The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 16, No. 4, pp.41-46, Aug. 31, 2016. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2016.16.4.41
JIIBC 2016-4-7

웨어러블 디바이스 기반의 안전한 통신을 위한 인증기법 설계

A Design of Authentication Method for Secure Communication based on Wearable Device

박중오*

Jung-Oh Park*

요 약 최근 들어 국내외 대기업에서는 웨어러블 디바이스 사업에 전폭적으로 투자하고 있으며, 지난해 대비 26% 가량 많은 사용자들이 웨어러블 디바이스 기반의 다양한 서비스를 제공받고 있다. 기존의 헬스케어, 스마트워크, 스마트 홈 환경에서 폭넓게 사용되고 지고 있으며 융합서비스 환경에서 접목할 수 있도록 도입되어지고 있다. 그러나 G사의 제품이 상용화 되면서 개인정보보호 이슈가 사회적으로 큰 파장을 불러일으키고 있으며, 통신의 데이터 관리 및 보안 쪽에서 위험성이 증대되고 있다. 또한 기존의 무선 환경에서 사용되었던 암호체계를 사용ㅎ고 있어 신규 및 변종 보안 위협에 대한 취약성이 발생하고 있다. 본 논문에서는 웨어러블 디바이스 기반에서 안전한 통신을 수행할 수 있는 프로토콜에 대해서 연구를 한다. 등록 및 인증과정에서 코드 값을 기반으로 서명값을 생성한다. 서명 값을 기반으로 안전한 통신을 수행할 수 있도록 통신기법을 설계하도록 한다. 웨어러블 디바이스환경에서 발생하는 공격기법에 대해서 안전성을 분석하여, 기존의 암호시스템과 제안시스템의 성능평가를 수행하여 대략 14%의 효율성을 확인할 수 있었다.

Abstract Recently, many domestic and foreign corporates are concentrating in investment to wearable devices and users are provided with various service based on wearable devices 26% more than compared to last year. It is widely used in previous healthcare, smart work, smart home environment, and it is now introduced to get connection to fused service environment. However, as products of G company are commercialized, the security issue of personal information is causing dispute in society, and the danger of data management and security regarding telecommunication is increasing. Also, because the password system used in previous wireless environment is still in use, there are possible vulnerability considering the new and mutant security threat. This thesis conducted study about protocols that can exercise safe telecommunication in the basis of wearable devices. In the registration and certification process, the signature value is created based on the code value. The telecommunication method is designed to conduct safe telecommunication based on the signature value. As for the attack method occurring in the wearable device environment, the safety was analyzed and conducted performance evaluation of previous password system and proposal system, and verified about 14% of efficiency.

Key Words : Wearable Device, Authentication, Communication Protocol

*정회원, 성결대학교 파이데이아 칼리지
접수일자 : 2016년 6월 9일, 수정완료 : 2016년 7월 8일
게재확정일자 : 2016년 8월 5일

Received: 9 June, 2016 / Revised: 8 July, 2016 /
Accepted: 5 August, 2016
*Corresponding Author: jopark02@sungkyul.ac.kr
Dept. of Computer Engineering, Sungkyul University, Korea

Ⅰ. 서 론

통신 모듈을 탑재한 웨어러블 디바이스의 인기가 높아지며 가입자들이 빠르게 늘고 있다. 과거에는 고가의 가격과 사용성이 미비하다는 평가를 받아 외면 받았지만, 현재는 저가의 디바이스들이 생겨나고 호환성을 높이고 다양한 기능들이 추가됨으로서 사용자의 수요가 늘어나고 있는 상황이다[1][5].

웨어러블 디바이스는 항시성, 사용자 인터페이스, 착용감, 안전성, 사회성에 대한 기본 기능을 제공하고 있으며, 용도에 따라서 스마트폰 대체와 업무용 보주도구들에 대한 기능을 수행하고 있다. 하지만 웨어러블 디바이스 사용으로 인한 사생활 침해 및 개인정보 유출에 대한 우려도 발생하고 있으며, 사생활 침해문제가 심각할 수 있다고 예견할 수 있다[2-3].

그러므로 본 논문에서는 웨어러블 디바이스 기반에서 안전한 통신을 수행하기 위한 인증기법을 설계한다. 웨어러블 디바이스 등록 및 인증절차를 걸쳐서 안전한 통신 메시지를 설계에 대해서 연구한다.

본 논문은 5장으로 구성되어 있으며 2장에서는 웨어러블 디바이스 활용사례 및 취약점, 보안 요구사항에 대해서 작성한다. 3장은 제안부분으로 웨어러블 디바이스 등록 및 인증 절차, 통신 프로토콜 설계에 대해서 서술한다. 4장에서는 웨어러블 환경에서 발생하는 공격기법에 대한 안전성 분석, 보안성 및 암호성능 평가에 대해서 분석한다. 5장은 본 논문의 결론으로 웨어러블 디바이스 기반의 연구방향을 제시하고 끝낸다.

Ⅱ. 관련연구

1. 웨어러블 디바이스 활용 사례 및 취약점

스마트폰 중심의 컨버전스 환경에서는 사용자의 행동패턴을 인지한 다수의 웨어러블 디바이스가 발전하고 있다. 국내에서는 2015년부터 "웨어러블 스마트 디바이스 "개발로 주력하고 본격적으로 프로젝트 사업을 추진하고 있다. 웨어러블 디바이스의 특징은 휴대성 뿐만 아니라 그때 상황에서 발생하는 데이터를 수집하여 이를 적절하게 대치할 수 있는 영역을 말한다[1][5].

웨어러블 디바이스 활용사례를 살펴보면 콘텐츠 렌즈, 패치와 같은 부착형과 센서 타입의 이식 및 착용형이 있다. 의류일체형과 소품타입으로 다양한 서비스를 제공받을 수 있으며 활용사례는 그림 1과 같다[3-5].

이러한 편의성을 제공하는 부분이 있지만, 한편으로는 프라이버시 정책, 보안 기술 도입이 필요한 것으로 나타나고 있다. 평문형태의 데이터 전송, 프라이버시 정책 부재, 데이터 유출, 취약한 시스템 관리 등에서 취약점이 발생하고 있으며 무선 네트워크 및 IoT환경에서 발생하는 공격기법들이 발생하고 있다[4][6].

그림 1. 웨어러블 디바이스의 활용사례
Fig. 1. Use Cases of Wearable Device

취약점 및 공격기법에 대응하기 위해서 기기의 비인가 된 사용자에 대한 접근 차단, 패스워드 설정, 데이터 전송 시 암호화 기술, 프라이버시 정책에 맞은 서비스 제제 등에 대한 연구가 요구되어지고 있다[5].

2. 웨어러블 디바이스 보안 요구사항

웨어러블 디바이스 환경에서는 사용자 정보 노출, 스마트 폰의 내장된 금융정보 탈취 뿐 만아니라 의료기기 환경에서는 생명을 위협하는 행위가 가능함으로써 큰 문제점으로 대두되어지고 있다. 이에 대한 취약성을 보완하기위해 웨어러블 디바이스 환경에서 디바이스, 접속 네트워크, 서버 네트워크 영역에서 보안기술을 고려하고 있다[7].

우선 디바이스 영역에서는 추출된 데이터를 안전하게 전송하기 위해 기밀성, 무결성 및 기기간의 인증기술이 요구되어 지고 있다. 접근 네트워크에서는 상호간의 안전하게 통신할 수 있는 인증기술과 MAC(Message Authentication Code)를 활용한 데이터 무결성에 충족시켜야 한다. 마지막으로 서버 네트워크에서는 비인가 된 사용자의 접근, 펌웨어 관리, 악성코드 및 바이러스 공격에 대한 적절한 대응책들이 연구되어야 한다[5-6].

Ⅲ. 제안프로토콜

본 논문에서는 웨어러블 디바이스 기반의 사용자의 안전한 통신을 수행하기 위한 등록, 통신 프로토콜을 설계한다. 웨어러블 디바이스는 스마트폰을 활용하여 Management Server에 등록 및 인증하며 Service Server로 안전한 통신과정을 수행한다. 논문에서 제안된 전제조건은 아래와 같으며 제안기법의 약어는 표 1과 같다.

(1) 인증환경에서 스마트폰과 Management Server는 ECCSA 알고리즘을 수행할 수 있다.
(2) 웨어러블 디바이스는 추출된 데이터를 송신할 때 AES암호화 방식을 사용한다.

표 1. 약어표
Table 1. abbreviation

Symbol	Description
$Device_{SN}$	Serial Number by the device
E_{PUB_A}	Private key encryption of A
E_{PRI_A}	Public key encryption of A
E_{ECC}	ECC-based encryption
$Device_{Nonce}$	Random number generated by the device
IMEI	Subscriber Identifier
$Code_{Value}$	The generated code value in a hash function
Signauture	Signauture Value
$Situation_{Code}$	Converting the data extracted in the device parameters
$Feedback_{Code}$	Parameter corresponding to the value of the status from the server

1. 웨어러블 디바이스 등록 및 인증

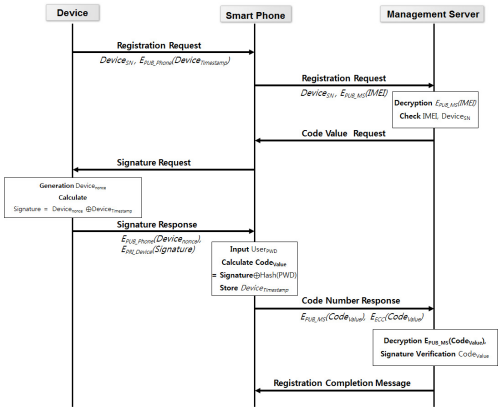

그림 2. 웨어러블 디바이스 등록 절차
Fig. 2. Wearable Device Registration Process

사용자는 웨어러블 디바이스와 스마트 폰을 Management Server로 등록한다. 디바이스의 일렬번호, 스마트 폰의 IMEI값을 검증 및 서명값을 생성한다. 서명값을 기반으로 코드값을 생성 후 이를 인증한다. 웨어러블 디바이스 등록 및 인증절차는 그림 2과 같다.

(1) 사용자는 Device를 사용하여 Smart Phone으로 등록과정을 수행한다.

$$Device_{SN}, E_{Pub-Phone}(Device_{Time\ Stamp})$$

(2) Smart Phone으로 Management Server로 등록 요청 메시지를 전송한다.

$$Device_{SN}, E_{Pub-MS}(IMEI)$$

(3) Management Server에서 송신되었던 메시지를 복호화 후 IMEI, $Device_{SN}$을 확인한다.

(4) Smart Phone으로 검증 값을 요청한다. 이후 Smart Phone에서 서명값을 Device로 요청한다.

(5) 수신된 메시지를 받은 Device는 $Device_{Nonce}$를 생성 후 $Signaure$를 계산하여 Smart Phone으로 발송한다.

$$Signature = Device_{nonce} \oplus Device_{time\ stamp}$$
$$E_{Pub-Phone}(Device_{nonce}),$$
$$E_{PRI-Device}(Signature)$$

(6) Smart Phone은 사용자의 패스워드를 입력 받은 값을 기반으로 $Code_{Value}$를 생성한다. 이후 $Device_{Time\ Stamp}$를 저장 후 Management Server로부터 코드값을 전송한다.

$$Code_{Value} = Signature \oplus Hash(PWD)$$
$$E_{Pub-MS}(Code_{Value}), E_{ECC}(Code_{Value})$$

(7) Management Server에서는 수신된 메시지를 복호화 후 서명값을 검증한다. 이후 Smart Phone으로 등록 완료 메시지를 전송한다.

2. 웨어러블 디바이스 기반의 통신 프로토콜 절차

앞 절에서 등록 및 인증과정을 마치고 스마트폰과 웨어러블 디바이스에서 생성된 데이터를 Service Server로 통신하는 절차를 진행한다. Service Server는 추출된 데이터와 코드 값을 검증 후 이에대한 결과값을 사용자로 전송한다. 제안된 통신 프로토콜 그림 3와 같다.

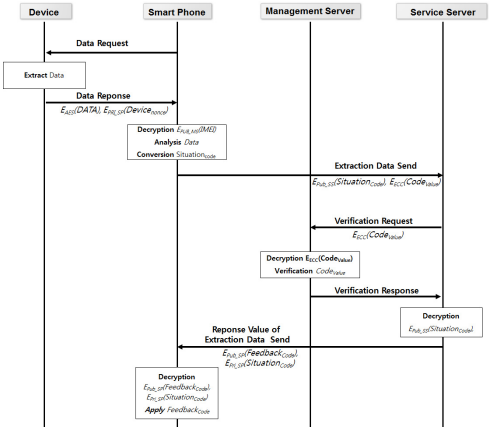

그림 3. 웨어러블 디바이스 통신 절차
Fig. 3. Wearable Device Communication Process

(1) 사용자는 Smart Phone을 활용하여 Device로부터 데이터를 요청한다. Device는 데이터를 추출 후 Smart Phone으로 데이터를 전송한다.

$$E_{AES}(DATA), E_{PRI-SP}(Device_{Nonce})$$

(2) 수신된 데이터를 복호화 후 데이터를 분석한다. 이후 $Situation_{code}$로 변환 후 Service Server로 추출된 데이터를 전송한다.

$$E_{Pub-SS}(Situation_{Code}), E_{ECC}(Code_{Value})$$

(3) Service Server는 Management Server로 검증 요청 메시지를 전송한다.

$$E_{ECC}(Code_{Value})$$

(4) Management Server에서는 메시지를 복호화 후 $Code_{Value}$를 검증한다. 이후 검증 완료 메시지를 전송한다.

(5) Service Server에서는 수신된 메시지를 복호화 하고 Smart Phone으로 추출된 데이터의 응답 메시지를 전송한다.

$$E_{Pub-Sp}(Feedback_{Code}),$$
$$E_{PRI-SP}(Situation_{Code})$$

(6) Smart Phone에서 수신된 메시지를 복호화 하고 $Feedback_{code}$를 적용한다.

Ⅳ. 성능평가

1. 안전성 분석

– 중간자 공격

웨어러블 디바이스와 스마트 폰에서 통신을 수행할 때 네트워크 벡터 공격영역에서 중간자 공격에서 노출되었던 사례가 발생하고 있다. 이러한 공격기법을 방어하기 위해 제안된 시스템에서는 등록과정에서 생성 된 $Code_{Value}$를 생성 하고 확인함으로써 중간자 공격이 실패로 끝난다.

– 비인가된 사용자 및 서비스 접근

웨어러블 디바이스 특성상 휴대성과 사용성의 편리함을 제공 하지만, 도난 및 분실에 대한 위험성이 존재한다. 도난당한 디바이스를 비 인가된 사용자의 접근 및 서비스 서버의 데이터 유출에 대한 피해가 발생할 수 있다. 그러므로 이를 방지하기 위해서 등록과정에서 사용자의 PWD를 입력 후 Management Server에서 인증받으며, 스마트폰의 Signature Value를 기반으로 $Code_{value}$를 통신 프로토콜에서 사용함으로서 인가되지 않은 사용자의 접근에 대해서 안전하다.

– 개인정보 및 프라이버시 위협

웨어러블 디바이스는 사용자로부터 수집된 데이터를 안전하게 관리되어야 한다. 수집된 데이터는 빅데이터 환경과 융합되어 효과서비스를 제공할 수 있다. 하지만 데이터의 대한 민감도가 높아지고 위협성이 커질 수 있다. 사용자의 서명값과 $Code_{value}$를 전송하여 데이터에 대한 $Feedback_{Code}$과 $Situation_{code}$를 변환함으로써 데이터에 대한 안정성을 높일 수 있다.

– 기밀성 및 무결성 위협

웨어러블 디바이스 기반의 생성 된 데이터는 공격기법에 대해서 안전성이 보장되어야 한다. IoT환경에서 발생하는 공격기법에 대해서 취약성이 존재할 수 있으며, 신규공격기법이 존재할 수 있다. 본 논문에서는 위협을 방지하기 위해서 통신 프로토콜 절차에서 추출된 데이터를 $Situation_{code}$로 변환 후 공개키 방식의 암호화로 전송하고, ECC기반의 암호화를 수행하여 서명값을 검증한다.

2. 보안성 및 암호성능 분석

본 절에서는 제안된 프로토콜의 웨어러블 디바이스의 보안요구사항을 기반으로 보안성을 평가하였다. 기존의 시스템에서도 데이터 기밀성 및 무결성을 지원하지만, 제안된 시스템에서는 서명값을 기반으로 ECC 암호를 수행해서 보완성을 강하였다. 또한 상호인증을 수행함으로써 중간자 공격, 프라이버시 위협, 비 인가된 사용자의 접근에 대한 취약점을 보안하였다. 마지막으로 인증 수행과정에서 기존의 해쉬함수 Seed, MD5, PKI(Cert)가 아닌 ECC암호를 수행함으로서 효율성을 높였다. 기존 시스템과 제안된 시스템의 보안성 분석한 자료는 표 2와 같다.

표 2. 기존 시스템과 제안된 방식의 보안성 비교
Table 2. Comparison of the security of the conventional method with the proposed method

Classification	Existing System	Proposed System
Data confidentiality and integrity	Support	Support
Mutual authentication	Not Support	Support
Process of execution of authentication	2Encryption + 1Hash(Cert)	2Encryption +1Hash(ECC)
Attack Technique	MITM Privacy Threat Unauthorized user access	-

제안된 인증기법과 통신 프로토콜의 암호성능을 분석하기 위해 시스템 환경은 Inter(R) Core i7-4970(3.6GHz), 8.00 GB, Windows Professional 64 bit환경에서 Eclipse IDE for JAVA Developers을 사용하여 구현하였다. 기존의 SEED, MD5, PKI(Cert)와 제안된 인증기법의 ECCSA은 그림 4과 같다. 인증 성능 부분에서 기존의 시스템의 PKI(Cert)보다 대략 15%향상되었으며, 통신 과정에서는 대략 13%향상된 수치를 확인할 수 있었다.

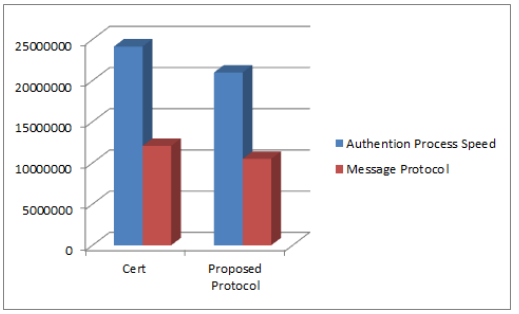

그림 4. 제안된 기법과 기존시스템의 암호성능 비교
Fig. 4. Password performance comparison of the proposed method with the existing system

V. 결 론

본 논문은 웨어러블 디바이스 기반의 안전한 통신을 위한 인증기법에 대해서 연구하였다. 웨어러블 디바이스와 스마트 폰의 식별값을 기반으로 등록을 수행하였으며, 식별값으로 서명메시지를 생성 후 ECCSA를 통하여 해쉬값으로 인증하였다. 그리고 통신 프로토콜에서는 해쉬값을 기반으로 안전한 통신을 수행하도록 설계하였다.

웨어러블 디바이스기반의 통신환경은 중간자 공격, 비인가된 서비스 및 사용자 접근뿐만 아니라 개인정보 유출에 대한 피해가 발생할 수 있다. 또한 사용자의 정보를 통심함으로써 관리에 따른 보안대책이 요구된다. 그리고 무선네트워크에서 발생하는 취약점이 존재할 수 있다. 제안된 프로토콜에서는 보안성 및 안전성을 강화하였으며, ECCSA를 활용하여 기존의 PKI(Cert)대비 대략 15%, 13%를 향상시켜 효율성을 개선하였다.

향후 제안된 기법을 활용하기 위해서는 IoT환경하고 접목할 수 있는 연구가 필요하고, 프라이버시 보호와 기기 기기사용에 대한 올바른 대책 및 정책에 대한 규정이 요구되어 지고 있다. 빠르게 발전되어지는 IoT환경의 취약점 분석 및 공격유형 분석에 대한 연구가 필요하다.

References

[1] Wen-Quan JIN, D. H. Kim, "Implementation and

Experiment of CoAP Protocol Based on IoT for Verification of Interoperability," The Journal of The Institute of Internet, Broadcasting and Communication(JIIBC), Vol. 14, No. 4, pp. 7-12, 2014.

[2] I. k Im, J. p Jeong, "Authentication eXtention Scheme of Fast Handover for Secure NEMO-based PMIPv6 Networks ," The Journal of The Institute of Internet, Broadcasting and Communication(JIIBC), Vol. 13, No. 4, pp. 107-119, 2013.

[3] S. T. Yoo, S. H. Oh, " OAuth-based User Authentication Framework for Internet of Things". KAIS, Vol 16, No. 11, pp.8057-8063, 2015.

[4] Y. H. Lee, H. S. Kim, "Remarks on Smart Watch Security Vulnerability and Solution", JSE, Vol. 12, No. 3, pp. 191-206. 2015

[5] S. T. Kim, "Wearless OS Technology Trends", TTA Special Report. Vol 154, pp44-50. 2014

[6] Toorani, Mohsen. "On vulnerabilities of the security association in the IEEE 802.15. 6 standard." Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2015. 245-260.

[7] Luyi Xing, Xiaolong Bai, Tongxin Li, XiaoFeng Wang, Kai Chen, Xiaojing Liao, "Unauthorized Cross-App Resource Access on MAC OS X and iOS", May 2015

저자 소개

박 중 오(정회원)

- 2000년 7월 : 성결대학교 컴퓨터공학과 졸업
- 2003년 3월 : 명지대학교 전자계산교육 석사
- 2011년 8월 : 숭실대학교 컴퓨터공학 박사
- 2013년 3월 ~ 2016년 2월 : 동양미래대학교 조교수
- 2016년 3월 ~ : 성결대학교 조교수
- 관심분야 : PKI, Network security, 암호학
- E-Mail : jopark02@sungkyul.ac.kr