논문 2022-2-23 http://dx.doi.org/10.29056/jsav.2022.12.23

사물인터넷을 위한 UAF 인증 시스템 분석 및 평가

김상윤*, 이기영*†

Analysis and Evaluation of UAF Authentication System for IoT

Sang-Yoon Kim*, Ki Young Lee*†

요 약

4차 산업혁명 시대에는 IoT 시장의 성장을 통해 다양한 서비스와 편의가 제공되었다. 이용자가 늘면서 개인정보 유출 등 보안 위협이 존재해 보안의 중요성이 커지고 있다. 본 논문에서는 IoT 및 FIDO 기반 다중 인증을 활용하여 사용자 인증 방법을 제안한다. eBay에서 제공한 FIDO 데모 서버를 활용하여 IoT 환경에서 기존의 인증 방식에 추가로 FIDO 인증을 도입해 인증 프로세스를 제시하고 사용자 인증을 통해 보안성을 강화하는 모델을 제시하고자 한다. 본 논문은 UAF 다중 인증 프로세스를 통해 사물인터넷 환경에서 사용자 인증 기술을 제시하고, 성능 평가를 통해 기존의 단일 인증과의 차별점을 확인하였고 정성 평가를 통해 다중 인증 정책의 효과를 확인하였다. 이를 바탕으로 더 넓은 분야에 다중 인증 프로세스가 적용될 것을 기대한다.

Abstract

In the era of the 4th industrial revolution, various services and convenience were provided through the growth of the IoT market. As the number of users increases, security threats such as personal information leakage exist, and the importance of security is increasing. In this paper, we propose a user authentication method using IoT and FIDO-based multiple authentication. Using the FIDO demo server provided by eBay, we intend to present the authentication process by introducing FIDO authentication in addition to the existing authentication method in the IoT environment and present a model that enhances security through user authentication. This paper presents the user authentication technology in the IoT environment through the UAF multi-authentication process, confirms the difference from the existing single authentication through performance evaluation, and confirms the effect of the multi-authentication policy through qualitative evaluation. Based on this, it is expected that multiple authentication processes will be applied to a wider field.

한글키워드 : 사물인터넷, 사용자 인증, 다중 인증, 파이도, 이베이

keywords : IoT, User Authentication, Multi-Factor Authentication, eBay

1. 서 론

4차 산업 혁명을 맞아 기술이 빠르게 발전됨에 따라 사물인터넷 환경이 가정 공간에서부터 사무 공간까지 적용 범위가 확산하고 있다. 사물인터넷 기술은 현대사회에 사용되고 있는 디바이스와 사람이 연결될 수 있게 해주고 디바이스에서 수

* 국립인천대학교 정보통신공학과
† 교신저자: 이기영(email: kylee@inu.ac.kr)
접수일자: 2022.11.18. 심사완료: 2022.12.07.
게재확정: 2022.12.20.

집된 여러 데이터 및 프로세스가 서로 연계되어 다양한 분야에서 활용이 가능하다. 이처럼 사물인터넷 디바이스는 사용자 입장에서 편의성뿐만 제공해주는 것이 아니라 일상생활에 필요한 기술이 되었다[1]. 그러나 다양한 정보를 생산해내는 역할을 수행함으로써 사물인터넷은 항상 보안 이슈를 동반했다. 특히 편의성이 증대됨에 따라 인가되지 않은 사용자의 접속이 쉽고 이를 악용하는 사건이 발생하고 있다. 사물인터넷 기술에서 데이터를 수집하고 분석하기 위해 개인정보가 필수적이기 때문에 이를 악용하는 경우가 발생해 사생활 침해와 같은 보안 문제가 발생할 수 있다[2]. 또한 산업 현장과 같은 곳에서 사물인터넷 환경이 구축되어 중요한 정보의 유출은 디바이스 제조 기업 및 사용 기업에 큰 타격을 입힐 수 있다[3]. 사물인터넷에서 발생하는 보안 문제는 기존의 네트워크에서 자주 발생하는 MITM(Man in the Middle), DOS(Denial of Service) 공격 등과 같은 공격 기법이 사물인터넷 환경에서도 발생하는 것을 볼 수 있다[4]. 이에 따라 인가되지 않은 사용자로 사생활 침해 및 개인정보가 유출될 수 있고 기업 입장에선 중요 정보의 유출 우려가 커 사물인터넷 디바이스로 구성된 환경에서 더욱 강력한 사용자 인증에 관한 연구가 필요해 사물인터넷 환경에서 편의성과 안전성, 신뢰성을 가진 인증 방법을 기술하고자 한다.

사물인터넷 기기의 대중화로 많은 피해사례가 증가하고 있다. 특히 작년에는 월패드 해킹으로 인해 많은 피해사례가 발생했다. 기술의 발전으로 월패드의 사양이 높아졌고 IoT의 기능을 위해 외부 연결이 되는 스마트한 기기가 되었다. 외부 연결이 되기 때문에 이와 같은 보안 이슈가 동반되어 이러한 부분을 해결해야 사용자가 IoT 제품을 믿고 이용할 수 있다.

이를 해결하기 위해 별도의 암호를 설정해야 하는데 단순히 아이디/패스워드 기반이 아닌 하나의 인증이 추가된 다중 인증을 통해서 IoT 기기를 인증할 수 있다면 좀 더 나은 보안 수준을 제공할 수 있다고 생각한다. 따라서 본 논문에서는 접근성이 좋은 사물인터넷 디바이스에 추가 인증 방식을 적용하여 기존 방식과 비교하여 기술하고자 한다.

본 논문에서는 2장에서 사물인터넷 개요와 보안 위협 분석, 다중 인증 과정에 대해 기술한다. 3장에서는 관련 연구를 바탕으로 구현 과정을 기술하고 4장에서 구현 결과를 기술하고 5장에서 결론을 제시한다.

2. 관련 연구

2.1 사물인터넷 정의

1999년에 사물인터넷(IoT : Internet of Things)의 개념에 대해 최초로 정의되었다. 이는 유무선 네트워크에서의 엔드디바이스는 물론 인간과 자연환경을 구성하는 모든 물리적 사물 등이 사물인터넷의 구성요소에 포함된다[1]. 이러한 기술은 언제어디서나 가상의 네트워크를 통해 서로 소통할 수 있는 인터넷 기술로, 다양한 구성요소와 사물인터넷 망이 연결됨으로써 RFID(Radio-Frequency-Identification)·USN(Ubiquitous Sensor Network) 기반의 유비쿼터스 및 초연결사회를 구현할 수 있는 기반을 제공하고 있다[1].

2.2 사물인터넷 활용

2.2.1 스마트 워크 센터

스마트워크는 종래의 지정된 업무공간인 사무실의 개념을 탈피하여, 다양한 장소와 이동환경에서도 언제 어디서나 편리하고, 효율적으로 업무에 임할 수 있도록 하는 미래지향적인 업무를 구축한 환경이다[3]

스마트 워크 시스템은 그림 1과 같이 홈오피스, 모바일오피스, 스마트오피스로 구성된다.

그림 1. 스마트 워크 유형[5]
Fig. 1. Smart Work Type
(출처 : 국민대학교 웹진)

스마트오피스는 전통적인 비즈니스 환경에서 벗어나 스마트 업무 처리를 위해 적은 자원으로 최선의 결과를 끌어낼 수 있는 근무 환경 및 형태를 의미한다[4].

스마트 환경에서는 사물인터넷의 구성요소인 센서, 메모리, 등 의사소통 기능을 포함하여 주변의 상황을 파악하고 분석하여 데이터를 교환할 수 있도록 한다. 이를 통해 전통적인 사무업무에서 발전된 사무업무 환경을 만들 수 있다[4].

현대 사무 환경은 사물인터넷 디바이스의 보급이 보편화되었고 사용이 증가함에 따라 스마트오피스화가 진행 중이다. 스마트워크를 통해 사용자의 사물인터넷 디바이스 및 여러 디바이스 등이 연결되어 같은 업무를 하는 사용자끼리 업무를 공유하는 것이 가능하고 나아가 사무실과 같은 특정 정해진 공간이 아니어도 업무 관련 정보를 공유할 수 있다. 스마트오피스화가 진행되면서 현재 많은 기업이 사무공간을 활용하여 업무의 효율성을 높이고 있다[5].

그렇지만 사물인터넷 보급의 대중화로 스마트오피스 환경 또한 보안 위협이 증가하고 있다. 중앙집중형의 데이터 구조로서 보안 위협에 주의할 필요가 있다.

2.2.2 가정용 사물 인터넷

가정용 사물인터넷은 가정환경에 ICT(Information & Communications Technology)를 융합하여 우리 생활에 편의성과 안전한 생활 등 인간 중심적인 생활방식을 제공하고 있다[6].

가정용 사물인터넷 디바이스의 종류는 스마트 스피커, 스마트 TV, 세탁기, 초인종, 도어락 등 다양한 기기로 구성되어 있다. 가정용 사물인터넷 제품은 단순히 해당 제품의 본연의 목적만을 위한 것이 아니라 사용자로부터 수집된 데이터를 토대로 기타 부가서비스를 제공하고 있다. 이러한 제공은 보통 통신사나 IoT 제품 제조 업체에서 사물인터넷 디바이스를 관리해주고 수집된 데이터를 바탕으로 편의성을 바탕으로 하는 부가서비스를 제공한다. 그렇지만 가정용 사물인터넷 또한 스마트오피스와 마찬가지로 가정환경에서의 데이터를 이용하고 그 해당 데이터가 중앙 집중화되어있어 사생활에 대한 노출이 발생할 수 있고, 개인정보의 유출로 이어질 수 있어 보안 위협이 점차 커지고 있다 볼 수 있다.

2.3 사물인터넷 환경 인증 취약점

대부분의 사물인터넷 디바이스의 인증 방식은 사용자 기억에 의존한 것을 바탕으로 한 ID/PW 방식을 사용하고 있다. 서버에 ID/PW를 전달함으로써 사용자를 인증하는 방식이고, 현재 가장 많이 사용되고 있다[7]. 그러나 사물인터넷 디바이스 제조사에서 제공하는 기본값으로 설정된 ID/PW를 그대로 사용하는 사용자가 대다수를 이루고 이와 관련된 악용 사례도 증가하고 있다. 특히 공용 네트워크 환경에서 여러 디바이스로 관리자 페이지에 쉽게 접속이 가능하고 이때 기본값으로 설정으로 인해 취약점이 발생할 수 있다.

2.4 보안 위협 분석

스마트오피스 보안 위협 시나리오에는 대부분의 업무 환경에서 복합기는 개인용 복합기가 아닌 공용 복합기를 네트워크에 연결하여 사용한다. 네트워크에 연결하기 때문에 같은 네트워크 안에 있는 사용자는 복합기에 접근하기 쉬운 구조이다. 또한 복합기를 사용할 때 해당 데이터를 클라우드에 저장할 수 있는 복합기를 사용하는 경우도 있다. 이렇게 저장된 데이터는 클라우드에 접속하면 쉽게 얻을 수 있는데 접근 방식은 주로 아이디/패스워드 기반으로 이뤄진다. 이러한 암호관리가 미비할 경우 데이터가 노출될 수 있다. 또한 접근통제를 제대로 하지 않는다면 권한 등급이 낮은 사용자가 권한 등급이 높은 자료에 접근할 수 있게 된다[8].

가정용 사물인터넷 보안 위협 시나리오에는 주로 가정환경에서 사용이 되고 사용자에게 더 나은 편의성을 제공하기 위해 형성된 환경이다. 주로 가정에서 사용하는 공유기를 기점으로 제품군들이 서로 연결되어 있다. 이렇게 공유기 및 게이트웨이에 연결되었을 경우 발생할 수 있는 문제점은 사용자들이 사물인터넷 디바이스 및 공유기를 설치할 경우 기본으로 제공되는 아이디/패스워드를 변경하지 않고 관리자 권한의 기본값으로 사용할 경우 같은 네트워크 공간이기 때문에 다른 곳에서 해당 네트워크에 쉽게 접근할 수 있고 어떠한 제품군은 관리자 권한의 암호들이 인터넷에도 공개된 경우가 있다. 다른 문제점은 가정용 사물인터넷 디바이스를 사용할 때 최신 펌웨어 업데이트를 하지 않는 경우다. 업데이트 미실시로 인해 기존의 보안 취약점이 개선되지 않아 취약한 상태가 지속된다[6].

가정용 사물인터넷 디바이스에서 발생할 수 있는 보안 위협 시나리오는 표 1과 같다.

표 1. 보안 위협 시나리오[9]
Table 1. Security Threat Scenario

분야	주요 내용
IoT Hub	스마트홈 구축을 위해 IoT Hub의 펌웨어 추출 및 취약점 분석을 통해 IoT Hub에 연결된 사물인터넷 디바이스의 권한을 장악하여 사생활 침해, 물리적, 경제적 피해 등 스마트홈에서 발생 가능한 시나리오
스마트 초인종	외부에 노출된 스마트 초인종의 포트를 이용해 홈네트워크에 침입하여 IoT 허브를 해킹하고 최종적으로 스마트 시티 단지 시스템을 장악할 수 있는 시나리오
AI 스피커	AI 스피커의 음성인식과 스마트폰의 취약점을 통해 스피커를 장악하여 보이스피싱,RFID 등을 통해 연결된 기기를 공격해 스마트 홈 디바이스 제어권이 공격자에게 넘어갈 수 있는 시나리오
스마트 TV	스마트 TV에 탑재된 카메라를 해킹하여 사생활이 유출될 수 있는 시나리오
공유기	수십만대의 공유기를 해킹하여 악성코드를 넣어 디도스 공격 창구로 활용 가능한 시나리오

(출처 : 과학기술정보통신부)

2.5 다중 인증 프로세스

2.5.1 Fast IDentity Online

FIDO는 Fast Identity Online의 약자이고 FIDO Alliance에서 제안한 기존의 인증방식인 아이디/패스워드 대신 생체인증을 토대로 한 인증 방식 및 다양한 2차 인증을 통해 개방성, 확장성 등 사용자에게 다양한 인증 방법의 효과를 제공하는 새로운 인증 방식이다. FIDO 인증은 인증 과정을 통해 온라인 환경에서 생체인증 기반의 기술을 활용해 사용자의 신원을 더욱 편리하게 인증하고 보안성 또한 보장하는 기술 표준이다.

FIDO에서 언급한 생체인증은 대부분 사용자가 사용했던 스마트폰과 같은 디바이스에서 사용한 생체인증과는 다르다. 스마트폰 및 노트북에서 사용하는 생체인증은 디바이스에 생체정보 등

록 과정을 거쳐 저장된 생체정보를 바탕으로 등록된 아이디/패스워드를 자동으로 입력해주는 방식이므로 FIDO에서 언급한 생체정보와는 차이가 있다.

현재 FIDO에는 FIDO 1.0과 FIDO 2.0으로 구분된다. FIDO 1.0에는 음성, 지문, 얼굴 인식과 같은 생체 정보를 인증과정에 적용하여 비밀번호를 사용하지 않는 방식인 UAF(Universal Authentication Framwork) 방식과 기존의 인증 방식에 추가로 일회용 보안키를 저장한 별도의 디바이스를 이용하는 U2F(Universal 2nd Factor) 방식으로 구성되어 있다. FIDO 2.0에는 FIDO 1.0에 사용된 두 가지 방식 이외에 웹 애플리케이션을 통해 인증을 수행하는 WebAuthn(Web Authentication)과 CTAP(Client to Authenticator Protocol)가 추가되었다[10].

2.5.2 Universal Authentication Framwork

UAF로 불리는 기술은 주로 모바일 환경에서 사용이 되고 서비스 제공자가 보안 요구사항에 맞게 선택해 사용할 수 있는 기술이다. 기존의 아이디/패스워드 기반 인증의 단점을 극복하기 위해 개발되었는데 중앙 서버에 데이터를 보관해 발생하는 정보 탈취와 같은 문제점을 해결해주고 피싱 공격에 대한 취약점, 서비스마다 다른 패스워드 관리 방식의 어려움 등 여러 가지 문제점을 극복하기 위해 고안되었다[10].

2.5.3 사물인터넷 디바이스 인증의 한계점

사물인터넷 환경에서 여러 위협으로부터 안전하게 사용하기 위해선 사용자의 인증이 필수이다. 대부분의 사물인터넷 디바이스는 아이디/패스워드 기반인 단일인증을 사용하고 있다. 간편하다는 장점이 있지만 쉽게 노출될 수 있기 때문에 추가적인 인증이 필요하다. 하지만 사물인터넷 특성상 복잡한 인증 메커니즘을 수행할 수 있는 고사양의 디바이스를 구축하기 어렵기 때문에 디바이스와 디바이스 간, 디바이스와 서버 간의 인증을 효과적으로 수행할 수 있는 인증 방안이 필요하다[11].

3. 다중 인증 프로세스 설계

3.1 다중 인증 요구사항

사물인터넷에 적용할 다중 인증 기술을 선정하기 위해 몇 가지 고려사항이 필요하다. 그림 2와 NIST에서 제안한 가이드라인의 인증 기술 선정 절차는 잠재적 위험평가를 구분한 후 인증보증 수준을 결정하고 최종적으로 인증보증 수준에 적합한 인증 기술을 선정하였다.

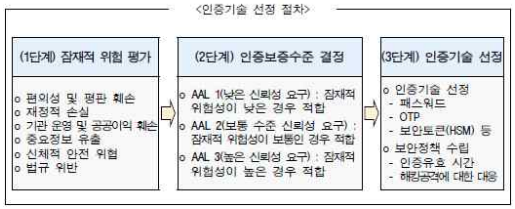

그림 2. 인증기술 선정 절차[12]
Fig. 2. Selecting Authentication Assurance Level
(출처: 금융보안원)

사물인터넷 기기 중 센서가 부착된 의료기기 같은 경우 '신체적 안전'에 위협이 될 수 있다. 또한 월패드나 스마트 TV에 부착된 카메라 같은 경우 사생활 침해로 인해 '평판 훼손'에 영향을 미칠 수 있다. 이런 경우 기업에서는 정보 유출로 인한 '재정적 손실'이 발생할 수 있다. 따라서 사물인터넷 환경에서 사용할 수 있는 인증 기술 선정을 위한 절차를 진행한 결과 3개의 항목('편의성 및 평판 훼손', '신체적 안전 위협', '재정적 손실')에서 '높음'으로 평가된다. 따라서 AAL

3(Authentication Assurance Level 3)에 해당하는 인증 기술을 적용해야 한다. AAL 3에 해당하는 인증 기술은 MF(Multi Factor) 암호화 디바이스 또는 암호화 알고리즘을 사용한 SF(Single Factor) 암호화 디바이스이다. 그림 3과 같이 AAL 3 인증 기술에 FIDO가 포함되어 있다[13].

그림 3. NIST 인증 보증 수준에 따른 기술[13]
Fig. 3. NIST GUIDANCE - NIST AAL
(출처 : FIDO Alliance)

3.2 프레임워크 설계

현재 공유기에서 사용되는 아이디/패스워드 기반의 인증에서 추가로 강력한 인증을 도입하면 더 안전하게 사용할 수 있다. 인증방식을 추가하기 전 고려해야 할 조건이 존재한다.

사물인터넷 특성상 복잡한 연산이 들어가면 안 되는 저사양 디바이스로서 많은 데이터를 저장할 수 없고 인증 응용프로그램의 설치 또한 번거로움을 유발하기 때문에 설치 없이 간편하게 인증할 수 있는 인증 방식을 적용해야 한다. 이에 적합한 인증 기술인 FIDO 인증을 도입해 보안성을 강화하고 사용자에게 더 나은 인증법을 제안하고자 한다.

3.2.1 UAF 다중 인증 프로세스

본 논문에서 제안하고자 하는 다중 인증 방식은 FIDO 기술의 UAF 기술을 통해 설계하였다. 다중 인증 프로세스를 적용하기 위해 일상생활에 자주 접하며 사용자가 관리할 수 있는 사물인터넷 디바이스인 공유기의 관리자 페이지 환경에서 프레임워크를 설계하였다.

제안하고자 하는 프레임워크의 동작은 그림 4와 같다. 유저 디바이스를 통해 모바일 환경의 관리자 페이지를 이용하여 ID/PW 기반 1차 인증 수행하고 공유기에서 유저 디바이스에 FIDO 인증 요청한 후 응용 어플리케이션에서 서버에 인증 요청한다. 서버에서 메시지 생성 후 응용 어플리케이션을 통해 유저에게 전달 후 유저는 디바이스에 설치되어있는 프로그램을 통해 FIDO 인증을 완료 후 개인키를 통해 전자 서명 메시지를 FIDO 서버로 전송한다. 서버에서 인증 응답을 등록하고 사전에 등록되었던 공개키를 통해 검증한 후 성공 시, 메시지를 유저 디바이스 및 공유기에 전송한다.

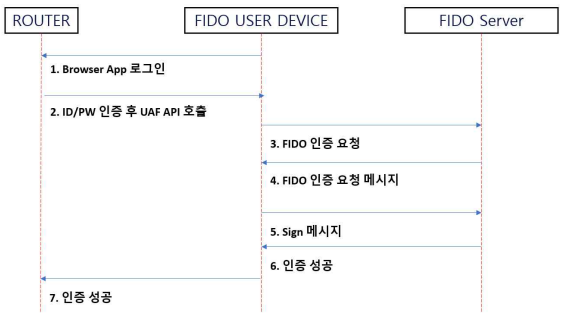

그림 4. UAF 기반 다중 인증 프로세스
Fig. 4. UAF based Multi-Factor Authentication process

3.2.2 Open-Source on eBay

현재 기업들이 FIDO UAF를 구축하고 상품을 소비자에게 제공하고 있으나, 테스트를 위한 개발이나 참조할 수 있는 openSource가 적어 서버 구축을 위한 개발이 어려운 상황이다. 이를 해결하기 위해 UAF Client - Server 개발에 필요한 부분을 실제 ebay에서 제공하는 UAF 오픈 소스를 활용하였다. ebay에서 제공한 FIDO ebay는 안드로이드 환경에서 구동 가능한 앱이다[14].

그림 5. 인증 화면
Fig. 5. Authenticate Layout

eBay에서 제공한 오픈 소스를 바탕으로 FIDO 데모 서버를 안드로이드 스튜디오를 통해 가상의 서버를 구축하고 공유기의 로그인과 동일한 페이지를 구축 후 그림 5의 인증 화면에서 FIDO 인증 과정을 수행해 지연시간을 측정하였다. 지연시간을 통해 사물인터넷의 다중 인증에 사용된 FIDO의 장점인 빠르고 편리해, 언제든지 안전한 사용이 가능하다는 점을 강조할 수 있는 지표이다. 따라서 FIDO를 사용할 때 지연시간이 짧은 경우 위 사항에 부합한다고 판단하여 지연시간을 측정하였다.

4. 연구 결과 및 분석

4.1 정량적 성능 평가

본 논문에서는 FIDO 다중 인증 방식이 단일 인증과 비교를 통해 다중 인증의 우수성을 평가하기 위해 접근성에 초점을 두어 로그인 응답시간을 평가의 대상으로 진행하였다. 단일 인증과 다중 인증의 응답 시간을 비교하여 지연시간 측정을 통해 안전성이 뛰어난 FIDO 기술을 빠르고 편리하게 사용할 수 있는 점을 강조할 수 있기 때문이다.

지연 시간 측정은 UAF를 적용한 인증방식에 대한 평가를 진행하였다. eBay에서 제공한 FIDO 데모 서버를 통해 인증을 진행했으며 응용프로그램에서 인증을 호출하였다. 인증 프로세스의 완료 시간을 총 30회 측정하여 평균값을 비교하여 지연시간을 반환한다.

그림 6과 같이 기존 단일 인증 수행 시간은 평균 2.73초로 측정되었고 UAF 기반 다중 인증을 적용한 인증 수행시간은 평균 3.43초로 대략 0.73초의 지연시간을 확인할 수 있다.

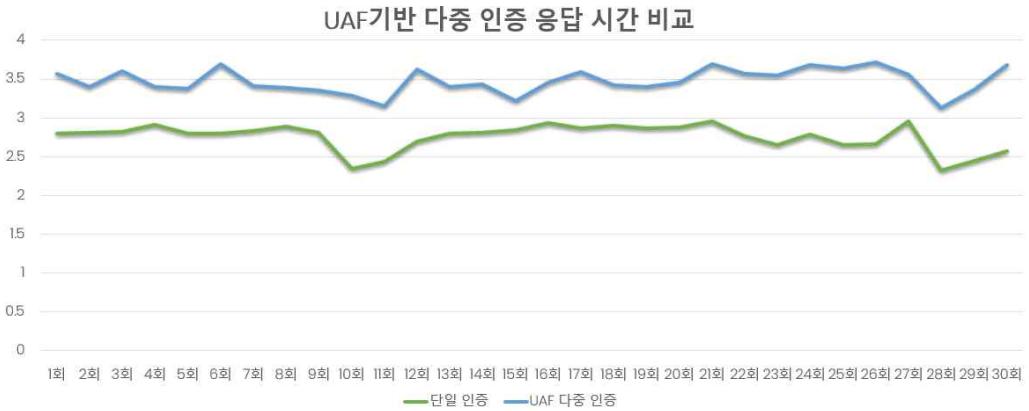

그림 6. 성능 평가 결과
Fig. 6. Performance Evaluation

본 연구에서 제안한 UAF에 대한 성능 평가는 단일 인증과 비교하여 수행 시간을 측정하였다. 현재 대부분의 사물인터넷 디바이스는 ID/PW 기반의 인증 방식만을 사용하고 있다. 본 연구에서 제안한 방식을 통해 단일 인증에 비해 성능 차이가 적음을 확인할 수 있다. 사물인터넷 환경에 따라 구성 방식에 따라 성능 차이가 발생할 수 있다[15]. 따라서 실제 사물 인터넷 환경이 주로 이루는 산업현장에서는 성능 차이가 발생할 것으로 보인다.

4.2 정성적 평가

본 논문에서는 다중 인증 프로세스를 적용에 대한 보안 정책을 평가하기 위해 한국인터넷진흥원의 '사물인터넷 보안 시험 인증 기준 해설서'를 참고하여 문건에 언급된 기준('인증' 유형, '암호' 유형, '데이터 보호' 유형, '물리적 보호' 유형)과 NIST-800 문건을 참고하여 안전성, 신뢰성, 편의성 총 3가지 항목을 기준으로 평가한다.

안전성은 FIDO 다중인증 방식을 적용 시 안전성과 키 관리 방식에 관한 평가이다. FIDO는 안전한 암호 관리를 위해 PKI(Public Key Infrastructure)를 사용하여 인증, 등록, 전자서명을 제공한다는 점에서 기존 방식과 비교하여 더 안전함을 보장할 수 있다. FIDO 알고리즘은 PKI에서 ECC(Elliptic Curve Cryptography)에 속하는 ECDSA(Elliptic Curve Digital Signature Algorithm) 알고리즘을 사용하여 '사물인터넷 보안 시험 인증 기준 해설서'에 언급된 보안 강도 112bit 알고리즘에 해당한다. 또한, 금융권에서 FIDO 인증을 확대하는 추세를 통해 안전성이 보장되어 있다고 판단할 수 있다[16]. 따라서 본 논문에서 제시한 다중 인증 프로세스에 대한 안전성을 확인할 수 있다.

신뢰성은 사물인터넷 환경에서 FIDO 기술이 적절한 사용자 인증이 수행되고 무결성이 보장되는지에 대한 평가이다. 무결성 보장은 ECDSA 알고리즘을 통해 기존 전자서명에서 보장 못한 '올바른 공개키 수집 문제'를 해결하였다. 전자서명을 통해 메시지 인증, 서명자 인증, 메시지 무결성, 부인 방지를 지원하여 적절한 사용자 인증이 수행되는 것을 확인할 수 있다. 따라서 본 논문에서 제시한 다중 인증 프로세스에 대한 신뢰성을 확인할 수 있다.

편의성은 사용자가 직접 사용하면서 느낀 접근성과 편의성에 대한 평가이다. 본 논문에서는 ID/PW 방식에 UAF 기술을 추가한 프로세스로 지연시간을 측정한 결과 공유기와 같은 저사양 디바이스에서 큰 차이가 없음을 확인하였다. 또한, UAF 기술은 모바일 어플리케이션으로 생체인증 등 추가 인증이 가능하므로 접근성과 편의성 측면에서 보장되어 있다고 판단할 수 있다.

5. 결 론

가정 공간에서 사용하는 개인용 사물인터넷 디바이스 이외에도 사무공간에서 사용하는 사물인터넷의 사용이 점차 늘어나는 추세다. 사물인터넷의 보급과 사용이 늘어남으로써 사물인터넷 디바이스를 대상으로 하는 보안 공격 사례도 많이 대두되고 있다. 특히 공용 공간에서 많은 사람이 사용하고 있어, 적절한 접근통제가 이뤄지지 않으면 피해가 발생할 수 있다. 공용 공간에서 사용하는 사물인터넷 디바이스는 공유기를 통해 통신하기 때문에 공유기에 대한 적절한 인증을 도입해야 한다.

본 논문에서는 저사양 사물인터넷 다중 인증을 통해 사물인터넷 환경에서 보다 강력한 사용자 인증을 제시했고 eBey에서 제공한 UAF 오픈소스를 통해 FIDO 데모 서버를 구축하고 모바일 어플리케이션 환경에서 사용자 인증 프로세스를

설계하였다.

해당 프로세스 평가를 위해 지연시간을 측정해, 지연시간이 짧은 것을 확인하였다. 이를 통해 사물인터넷 환경에서 적용 가능함을 확인하였고, KISA와 금융 보안원의 문건을 통해 보안 요구사항을 확인하였다.

하지만 가정용과 사무 환경에서 사용하는 사물인터넷이 아닌 산업 현장에서 사용하는 고사양의 사물인터넷일 경우 많은 연산이 수행되어 성능 저하가 발생할 수 있고 사물인터넷 종류에 따라 적절한 인증 기술을 찾기가 어려울 수 있어, 이와 관련된 연구는 지속해서 이루어져야 한다.

또한 다중 인증 프로세스 적용하더라도 사용자의 보안 인식 부재로 인해 발생하는 보안 위협은 여전히 존재하기 때문에 경각심을 가져야 한다는 한계점이 존재한다.

이 본문은 인천대학교 2018년도 자체연구비 지원에 의하여 연구되었음

참 고 문 헌

[1] M. S. Kong & H. J. Chae & B. H. Ryu. (2016). Trends and Prospects of Internet of Things. Journal of the KSME, 56(2), 32-36. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE06599541

[2] H. H. Kim & H. J. Lee & Y. S. Lee. (2020). A Survey Analysis of Internet of Things Security Issues and Combined Service. Journal of the Korea Society of Computer and Information , 25(8), 73-79. DOI:10.9708/jksci.2020.25.08.073

[3] Korea Communications Commission. (2011). Guidebook for Introducing and Operating Smart Work for Enterprises. National Information Society Agency. https://kcc.go.kr/user.do?mode=view&page=A05030000&dc=K00000001&boardId=1113&boardSeq=30589

[4] Y. G. Kim & J. H. Lee & G. S. Yoon. (2014). A Study on the Smart Office Fit Model of Government and Local Government. KOREA INSTITUTE OF PUBLIC ADMINISTRATION. https://www.kipa.re.kr/site/kipa/research/selectBaseView.do?gubun=SU&seqNo=BASE_000000000000176

[5] G. H. Kim. (2013). Smart Work Fundamentals are Trust and Responsibility. Kookmin Webzine, 24(). https://webzine.kookmin.ac.kr/webzine.php?syear=2013&svolume=6&mcode=4&scode=2

[6] Korea Internet & Security Agency. (2017). Home appliance IoT security guide. Korea Internet & Security Agency. https://www.krcert.or.kr/data/guideView.do?bulletin_writing_sequence=36355&queryString=YnVsbGV0aW5fd3JpdGluZ19zZXF1ZW5jZT0zNTI5Ng

[7] J. M. Kang. (2017). A Verification of Smart TV Security in IoT Environment. SoongSil Univ Graduate School of Information Science. http://www.riss.kr/search/detail/DetailView.do?p_mat_type=be54d9b8bc7cdb09&control_no=efcdde7de1c06980ffe0bdc3ef48d419

[8] Ministry of the Interior and Safety. (2014). Guidelines for Efficient Use and Operation of Smart Work Centers. Ministry of the Interior and Safety. https://www.mois.go.kr/frt/bbs/type001/commonSelectBoardArticle.do;jsessionid=ump6hSc+YDm89Vu2HRTSphyu.node50?bbsId=BBSMSTR_000000000012&nttId=44430

[9] Ministry of Science and ICT. (2019). The "IoT Security Threat Scenario Contest" award ceremony will be held. Ministry of Science and ICT. https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=112&bbsSeqNo=94&nttSeq

No=2418998&formMode=&pageIndex=&searchCtgry=&searchCtgry2=&searchCtgry3=&RLS_YN=&searchOpt=&searchTxt=
[10] S. R. Jo & S. H. Kim. (2017). FIDO technology standardization trend. TTA Journal, 172(), 65-70. https://www.tta.or.kr/tta/publicationHosuList.do?key=80&rep=1&searchKindNum=1
[11] K. Y. Lee & B. S. Kim & J. S. Cho. (2018). Design and Implementation of Security System for Providing Secure Boot and Firmware Update in Low-end IoT Device. Journal of KIISE, 45(4), 321-331. DOI:10.5626/JOK.2018.45.4.321
[12] Financial Security Institute. (2017). Introduction to the selection process for the introduction of certification technology. Financial Security Institute, 2017-003. https://www.fsec.or.kr/bbs/detail?bbsNo=5716&menuNo=241
[13] FIDO Alliance. (2017). NIST 800-63 Guidance & FIDO Authentication. FIDO Alliance Proposed Standard. https://fidoalliance.org/nist-800-63-guidance-fido-authentication/?lang=ko
[14] H. J. Lee & H. J. Cho & Y. K. Kim & C. J. Chae. (2020). A study on the FIDO authentication system using OpenSource. Korea Convergence Society, 11(5), 19-25. DOI:10.15207/JKCS.2020.11.5.019
[15] W. Y. Yu. (2018). A Study on Access Control Policy Management between IoT Devices for Smart Home Security. ChungAng Univ Graduate School. http://www.riss.kr/link?id=T14914424
[16] T. H. Kim. (2016). Era of non-face-to-face real-name authentication for biometric authentication in the financial sector. boannews. https://www.boannews.com/media/view.asp?idx=64444

저 자 소 개

김상윤(Sang-Yoon Kim)

2021.3 ~ 현재 : 인천대학교 정보통신공학과 학사과정

<주관심분야> IoT, 정보보호, 데이터 분석

이기영(Ki Young Lee)

1982년 2월 : 연세대학교 전기공학과(공학사)

1984년 2월 : 연세대학교 대학원 전기공학과(공학석사)

1987년 12월 : 미국 콜로라도 대학 전기 및 컴퓨터공학과(MS)

1993년 12월 : 미국 알라바마 대학 전기 및 컴퓨터공학과 (Ph.D)

1994년3월~현재: 인천대학교 정보통신공학과 교수

<주관심분야> 인터넷 트래픽 제어 및 프로토콜, 정보보호, 사용자 인증시스템, IoE 응용 및 보안