반의 대응 방법은 사물 인터넷에 대한 지능형 지속 공격을 지연시키거나 무력화시키는 효과적인 보안 체계로 활용된다. 예를 들면 연결된 IoT 기기들을 탐지 단계에서 미리 검사하여 운영 환경과 관련된 취약점을 파악할 수 있다. 하나의 네트워크에 연결된 IoT 기기들은 다른 네트워크와는 연결될 수 없도록 망분리 되어야한다 (거부 단계). 또한 미리 IoT 기기의 기능 및 데이터에 대한 백업 장치를 갖춰 놓음으로써 공격 효과를 낮출 수 있다 (저하 단계). 이와 같은 사이버 공격 체인에 대한 대응 단계가 사물인터넷 보안에 효과적으로 접목될 수 있다.

4. 사물인터넷 보안

4.1 해시를 활용한 사이버킬체인 기반의 사물인터넷 보안

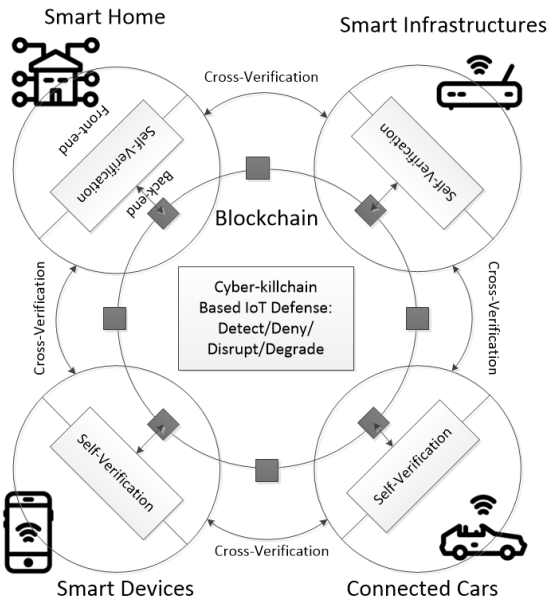

Fig. 2. IoT security system for cyberkill chain defense utilizing hash code on blockchain

본 논문에서는 블록체인의 해시 기술을 사용해 IoT 소프트웨어 무결성을 체크하고 연결하려는 인접 IoT 장치의 보안성을 측정해 사이버킬체인 상의 탐지, 거부, 방해 단계를 강화할 수 있는 효과적인 IoT 보안 체계를 제안한다. Fig. 2는 이러한 제안에 따라 해시 값을 이용한 사물인터넷보안 방법이 사이버킬체인의 방어 단계 중, 탐지, 거부, 방해의 3단계에 해당됨을 보여준다.

Fig. 3은 소프트웨어, 라이브러리, 펌웨어 등의 IoT를 동작시키는 소프트웨어 코드를 해시코드 데이터베이스로 관리해 IoT 기기에서 소프트웨어를 업데이트하거나 데이터를 공유하는 장치와 연결할 때 소프트웨어의 해시코드를 비교하는 방법을 보여준다.

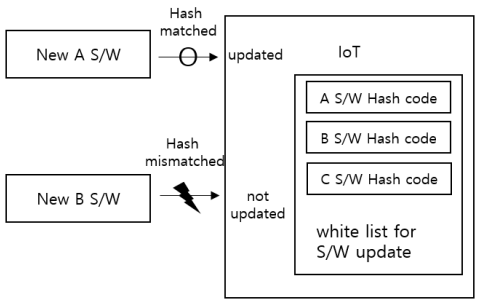

Fig. 3. Integrity verification for software update.

그림에서와 같이 새로운 소프트웨어 A는 IoT 장치의 화이트리스트 상의 소프트웨어 A의 해시코드와 일치하므로 업데이트되지만, 소프트웨어 B는 일치하지 않아서 업데이트되지 않게 된다. 업데이트 혹은 설치할 소프트웨어에 악성코드가 추가되었다면 등록된 해시코드와 다른 값을 가지게 되므로 공격을 빠르게 감지해 공격 체인을 끊어 사이버 공격을 무력화 시킬 수 있게 된다.

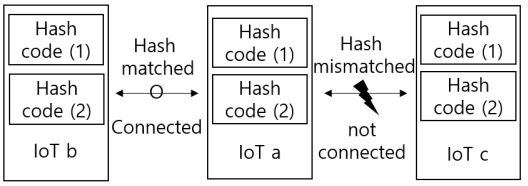

Fig. 4. Integrity verification for IoT connection.

Fig. 4는 인접한 사물과 데이터를 공유할 때, 연결할 장치의 소프트웨어 해시코드를 체크한 후 비정상적인 해시코드를 가질 경우에는 연결을 거부함으로써 사이버 위협에 대한 노출을 줄이고, 비정상적인 해시코드를 가진 IoT 장치는 네트워크 참여 기회가 제한되므로 자연스럽게 소프트웨어 업데이트를 할 수 밖에 없는 상황을 보여준다.

그림에서와 같이 사물인터넷 기기 A, B, C를 안전하게 연결하기 위해 각 기기의 소프트웨어의 해시 값을 비교함으로써, 위험에 노출되었을지도 모를 기기에 대해 사전적으로 연결을 차단한다. 연결할 사물인터넷 기기에 악성코드가 내재되어 해시 값이 일치하지 않는다면 이 기기는 해당 네트워크에 연결될 수 없으므로 이는 사이버킬체인의 방어 단계 중 탐지, 거부, 방해 단계에 해당된다.

위의 두 방법은 보안성이 확인된 소프트웨어의 해시코드를 화이트 리스트로 사용해 IoT에 사용되는 소프트웨어와 인접한 IoT 장치의 보안성을 확인하는 무결성 검증 방법이다.

4.2 해시를 활용한 사이버킬체인 기반의 사물인터넷 보안을 위한 정책 제언

현재 우리나라에는 IoT 산업과 관련하여 권고에 불과한 가이드라인이나 보안인증제도만 있을 뿐 강제적인 법적인 정책이나 제도는 없는 실정이다. 그러나 현재 우리나라를 비롯하여 여러 나라들에서는 정보보호제품의 보안성을 평가하는 CC (Common Criteria) 평가 제도를 도입하여 평가하고 있다. CC 평가 제도는 ISO/IEC 15408의 또 다른 이름이며, IT 제품의 보안성을 평가하기 위한 보증 수단의 공통 요구사항들을 제시함으로써, 보안 기능성이 있는 IT 제품의 개발 및 평가를 위한 지침으로 활용된다[19]. CC는 총 3부로 구성되어 있는데, 1부는 소개 및 일반 모델, 2부는 보안기능요구사항이고 3부는 보증요구사항이다. 이번 논문에서는 평가대상인 제품과 관련된 요구사항을 정의하는 CC 2부의 보안기능요구사항에 정책적 항목을 추가하는 것으로 한다.

CC 2부의 보안기능요구사항들은 TOE 보안 행동을 설명하고자 하는 것으로 보호프로파일 및 보안목표 명세서에서 서술된 보안 목적을 만족시키기 위해 사용된다. 보안기능요구사항은 모두 보안감사, 통신, 암호지원, 사용자 데이터 보호, 식별 및 인증, 보안관리, 프라이버시, TSF보호, 자원 활용, TOE 접근, 안전한 경로 채널의 11개의 클래스로 이루어져 있다.

Table 1. Newly suggesting FAU class of Security Functional Requirement.

Class	Family	Component	Element
FAU	FAU_GEN	1. Audit data generation	1.1
			1.2
		2. User identity correlation	2.1
		3. List generation of hash value for security function	3.1

본 논문에서 제안한 사이버 킬체인 기반의 IoT 보안 기술의 보안성을 실현하고 활용하기 위해서는 소프트웨어의 해시 값이 기본적으로 필요하다. 그러나 이 해시 값을 파악하기 위해 매번 연산하는 것은 시간 및 경제적 낭비가 될 수 있다. 따라서 해시 값을 해당 소프트웨어의 제조 시 연산하여 목록으로 구성해 놓아야 한다.

이를 위해 Table 1에 나타낸 것처럼 CC 2부의 보안기능 요구사항의 11개의 클래스 중, 보안관련 행동에 관련된 정보의 인식, 기록, 저장, 분석을 포함하는 보안감사 클래스인 FAU의 보안 감사 데이터 생성 패밀리에 FAU_GEN.3으로서 새로운 컴포넌트를 추가해야 한다. 추가하는 컴포넌트의 내용은 IoT에 사용될 소프트웨어에 내장된 보안 기능들의 해시 값을 제조 단계에서 미리 연산하여 소프트웨어 내부에 목록으로 갖춰 놓는 것으로 한다. 추후에 보호프로파일이나 보안 목표명세서를 작성할 때, 해당 TOE가 IoT용 소프트웨어인 경우 FAU_GEN.3을 고려해서 작성해야 하며 이것이 제대로 목록화 되어 있는지에 대해 CC 평가 요소로 추가해야 한다. 이와 같이 추가된 평가 항목은 IoT 기기의 보안성을 검증하기 위한 핵심 요소로서 IoT 설계, 개발, 테스트, 배포, 유지보수, 폐기의 전체 생명주기에서 반드시 충족해야 하는 보안성 평가·인증의 기본 필수 요건으로 정책적 강제성이 요구된다.

5. 결론

4차 산업혁명을 대표하는 기술 중 하나인 IoT의 보안은 날로 중요해지고 있다. IoT 제품 및 서비스의 편리함과 보안성을 동시에 만족시키기 위해서는 기획과 설계 단계부터 보안을 고려하여 취약점을 줄이는 코딩 방식인 시큐어 코딩 방식과 IoT 보안 인증 제도가 필수적이다. 그러나 이 제도는 권고에 불과하며 강제성을 띄고 있는 방안이 아니라서 실효성이 그리 크지는 않고, 악성코드 기반의 지능형 지속 공격 위협에 노출되어 있다.

본 논문에서는 IoT의 보안을 위해 소프트웨어를 설계할 때에 내재된 보안 기능의 해시 값을 미리 연산하여 목록화하고 이를 이용해 소프트웨어의 보안성을 검사하는 블록체인 기반의 무결성 검증 방식인 IoT 사이버킬체인 방식을 제안하고, 이 방식이 실현되기 위해 정보보호 제품의 보안성을 평가하는 CC의 항목에 적용하는 것을 제안했다.

본 연구 결과를 토대로 IoT 사이버킬체인 플랫폼을 구축하고 제안한 방식의 효율성을 검증할 계획이다. 본 연구 결과는 사용하는 소프트웨어 해시값으로 구성된 정적 화이트리스트에 기반하고 있는데, 후속 연구에서는 IoT 서비스 제공자와 사용자 편의성을 제고하기 위해 동적으로 화이트리스트를 업데이트하는 방식도 연구할 계획이다.

또한 CC 요구사항의 평가 후, 보안성으로 표시된 보안레벨 또는 퍼센트 형식의 보안성은 시각화하여 주변의 IoT기기의 보안성을 측정하고 관리하는 테스트베드를 구축해 본 연구에서 제안한 사이버킬체인 기반의 IoT 보안의 유효성을 증명하는 연구를 진행할 계획이다.

REFERENCES

[1] O. Bello & S. Zeadally. (2016). Intelligent device-to-device communication in the internet of things. *IEEE Systems Journal, 10(30),* 1172-1182.

[2] S. H. Lee & D. W. Lee. (2016). Actual Cases for Smart Fusion Industry based on Internet of Thing. *Journal of the Korea Convergence Society, 7(2),* 1-6.

[3] S. H. Lee, D. H. Shim & D. W. Kee. (2016). Actual Cases of Internet of Thing on Smart City Industry. *Journal of Convergence for Information Technology, 6(4),* 65-70.

[4] CISCO, Internet of Things, https://www.cisco.com/c/dam/en/us/products/collateral/e/internet-of-things/at-a-glance-c45-731471.pdf (last access: 2018.07.10.).

[5] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang & W. Zhao. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal, 4(5),* 1125-1142.

[6] Y. Yang, L. Wu, G. Yin, L. Ki & H. Zhao. (2017). A survey on security and provacy issues in internet-of-things. *IEEE Internet of Things Journal, 4(5),* 1250-1258.

[7] S. Hong & H. J. Sin. (2017). Analysis of the Vulnerability of the IoT by the Scenario. *Journal of the Korea Convergence Society, 8(9),* 1-7.

[8] H. J. Mun, G. H. Choi & Y. C. Hwang. (2016). Countermeasure to Underlying Security Threats in IoT communication. *Journal of Convergence for Information Technology, 6(2),* 37-44.

[9] C. Kolias, G. Kambourakis, A. Stavrou & J. Voas. (2017). DDoS in the IoT: Mirai and other botnets. *Computer, 50(7),* 80-84.

[10] J. Gubbi, R. Buyya, S. Marusic & M. Palaniswami. (2013). Internet of Things (IoT): A vision, architecture elements, and future directions. *Future generation computer systems, 29(7),* 1645-1660.

[11] Symantec. (2018). *Internet Security Threat Report, Vol.23.*
[12] NIST. (2016). Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, NIST Special Publication 800-160 Volume 1.
[13] ENISA. (2015). Privacy and Data Protection by Design.
[14] NISC. (2016). General Framework for Secure IoT Systems.
[15] KISA. (2016). IoT common security guide for security internalization of ICT convergence products and services, *IoT Security Alliance of KISA.*
[16] I. C. Lin & T. C. Liao. (2017). A Survey of Blockchain Security Issues and Challenges, *International Journal of Network Security, 19(5),* 653-659
[17] T. Yadav & A. M. Rao. (2015). Technical Aspects of Cyber Kill Chain. *International Symosium on Security in Computing and Communication,* 438-452.
[18] Lockheed Martin Cyber KillChain, url: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (last access: 2018.07.10.).
[19] CC v3.1 Release 5. Common Criteria for Information Technology Security Evaluation (CC). url: https://www.commoncriteriaportal.org/cc/ (last access: 2018.07.10.).

정 소 원(Jeong, So Won) [학생회원]

- 2015년 3월 ~ 현재 : 성신여자대학교 융합보안학과
- 관심분야 : 정보보호
- E-Mail : wsswj123@gmail.com

최 유 림(Choi, Yu Rim) [학생회원]

- 2015년 3월 ~ 현재 : 성신여자대학교 융합보안학과
- 관심분야 : 정보보호
- E-Mail : 330julie95@gmail.com

이 일 구(Lee, Il Gu) [정회원]

- 2003년 2월 : 서강대학교 전자공학과 (공학사)
- 2005년 2월 : 한국과학기술원 정보통신대학원 (공학석사)
- 2012년 2월 : 한국과학기술원 지식재산대학원 (경영학석사)
- 2016년 2월 : 한국과학기술원 정보보호대학원 (공학박사)
- 2017년 2월 ~ 현재 : 성신여자대학교 융합보안공학과 조교수
- 관심분야 : 정보통신, 정보보호, 지식재산
- E-Mail : iglee@sungshin.ac.kr