http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.24, No.2, May 2019, pp.217-228
https://doi.org/10.7838/jsebs.2019.24.2.217

사물인터넷 기기의 안전한 사용자 인증 방안에 관한 프레임워크

Framework for Secure User Authentication of Internet of Things Devices

송용택(Yongtaek Song)*, 이재우(Jaewoo Lee)**

초 록

4차 산업혁명을 맞아 사물인터넷이 떠오르며 다양한 서비스가 생겨나고 편의성이 개선되었다. 사용빈도가 높아짐에 따라 개인정보의 유출 등과 같은 보안위협이 공존하게 되었으며 보안의 중요성이 증가하고 있다. 본 논문은 사물인터넷의 보안위협에 대해 분석하여 Fast IDentity Online(FIDO)을 사용한 사용자인증을 통하여 보안성을 강화하는 모델을 제시하고자 한다. 연구결과 향후 FIDO를 통한 2차 인증 도입을 통하여 강력한 사용자인증을 구현할 것을 제안한다.

ABSTRACT

In the 4th Industrial Revolution, the Internet of Things emerged and various services and convenience improved. As the frequency of use increases, security threats such as leakage of personal information coexist and the importance of security are increasing. In this paper, we analyze the security threats of the Internet of things and propose a model for enhancing security through user authentication using Fast IDentity Online (FIDO). As a result, we propose to implement strong user authentication by introducing second authentication through FIDO.

키워드 : 보안, 사물인터넷, 인증, FIDO
Security, Internet of Things, Authentication, FIDO

* First Author, Department of Security Convergence, Chung-Ang University(ionsea91@gmail.com)
** Corresponding Author, Assistant Professor in Department of Industrial Security, Chung-Ang University(jaewoolee@cau.ac.k)
Received: 2019-04-02, Review completed: 2019-05-27, Accepted: 2019-05-29

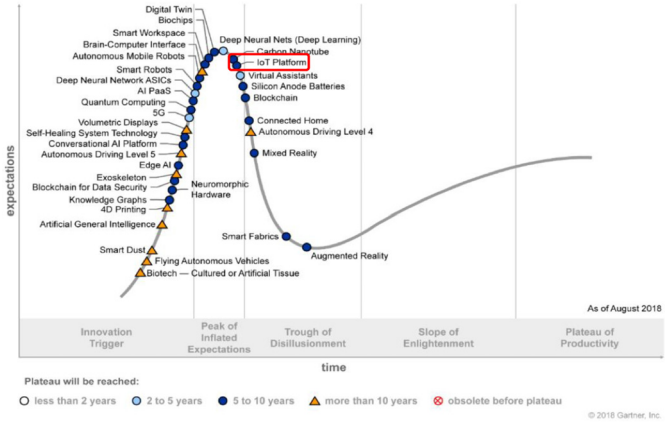
1. 서 론

사물인터넷(Internet of Things, IoT)의 도입은 일상생활과 사무공간 등에 편의성을 제공하고 업무의 효율을 증가시켰다. 하지만 동시에 Mirai Botnet과 IP 카메라의 해킹과 같은 보안 위협이 증가하고 있으며 기업정보와 개인정보의 유출이란 위협이 존재한다. 이에 따라 보안의 중요성에 대한 인식이 증가하고 있으며, 정보보호를 위한 다양한 대응책들이 나오고 있다.

해외에서는 사물인터넷을 인간과 사물, 서비스 세 가지 분산된 환경 요소에 대해 인간의 명시적 개입 없이 상호 협력적으로 센싱, 네트워킹, 정보 처리 등 지능적 관계를 형성하는 사물 공간 연결망을 뜻한다고 정의한다[6]. 사물인터넷은 새롭게 등장한 개념이기보다는 기술의 발전에 따라 기존의 무선 주파수 인식(Radio Frequency Identification), 사물 통신(Machine to Machine), 유비쿼터스 센서 네트워크(Ubiquitous Sensor Network), 무선 센서 네트워크(Wireless Sensor Network)의 개념에서 확장된 것으로 볼 수 있다[12].

사물인터넷에서 사물은 유무선 네트워크에서의 단말장치(end device)뿐만 아니라, 인간, 차량, 교량, 각종 전자장비, 문화재, 자연환경을 구성하는 물리적 사물 등이 포함된다. 또한, 이동통신망을 통해 사람과 사물, 사물과 사물 간 지능통신이 가능한 M2M의 개념을 인터넷으로 확장하여 사물은 물론, 현실과 가상세계의 모든 정보가 상호작용하는 개념으로 진화하고 있다.

사물인터넷 기기들은 전례 없는 속도로 점점 더 많은 개체가 인터넷과 연결되고 있다. 시장조사기관인 가트너(Gartner)의 유망기술 하이프 사이클(Hype Cycle)인 Fig.1 에 따르면 사물인터넷 플랫폼은 디지털화한 생태계를 이끌 기술로 선정되었다[13]. 하이프 사이클은 신기술의 성장 과정을 표현한 것이며 5~10년간 시장 변화를 주도할 기술 동향을 반영한다. 뿐만 아니라 IoT Forum에서는 헬스케어, 스마트 에너지, 스마트 운송, 스마트 팩토리, 스마트 홈 등과 같이 광범위한 영역에서 사물인터넷이 이용될 것으로 제시하고 있다.



출처: Gartner Inc[13].

〈Figure 1〉 Gartner Hype Cycle for Emerging Technologies, 2018

시장 규모가 커져가며 다양한 분야에서 사용되는 사물인터넷 서비스의 활성화를 위해서는 다양하고 복잡한 보안 문제들이 해결되어야 한다. 보안 문제를 살펴보기 위해서는 사물인터넷의 특징으로 인해 발생하는 보안 적용의 한계성을 알아야 한다. 사물인터넷의 특징으로는 저전력, 메모리의 부족, 낮은 성능의 CPU, 디바이스 간 성능 격차 등이 있다. 이러한 특징 중 소형화와 저전력화를 위해 사물인터넷 기기들은 경량화된 통신과 제한된 메모리를 사용하는데, 이로 인해 발생하는 보안 취약점이 대표적인 한계성의 예이다. 또한, 사물인터넷의 보안 문제로 기존의 컴퓨터 네트워크에서 발생하는 DoS(Denial of Service), 변조, 중간자 공격과 같은 공격수법 역시 사물인터넷 환경에서 동일하게 발생할 수 있다[7].

본 논문에서는 가정과 업무환경에서 사용되는 사물인터넷 인증 문제에 관해 기술하고자 한다. 업무환경에서의 사물인터넷이 보편화되고 있으나 미인증, 부인방지와 같은 문제가 발생할 경우 책임 소재가 불분명하고, 기술특허나 영업비밀과 같은 재산이 노출될 가능성이 있다.

따라서 본 논문에서는 제2장 관련 연구에서 스마트워크 환경에 대한 개념과 가정용 사물인터넷에 대한 개념, 현 사물인터넷 기기들의 인증 방식의 문제점, 사물인터넷 기기의 보안사고 사례를 기술하고자 한다. 제3장 연구시나리오에서는 가정과 사무환경에서 발생 가능한 보안시나리오 작성을 통해 발생 가능한 보안위협을 기술하고자 한다. 제4장에서는 사물인터넷 사용자 인증을 위한 방안을 제시하고 마지막으로 제5장 결론을 제시한다.

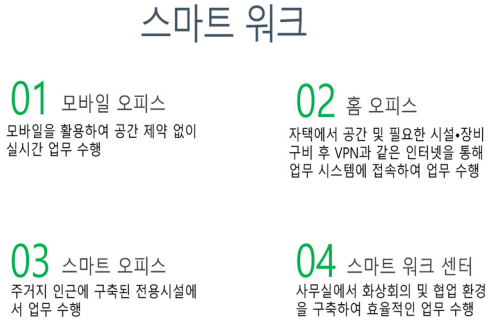
2. 관련 연구

2.1 스마트오피스

스마트오피스(Smart Office)는 스마트한 업무처리를 통해 전통적인 비즈니스 환경보다 적은 자원으로 향상된 결과물을 얻을 수 있는 근무 환경 및 근무 형태를 의미한다[10].

스마트 환경에서는 센서, 메모리, 의사소통의 기능을 포함하고 주변의 상황을 파악하여 정보를 교환할 수 있도록 하고 있다. 이를 통해 사무업무의 효율성과 조직의 능률성을 증가시킬 수 있다.

현대 사무 업무 환경은 사물인터넷 기기의 사용이 보편화됨에 따라 스마트오피스화가 진행 중이다. <Figure 2>에 따르면, 스마트오피스를 통해 같은 업무를 하는 사용자의 사물인터넷기기 또는 컴퓨터, 모바일 디바이스 등이 연결되어 실시간으로 업무를 공유할 수 있으며 나아가 물리적 공간을 공유하지 않아도 업무 데이터를 공유할 수 있다. 실제로 많은 기업들은 사무공간을 다양하게 조성하여 업무의 효율성을 높이고 있다.

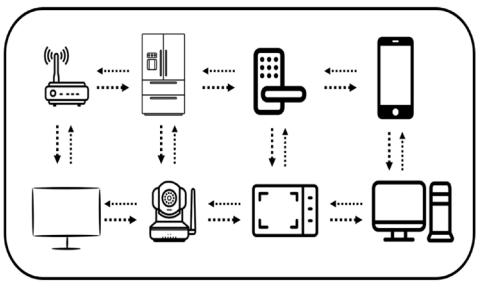


〈Figure 2〉 Smart work Configuration System

한편 이러한 장점과 마찬가지로 스마트오피스 환경에서의 보안위협 또한 증가하고 있다. 데이터의 집중화가 이루어질 수 있어 보안위협에 특히 주의할 필요가 있다.

2.2 가정용 사물인터넷

가정용 사물인터넷(Home IoT)은 주거환경에 ICT를 융합하여 생활에 편의성과 안전한 생활, 복지 증진 등 인간 중심적인 생활방식으로 변화하고 있다. 이러한 주거환경을 스마트홈 주거환경이라 한다[8]. 가정용 사물인터넷의 종류는 <Figure 3>과 같이 TV, 냉장고, 월 패드, 블루투스 스피커, IP 카메라 등 다양한 제품군으로 구성되어 있다. 가정용 사물인터넷 제품들은 단순히 기기를 통한 1차적 서비스를 제공하는 것이 아니라 수집된 데이터를 바탕으로 한 부가서비스를 제공하고 있다. 대표적으로 통신사나 IT 업체에서 사물인터넷 기기를 관리해주고 수집 데이터를 바탕으로 사용자의 편의성을 도모하는 부가서비스를 제공한다. 가정용 사물인터넷은 주거환경에서의 데이터를 이용하기 때문에 사생활에 대한 노출이 발생할 수 있으며, 나아가 개인정보의 노출로 이어질 수 있어 보안의 위협 또한 커졌다고 할 수 있다.



〈Figure 3〉 Home IoT Configurations

2.3 사물인터넷 기기 아이디/패스워드 인증 취약점

현재 사물인터넷 기기 인증 방식은 사용자의 기억을 바탕으로 한 아이디/패스워드를 채택하고 있다. 서버에 사용자의 아이디/패스워드를 공유함으로써 사용자를 인증하는 방법이며, 이는 현재 가장 많은 제조사와 기기들에서 사용되는 방식이다[9]. 그러나 많은 사용자들이 기본값으로 설정되어 있는 아이디/패스워드를 그대로 사용하고 있으며 실제로 이를 악용한 공격 사례도 증가하고 있다. 공용 네트워크 환경에서 모바일 디바이스 및 컴퓨터, 노트북으로 관리자 페이지에 접속할 수 있으며 이때 공유기에 대한 기본 비밀번호로 인하여 보안취약점이 발생할 수 있다.

〈Figure 4〉 Example of ID/Password

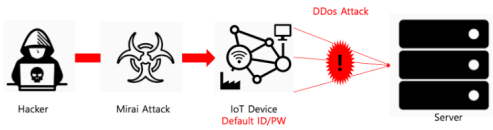
2.4 사물인터넷 기기 인증취약점으로 인한 보안 위협 사례

2.4.1 Mirai Botnet

Mirai Botnet은 수십만 대의 사물인터넷 디바이스를 감염시켜 대규모 Distributed Denial of Service(DDoS) 공격을 일으킨 트로이목마 프로그램이다. Mirai Botnet은 <Figure 5>에서

보이는 바와 같이 관리자 페이지에서 기본 아이디/패스워드를 사용하는 기기들을 대상으로 약 60여 개의 공장출하 아이디/패스워드를 통해 전사공격을 진행하여 접속한다. 접속 후 악성 코드를 감염시키며 주변을 스캐닝한 후 감염되지 않은 취약한 사물인터넷 디바이스를 찾아 전파 시켜 초당 400~500GB의 패킷을 전송하는 대규모 DDoS 공격을 시행하였다.

Mirai Botnet 사례는 DDoS 공격의 사례로 볼 수도 있지만 사실상 공유기의 사용자 아이디/패스워드의 재설정을 통하여 사용자 인증에 대해 관리를 하였다면 예방 가능했던 사례로 볼 수 있다.



〈Figure 5〉 Operation Principle of Mirai Botnet

2.4.2 IP 카메라

가정뿐만 아니라 다양한 분야에서 사용되는 IP 카메라의 해킹 사례도 많이 일어나고 있다. Insecam, Censys 등에서는 노출된 IP를 통해 기본 아이디/패스워드를 사용하고 있는 IP 카메라를 해킹하여 실시간으로 카메라의 영상을 보여주고 있다. Shodan 에서도 특정 검색어를 입력하면 해당 IP와 지역 열려있는 포트 등이 확인 가능하며 기본 아이디/패스워드를 사용할 경우 해당 포트에 접속할 수 있다.

2.4.3 공용 공유기

스마트폰부터 시작하여 노트북, 태플릿 PC 등과 같이 스마트기기의 사용이 증가하면서 공용 공유기를 대부분 설치하고 있다. 이러한 점을 악용하여 불특정 다수의 공유기를 해킹하여 해당 공유기를 사용하는 스마트폰을 허위의 포털사이트로 접속하도록 유도해 악성 앱을 유포한 후, 감염된 스마트폰으로부터 포털 사이트 가입에 필요한 인증번호를 수신받아 계정을 부정 생성하는 사례가 발생하였다.

사물인터넷 기기의 위협 사례에서 보이는 것처럼 가정용 사물인터넷의 보안위협과 스마트 호피스에서의 보안위협은 큰 차이점이 없다. 기본적으로 사물인터넷 기기의 구성 원리가 공유기를 사용한 경우가 대부분이며 이에 따라 유사한 보안사고 사례들이 보고되고 있다. 따라서 가정용 사물인터넷과 스마트오피스에서의 사물인터넷 보안 취약점을 동일하게 봐도 무방할 것이다. 사물인터넷 보안에서 가장 큰 취약점은 사용자들의 보안인식 부재이다. 대표적으로 처음 제공되는 기본 아이디와 비밀번호를 변경하지 않고 사용하는 것이 그 예가 될 수 있다. 이를 통해 공격자가 공유기의 관리자 권한을 쉽게 탈취해 보안 사고가 발생시킬 수 있다.

2.5 Fast Identity Online

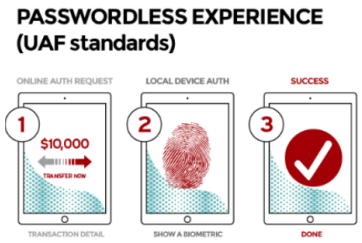
Fast IDentity Online(FIDO)는 FIDO Alliance 에서 패스워드 기억 없이 생체인증 기반 및 다양한 인증기반으로 개방성, 확장성, 상호 운용성까지 모두 제공하는 새로운 인증 방식이다. 최근 FIDO 생체인증은 패스워드를 대체할 차세대 인증 방식으로 급부상하고 있다[11]. FIDO 인증이란 온라인 환경에서 생체인증 기술을 활용하여 사용자의 신원을 편리하고 안전하게 인증하기 위한 기술 표준이다.

생체인증을 사용한 인증을 말하면 모바일 디바이스에서 제공되는 생체인증을 떠올릴 수 있을 것이다. 현재 대부분의 디바이스에는 제조사에서 제공하는 간편 인증 응용프로그램을 통해 생체인증을 통하여 사용자 인증을 할 수 있다. 이를 FIDO의 생체인증과 같은 인증으로 오해할 수 있다. 제조사에서 제공해주는 기능은 디바이스에 저장된 생체정보를 통하여 등록한 아이디/패스워드를 자동으로 입력해주는 것이며 생체인증정보와 공개키를 이용한 인증 방식은 아니다.

FIDO 1.0에는 생체 정보(음성, 지문 및 얼굴 인식 등)를 인증 과정에 사용하여 비밀번호를 사용하지 않는 인증 표준인 UAF 방식과 별도의 인증장치를 사용하는 U2F 방식으로 구성되어 있다. FIDO 2 기술에는 웹 응용프로그램을 통해 인증을 수행하는 Web Authentication과 CTAP 기술이 추가되어 있다. 본 논문에서는 FIDO의 전반적인 기술을 소개하고 U2F 디바이스를 이용한 이중 인증을 다루려고 한다.

2.5.1 Universal Authentication Framework

Universal Authentication Framework(UAF) 기술은 주로 모바일 환경에서 다양한 인증장치를 서비스 제공자가 보안요구사항에 맞게 선택하여 쓸 수 있는 기술이다. 기존 패스워드 기반 인증의 단점인 사용자 인증정보를 중앙 서버에 보관함으로써 발생하는 인증정보의 대량 탈취 위험성 상존, 피싱 공격에 대한 취약점, 스마트폰에서의 사용 불편, 서비스마다 다르게 사용하는 패스워드 관리의 어려움 등을 극복하기 위해 고안되었다[2]. UAF 인증의 인증과정은 <Figure 6>과 같으며 로컬인증과 원격인증으로 구분된다. 로컬인증은 사용자 디바이스에서 지문, 홍채, 정맥 등의 생체정보 혹은 PIN을 이용하여 사용자 확인을 하는 것을 말한다. 원격인증은 공개키 기반 전자서명을 이용하여 기존에 등록된 디바이스인지 검증하는 방식이다.

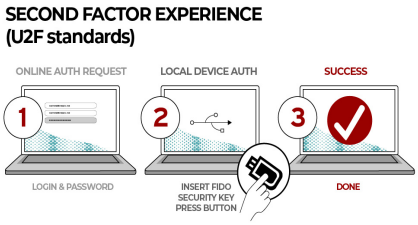


출처: FIDO Alliance.

〈Figure 6〉 FIDO UAF Certification Process

2.5.2 Universal Second Factor

Universal Second Factor(U2F) 프로토콜은 <Figure 7>의 인증과정과 같이 기존의 인증방식인 아이디/패스워드 기반으로 1차 인증한 후, 일회용 보안키를 저장한 USB 동글 또는 스마트카드와 같은 별도의 디바이스를 이용하여 2차 인증을 하는 기술이다[1]. UAF와 동일하게 전자서명을 이용하며 개인키를 U2F 디바이스 내의 안전한 영역에 저장한다. U2F 프로토콜을 이용하여 온라인 서비스에 강력한 2차 인증을 추가하여 기존 아이디/패스워드방식에 보안성을 추가할 수 있다[5].



출처: FIDO Alliance.

〈Figure 7〉 FIDO U2F Certification Process

2.5.3 Web Authentication

Web Authentication(WebAuthn)은 온라인 서비스에서 FIDO 인증을 사용할 수 있도록 브라우저 및 관련 웹 플랫폼 인프라에 내장할 수 있는 표준 웹 API이다. WebAuthn은 웹 사이트에서 등록, 인증 및 2단계 인증을 위해 암호 또는 SMS 텍스트 대신 비대칭 (공개키) 암호화를 사용한다. WebAuthn은 CTAP을 사용하여 모바일 디바이스나 FIDO 보안키와 같은 외부 장치와 연동해 데스크톱 응용프로그램 및 웹서비스의 인증자 역할을 할 수 있다.

Client To Authenticator Protocol(CTAP)은 외부 인증장치를 위한 플랫폼 독립적인 범용 API 및 프로토콜이다. 인증장치로는 핸드폰, USB 생체인증 모듈 등이 있으며 연결 방법으로는 USB, NFC, Bluetooth 지원이 있다[4]. CTAP은 스마트폰을 인증장치로 이용하여 다른 디바이스에 인증 가능하며 Online to Offline Service(O2O) 서비스에서 FIDO 인증을 적용할 수 있는 기반을 제공한다.

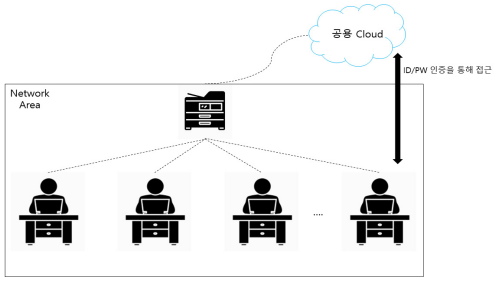
WebAuthn을 이용하면 피싱, 데이터 유출 및 SMS 텍스트 또는 기타 2단계 인증 방법에 대한 공격과 관련된 중요한 보안 문제를 해결하는 동시에 사용자가 복잡한 암호를 관리 할 필요가 없으므로 사용자의 편의성을 크게 향상시킨다.

3. 연구 시나리오

본 장에서는 사무 공간에서 사물인터넷을 활용하는 사례를 예시로 인증 취약점으로 인해 발생할 수 있는 보안위협 시나리오를 제시한다.

3.1 스마트오피스 시나리오

많은 업무환경에서 개인용 복합기를 사용하지 않고 <Figure 8>과 같이 공용 복합기를 네트워크에 연결하여 사용한다. 즉, 같은 네트워크 안에 있는 사용자는 누구든지 복합기에 접근 가능한 환경이다. 또한, 인쇄된 문서나 스캔한 문서 등이 클라우드에 저장되는 복합기를 사용하는 경우도 있다. 이렇게 저장된 문서는 특별한 드라이버 설치 없이 클라우드와 연결된 인쇄기(프린터)라면 어떠한 장치를 사용하든 출력할 수 있다. 해당 클라우드에 접속하는 방식은 주로 아이디/패스워드를 통해 이뤄지는데, 이러한 아이디/패스워드의 관리가 미비할 경우 부서 전체의 데이터가 노출될 수 있다. 또한, 문서파일에 대한 접근이 권한별로 나누어지지 않는다면 권한이 없는 사용자가 높은 권한을 요구하는 문서를 보게 될 수도 있다는 취약점이 있다.



〈Figure 8〉 Example of Using Smart Office Multifunction Printer

3.2 가정용 사물인터넷 시나리오

가정용 사물인터넷은 주거환경에서의 편의성 증진을 위해 사물인터넷 사용이 증가함에 따라 형성된 환경으로, 가정의 공유기 또는 게이트웨이의 역할을 해주는 사물인터넷 기기를 기

점으로 연결되어 있다. 이러한 상황에서 발생할 수 있는 문제점은 크게 두 가지가 있다. 첫 번째 문제점은 대부분의 사용자는 사물인터넷 기기 또는 공유기를 설치하였을 때 관리자 권한의 아이디/패스워드를 변경하지 않고 그대로 사용하며 사용자 디바이스 등록만을 진행하고 있다. 공유기의 경우 아래층 또는 위층, 인접해 있는 다른 곳에서 접속을 쉽게 할 수 있으며 관리자 권한의 아이디/패스워드는 인터넷에도 공개되어 있다. 두 번째 문제점은 가정용 사물인터넷 기기들을 사용할 때에 펌웨어(Firmware)의 업데이트를 하지 않는 경우가 많다. 이로 인해 펌웨어 버전의 최신화가 이뤄지지 않아 기존의 보안 취약점이 개선되지 않는다. 즉, 초기 펌웨어의 보안이 매우 취약한 상태가 지속된다는 의미이다. 가정용 사물인터넷의 기기들을 통제하는 기준이 되는 장비의 관리자 권한이 노출될 경우 여러 보안 취약점들이 생기게 될 것이며 각 디바이스에 저장되어 있는 개인 데이터들이 노출될 가능성이 높다. 가장 대표적으로 핸드폰이 접속되어 있을 경우 핸드폰 내에 저장되어있는 개인 데이터(전화번호, 사진, 동영상 등)에 대한 유출될 가능성이 있다.

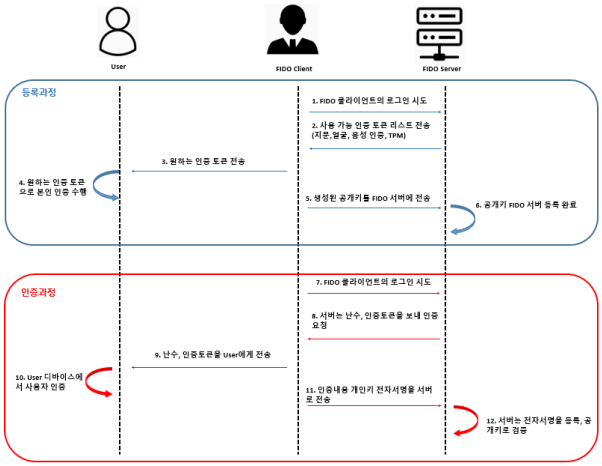
4. 프레임워크 설계

앞서 연구시나리오에서 언급되었던 스마트오피스와 스마트 홈에서 사용되는 사물인터넷 기기의 구성은 대부분 공유기를 중심으로 연결되어 있다. 따라서 공유기의 보안성을 강화하면 사물인터넷 기기를 더욱 안전하게 사용할 수 있다.

현재 공유기의 관리자 페이지에서 사용되고 있는 아이디, 패스워드 기반의 사용자 인증에서 인증 응용프로그램의 설치 없이 간편하게 추가 인증을 할 수 있는 FIDO 인증을 도입하여 보안성을 강화하고자 한다.

4.1 Universal Second Factor를 이용한 사용자 등록 및 인증

FIDO U2F 프로토콜을 통해 사용자 인증을



〈Figure 9〉 FIDO User Registration and Certification Process

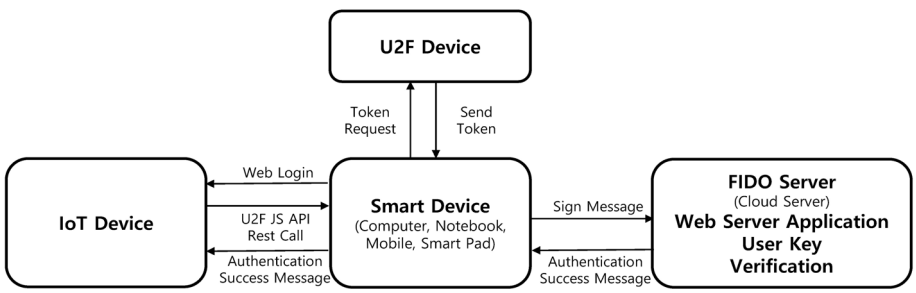
하기 위해서는 U2F 인증 디바이스를 등록하는 과정을 거쳐야 한다. <Figure 9>에서는 사용자의 등록과정과 인증과정을 보여주고 있다. 사용자가 아이디/패스워드로 로그인하여 FIDO 서버에 접속시도를 하면 FIDO 서버에서는 사용 가능한 인증토큰 리스트를 전송하게 된다. 본 논문에서는 U2F 프로토콜을 사용할 것이므로 USB 형식의 U2F 디바이스를 이용하며, 이 과정에서 사용자는 보안 인증을 수행하며 공개키와 개인키를 생성하게 된다. 생성된 공개키를 FIDO 서버에 전송하면 전송된 공개키는 FIDO 서버에 등록된다.

사용자의 인증을 위해서 사용자가 FIDO 서버에 로그인 시도를 하면 서버는 난수, 인증토큰을 보내 인증을 요청한다. 사용자는 등록된 U2F 디바이스를 이용하여 사용자 인증을 수행하며 인증내용을 개인키로 전자서명을 한 후 서버로 전송한다. 서버는 전자서명을 등록하고 공개키로 검증한다. 이를 통해 사용자가 U2F 인증 디바이스를 소유하고 있는지 확인한다.

4.2 Universal Second Factor를 사용한 공유기 사용자 인증

공유기 사용자 인증을 위해 FIDO U2F 기술을 사용하여 2차 인증을 제안하고자 한다. FIDO U2F의 장점으로는 OTP 방식이고 PKI를 이용하며 보안키 소유자 외에는 물리적 인증 장치를 가질 수 없으므로 안정성을 보장한다. 하나의 보안 기기로 윈도우, MAC OS 등 모든 환경에서 사용 가능하며 여러 계정에서 사용하면 매번 OTP 번호를 찾아 입력해야 하는 불편함을 개선시켜줄 수 있다. 또한, 휴대폰의 사용이 불가능할 때에도 보안 기기만으로 본인인증을 할 수 있다.

제안하고자 하는 프레임워크는 <Figure 10>과 같다. 프레임워크의 동작 원리로 첫 번째로 스마트 디바이스를 통해 공유기에 접속하고자 할 때 아이디, 패스워드를 통한 1차 인증을 한다. 2차 인증 시 FIDO 서버에서 난수, 인증 토큰을 보내 인증을 요청하고 후 USB 디바이스를 통해 토큰을 발행해 인증을 수행한다. 인증이 완료되면 개인키를 통해 전자서명을 한 후 서버로 전송하며 서버는 저장되어 있는 공개키로 검증한다. 검증이 완료되면 인증 성공 메시지를 스마트 디바이스를 거쳐 공유기로 전달되며 사용자 인증이 마무리된다. U2F 디바이스를 이용한 인증시스템을 구현한다면 사용자 인증의 보안성을 강화시킬 수 있다.



〈Figure 10〉 U2F Based Multi-Factor Authentication Framework

4.3 시사점

FIDO를 사용한 공유기 사용자 인증은 FIDO의 U2F 기술을 사용한 USB 형식의 인증 장치를 통하여 사용자의 2차 인증을 구성하고 있다. 향후 FIDO 2의 표준화가 완료되면 더 편리하게 별도의 응용프로그램을 설치하지 않더라도 주요 웹 브라우저를 통해 생체인증을 수행할 수 있을 것으로 예상한다.

웹 인증은 Microsoft의 Edge, 구글의 Chrome, 모질라의 Firefox를 포함한 주요 웹 브라우저가 표준을 구현하였으며 Android 및 Windows 10에는 FIDO 인증에 대한 지원 기능이 내장되어 있다. FIDO2에서는 브라우저와 데스크톱에 동일한 표준을 제공한다. 범위를 확장하는 이유는 대부분의 온라인 거래가 여전히 브라우저에서 이루어지기 때문이다[3].

5. 결 론

가정에서 사용하는 개인용 사물인터넷 이외에도 스마트워크 환경에서 사물인터넷의 사용이 늘어가고 있다. 사물인터넷의 사용이 늘어남으로써 사물인터넷 기기를 대상으로 한 보안 침해 사례도 많이 보고되고 있으며, 대부분의 보안 사고들은 인증 메커니즘 부재, 강도가 약한 비밀번호, 펌웨어 업데이트 취약점, 물리적 보안 취약점, 접근 통제 부재, 전송 데이터 보호 부재의 문제로 발생하고 있다. 특히 사무실은 많은 사람이 공용으로 사용하는 공간이며 이에 따라 사용자의 식별이 이루어지지 않으면 어떤 사람이 이용했는지 확인이 되지 않는다. 사물인터넷의 특성상 사용자의 데이터를 많이 저장할 수 없는 상황이며 추가 응용프로그램 설치를 통한 사용자인증 또한 부담스러운 상황이다.

본 논문에서 제시하는 사용자 인증을 도입하더라도 사용자가 보안에 대한 경각심을 가지지 않는다면 동일한 보안 위협을 받을 수 있다. 또한, 소지기반의 인증이기 때문에 인증장치의 분실에 대한 우려가 있을 수 있다는 한계점을 가지고 있다.

본 논문에서 제안한 방식인 FIDO U2F 프로토콜을 이용한 사용한 사용자 인증 모델을 통하여 간단한 U2F 인증 디바이스만 소유하고 있으면 어디에서든 간편하고 안전하게 사용자 인증과 식별이 가능해질 것이다. 공유기 인증을 위한 사용자 인증 프레임워크는 현재 사물인터넷에 있어 가장 취약한 부분인 공유기의 사용자 인증을 상당부분 개선시킬 것으로 보인다.

References

[1] Chae, C., Cho, H., and Jeong, H., “Authentication Method using Multiple Biometric Information in FIDO Environment,” Journal of Digital Convergence, Vol. 16, No. 1, pp. 159-164, 2019.

[2] Cho, S. and Kim, S., “FIDO technology standardization trend,” Telecommunications Technology Association, TTA Journal, Vol. 172, pp. 65-70, 2017.

[3] Dunkerberger, P., “FIDO2 puts biometrics at heart of web security,” ELSEVIER Vol. 2018, No. 8, pp. 8-10, 2018.

[4] FIDO Alliance, “Client to Authenticator

Protocol(CTAP)," Propose Standard, 2019.
[5] FIDO Alliance, "Universal 2nd Factor (U2F) Overview," FIDO Alliacne Proposed Standard, 2017.
[6] Gubbi, J. and Buyya, R., Marimuthu, S., and Palaniswami, M., "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, Vol. 29, No. 7, pp. 1645-1660, 2013.
[7] Hossain, M., Fotouhi, M., and Hasan, R., "Towards an Analysis of Security Issues, Challenge and Open Problems in the Internet of Things," 2015 IEEE World Congress on Services, pp. 21-28, 2015.
[8] IoT Security Alliance, "Home · Appliance IoT Security Guide," Korea Internet & Security Agency, 2017.
[9] Kang, J., "A Verification of Smart TV Security in IoT Environment," Soongsil University, 2017.
[10] Kim, Y., Lee, J., and Yun, G., "Study on Smart Office Fit Model of Government and Local Governments," The Korea Institute of Public Administration, Frequent assignment 2014-04, 2014.
[11] Lee, G. H., "Exploring the standardization forum _Special Theme Bio-recognition," Telecommunications Technology Association, TTA Journal, Vol. 165, pp. 12-17, 2016.
[12] Lee, S. and Jahng, J., "The Diffusion of Internet of Things: Forecasting Technologies and Company Strategies using Qualitative and Quantitative Approach," The Journal of Society for e-Business Studies, Vol. 20, No. 4, pp. 19-39, 2015.
[13] Walker, M., "Hype Cycle for Emerging Technologies, 2018," Gartner Inc., 2018.

저 자 소 개

송용택 (E-mail: ionsea91@gmail.com)
2014년 목포해양대학교 전자공학 (학사)
2017년～현재 중앙대학교 융합보안학과 (석사)
2017년～현재 한국FIDO산업포럼 주임연구원
관심분야 사물인터넷 보안, 생체인증, 사이버 물리 시스템 보안

이재우 (E-mail: jaewoolee@cau.ac.kr)
2006년 서울대학교 컴퓨터공학부 (학사)
2008년 서울대학교 컴퓨터공학부 (석사)
2017년 University of Pennsylvania, Ph.D in Computer and Information Science
2018년～현재 중앙대학교 산업보안학과 조교수
관심분야 실시간 시스템, 사이버 물리 시스템 보안