비콘을 이용한 악성코드 배포 및 비콘 신호 캡처에 관한 연구

방민제[O*], 김양우[*], 이성원[**], 조태남[***]
[O*]우석대학교 정보보안학과
[**](주)아이제론
[***]우석대학교 IT전자융합공학과
e-mail: bmj8777@naver.com[O*], kyu21217@gmail.com[*], forensic@izerone.co.kr[**], tncho@ws.ac.kr[***]

A Study on Deploying Malicious Code with Beacon and Capture Beacon Signal

Min-Je Bang[O], Yang-U Kim[*], Seong-Won Lee[**], Teanam Cho[***]
[O*]Dept. of Information Security, Woosuk University
[**]Ltd. Izerone
[***]Dept. of IT&Electronics Engineering, Woosuk University

● 요 약 ●

최근 백화점, 편의점, 미술관 등 다양한 장소에서 비콘을 활용하여 매장 내의 고객에게 쿠폰을 제공하거나 관람객에게 작품 설명 등 서비스를 제공하고 있다. 본 논문에서는 비콘을 이용하여 악성코드를 배포했을 때의 위험성을 분석하고 비콘의 신호 캡처를 통하여 비콘의 정보를 파악하는 방법에 대해 연구하였다.

키워드: 비콘(beacon), 블루투스(bluetooth), BLE, 악성코드 배포(malicious code deploying)

I. Introduction

비콘은 매장 내에 고객의 내점 여부에 따라 자동으로 쿠폰이나 포인트를 부여하거나, 관람객이 감상하는 작품에 대한 자동 설명 등 서비스를 제공하는데 활용되고 있다. 비콘을 악용하여 쿠폰이나 포인트가 아닌 악성코드를 부여하게 된다면 고객과 관람객들의 스마트폰은 악성코드에 감염되어 큰 피해를 볼 수 있다. 본 논문에서는 비콘을 이용한 악성코드 배포 실험을 통하여 비콘 악용의 위험성을 분석하고, 비콘 신호 캡처 방법을 제시한다.

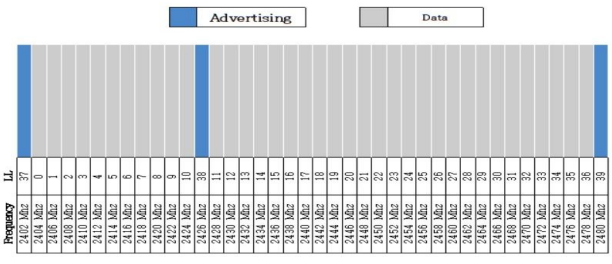


Fig. 1. BLE Channel

II. Preliminaries

1. BLE (Blutooth Low Engerge) 통신 채널

BLE는 블루투스4.0 프로토콜을 사용하는 저전력 근거리 통신 기술로서, Fig. 1과 같이 3개의 Advertising 채널(37-39)과 37개의 Data 채널(0-36)로 구성된다[1]. Advertising 채널은 두 장치간의 페어링을 할 때 사용되고 Data 채널은 페어링 이후 데이터를 전송할 때 사용된다.

2. 비콘(Beacon)

2.1 동작원리

비콘 BLE 프로토콜 기반의 근거리 무선통신 장치로서 Advertising 채널을 이용하는 장치이다. 실제 필요한 데이터는 WiFi 등의 통신 채널을 통해 송수신된다. Fig. 2는 비콘의 동작 원리를 보여준다. 각 비콘은 UUID+Major+Minor+RSSI로 구성된 유일한 ID값을 가지고 있는데, 블루투스 Advertising 채널을 이용하여 자신의 ID값을 주기적으로 주변에 송출한다. 해당 서비스 App이 설치된 스마트폰을 지니고 비콘 근처에 접근하면, App은 ID값을 수신하고 서버에 전송한다. 비콘 서버는 값을 확인한 후, 등록되어있는 컨텐츠를 제공한다.

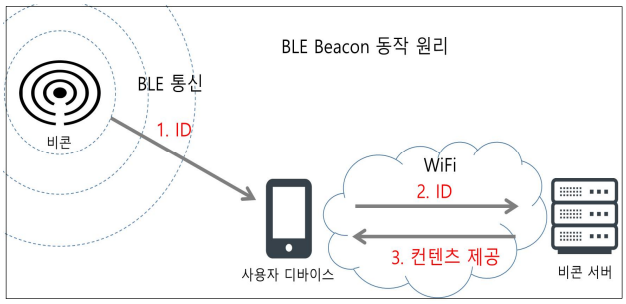


Fig. 2. 비콘의 동작 원리

2.2 패킷 구조

비콘은 BLE 패킷 구조를 사용하며 비콘의 Data 영역은 제조사마다 다르게 구성된다. Fig. 3은 비콘의 대표적인 모델인 iBeacon의 패킷구조이다[2]. 비콘은 UUID 값을 통해 처음 식별되고 동일한 UUID 값을 지닌 비콘을 지역별로 나누기 위해 Major 값을 사용하며, 같은 지역 내에서는 Minor 값을 사용하여 구분한다. 예로서, Major가 백화점이고 Minor가 백화점 내의 매장들로 매칭하여 사용할 수 있다.

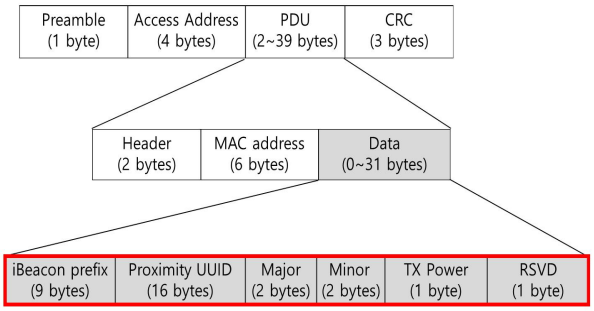


Fig. 3. 비콘 패킷 구조

3. 블루투스 HCI 스눕 기록

안드로이드나 아이폰과 같은 스마트폰은 다양한 개발자 옵션정보를 보유한다. 그 중의 하나가 블루투스 HCI 스눕 기록으로서, 스마트폰과 블루투스로 통신하는 모든 신호를 저장한 로그이다. 로그 파일의 위치는 기기마다 다르지만, 본 연구에서 사용한 안드로이드 스마트폰의 경우에는 /Android/data에 btsnoop_hci.log.last라는 파일로 존재한다.

III. Main Subject

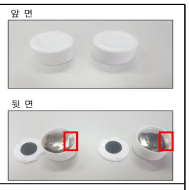
비콘을 이용하여 제공할 수 있는 컨텐츠는 URL, 이미지, 텍스트가 있다. 공격자가 악의적으로 악성코드를 공격자 URL에 업로드 해놓은 후, 비콘 컨텐츠로서 공격자 URL을 등록한다면 고객과 관람객들은 악성코드를 제공받게 되고 상당한 피해를 입을 것이다. 본 연구에서는 비콘이 악용되어 악성코드가 배포되는 과정을 실험하고 비콘의 정보를 파악하기 위한 신호를 캡처해서 확인하였다.

1. 비콘을 이용한 악성코드 배포

1.1 환경 구성

Table 1은 실험을 진행하기 위한 환경 구성을 나타낸다. 실험에 사용한 비콘은 애플에서 제작한 iBeacon i4이다. 사용자 환경은 스마트폰 Galuxy note5(Android 5.0)와 비콘 신호를 인식하고 컨텐츠를 수신할 Basbea User 앱으로 구성된다. 공격자 환경은 비콘의 값(UUID, Major, Minor)을 설정하는 Basbea CFG 앱과 비콘의 컨텐츠(URL, 이미지, 텍스트)를 설정하는 Basbea Manager 앱으로 구성된다. 공격자 컴퓨터의 OS는 Kali_Linux(2017.01), Web Server는 Apache2이다.

Table 1. 실험 환경

비콘 제품	iBeacon i4	
사용자 스마트폰	Android OS	Galuxy note5 (android 5.0)
비콘 사용자 앱	Basbea User	비콘 신호 인식, 비콘 컨텐츠 수신
공격자 환경	Basbea CFG	비콘 값 설정 (UUID, Major, Minor)
	Basbea Manager	비콘의 컨텐츠 설정 (URL, 이미지, 텍스트)
	OS	Kali_Linux 2017.01
	Web Server	Apache2

1.2 시나리오

공격자는 공격을 위한 사전준비로서, Kali_Linux에서 제공하는 취약점 진단 툴인 msfvenom을 이용하여 악성코드를 생성[3]하고, 공격에 사용할 웹서버의URL에 악성코드를 업로드 해놓는다. 사용자가 이 악성코드를 PC 또는 안드로이드에서 실행했을 경우, 악성코드는 root 권한을 획득하여 제어 및 정보 탈취를 할 수 있게 된다.

공격 시나리오는 Fig. 4와 같다. (1) 관리자 앱의 ID, PW, 사용할 비콘의 UUID, Major, Minor 값을 비콘 서버 관리자로부터 할당받는다. (2) 제공받은 정보를 통하여 관리자(Basbea CFG, Basbea Manager) 앱에 접속한다. (3) 비콘의 값을 설정하는 Basbea CFG 앱에서 서버에 등록한 UUID, Major, Minor 값들을 비콘에 설정하고 Basbea Manager 앱에서 악성코드를 업로드 해놓은 URL주소를 사용자가 비콘을 인식했을 때 제공할 컨텐츠로 설정한다. (4) 사용자가 블루투스를 켠 후, Basbea User 앱을 실행하면 비콘을 인식하고 알림창이 뜨게 된다. (5) 알림을 클릭하게 되면 공격자가 설정해놓은 컨텐츠인 공격자 URL에 접속하게 되고 악성코드를 다운로드 받게 된다. 사용자가 다운로드된 악성 앱을 실행했을 경우, 감염이 되고 공격자는 사용자의 스마트폰을 마음대로 컨트롤할 수 있게 된다.

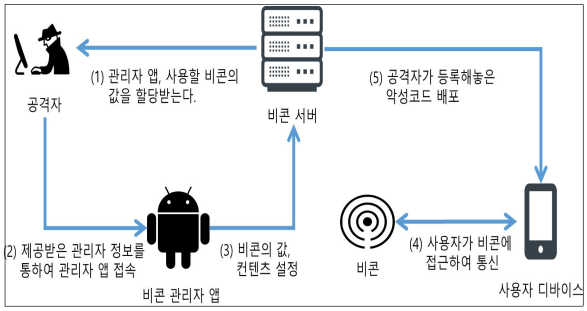


Fig. 4. 비콘을 이용한 악성코드 배포 시나리오

2. 비콘 신호 캡처

2.1 Ubertooth One을 이용한 비콘 신호 캡처

Ubertooth One은 오픈소스 개발 플랫폼으로 블루투스 신호를 스니핑하여 캡처하거나 실시간으로 블루투스 신호 스펙트럼을 확인할 수 있는 장치이다[4]. 본 연구에서는 Wireshark와 연동하여 실시간으로 비콘의 블루투스 신호를 캡처하였고 비콘의 정보를 파악하였다. 파악한 정보는 신호의 목적지, 블루투스 채널, 제조사, UUID 값 등이다. Fig. 5에서와 같이 신호의 목적지는 Broadcast로 표기되어 무작위로 송신하는 것을 확인할 수 있었으며 동일한 정보가 계속 캡처되는 것을 통해 주기적으로 송신하는 것을 확인하였다. Advertising 채널 37을 통신채널로 사용하는 것을 확인하였고 제조사는 iBeacon을 제작한 Apple, Inc로 표기되어 Apple사 제품인 것을 확인할 수 있었다. 신호의 Data 값에 비콘의 UUID 값이 포함되어 있는 것을 볼 수 있다. 이 정보를 통해 비콘 서버에 등록되어 있는 값과 비교하면 악성코드가 배포되는 비콘을 찾을 수 있다.

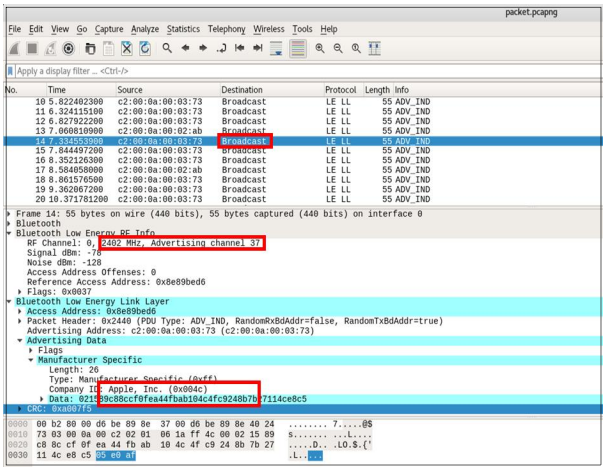


Fig. 5. Ubertooth를 이용한 비콘 신호 캡처

2.2 스마트폰 개발자 옵션을 이용한 비콘 신호 캡처

스마트폰의 개발자 옵션에서 블루투스 HCI 스눕 기록을 켠 후, 블루투스를 실행하고 비콘 근처에 접근하여 비콘의 UUID 값, 제조사, Advertising 사용, 비콘 장치 이름을 파악하였다. 기록된 파일을 Wireshark에서 실행하면 블루투스 신호에 대한 정보가 담긴 것을 확인할 수 있다. Fig. 6에서와 같이 Advertising을 사용한 것을 확인할 수 있고 Company ID에 Apple, Inc로 표기되어 Apple 제품인 것을 파악할 수 있었다. Data 값에서 UUID 값을 확인할 수 있고 다른 신호인 Fig. 7으로부터 비콘의 장치 이름을 파악하였다. 파악한 정보를 통해 비콘 서버와 비교해보면 악성코드가 배포되는 비콘을 찾을 수 있다.

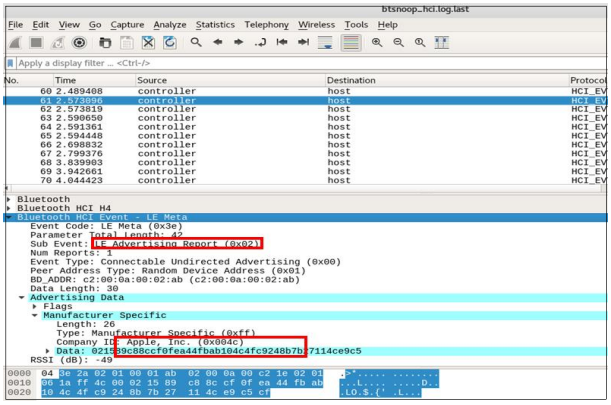


Fig. 6. 개발자 옵션을 이용한 비콘 신호 캡처

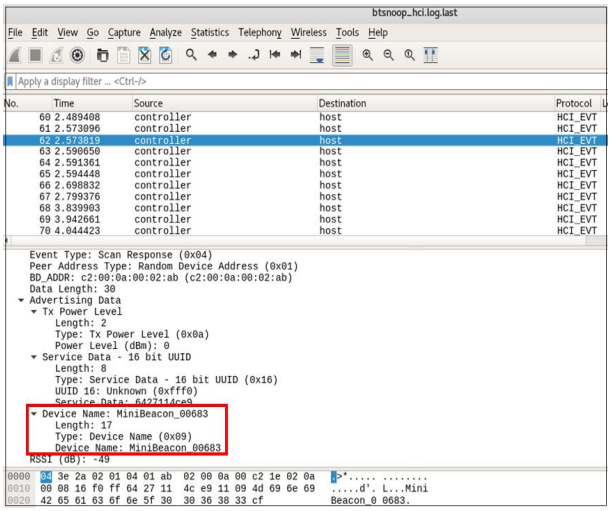


Fig. 7. 비콘 장치 이름 정보

2.3 앱을 이용한 비콘 신호 캡처

"Packet Capture" 앱은 사용자 스마트폰과 통신하는 모든 패킷을 캡처하는 어플리케이션이다. Packet Capture 앱을 실행하고 기록시작을 실행한 후, Basbea User 앱을 실행하여 비콘의 신호를 수신하였다. 남겨진 기록을 통해 비콘의 Major, Minor 값, 비콘의 컨텐츠로 설정되어 있는 이름, URL주소, 정보 업데이트 날짜를 파악하였다. Fig. 8과 같이 비콘에서 받은 Major값과 Minor 값을 비콘 서버 측에 요청하는 정보로 값을 확인할 수 있다. 비콘 서버에서 사용자 측으로 보내준 정보를 보게 되면 설정되어있는 컨텐츠 이름, URL주소, 정보 업데이트 날짜를 볼 수 있다. 해당 정보를 통해 비콘 서버에 등록되어 있는 값과 비교하면 악성코드가 배포되는 비콘을 찾을 수 있다.

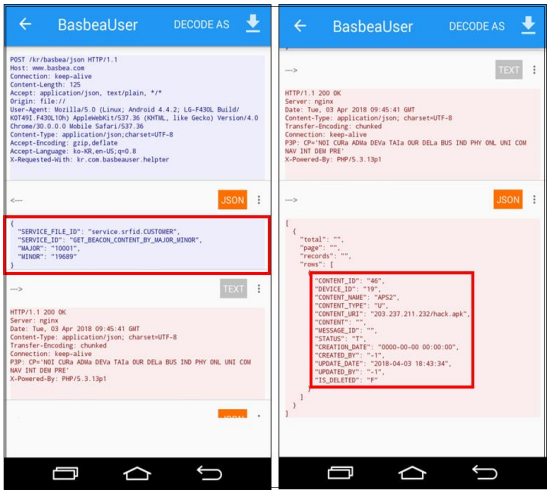


Fig. 8. Packet Capture 앱을 이용한 비콘 신호 캡처

IV. Conclusions

본 논문에서는 비콘을 이용하여 악성코드를 배포하는 실험을 통해서 비콘 악용의 위험성을 보여주고, 비콘의 신호를 캡처하여 정보를 파악함으로써 문제되는 비콘을 찾는 방법을 제시하였다. 공격의 피해 대상자가 불특정 다수인만큼 피해효과는 막대하다. 본 논문에서 제시한 방법은 악성코드를 배포하는 비콘을 파악하고 찾아내는 방법이다. 향후에는 업로드 파일 필터링과 컨텐츠 제공에 대한 실시간 모니터링을 통해 안전성을 강화하는 방안과 비콘과 블루투스의 포렌식 등 사후 분석 방안에 대한 연구가 필요하다.

REFERENCES

[1] Bluetooth SIG, "BLUETOOTH SPECIFICATION Version 5.0", Vol. 6, Part B, No. 1.4, pp. 2560-2561, Dec. 2016.

[2] Apple "Proximity Beacon Specification", Vol. 2, No.2.1 PP. 6-7, Sep. 2015.

[3] DongJin Oh, “MetaSploit-centric simulation penetration for Kali Linux beginners", Vol. 10, pp. 214-217, October 2015.

[4] Ubertooth One, http://ubertooth.sourceforge.net/hardware/one