블루투스 v4.1 비콘 서비스를 활용한 새로운 해킹 기법 연구

이광재, 안예찬, 이근호
백석대학교 정보통신학부
e-mail:kwang291@bu.ac.kr, yechan821@bu.ac.kr, root1004@bu.ac.kr

A Study of New Hacking Scheme using Bluetooth v4.1 Beacon Services

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

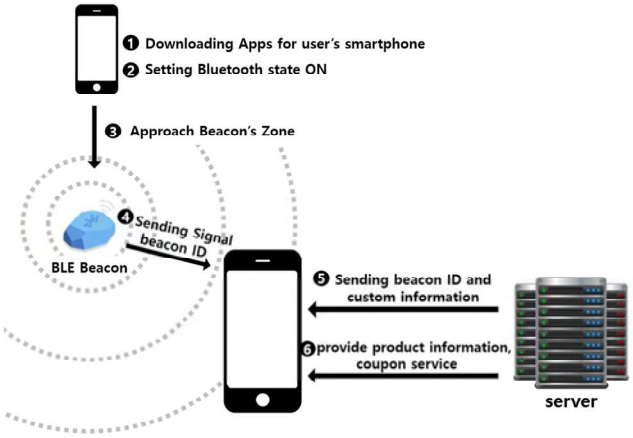
요 약

사물인터넷(IoT), 핀테크(Fintech) 등 새로운 기술의 등장으로 보안성에 대한 부분이 커지고 있다. 모든 사물이 인터넷과 연결되는 사물인터넷 기술로 인해 악성행위와의 접점이 크게 증가했으며, 핀테크(Fintech)는 전통적인 보안시스템의 개혁을 요구하고 있기 때문이다. 사물인터넷 환경에서 이루어지는 간편 인증 결제시스템이 발전함에 따라 다양한 보안위협요소가 발생할 것으로 예상한다. 접점의 증가로 인해 고객이 실수로 악성코드를 받게 될 가능성과 사물인터넷의 핵심 기능인 원격접속에 대한 위협이 대표적인 예라고 할 수 있다. 그러나 현재 고객의 단말을 강제로 통제할 수 있는 방법이 전무한 상황이고, 향후 서비스에서 필요한 고객정보수집과 활용에 대한 정책이 필요한 시점에서 발생할 수 있는 해킹 기법을 제안하고자 한다.

1. 서론

최근 IoT(Internet of Things) 사물인터넷 분야의 기술이 발전함에 따라 위치 기반 기술이 핵심으로 떠오르고 있다. 그 중 저전력 블루투스(BLE) 기술인 '블루투스 v4.1' 기반으로 한 비콘 서비스가 활성화 되고 있는 추세이다. 비콘(Beacon)은 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. 또 사람들의 소비 패턴까지 바꾸고 있으며 이제는 펀드·보험 등 개인자산 관리와 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[5].

2. 비콘(Beacon)서비스



(그림 1) 비콘(Beacon)서비스 과정

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

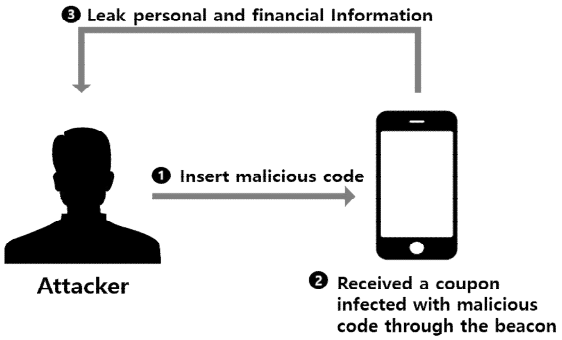
인지할 수 있다. 사용자가 스마트폰 앱을 다운로드하고, 블루투스를 ON으로 설정한 뒤 비콘 기기가 설치된 매장에 진입하면 매장에 설치된 비콘은 비콘 신호를 보내고, 사용자가 가지고 있는 스마트폰은 신호를 인지한다. 스마트폰이 비콘 신호를 전송한 비콘 ID를 받고, 스마트폰이 비콘 ID와 고객정보(설치한 앱에 로그인한 고객의 정보)를 서버에 전송한다. 비콘 ID와 고객정보를 받은 서버는 사용자는 고객에게 필요한 제품정보, 쿠폰 등을 고객의 스마트폰으로 전송한다[1,2].

3. 쿠싱(CUshing)

(그림 2) 인터넷에서 발급되고 있는 쿠폰(Coupon)

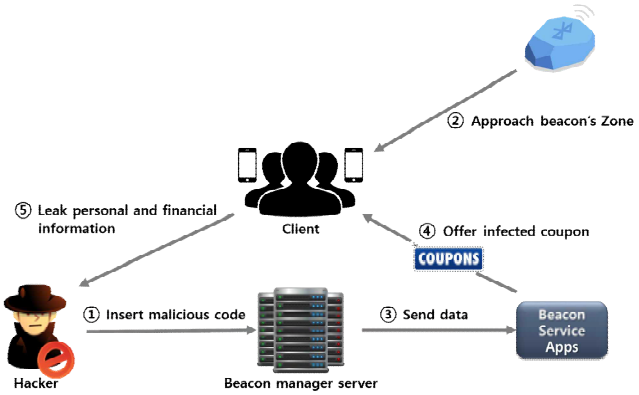
본 논문에서 제시하는 새로운 해킹 기법 형태로 쿠폰(Coupon)과 피싱(Phishing)의 합성어로 스미싱(SMishing)과 유사하지만 비콘을 이용한 O2O(Online to Offline) 서비스를 활용한 해킹 기법이다. 온라인에 잠식당하던 오프라인 상점들이 적극적으로 비콘 서비스를 활용하고 마케팅이 가능해 질것이라고 판단하여 충분히 서비스가 활성화가 되면 발생할 수 있는 공격이다. 근접위치의 가치를 제공하는 비콘 서비스가 활성화가 됨에 따라 실내에서의 객체 이동 위치 데이터와 이동 경로를 측정할 수 있게 된다. 즉, 사용자의 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[3,4].

4. 쿠싱(CUshing) 시나리오



(그림 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.



(그림 4) CUshing 공격 과정

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 수 도 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.

5. 결론

블루투스 v4.1 프로토콜 기반으로 한 비콘 서비스의 맥락인 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 금융 솔루션을 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 응용해 새롭게 등장할 수 있는 서비스에 대한 예측과 그에 따른 보안 위협 및 대책에 대한 적극적이고 활발한 연구가 진행되어야 할 것이다.

감사의 글

이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2013R1A1A1A05012348)

참고문헌

[1] 서영석, "Bluetooth v4.1이 여는 새로운 사물인터넷 세상에 대한 기대" 전자공학회지 2014.8

[2] Myong-Lyol Song, "Search of Beacon in Low Power Wireless Interface" 07-4 Vol. 32 No. 4

[3] Keum-Ryeol Lee, "Omni Channel-based I-LBS Service Case Study with smart commerce- Focus on iBeacon Based Service -" Digieco, 2014.

[4] Smart-Commerce Report, DMC Report, 2013.

[5] 창조적 가치연결 초연결사회의 도래, 한국정보화진흥원, 2013.

[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" KCONS Vol. 6, No. 1. pp. 85-92, 2015