http://dx.doi.org/10.15207/JKCS.2015.6.2.065

블루투스 v4.1 비콘 기반 쿠폰 융합서비스에서의 보안위협 연구

이광재, 이근호
백석대학교 정보통신학부

A Study of Security Threats in Bluetooth v4.1 Beacon based Coupon Convergence Service

Kwang-Jae Lee, Keun-Ho Lee
Division of Information and Communication, Baekseok University

요 약 사물인터넷(IoT), 핀테크(Fintech) 등 기존에 없던 새로운 기술이 등장함에 따라 기존 시스템의 보안위협의 범위가 늘어나고 있다. 특히 사물인터넷은 IT 인프라의 범위가 늘어나 특정 시스템에 악의적인 행위를 수행할 수 있는 범위가 늘어나게 된다. 핀테크(Fintech) 역시 기존에 존재하지 않은 새로운 구조를 가지고 있어 전통적인 보안시스템의 개혁이 요구된다. 향후 사물인터넷과 핀테크(Fintech) 기술이 상용화되고 시장이 발전함에 따라 구조상의 보안위협은 실제 공격으로 이어지고, 공격자가 사물인터넷 단말기에 백도어를 심어 원격 접속을 하여 2차 공격으로 이어질 수 있다. 이처럼 다양한 보안위협이 내제된 새로운 시스템에서 고객이 소유한 단말기를 보안을 위하여 강제적으로 통제할 수 없다. 그러므로 이와 같은 서비스는 수집하는 정보를 최소화 하여야 하며, 수집한 정보를 활용하는 방안에 대하여 정책적으로 통제가 필요한 시점이다. 본 논문에서는 사물인터넷(IoT), 핀테크(Fintech) 등 새롭게 등장하는 모바일 서비스에서 발생할 수 있는 보안위협을 제안하고자 한다.

• **주제어** : 사물인터넷, 핀테크, 블루투스 v4.1, 비콘, 융합

Abstract As the new technologies like IoT and Fintech appear which have not existed before, security threat ranges in existing system are increasing. Especially, IoT has increasing ranges to cause malicious behaviors in specific systems because related IT infrastructure ranges are increasing. Fintech also requires the innovation of traditional security system because it has new structure which didn't exist in the past. As IoT and Fintech technologies are commercialized and related markets are developing in the future, structural security threats could be connected to actual attacks and secondary attacks by the attackers' imbedding of back door in IoT internet devices through remote access. Customer's device cannot be compulsively controlled for security in new system where these various security threats exist. Therefore, these services should minimize the collected information, and now is the time to politically control the utilizing methods of the collected information. In this thesis, security threats are to be suggested which could occur in newly appearing mobile services like IoT and Fintech.

• **Key Words** : IoT, Fintech, Bluetooth v4.1, beacon, convergence

*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2015년 2월 3일 수정일 2015년 3월 30일 게재확정일 2015년 4월 20일

1. 서론

최근 차세대 기술로 여러 분야에서 주목되고 있는 사물인터넷 IoT(Internet of Things)은 사람, 사물, 데이터 등 모든 것이 인터넷으로 연결되어 정보가 생성, 수집, 활용하는 등의 기술을 통칭하는 개념이다. 모든 사물이 인터넷과 연결되는 사물인터넷 기술로 인해 악의적인 행위와의 서로 연결되는 접점이 크게 증가할 것이라 예상하고 또한 사물인터넷 기반 분야의 기술이 발전함에 따라 위치 기반 기술이 핵심으로 떠오르고 있는 현재에 저전력 블루투스(BLE) 기술인'Bluetooth v4.1'기반으로 한 비콘 서비스의 보안위협을 다루고자 한다. 최종적으로 사물인터넷 환경에서 이루어지는 간편 인증 결제시스템인 핀테크(Fintech)의 관련된 기술과 서비스를 분석하고자 한다. 핀테크(Fintech) 기술을 뒷받침해주는 비콘(Beacon)기술은 근거리 무선통신 장치로서 반경 50m 범위 안에 있는 사용자의 위치를 찾아 메시지 전송, 모바일 결제 등을 가능하게 해주는 스마트폰 근거리 통신 기술이다. 이 기술을 이용하면 특정 장소에서 안내 서비스, 모바일 쿠폰 등을 이용할 수 있게 된다. 이처럼 향후 스마트폰을 활용한 서비스 간편 인증 결제시스템 기술 개발이 활발하게 이루어진 결과인 핀테크(Fintech)는 인터넷 뱅킹 결제시스템에서 태동해 다양한 형태로 발전하고 있다. 특히 전자결제시스템의 등장으로 금융서비스의 질적인 향상과 비용 절감 효과가 커지고 있다. 또한 사람들의 소비패턴까지 바꾸고 있으며 이제는 펀드・보험 등 개인 자산관리와 소액대출 상품서비스까지 선보이고 있다. 최근에는 해외직접구매까지 생겨나는 등 온라인 쇼핑도 급속도로 성장하고 있다. 이러한 소비경향에 따라 발전하고 있는 간편 인증 결제시스템에서 발생할 수 있는 다양한 보안위협을 연구하여 새로운 해킹 공격 형태를 제시하고 분석하고자 한다[1,2].

2. 관련기술

2.1 블루투스(Bluetooth) v4.1

〈Table 1〉 Bluetooth process of transition

Year	*Technical contents*
1999.07	Bluetooth v1.0 draft, a
1999.12	Bluetooth v1.0B
2001.02	Bluetooth v1.1
2003.11	Bluetooth v1.2
2004.08	Bluetooth v2.0 + EDR(Enhanced Data Rate)
2007.07	Bluetooth v2.1 + EDR(Enhanced Data Rate)
2009.04	Bluetooth v3.0 + HS(High Speed)
2010.06	Bluetooth v4.0
2013.12	Bluetooth v4.1

블루투스(Bluetooth)는 1994년 에릭슨이 최초로 개발한 개인 근거리 무선 통신(PANs)을 위한 산업 표준이다. 블루투스는 나중에 블루투스 SIG(Special Interest Group)가 정식화하였고, 1999년 5월 20일 공식적으로 발표되었다. IEEE 802.15.1 규격을 사용하는 블루투스는 PANs(Personal Area Networks)의 산업 표준이다. 블루투스는 다양한 기기들이 안전하고 저렴한 비용으로 전 세계적으로 이용할 수 있는 무선 주파수를 이용해 서로 통신할 수 있게 한다. 블루투스는 ISM 대역인 2.45GHz를 사용한다. 버전 1.1과 1.2의 경우 속도가 723.1kbps에 달하며, 버전 2.0의 경우 EDR(Enhanced Data Rate)을 특징으로 하는데, 이를 통해 2.1Mbps의 속도를 낼 수 있다. 블루투스는 유선 USB를 대체하는 개념이며, 와이파이(Wi-Fi)는 이더넷(Ethernet)을 대체하는 개념이다. 암호화에는 SAFER(Secure And Fast Encryption Routine)+을 사용한다. 장치끼리 믿음직한 연결을 성립하려면 키워드를 이용한 페어링(pairing)이 이루어지는데, 이 과정이 없는 경우도 있다.

〈Table 2〉 New features of Bluetooth v4.1

Improving Usability	• Mobile Wireless Service Coexistence Signaling
	• Train Nudging
	• Generalized Interlaced Scanning
	• Low Duty Cycle Directed Advertising
	• L2CAP Connection Oriented Channels
Empowering Developer Innovation	• Dual Mode Topology and Link Layer Topology Software Features
Enabling the Internet of Things	• L2CAP Dedicated Channels (This is a foundational step for future support of IPv6 at the sensor level)

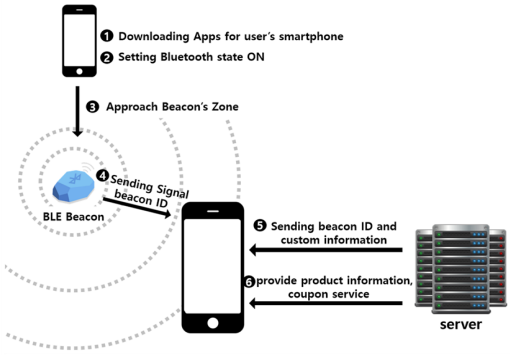
본 논문에서는 사물인터넷(IoT)과 밀접한 관련이 있는 Bluetooth v4.1 기술이 사물인터넷 산업에 어떠한 보안위협이 발생할 수 있는지에 대해 연구하고자 한다. 2013년 12월 발표된 블루투스 v4.1은 사용자에게 LTE와의 공존성을 높여 사용편의성을 향상시키고, 대용량 데이터 전송을 가능하게 할 뿐만 아니라, 기기들이 동시에

다양한 역할들을 수행할 수 있도록 지원함으로써 개발자들에게는 보다 혁신적이고 유연한 개발이 가능할 수 있도록 하였다. 또한 IP (Internet Protocol) 기반의 연결을 위한 초석을 마련하여 사물인터넷에 필수적인 무선 연결로서의 블루투스 기술 역할을 확대하였다. 블루투스 SIG의 CMO인 Suke Jawanda는 향후 5년 동안 블루투스 제품 출하량은 45억대 이상 치솟을 것이라 예상된다고 발표하였고, 이러한 시장의 확장에 대비해 블루투스 규격을 업데이트 하였으며 이를 통해 개발자들에게는 제품에 대한 컨트롤할 수 있는 권한을 높이고, 다른 무선 기술들과의 간섭을 줄이며, 기기들 간에 데이터들을 보다 빠르게 교환할 수 있게 되고 사용자의 수동적인 개입을 줄이더라도 연결을 유지할 수 있도록 해준다고 소개하였다. 추가적으로 이러한 모든 업데이트들은 현재 시장의 수요 및 상황을 반영하는 것이고, 향후 Bluetooth 무선기술이 사물인터넷 분야에서 매우 중요한 역할을 계속적으로 담당할 수 있게 하여 OEM, 개발자, 및 소비자들에게 가장 최고의 무선기술 및 솔루션이 될 수 있도록 발전시켜 나갈 것이라고 밝혔다[3].

기존의 블루투스 v4.0이 장치들 간의 통신 (M2M)이었다면, 블루투스 v4.1에서는 v4.0의 저전력 기술과 더불어 사물인터넷에 대응하는 특징을 지닌 규격이다. 블루투스 v4.1에서는 단순히 장치들 간의 통신에 머물지 않고 우리 생활에 더욱 밀착된 서비스와 편리하게 연동되도록 하여 24시간 깨어있는 지능형 장치가 될 수 있고 각 장치별로 축적된 데이터들을 블루투스로 연결해 능동적으로 데이터를 활용하도록 할 수 있다. 특히, 블루투스 v4.1에서는 소프트웨어적인 업데이트를 통해 기기간의 연결이 보다 쉽도록 규격을 개선하였기 때문에 모든 사물을 인터넷에 연결할 수 있는 사물인터넷의 기반 플랫폼이 될 수 있고, 이에 따라 장치에서 바로 웹이나 앱에 접근이 가능해진다. 또한 블루투스를 채택한 웨어러블 제품이 급격히 늘어나고 있는 현재 흐름과 더불어 블루투스 v4.0 이후부터 Bluetooth SMART 무선기술을 활용해 자동으로 스마트폰과 동기화가 이루어질 수 있도록 하고 코인셀 배터리를 삽입하여 배터리의 수명을 1년까지 늘일 수 있도록 하였다. 뿐만 아니라 블루투스를 통해 점점 더 많은 사물들이 서로 통신한다면 보안문제가 주요 이슈가 될 수 있기 때문에 이에 대응하기 위하여 128bit AES 암호화를 지원하고 있다[4].

2.2 비콘(Beacon)서비스

블루투스 무선통신기술을 이용해서 비콘 단말기가 발신하는 ID신호를 도달 거리 내 스마트폰에 설치된 애플리케이션이 인식한 후 비콘 서비스 서버로 전송 후 서버에서 확인된 위치 내 매장의 설정 서비스(메시지, 쿠폰 등)를 스마트폰으로 다시 전송해주는 방식으로 새로운 서비스 형태로 나타나고 있다. 블루투스 v4.1은 별도의 페어링 과정 없이 디바이스 상의 블루투스만 켜두면 비콘 신호를 인지할 수 있다. 사용자가 스마트폰 앱을 다운로드하고, 블루투스를 ON으로 설정한 뒤 비콘 기기가 설치된 매장에 진입하면 매장에 설치된 비콘은 비콘 신호를 보내고, 사용자가 가지고 있는 스마트폰은 신호를 인지한다. 스마트폰이 비콘 신호를 전송한 비콘 ID를 받고, 스마트폰이 비콘 ID와 고객정보(설치한 앱에 로그인한 고객의 정보)를 서버에 전송한다. 비콘 ID와 고객정보를 받은 서버는 사용자는 고객에게 필요한 제품정보, 쿠폰 등을 고객의 스마트폰으로 전송한다[5].



[Fig. 1] Beacon service process

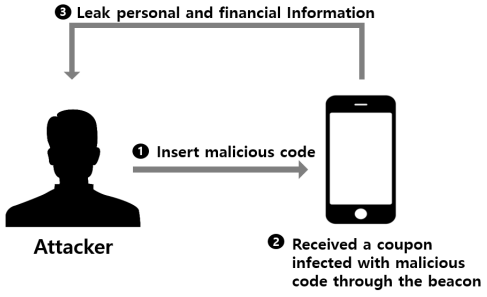
3. 보안위협

3.1 CUshing

[Fig. 2] 인터넷에서 발급되고 있는 쿠폰(Coupon)

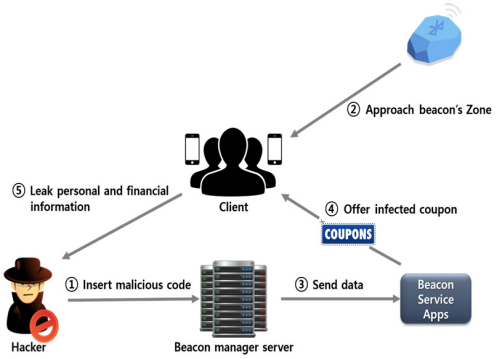
본 논문에서 제시하는 새로운 해킹 기법 형태로 쿠폰(Coupon)과 피싱(Phishing)의 합성어로 스미싱(SMishing)과 유사하지만 비콘을 이용한 O2O(Online to Offline) 서비스를 활용한 해킹 기법이다. 온라인에 잠식당하던 오프라인 상점들이 적극적으로 비콘 서비스를 활용하고 마케팅이 가능해 질것이라고 판단하여 충분히 서비스가 활성화가 되면 발생할 수 있는 공격이다. 근접위치의 가치를 제공하는 비콘 서비스가 활성화가 됨에 따라 실내에서의 객체 이동 위치 데이터와 이동 경로를 측정할 수 있게 된다. 즉, 사용자의 기기가 비콘 단말기 근처에 오면 해당 애플리케이션에 신호(beacon)를 보내는 것이다. 예를 들어 특정 상점을 지나갈 때 상점에 설치된 비콘이 할인 쿠폰을 보낸다거나 박물관에서 특정 전시물 앞에 가면 관련된 내용을 휴대폰 기기로 보내주는 식이다. 자동적으로 사용자는 무분별하게 비콘 서버에서 보내는 데이터를 받을 것이다. 쿠폰에 악성코드를 삽입하는 방식인 이 공격은 공격자가 준비해놓은 악성코드, 트로이목마 등을 쿠폰받기에 URL을 걸어놓거나 피해자가 의심 없이 쿠폰을 받아 악성코드를 다운 받게끔 만든다. 악성코드가 포함된 앱이 스마트폰에 설치가 되면 그때부터 공격자는 자유롭게 피해자 스마트폰의 권한을 획득할 수 있게 되어 개인정보나 금융정보 등을 탈취할 수 있게 된다[6].

3.2 Cushing hacking techniques



[Fig. 3] 비콘서비스를 활용한 악성코드 삽입 및 공격

먼저 공격자는 블루투스 신호를 송수신을 받는 디바이스 주소를 위, 변조 후 서버에 침투한다. 비콘서비스 서버에서 제공하는 데이터 값에 악성코드를 삽입하여 사용자 스마트폰을 장악한다. 사용자 스마트폰을 장악한 후 정보를 탈취하거나 결제방해 및 쿠폰조작 등 다양한 공격을 할 수 있다.



[Fig. 4] CUshing attack process

CUshing 공격은 우선 악성앱 제작자가 비콘 매니저 서버에 수집한 개인정보를 기반으로 특정 사용자들에게 악성앱 설치용 쿠폰을 발송한다. 이 때, 이용자가 쿠폰 속 단축 URL을 클릭하거나 쿠폰을 받는 순간 악성앱을 설치함과 동시에 감염된다. 공격자는 악성앱에 감염된 이용자 단말기에서 정보를 수집해 해외서버로 전송할 수도 있으며 게임사이트 등 각종 인터넷 구매사이트 등에서 소액결제 서비스 진행할 수 있다. 구매사이트에서 결제대행사 등을 통해 본인 인증용 승인 문자번호를 사용자의 스마트폰으로 발송하고, 이미 설치된 악성앱에 의해 사용자의 스마트폰은 수신된 문자번호가 보이지 않도록 조작한다. 악성앱이 승인번호를 문자메시지 해외 서버로 몰래 전송하고, 공격자는 서버에 수집된 승인번호를 가로채서 정상적 구매절차를 수행한다. 최종적으로 공격자는 작성된 사이버머니 등을 불법적으로 현금화해 부당이득을 취할 수 도 있다.

4. 결론

블루투스 v4.1이 발표되면서 사물인터넷이 더 이상 개념에만 머물러있지 않고 실제 이를 구현한 제품으로서 시장에 출시될 수 있게 된 현재 폭발적으로 증가하고 있는 휴대용 기기들과 사물인터넷 사이의 연결을 만들어낸 만큼 관련 제품이나 서비스에서는 여러 아이디어가 제안될 것이고 그에 따라 플랫폼 확장들도 이루어질 것이다. 이러한 다양한 시도들이 사물인터넷 분야의 변화를 가속시킬 것이고 신규 중소기업들의 설립과 투자가 확대될 것이라는 점에서 국내 산업에 미칠 수 있는 영향도 매우 클 것으로 예상된다. Bluetooth v4.1 기반인 O2O(Online

to Offline) 서비스를 활용한 해킹 기법 쿠싱(CUshing)은 쇼핑, 학습, 취미생활 등 온라인에서의 대부분이 공격대상이 될 수 있다. 현재 스마트폰 보급 이후 O2O 서비스를 통한 마케팅이 더욱 활발해지고 있고, 스마트폰, 태블릿 PC등 모바일 기기의 확산과 비콘, NFC 등과 같은 사물인터넷 기술의 발전, 그리고 IT기반의 혁신적인 금융솔루션을 의미하는 핀테크(Fintech)가 금융을 넘어 유통, 택시, 외식업 등 다양한 오프라인 산업에 적용이 되고 있는 시점에 보안성을 언급할 필요가 있다. 이러한 내용을 바탕으로 앞으로 사물인터넷(IoT)과 핀테크(Fintech)기술을 응용한 새롭게 등장할 수 있는 서비스에 대한 예측과 그에 따른 보안 위협 및 대책에 대한 적극적이고 활발한 연구가 진행되어야 할 것이다.

ACKNOWLEDGMENTS

이 논문은 2015학년도 백석대학교 대학연구비에 의하여 수행된 것임

REFERENCES

[1] Seong-Hoon Lee, Dong-Woo, “A Study on Internet of Things in IT Convergence Period”, The Journal of Digital Convergence, Vol. 12, No. 07.6, pp. 267-272, 2014.

[2] Yoon-Su Jeong, Kun-Hee Han, Sang-Ho Lee, “Access Control Protocol for Privacy Guarantee of Patient in Emergency Environment”, The Journal of Digital Convergence, Vol. 12, No. 07.6, pp. 279-284, 2014.

[3] Hyun-Jhin Lee, "Service Vision and Design Issues of Mobile based Internet of Things for Smart Home Service", Korea Digital Design Council, Vol. 14, No. 4, pp. 341-350, 2014.

[4] Joo-Hyeon Park, Chang Geun Song, "The design of an external Bluetooth device and its library based on WIPI for the short-range wireless communication between cellular phone and smart phone", Korean Society of Computer Game, Vol. 24, No. 1, pp. 53-61, 2011.

[5] Chang-Yong Choi, Dong-Myung Lee, “Design and Implementation of the Localization System Using Distance Identification Code in Wireless Sensor Network", Korea Institute of Communications and Information Sciences, Vol. 34, No. 8, pp. 575-582, 2009.

[6] Jung-Hoon Kim, Jun-Young Go, Keun-Ho Lee, “A Scheme of Social Engineering Attacks and Countermeasures Using Big Data based Conversion Voice Phishing", Korea Convergence Society, Vol. 6, No. 1, pp. 85-92, 2015.

[7] Ha-Young Lee, Hae-Sool Yang, “Quality Evaluation Model for Intrusion Detection System based on Security and Performance”, The Journal of Digital Convergence, Vol. 12, No. 6.7, pp. 215-222, 2014.

[8] Jung-Soo Han, "Security Threats in the Mobile Cloud Service Environment", The Journal of Digital Convergence, Vol. 12, No. 5.7, pp. 263-270, 2014.

[9] Jinkeun Hong, “Security Characteristics of D-MAC in Convergence Network Environment”, The Journal of Digital Convergence, Vol. 12, No. 12.6, pp. 323-328, 2014.

[10] MyounJae Lee, “Prevention Method for Wireless LAN Threats and War Driving Attack”, The Journal of Digital Convergence, Vol. 12, No. 10.7, pp. 501-508, 2014.

[11] WooSik Bae, “Mutual authentication and Formal Verification in M2M Environment”, The Journal of Digital Convergence, Vol. 12, No. 09.5, pp. 219-224, 2014.

[12] Pil-ju Choi, Sang-Seon Park, Dong-Ggyu, "Mobile payment and biometric fusion technology trend", KIPS, Vol. 22, No. 4, pp. 21-28, 2012.

[13] Kwang-Sun Park, Sang-jin Lee, "A Study on Structural Vulnerability of MobilePhone Micropayment System And Improvement of Standard Payment Module for User Protection", KIPS, Vol. 23, No. 8, pp. 1007-1015, 2013.

[14] Jun-Yeop Lee, Gyeong-Jeon Lee, "Virtualization Smart Card (ViSCa) platform based mobile payment

Service offerings and other comparative analysis of the case", KIISS, Vol. 20, No. 2, pp. 163-178, 2014.
[15] Byeong-Gwan Lee, Eun-hui Jeong, "Safe AKA (Authentication Key Agreement) module designed for mobile payment systems for open smartphone environment", KMMS, Vol. 13, No. 11, pp. 1687-1697, 2010.

저자소개

이 광 재(Kwang-Jae Lee) **[정회원]**

- 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 학생

<관심분야> : IoT, M2M, 지능형자동차, Fintech

이 근 호(Keun-Ho Lee) **[종신회원]**

- 2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)
- 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
- 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수

<관심분야> : M2M 보안, 이동통신 보안, 융합 보안, 개인정보보호