http://dx.doi.org/10.14400/JDC.2015.13.8.331

빅데이터 플랫폼과 모니터링 시스템의 융합을 이용한 BLE기반의 ZEP시스템 공격 기법에 대한 대응방안 연구

안예찬, 신영현, 이근호
백석대학교 정보통신학부

A study on BLE-based ZEP System Attack Techniques and Countermeasures Utilizing the Convergence of Big data Platform and Monitoring System

Ye-Chan Ahn, Young-Hyun Shin, Keun-Ho Lee
Dept. of Information and Communication, Baekseok University

요 약 최근 사물인터넷(IoT), 핀테크(Fintech) 기술의 발전과 활용이 늘어나고 있고, 시스템과 서비스의 융합이 떠오르고 있는 가운데 무선결제 시스템과 위치기반서비스 기술이 관심을 받고 있다. 스마트폰의 사용자들이 현재 무선결제를 많이 이용하고 있는 상황을 고려하여 많은 기업들에서 소비자들의 간편한 결제를 위하여 다양한 기술들을 접목하여 시장에 내놓고 있으며, BLE 기술과 위치기반을 바탕으로 한 기술을 활용하여 간편 결제가 이루어질 수 있도록 ZEP과 같은 결제서비스의 새로운 방식으로 적용되어 나타나고 있다. 이러한 결제 서비스에서 보안의 위협이 존재하는 여부를 확인하고 발생할 수 있는 공격기법을 연구하여 그에 대한 빅데이터 플랫폼 기반의 대응방안을 제시하고자 한다.

주제어 : 사물인터넷, 저전력 블루투스, 핀테크, ZEP, 빅데이터, 융합, 통합보안

Abstract Lately, the development and utilization of technology of the Internet of Things(IoT), and Fintech have been on the rise and amid the emerging convergence of system and service, mobile payment system and location based service technology have received much attention. Considering the fact that smartphone users are currently utilizing mobile payment frequently, many corporations are introducing various methods to the market for easy payment process of consumers by grafting various technologies, and by utilizing the technology based on BLE technology and location based technology, it is emerging as new method applied to payment service such as ZEP, for easy payment process. And by checking the existence of security threats and studying the attack techniques in these payment services, we strive to suggest a method of response based on big data platform.

Key Words : IoT, Bluetooth Low Energy, Fintech, Zero Effort Payment, Big Data, Convergence, Integrated security

*본 논문은 2015년도 한국 산학협동재단의 지원을 받아 수행하였음.
Received 26 June 2015, Revised 27 July 2015
Accepted 20 August 2015
Corresponding Author: Keun-Ho Lee(Baekseok University)
Email: root1004@bu.ac.kr,

ISSN: 1738-1916

1. 서론

최근 차세대 기술로 다양한 분야에서 각광받고 있는 사물인터넷 IoT(Internet of Things)는 가전제품, 전자장비, 스마트팜, 스마트홈, 헬스케어, 스마트카 등과 같은 다양한 분야의 사물들을 네트워크로 연결하여 정보를 생성, 공유, 활용하는 등의 기술을 통칭하는 개념이다. IoT 기술의 발전과 활용이 늘어나고 있고, 시스템과 서비스의 융합이 떠오르고 있는 가운데 위치기반 기술이 관심을 받고 있다. 그 중에서도 Bluethooth v4.0 기반의 저전력 블루투스 BLE(Bluetooth Low Energy) 기술이 기반이 된 비콘 서비스가 IT시장에 화제가 되고 있다. BLE 기술은 근거리 무선통신을 가능케 하는 기술로서 위치기반서비스와 비콘의 핵심적인 부분이다. 최근 사물인터넷 환경에서 많이 이루어지는 간편 인증 결제 시스템인 핀테크(Fintech)과 관련된 기술들을 연구하고자 한다. 스마트폰의 사용자들이 현재 무선 결제를 많이 이용하고 있는 상황을 고려하여 많은 기업들에서 소비자들의 간편한 결제를 위하여 핀테크 기술들과 다양한 사물인터넷 제품들을 접목하여 시장에 내놓고 있으며, BLE 기술과 위치기반 서비스를 바탕으로 한 기술을 활용하여 간편 결제가 이루어 질 수 있도록 ZEP과 같은 결제서비스의 새로운 방식으로 적용되어 나타나고 있다. 이 기술은 스마트폰을 가지고 있는 고객이 매 결제마다 번거로운 인증절차를 거쳤던 것과 다르게, 오프라인에서 카드, 비밀번호 입력 또는 애플리케이션을 실행하는 등의 행동을 하지 않아도 최소 1회의 인증을 하면 이후의 처리되는 결제는 자동으로 진행되는 방식이다. 전자결제시스템이 등장함으로써 금융서비스의 질적인 향상과 비용절감 효과가 커지는 반면, 결제 시스템의 과정에서 보안의 위협들이 많이 발생하고 있다. 이러한 결제 시스템에 존재하는 보안 위협들의 여부를 확인하고 발생할 수 있는 다양한 공격 기법을 연구하여 그에 대한 대응방안을 제시하고자 한다[1,2].

2. 관련연구

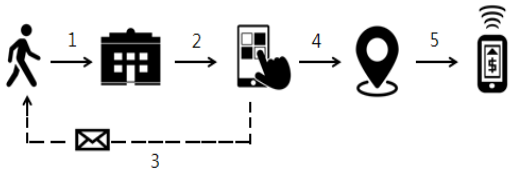
2.1 BLE(Bluetooth Low Energy)

BLE는 Bluetooth SMART 또는 Bluetooth v4.0 으로 불려진다. 일반 블루투스 보다 적은 채널수와 음성을 지원하지 않는 다는 단점을 가지고 있다. 하지만 최대 범위가 많이 넓어 졌고 전력 소비량이 절반이상으로 줄었다는 점에서 매우 효율적인 버전이다. 기존의 Bluetooth와 같이 2.4GHz ISM 대역을 이용하며, 2.400GHz ~ 2.4835 GHz 대역을 자주 사용하지만 40 2-MHz 채널을 이용한다는 점에서 차이가 있다[1].

비콘의 주 기술로써 블루투스 기반의 프로토콜을 이용하여 통신하는 기술이다. 저전력을 사용해 전력 소모량을 줄이고 송수신 거리가 20cm 이내로 가능한 NFC 기술과 비교하면 상대적으로 넓은 5cm~50m까지의 거리가 파악 가능하여, 근거리 통신의 발전을 기대하는 기술이다[2,3].

2.2 ZEP(Zero Effort Payment)

핸즈프리 또는 하이패스 결제 기술이라고 말할 수 있으며 사용자가 스마트 폰을 가지고 결제존을 통과하면 지불이 이루어지는 형태의 서비스를 제공할 수 있다. 예를 들어 사용자가 어플리케이션을 설치하고 오프라인 가맹점을 방문하면 비치되어 있는 비콘이 자동적으로 어플리케이션을 실행시키고 사용자의 ID를 인식한다. 결제 시점에 사용자가 POS 근처로 접근하면 결제정보가 나타나게 되며, 본인 인증 절차를 진행하면 바로 결제가 이루어지게 된다. 이처럼 스마트 폰을 소지한 사용자가 오프라인 가맹점에서 카드를 제시하거나, 비밀번호 입력 또는 어플리케이션을 직접 실행하지 않아도 자동으로 진행되는 결제서비스를 가능케 하는 기술이다[4,5].



[Fig. 1] ZEP System Diagram

1) ZEP 어플리케이션을 다운받은 사용자가 가맹점에 들어간다.
2) 해당 어플리케이션이 사용자가 직접 실행하지 않아도 자동으로 활성화된다.
3) 비콘 신호를 이용하여 확인된 사용자의 위치 및 출

입 사실을 사용자의 스마트폰으로 문자메시지가 전송된다.

4) 사용자가 가맹점 이용 후 비콘 신호가 확인된 결제존을 통과한다.

5) 사용자의 스마트폰에 설치된 어플리케이션과의 통신을 통해 결제가 완료된다.

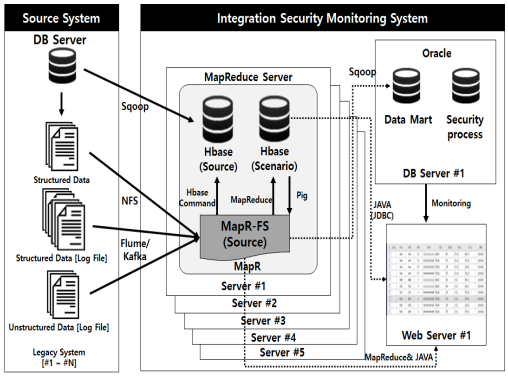
2.3 빅 데이터

현대사회에 정보화 사회를 넘어 가는 이 시점에서 방대한 양의 다양한 정보를 이 쏟아져 나오고 있다. 빅데이터는 IT환경에서 생성되는 데이터가 짧은 시간에 방대한 양의 데이터가 쏟아져 나오고 데이터의 형태 또한 문자, 영상, 수치 등등 다양한 형태의 데이터를 포함하는 대규모 데이터를 말한다. 최근 빅데이터는 5가지의 특징이 있다. 데이터의 양, 데이터 생성속도, 형태의 다양성, 가치, 복잡성이다. 이처럼 다양하고 방대한 규모의 데이터를 효율적으로 관리하고 처리하도록 도와주는 하둡(Hadoop), MapReduce, 분석용 패키지인 R 분산병렬처리, 클라우딩 컴퓨팅 등이 있다[6,7,8].

2.3.1 빅데이터 플랫폼 기반의 통합감시 시스템

최근 빅데이터를 활용한 복합적인 솔루션들이 많이 나오고 있는 가운데 회사나 기관 및 단체에서 빅데이터 기반의 통합적인 감시 시스템을 도입하는 추세이다. 이 시스템은 개인정보처리시스템, DRM, DLP, VPN, e-Mail, DB접근제어 등 보안장비 및 솔루션으로부터 수집된 다양한 로그를 분석하고, 정보보안 시나리오 기반으로 모니터링을 통하여 개인정보 유출 및 내부통제 위반 등의 보안사고 방지를 위한 시스템이다.

이 시스템은 시나리오 기반의 보안로그를 통합적으로 모니터링하여 복합적인 분석기능에 의한 보안 사고를 사전에 예방하고 대응할 수 있다. 또한 로그의 데이터 양이 방대할 경우에는 빅데이터 플랫폼(MapReduce 및 Hadoop)기반 기능을 적용하여 고속의 성능을 보이고 확장을 용이하게 하여 비용 절감 등의 효과를 볼 수 있다[9,10,11,12]. 그리고 개인정보 유출 및 내부통제 위반 중심의 위험을 사전에 탐지하여 조기에 경보를 울려 중요 리스크에 대해 차단하고 대응할 수 있다. 최근 기업 외부 또는 내부로부터 중요정보 침해 및 유출에 대한 수법들이 다양화, 고도화 되고 있는 추세이다. 이에 전사 차원에서 수집된 보안 분야의 로그를 활용하여 보안 사고를 방지하기 위한 통합된 보안 모니터링 시스템이 필요하다.



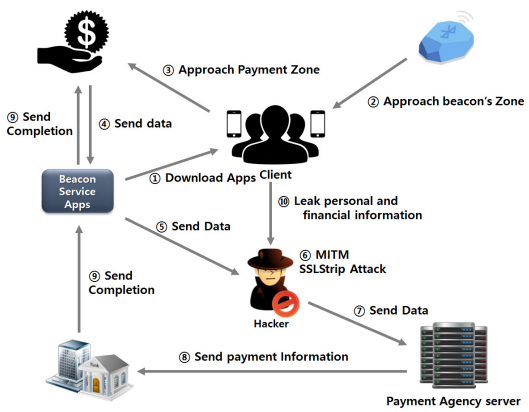
[Fig. 2] Integration Security Monitoring System

3. 공격 시나리오

스마트폰 사용자가 비콘을 사용하는 ZEP 애플리케이션을 다운받는다. ZEP 애플리케이션의 결제서비스에 대한 정보를 등록한다. 비콘이 설치되어 있는 오프라인 가맹점에 들어가면 사용자가 직접적으로 실행하지 않아도 자동으로 활성화가 된다. 스마트폰을 소지한 이용자가 카드제시, 비밀번호 입력 또는 애플리케이션 실행 등의 별도의 행동을 하지 않아도 결제 장소에 접근하게 되면 결제가 실행된다[13].

결제가 진행되는 순간을 자세히 보면 다음과 같다. 이용자가 결제 장소에 접근을 하면 이용자의 ID를 결제 대행사에게 정보를 넘겨주고 결제 대행사는 이 정보를 카드사나 은행에 결제 정보를 전달하게 된다. 결제 회사는 결제 대행업체의 정보를 받아 결제를 완료한 후에 완료했다는 내용을 결제대행업체에 전달한다. 결제 대행업체는 결제가 완료되었다는 정보를 이용자에게 전달하여 결제 완료를 이용자가 알게 된다.

여기서 공격자가 대행업체의 서버를 공격하여 패킷을 훔쳐보거나 패킷을 변조하여 이용금액을 자유자재로 변경하거나 송금대상을 변조하여 금융정보와 개인정보 등을 탈취할 수 있게 된다.



[Fig. 3] Hacking Scenario Flowchart

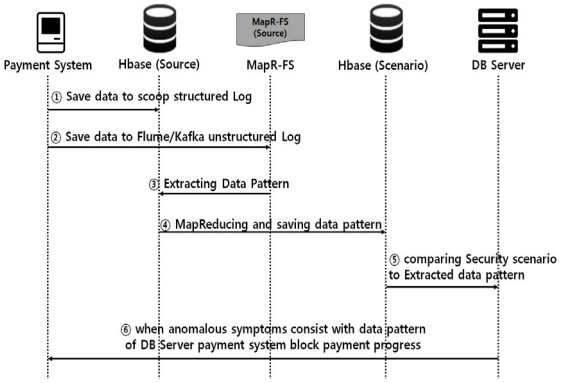
1) 스마트폰 사용자가 ZEP 애플리케이션을 다운받는다.
2) 앱을 다운받은 사용자가 비콘 서비스가 되어있는 가맹점 안으로 들어오면 사용자가 직접 실행하지 않아도 앱이 자동으로 활성화된다.
3) 사용자가 결제 장소에 접근하면 결제기기에 자동으로 인식되어 터치 한번으로 결제가 진행된다.
4) 결제기기가 스마트폰의 앱에 결제가 진행된다는 것을 알린다.
5) 스마트폰의 앱이 결제대행사의 서버에 개인의 ID와 결제에 관한정보를 알려준다.
6) 이때 해커가 MITM SSLStrip 공격을 하여 데이터를 훔쳐보거나 위조를 가능하게 된다.
7) 해커의 위조에 의해 결제된 정보를 카드사 또는 은행에 정보를 전달한다.
8) 결제가 완료되었다는 정보를 스마트폰의 앱에 전달한다.
9) 앱이 결제기기에게 결제가 완료되었음을 알린다.
10) 최종적으로 스마트폰 ZEP 어플리케이션에 의해 사용된 개인정보와 금융정보가 유출하게 된다.

4. 대응방안

핸즈프리 무선결제 서비스 ZEP 결제가 이루어 질 때 결제대행업체 서버단의 보안위협에 대해서 외부공격에 의한 분석기법과 내부공격에 의한 분석기법과 이러한 이상징후를 탐지했을 시에 모니터링하고 있는 보안담당자에게 알람을 주는 시스템에 대한 빅데이터를 활용한 이상 징후 분석 기법을 제안하고자 한다.

4.1 외부공격에 의한 분석기법

결제진행시 기기가 사용자 폰에 신호를 보내어 결제를 도와주도록 사용자의 금융정보와 사용자로그를 결제대행사에게 보내주게 된다. 이때 수집된 데이터 안에는 패킷의 길이와 프레임의 크기 등 데이터링크 계층과 네트워크 계층에서 확인 할 수 있는 정보들이 저장된다. 이때 외부에서 들어오는 로그들 중에 정형 로그는 Sqoop을 이용하고 비정형 로그는Flume을 이용하여 로그데이터를 수집하여 패턴을 추출한다. 또한 맵리듀스를 이용하여 데이터 마트를 구성하고 기존에 저장해둔 이상징후 보안 리크스의 시나리오 파일과 비교한다. 그리고 일반적인 결제진행 패턴 데이터베이스와 이상 징후들의 패턴만 인식한 데이터베이스를 구분하여 계속해서 들어오는 결제정보들과 비교하여 이상징후 패턴 데이터베이스와 일치하는 공격일 경우 보안담당자에게 알림과 동시에 바로 결제 진행을 차단하도록 하여 방어하도록 한다[14].



[Fig. 4] external attack countermeasure sequence diagram

4.2 내부공격에 의한 분석기법

최근 보안사고의 가장 큰 원인은 내부통제 소홀인 만큼 사내 혹은 기관 내에서 사고들이 자주 발생하고 있다. 내부공격에 의한 경우에는 여러 가지 핵심위험지표(KRI : Key Risk Indicator)를 활용하여 내부감시에 필요한 여러 가지 시나리오를 아래 표를 통해 정리해 보면 다음과 같다[15].

〈Table 1〉 Internal Key Risk Indicator

Risk Division	KRI : Key Risk Indicator
Information leakage symptom detection	surging user average number of working days compared to downloading customer information
	Increasing average holiday compared to the number of growing customer information
	Privacy increasing number of files held
	The number of servers connected to several ID from the particular PC
	History detected by sending a large file to the external network from the internal network
Network security	Signs detected by the mass transfer personal data to an external file from the Web
Business system security	Detection system leaves the company's business records connected
	The number of business systems that have left the company's operations recorded in the accounts
Security Polity Control	Network policy violations on a server

이와 같은 보안 시나리오를 적용하여 내부통제 위반 중심의 위험을 사전에 탐지하도록 한다.

4.3 경고 알림 시스템

위와 같은 방법으로 외부, 내부에서의 공격에 의한 보안 시나리오의 위험요소 KRI를 등록하여 지표를 설정한다. KRI의 정보수준을 정상, 경고, 비상 등의 수준을 주어 등록해 정보수준별 임계치 값을 설정하도록 한다. 임계값을 초과했을 알람이 울릴시 알람 대상을 설정하고 알람 메시지를 설정한다. 경보가 발생한 경우 알람 대상자에게 메일 또는 SMS가 발생함과 동시에 지불서비스 중단이나 권한을 낮추어 접근 제어하는 자동화 시스템을 작동시킨다. 알람대상자가 현황을 모니터링하고 신속하게 대응할 수 있도록 한다.

5. 결론

BLE기술이 IT시장에서 주목되는 신기술로 떠오르면서 사물인터넷이 더 이상 개념적으로만 머물러 있지 않고 실제 구현 가능하도록 제품화하여 시장에 출품 될 수 있도록 현재 폭발적으로 증가하고 있는 IT기기들이 사물인터넷 사이의 연결을 지속가능하게 만들어 관련 서비스나 제품에 더 발전된 아이디어가 제안될 것이고 플랫폼들의 확장도 이루어질 것이다. BLE기술을 활용한 무선결제시스템 또한 활발하게 연구되어 시장에 선보이고 있다. 이러한 발전으로 BLE기술이 기반이 되어 위치기반 서비스를 활용한 핸즈프리 결제 시스템이 개발되어 활성화를 눈앞에 두고 있다.

본 논문에서는 신기술이 적용된 만큼 보안에 취약하게 나온 부분을 분석하여 공격 시나리오를 구상해보았고, 그에 따라 빅데이터를 활용한 통합감시 솔루션을 적용하여 여러 가지 보안위협 시나리오, 핵심위험지표 등의 이상 징후를 체크를 통해 안전성 여부와 기본적 필터링을 거치고 담당자에게 알림을 해주는 대응방안을 제안하였다. 스마트폰을 통한 금융 결제 이용이 증가함에 맞춰 지능화된 공격이 가해 질 것으로 예상된다. 앞으로 사물인터넷(IoT)과 핀테크(Fintech)기술을 융합한 새로운 많은 기술의 등장으로 다양한 서비스가 나오고 있는 가운데 그 서비스들의 본질을 파악하여 그에 따른 보안 위협에 대한 즉각적인 대응책에 대해 적극적이고 활발한 연구가 진행되어야 할 것이다.

ACKNOWLEDGMENTS

This research was supported by Korea Sanhak Foundation in 2015.

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] Kwang-Jae Lee, Keun-Ho Lee, “A Study of Security Threats in Bluetooth v4.1 Beacon based Coupon Convergence Service“, The Journal of Digital Convergence, Vol 6, No. 2, p65, 2015

[3] 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.

[4] JongHyun Kim, Kwangsue Chung, "An Efficient Beacon Management Technique for Senor Network-Based Indoor Location Systems", 2009.8

[5] David Molnary, Stefan Saroi, AlecWolmany, "Zero-Effort Payments: Design, Deployment, and Lessons", 2014.

[6] Jun Young Park, Huy Kang Kim, "A Study on the Implementation of outdoor type Virtual Private Network Gateway for Smart Grid", 2011

[7] Lee Hyeonjong, "Use of Bug Data Hadoop platform", J-KICS, Vol. 29, No.11, pp. 43-47, 2012

[8] http://ko.wikipedia.org/wiki/hadoop

[9 J. W. Lee, S.K. Kim, "Complementary research and Analysis for hadoop" in The Korea Society of Computer and Information Winter Conference 2012, vol. 20, no. 2, pp.3- 6, 2012

[10] Kim Byung-moon"Design and Implementation of Hadoop-Based Mobile Streaming Application for Personalized Multimedia Service" Ph. M.S dissertation, Sejong University, 2014

[11] Hyun-wook Kim, Sung-eun Park, Seong-yul Euh "The Distributed Encryption Processing System for Large Capacity Personal Information based on MapReduce", Vol. 18, No. 3, 2014.

[12] Bae Jeong-min "Detection of Keywords in malicious packets using Hadoop MapReduce", 2015

[13]]http://view.asiae.co.kr/news/view.htm?idxno=2014120208403506820

[14] Byung-chul Kim, "A study on Utilization of Big Data Based on the Personal Information Protection Act ", Journal of Digital Convergence, Vol.12, no.12 pp. 87-92, 2014

[15] Sung-kyu Cho, Moon-seog Jun, "Privacy Leakage Monitoring System Design for Privacy Protection", Journal of Korea Institute of Information Security and Cryptology, Vol 22, No. 1, pp99-106, 2012

안 예 찬 (Ahn, Ye Chan)

- 2014년 3월 ~ 현재 : 백석대학교 정보통신학부 학생
- 관심분야 : IoT보안, 융합 보안, 개인정보보호, 취약점 분석
- E-Mail : zxcasd12567@naver.com

신 영 현 (Shin, Young Hyun)

- 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 학생
- 관심분야 : M2M, Bluetooth, 이동통신보안
- E-Mail : ahijah65@naver.com

이 근 호 (Lee, Keun Ho)

- 2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)
- 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
- 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수
- 관심분야 : M2M 보안, 이동통신보안, 융합 보안, 개인정보보호, ISMS (정보보호관리체계), 정보보호사전점검
- E-Mail : root1004@bu.ac.kr