BLE를 이용한 결제 프로세스에서 Relay Attack과 대응방안

Relay Attack and Counter Measure in Payment Process using BLE

최진춘*, 서승환*, 양대헌*, 이경희**[1)]
JinChun Choi, SeungHwan Seo, DaeHun Nyang, KyungHee Lee

(22212) 인천광역시 남구 인하로 100 인하대학교 하이테크센터 1008호 정보보호연구실*
(18323) 경기도 화성시 봉담읍 와우안길 17 수원대학교 전기공학과**
{noodlejin, snack}@isrl.kr, nyang@inha.ac.kr, khlee@suwon.ac.kr

요 약

최근 비콘을 활용한 다양한 서비스가 제공되고 있다. 비콘은 BLE 기술을 이용하여 근거리에서 사용자의 정확한 위치 정보를 파악할 수 있으며, 운동경기장, 극장, 전시장, 박물관과 쇼핑몰 등에서 사용자의 위치정보를 활용한 서비스를 제공하고 있다. 또한 비콘 메시지를 이용하여 사용자의 결제 프로세스를 빠르게 진행할 수 있으며, 이를 통해 사용자는 스마트폰을 꺼내 앱을 실행하거나 비밀번호 등을 입력하지 않고 결제를 진행할 수 있다. 하지만 비콘 서비스를 이용하여 결제 프로세스를 진행하는 경우, 충분한 보안성에 대한 고려를 수행하지 않으면 브로드캐스트 되는 비콘 메시지의 특성상 사용자의 결제 관련 정보가 유출되거나, 사용자를 위장한 공격자에 의해 비정상적으로 결제가 진행될 수도 있다. 이 논문에서는 이러한 공격자의 공격을 실험을 통해 분석하고, 그에 대한 대응 방안에 대해 연구하였다.

Abstract

Recently, there are various services using Beacon. Beacon can locate more accurately a user in stadium, theater, exhibition hall, museum and shopping center. Also Beacon can make a payment process more smarter and faster, so a user can proceed with the payment process without launching application or entering a password. However, when using Beacon for payment process, without considering the adequate security for Beacon, an attacker can impersonate as a legitimate user for abnormal payment or intercept sensitive user information. In this paper, we experiment relay attack and study about countermeasure.

키워드: 비콘, 저 전력 블루투스, 보안, 재전송 공격
Keyword: Beacon, BLE, Security, Relay Attack

※ "이 논문은 2015년도 정부(미래창조과학부)의 재원으로 수행된 연구임(시큐리티 큐레이션을제공하는 프라이버시강화형 개인정보 유통보안 핵심기술개발)"

1) 교신저자

논문투고일자 : 2015. 06. 03 심사일자 : 2015. 06. 04 게재확정일자 : 2015. 08. 21

1. 서론

블루투스(Bluetooth)는 근접한 기기 사이의 무선 통신 등을 지원하는 기술이다[1]. 이를 활용하여 키보드나 마우스 등 주변장치 뿐 아니라 스마트폰과 노트북과 같은 장비들 간에도 무선 통신을 이용한 활용이 가능하다. 정준영 등은 블루투스를 이용한 장치간의 거리 측정을 통하여 공간적 소셜리티를 형성하고 해제하는 방안에 대한 연구를 수행하였다[2].

BLE(Bluetooth Low-Energy)는 기존 블루투스 기술보다 저 전력을 이용하며, 다른 장비와의 연동, 알림 등의 서비스를 제공하는 기술이다. Apple사에서 제공하는 iBeacon은 비콘(Beacon)을 이용한 BLE 기술 중 하나이다. 이를 이용하면 비콘과 사용자의 스마트폰을 연동하여 실내에서도 더욱 정확한 위치를 파악할 수 있다. 특히 쇼핑몰, 병원이나 운동경기장, 극장이나 박물관, 전시장 등의 장소에서 사용자의 정확한 위치에 따라 다양한 종류의 서비스를 제공할 수 있다[3-5]. 예를 들어 박물관이나 전시장에서는 사용자가 특정 전시물 앞에 있을 때, 비콘을 이용하여 이를 감지하고 맞춤형 정보를 제공할 수 있다. 쇼핑몰에서는 사용자가 특정 가게 앞을 지나갈 때 해당 가게에서 판매중인 상품에 대한 홍보나 할인 쿠폰 등의 정보를 제공할 수 있다. 비콘을 이용하면 실내에서 GPS보다 정확한 위치 정보를 제공할 수 있기 때문에, 사용자의 위치정보를 추가적인 인증 요소로 활용할 수도 있다.

또한 비콘을 결제 프로세스를 간소화 하는 목적으로 사용할 수 있다. 기존에 스마트폰을 이용한 결제 프로세스를 진행하는 경우 사용자가 스마트폰의 앱을 실행하고, 사용자 인증을 위해서 PIN(Personal Identification Number) 등의 입력을 수행하는 동작이 요구되었다. 김진복 등은 스마트폰에서 사용자의 어플리케이션 사용 빈도와 개인정보의 중요도에 따라 인증 방식을 다양하게 적용하는 방법을 제안하였다[6]. 그리고 송정은 등은 기존의 PIN 입력 방법이 다양한 공격에 취약하기 때문에 스마트 디바이스에서 진동 피드백을 이용하여 PIN을 입력하는 방법을 제안하여 엿보기 공격과 레코딩 공격에 대한 저항성을 개선하였다[7]. 그러나 PIN을 입력하는 이러한 동작들은 사용자가 스마트폰을 활용한 결제를 진행하는 데 있어 방해요소로 작용하는 경우가 많다. BLE 기술을 결제 프로세스에서 활용하여 사용자의 불편을 최소화 하면서 안전한 결제를 수행하는 방법을 고려할 수 있다.

하지만 비콘을 이용하여 안전한 결제를 진행하기 위해서는 스마트폰 등의 모바일 기기에서 비콘 메시지를 수신하는 경우, 수신한 비콘 메시지가 올바른 송신자로부터 받은 것인지 확인하는 절차가 필요할 것으로 보인다.

이 논문의 구성은 다음과 같다. 2장에서는 관련 연구에 대한 논의를 수행하고 3장에서는 BLE를 이용한 결제 프로세스의 구성과 Relay Attack의 시나리오에 대한 설명과 실험에 대한 분석을 수행한다. 4장에서는 그 대응 방안에 대한 논의를 수행한다. 그리고 5장에서는 결론을 맺는다.

2. 관련 연구

이 장에서는 비콘의 활용과 블루투스의 보안과 관련된 연구에 대해 알아본다.

2.1 비콘의 활용

국내에서는 SKT가 체육관에 비콘을 설치하여 사용자가 자신의 지정된 좌석을 찾아가는 데 도움을 주는 서비스를 하고 있으며[8], KT에서는 비콘과 와이파이를 연계하여 실내 위치 측정과 내비게이션 기술을 개발하고 있다. 또한 비콘 기반의 세이프존 구축을 통해 여성, 노인 등 취약계층의 실시간 위치를 추적하거나, 미아방지 서비스 등에도 활용할 수 있다[9].

해외에서는 애플의 iBeacon 서비스가 iOS 7부터 지원하며 기존의 NFC(Near Field Communication)가 갖는 거리의 한계 등의 단점을 극복하여 이용할

수 있다. 매장에 설치된 iBeacon은 사용자가 앱을 설치한 뒤 블루투스 및 iBeacon을 활성화 하여 매장에서 제공하는 다양한 형태의 알림을 받을 수 있게 해 준다[10].

페이팔은 페이팔비콘을 공개하면서 카드와 스마트폰에 손을 대지 않고도 결제 할 수 있는 서비스를 발표했다. 고객이 매장에 들어서면 비콘을 통해 고객의 페이팔 계정 정보가 매장 POS 시스템에 표시되며, 사용자로부터 구두로 구매의사를 확인받은 직원은 고객의 스마트폰 페이팔 계정으로 결제 정보를 전송한다. 고객은 결제 수락 여부를 선택하고, 영수증을 스마트폰을 통해 수령하면 결제 과정이 완료된다. 또한 스마트폰을 이용해 테이블에서 직접 음식 주문을 하는 동시에 결제를 수행하거나 온라인을 통해 선주문 후 매장을 방문한 경우에 고객의 스마트폰을 인식해 결제하는 서비스도 제공하고 있다[11].

2.2 블루투스의 보안

BLE를 이용하는 비콘 메시지는 그 특성상 브로드캐스트 메시지로 전달되며, 그 통신반경 내에 있는 사용자는 비콘 메시지를 제한 없이 수신할 수 있다. 또한 비콘 메시지는 쉽게 복제하거나 수정하여 재전송 할 수 있다[12-14]. 정상적인 사용자에게만 전송되어야 하는 비콘 메시지를 공격자가 임의로 복제하여 재전송할 수도 있고, 특정 장소에서만 발생하는 비콘 메시지를 다른 곳에서 임의로 발생시킨다면 이는 다수의 이용자에게 불편을 유발할 수도 있다.

Levi 등은 블루투스 인증과정에서의 Relay Attack과 해결방안을 제시하였다[12]. [12]에서는 블루투스에서 Relay Attack을 다양하게 분석하고, 시뮬레이션을 통해 딜레이를 측정한 뒤 그것을 Relay Attack 탐지에 사용할 수 있는지 실험하였다. 또한 블루투스 인증 과정에서 공격자가 위조할 수 없는 정보를 계산에 이용하여 Relay Attack에 대한 해결방안을 제시하였다.

Ryan은 자신들이 개발한 툴을 이용하여 BLE에서 패킷을 모니터링하고 삽입할 수 있음을 보였다[13]. 또한 암호화 과정을 우회하거나 패킷 내용을 수정하는 등의 공격을 수행할 수 있음을 보였다.

Alessio Di Mauro 등은 공격자가 네트워크 내에서 패킷을 캡쳐하고 다시 보냄으로써 가짜 신분을 갖는 것을 방지하기 위해 시도-응답 방식의 프로토콜인 RAP(Receiver Authentication Protocol)을 제안하였다[14]. 이는 데이터를 송신하기 이전에 시도-응답 메시지를 보내고 송신자가 확인된 경우에만 데이터를 전송하는 방식으로 수행 된다.

Keijo Haataja 등은 블루투스에서의 MITM (Man-In-The-Middle) 공격과 그 대응방안에 대해 연구하였다[15, 16]. [15]에서는 공격자가 정상적인 사용자와 블루투스 프린터 사이에서 방해전파를 계속 생성하여 정상적인 연결을 못하도록 하고, 블루투스 장치에서 저장하고 있는 링크키를 삭제하도록 유도한 뒤 다시 연결을 수립하는 과정에서 공격자가 중간에서 정상적인 사용자인 것처럼 행동하여 연결을 하는 공격이 가능함을 보였으며, [16]에서는 블루투스 헤드셋과 핸드프리 장치를 대상으로 한 공격이 가능함을 보였다. [15, 16]에서는 이러한 MITM공격에 대응하기 위한 방법으로 어떤 블루투스 장치에 연결하는 지 확인할 수 있는 추가적인 디스플레이 장치를 추가하는 것을 제안하였으며, 블루투스의 Simple Pairing에서 Just Works 방식을 선택적으로 할 수 있도록 하고 OOB(Out of band) 방식을 의무화 하는 것을 제안하였다.

3. BLE를 이용한 결제 프로세스의 구성 및 Relay Attack 시나리오

이 장에서는 BLE를 이용한 결제 프로세스의 모습과 BLE를 이용한 결제 프로세스에서 가능한 Relay Attack의 구성 및 실험 결과를 보인다.

3.1 BLE를 이용한 결제 프로세스

기존의 스마트폰을 이용한 결제 프로세스에서는

〈표 1〉 WiFi와 3G 환경

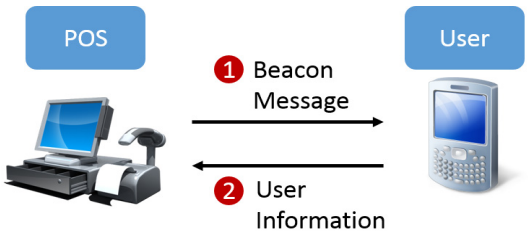
	WiFi	3G
평균 다운로드	31.3 Mbps	2.12 Mbps
평균 업로드	79.4 Mbps	2.45 Mbps
평균지연시간	8.62 ms	67.2 ms
평균 손실률	2.67%	0%
최대 다운로드	60.3 Mbps	2.76 Mbps
최소 다운로드	7.73 Mbps	1.13 Mbps
최대 업로드	92.7 Mbps	2.68 Mbps
최소 업로드	11.6 Mbps	2.20 Mbps
최대 지연시간	24.4 ms	177 ms
최소 지연시간	6.02 ms	48.5 ms
최대 손실률	8%	0%
최소 손실률	0%	0%

사용자가 결제를 위한 앱을 미리 설치하고, 결제하기 이전에 미리 실행하여야 한다. 또한 앱을 실행하거나 결제를 위해서는 추가적으로 PIN등의 정보를 입력해야 하는 불편함이 있었다. 이러한 과정을 간소화하기 위해서 (그림 1)과 같이 BLE 기술을 이용한 결제 프로세스를 제안할 수 있다.

POS(Point of Sale)에서 BLE를 이용한 비콘 신호를 내보내고, 이를 사용자의 스마트폰에서 확인한 뒤에 결제에 필요한 정보를 POS로 전송하는 과정으로 수행된다. 이는 사용자가 앱을 실행하는 동작을 수행하지 않아도 BLE를 이용하여 통신할 수 있으므로 사용자는 스마트폰을 가방이나 주머니에서 꺼내지 않은 상태로 결제를 진행할 수 있다. 이를 위해서는 사용자의 스마트폰에 결제와 관련된 앱이 미리 설치되어 있어야 한다. POS에서는 사용자가 보내준 결제 관련 정보를 수신하여 결제 과정을 진행하고 사용자에게 결제가 정상적으로 수행되었다는 확인 메시지를 보여주고 결제 과정을 끝내게 된다. 기존의 결제 프로세스에서는 사용자가 별도로 앱을 실행하고, PIN등의 추가적인 인증과정을 거쳐야 했지만 BLE를 이용한 결제 프로세스를 이용한다면 이러한 과정을 간소화 할 수 있다.

3.2 Relay Attack 시나리오

Relay Attack은 서로 통신하는 두 장치 사이의



(그림 1) BLE를 이용한 결제 프로세스

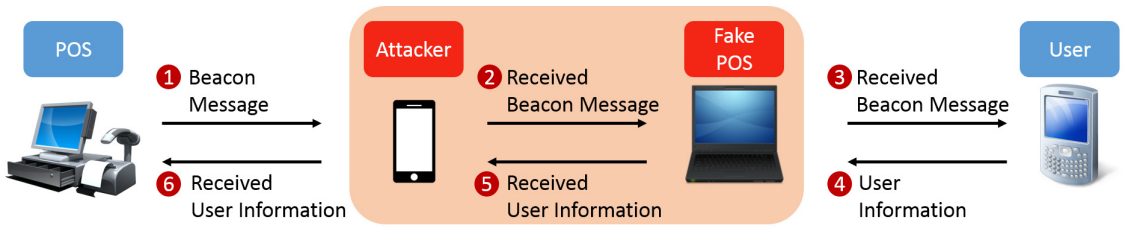
정상적인 메시지를 위·변조하여 전달하는 방법을 통해 이득을 취하거나 사용자에게 피해를 입히는 공격 방법이다[17].

BLE를 이용한 결제 프로세스는 POS가 보낸 비콘 메시지를 사용자가 확인하고, 사용자의 결제 관련 정보를 POS에게 보내주는 방식으로 수행된다. POS에서는 사용자가 보낸 결제 정보를 이용하여 나머지 결제 과정을 진행하게 된다. 하지만 이러한 프로세스 중간에 비콘 메시지를 전달해줄 수 있는 공격자가 존재한다면 사용자의 결제 관련 정보가 노출되거나, 사용자인척 행동하여 결제를 진행하는 공격이 가능할 수 있다.

BLE를 이용한 결제 프로세스에서 가능한 Relay Attack의 구성은 (그림 2)와 같이 나타낼 수 있다.

공격자 2명(공격자, FakePOS)이 Relay Attack을 시도할 수 있는데, 공격자는 POS 앞에서 사용자로 위장하여 결제를 시도하는 역할을 하며 FakePOS는 공격자로부터 전달받은 비콘 메시지를 사용자에게 보내서 사용자의 정보를 공격자에게 전달하는 역할을 한다. 먼저 공격자는 POS로부터 수신 받은 비콘 메시지를 WiFi나 3G/4G 등의 통신을 통해서 FakePOS에게 전달한다. FakePOS는 이 비콘 메시지를 사용자에게 전달해주고, 사용자는 전달받은 비콘 메시지에 응답하여 자신의 결제 관련 정보를 FakePOS에게 보내주게 된다. FakePOS는 사용자의 정보를 POS 앞에 있는 공격자에게 전달하고 최종적으로 공격자는 전달받은 사용자의 정보로 POS와 결제를 진행할 수 있다.

이러한 공격이 가능한 이유는 비콘 메시지를 POS만이 생성하여 보낼 수 있는 것이 아니라 공격자



(그림 2) BLE를 이용한 결제 프로세스에서의 Relay Attack

도 손쉽게 비콘 메시지를 복제하거나 위·변조하여 전달할 수 있기 때문이다.

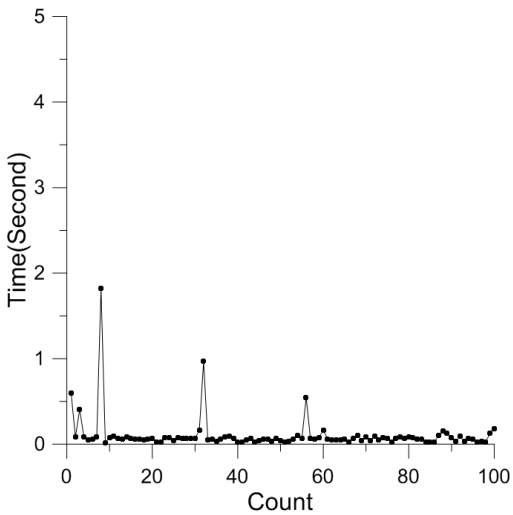
3.3 Relay Attack 실험

이 장에서는 3.2절에 설명한 BLE를 이용한 결제 프로세스에서의 Relay Attack을 실제 구현을 통해 실험을 수행하였다. 실험에 사용한 장비는 다음과 같다. 공격자와 사용자 역할에는 안드로이드 4.4.2 버전의 스마트폰 Vega LTE-A(A880)를 사용하였으며 실험에 사용된 앱은 Eclipse Kepler Service Release 1 version을 이용하여 개발하였다. POS와 FakePOS는 Macbook Pro 2013 OS X 10.9.4를 사용하였으며 실험에 사용된 프로그램은 XCODE version 5.1.1을 이용하여 개발하였다. 실험 환경에서 사용된 스마트폰으로 측정된 WiFi와 3G 환경은 <표 1>과 같다[18]. Macbook은 유선으로 연결되어 있으며, 스마트폰은 WiFi와 3G망에 접속한 경우를 각각 실험하였다.

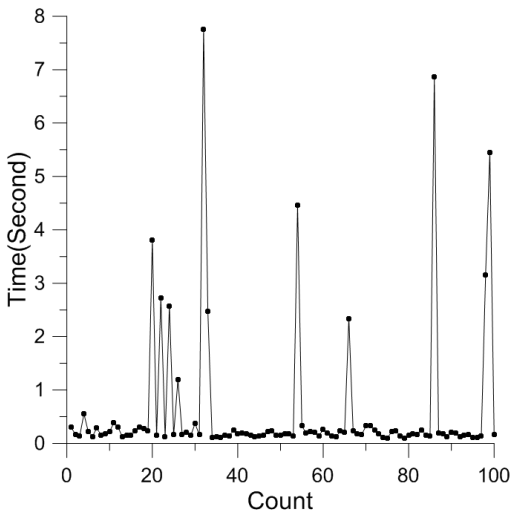
비콘 메시지를 전달하는 시간 간격은 최소 20ms부터 10s 까지 설정할 수 있다[19]. 이 논문에서는 이 값을 100ms로 설정하여 실험을 수행하였다.

실험은 (그림 1)의 정상적인 사용자와 POS 사이의 결제 프로세스 진행 시간을 측정하였으며, (그림 2)의 1-2 과정, 3-4 과정, 5-6 과정에 소요되는 시간을 각각 측정하였다.

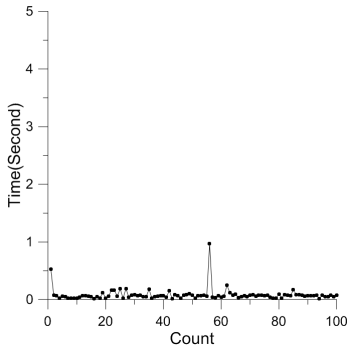
먼저 POS에서 정상적인 사용자에게 비콘 메시지를 전달하고, 사용자가 자신의 결제 관련 정보를 POS에게 전달하는 시간을 100회 측정하였다. 이 과정은 (그림 1)의 1-2 과정을 의미한다. 그 결과는 (그림 3, 4)와 같다.



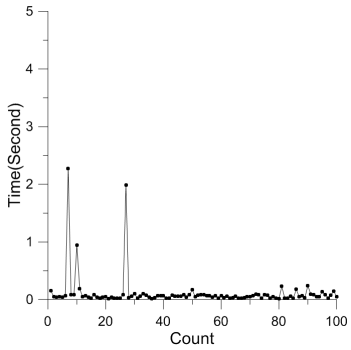
(그림 3) 정상 결제 과정(WiFi)



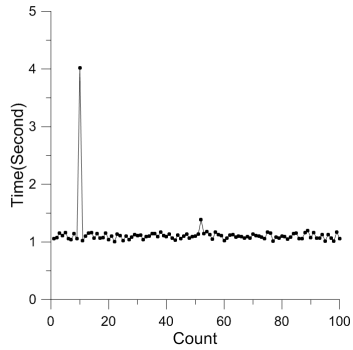
(그림 4) 정상 결제 과정(3G)



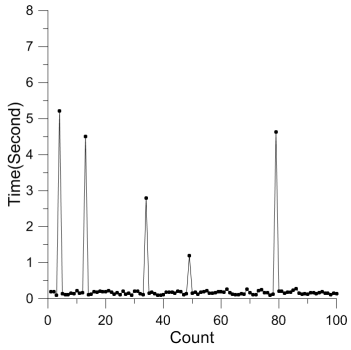
(그림 5) Relay Attack 1-2 과정(WiFi)



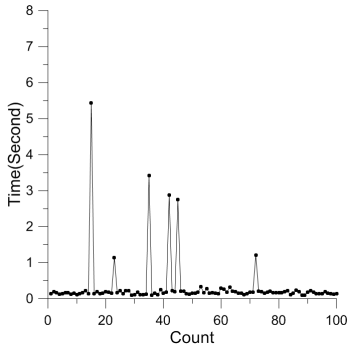
(그림 6) Relay Attack 3-4 과정(WiFi)



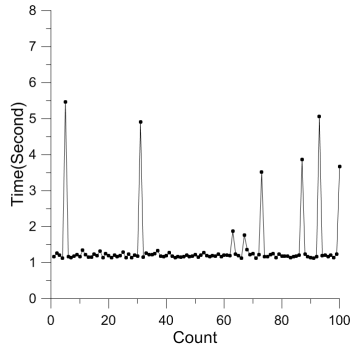
(그림 7) Relay Attack 5-6 과정(WiFi)



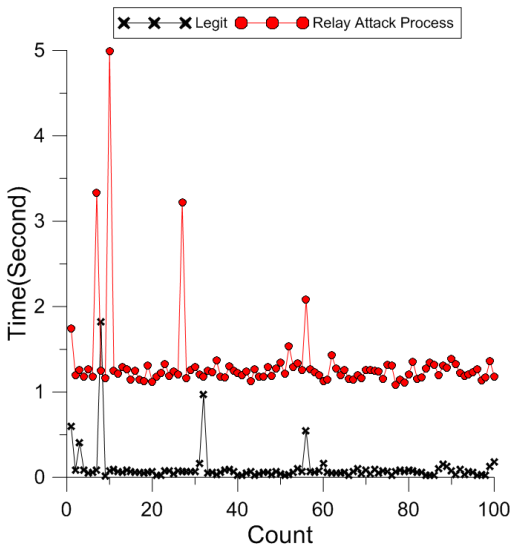
(그림 8) Relay Attack 1-2 과정(3G)



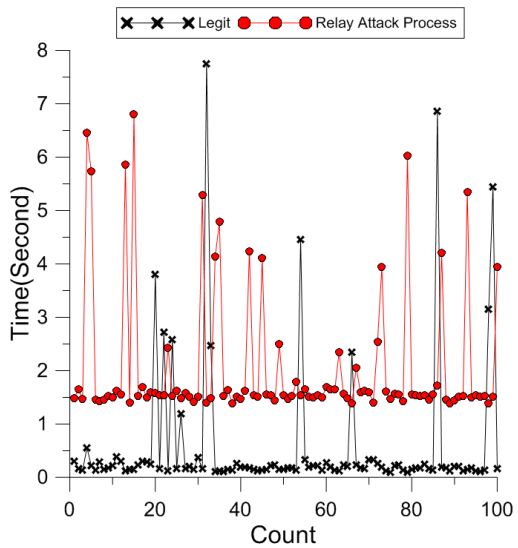
(그림 9) Relay Attack 3-4 과정(3G)



(그림 10) Relay Attack 5-6 과정(3G)



(그림 11) 정상 결제 과정과 Relay Attack 비교(WiFi)



(그림 12) 정상 결제 과정과 Relay Attack 비교(3G)

그림에서 볼 수 있듯 정상적인 사용자와 POS 간의 통신에 걸리는 시간은 매우 짧다. WiFi를 이용할 때와 3G를 이용하는 경우의 차이는 크지 않으나 3G를 이용하는 경우 몇몇 실험에서는 평균보다 높은 시간이 걸린 것을 볼 수 있다.

다음으로는 POS와 공격자 사이에 비콘 메시지를 전달받고, FakePOS에게 전달받은 비콘 메시지를 복제하여 보내주는 시간을 100회 측정하였다. 이 과정은 (그림 2)의 1-2 과정을 의미한다. 그 결과는 (그림 5, 8)과 같다.

이 과정에서 소요되는 시간은 정상적인 사용자가 POS와 통신하는 시간인 (그림 3,4)와 비슷하다. 역시 3G를 이용하여 실험한 경우 평균보다 많이 걸리는 경우가 측정된 것을 확인하였다.

다음은 FakePOS가 전달받은 비콘 메시지를 이용하여 사용자에게 비콘 메시지를 보내고, 사용자가 자신의 결제 관련 정보를 FakePOS에게 전달하는 시간을 100회 측정하였다. (그림 2)의 3-4 과정을 의미한다. 그 결과는 (그림 6, 9)와 같다.

그림에서 볼 수 있듯 이 과정에서 소요되는 시간 역시 정상적인 사용자와 POS간의 통신이나, 공격자가 POS에게서 전달받은 비콘 메시지를 FakePOS에게 복제하여 보내주는 시간과 비슷함을 알 수 있다. 이는 정상적인 결제 과정과 Relay Attack 에서의 1-2 과정, 3-4과정이 비콘 메시지의 전달과 WiFi/3G를 이용한 메시지 전달이 각각 한 번씩 수행되기 때문으로 보인다.

1 Measure $t_{3G,i}, t_{WiFi,i}$; $i = 1$ to N
2 compute $AVG_{3G} = (\sum_{i=1}^{N} t_{3G,i}) / N$
3 compute $AVG_{WiFi} = (\sum_{i=1}^{N} t_{WiFi,i}) / N$
4 compute $\sigma_{3G} = \sqrt{\frac{\sum_{i=1}^{N}(t_{3G,i} - AVG_{3G})^2}{N-1}}$
5 compute $\sigma_{WiFi} = \sqrt{\frac{\sum_{i=1}^{N}(t_{WiFi,i} - AVG_{WiFi})^2}{N-1}}$
6 compute threshold $T_{3G} = AVG_{3G} + \sigma_{3G}/2$
7 compute threshold $T_{WiFi} = AVG_{WiFi} + \sigma_{WiFi}/2$
8 Measure t_{user}
9 **if** user communication = 3G
10 compare t_{user} and T_{3G}
11 **if** $t_{user} \leq T_{3G}$
12 Proceed Transaction
13 **else if** user communication = WiFi
14 compare t_{user} and T_{WiFi}
15 **if** $t_{user} \leq T_{WiFi}$
16 Proceed Transaction
17 Stop Transaction, Show warning message

(그림 13) T값을 결정하여 Relay Attack을 탐지하는 알고리즘

마지막으로 FakePOS가 사용자에게서 전달받은 결제 관련 정보를 공격자에게 전달하고, 공격자는 이를 POS에게 전달하는 시간을 100회 측정하였다. 이 과정은 (그림 2)의 5-6 과정을 의미한다. 실험 결과는 (그림 7, 10)에서 볼 수 있다.

이 과정에 걸리는 시간은 이전의 과정에서 소요

〈표 2〉 WiFi와 3G를 이용한 Relay Attack 결과(단위 : 초)

통신 종류	과정	평균	최댓값	최솟값	표준편차
3G	(그림 1)의 1-2 과정(정상 과정)	0.497	4.198	0.065	0.6744
	(그림 2)의 1-2 과정	0.405	2.948	0.069	0.4461
	(그림 2)의 3-4 과정	0.405	2.810	0.045	0.4114
	(그림 2)의 5-6 과정	1.144	4.095	1.011	0.4088
	(그림 2)의 1-6 과정(Relay Attack 과정)	1.955	6.370	1.320	0.7809
WiFi	(그림 1)의 1-2 과정(정상 과정)	0.104	1.819	0.019	0.2113
	(그림 2)의 1-2 과정	0.082	0.969	0.017	0.1083
	(그림 2)의 3-4 과정	0.113	2.273	0.017	0.3050
	(그림 2)의 5-6 과정	1.129	4.020	1.008	0.2952
	(그림 2)의 1-6 과정(Relay Attack 과정)	1.324	4.987	1.083	0.4811

되는 시간보다 길다. 그 이유는 이전 과정에서는 비콘 메시지의 전달과 WiFi/3G를 통한 메시지 전달이 각각 한 번씩 있었지만, FakePOS와 공격자 사이, 그리고 공격자와 POS 사이에는 둘 다 WiFi/3G를 통한 메시지 전달이 있었기 때문으로 판단된다.

다음 (그림 11, 12)는 정상적인 사용자와 POS 간의 통신과, Relay Attack의 전체 과정에서 소요되는 시간을 비교한 것을 보인다. 전체적으로 정상적인 사용자와 POS간의 통신에 소요되는 시간보다 Relay Attack에 소요된 시간이 더 많음을 알 수 있다. 이는 공격자와 FakePOS가 정상적인 결제 프로세스에 개입하여 통신하는 과정이 추가되기 때문이다.

이 절에서 실험한 Relay Attack의 결과를 <표 2>와 같이 정리하였다. 평균적으로 정상 과정과 Relay Attack의 수행에 걸린 시간은 3G를 이용한 경우 보다 WiFi를 이용한 경우가 더 빠르게 수행된 것을 알 수 있다. 최댓값, 최솟값과 표준편차를 전체적으로 살펴보면 3G를 이용한 통신이 WiFi를 이용한 경우보다 편차가 큰 것을 볼 수 있다.

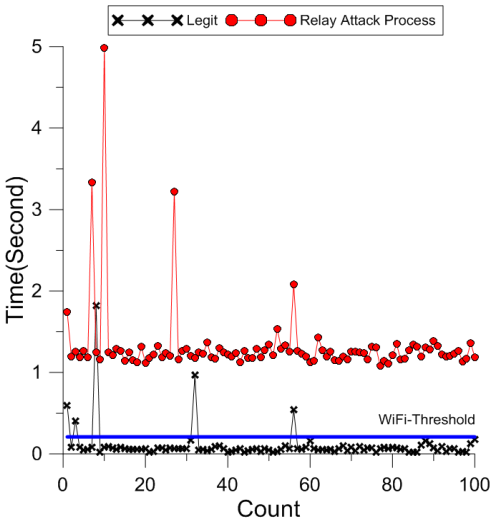
4. 대응 방안 연구

이 장에서는 BLE를 이용한 결제 프로세스에서의 Relay Attack 시나리오에 대한 대응 방안에 대한 연구를 수행한다. 3.2절에서 본 것과 같이 BLE를 이용한 결제 프로세스의 경우 Relay Attack에 취약할 수 있음을 알 수 있다. 이러한 공격에 대응하기 위해 다음과 같은 방법을 제안한다.

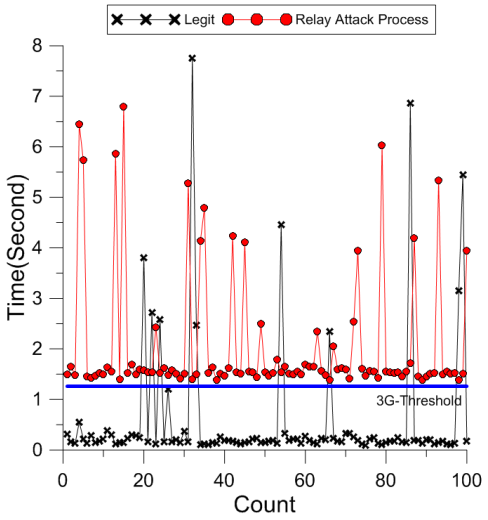
BLE를 이용한 결제 프로세스에서 정상적인 경우와 Relay Attack이 수행되는 경우 발생하는 시간 차이를 이용하여 공격을 구분할 수 있다. 정상적인 사용자의 경우 POS와 BLE를 이용한 결제 프로세스에서 통신을 수행하는 데 POS로부터 전송되는 비콘 메시지와 사용자가 POS로 자신의 결제 관련 정보를 보내주는 과정을 (그림 1)과 같이 수행한다. Relay Attack의 경우에는 (그림 2)와 같이 POS와 사용자 사이에 공격자와 FakePOS가 개입하여 비콘 메시지와 사용자의 정보를 전달하는 과정이 추가로 수행되어야 한다. 이 논문에서는 실험을 통하여 값(Threshold, T)을 설정하고, 이를 이용하여 정상적인 사용자와 Relay Attack을 시도하는 공격자를 구분한다. Relay Attack과 정상적인 사용자를 구분하기 위한 T값으로 <표 3>과 같은 값들을 고려해 볼 수 있다. 표에서 확인할 수 있듯이 3G와 WiFi 상태를 포함하여 구분하는 데에 평균값+표준편차/2를 T값으로 이용하는 것이 오거부(False Rejection)와 오인식(False Acceptance)을 낮출 수 있을 것으로 보인다. T값으로 중간값(Median) 값을 이용하는 경우 오거부 되는 경우가 많이 발생할 수 있으며, 평균+표준편차와 평균+표준편차*2의 경우 3G를 사용하는 경우에 오거부는 낮출 수 있으나 오인식되는 경우가 많이 발생할 수 있다. 따라서 오거부 되거나 오인식 되는 경우를 최대한 줄일 수 있는 평균+표준편차/2의 값을 T값으로 설정하는 것이 가장 타당하다 볼 수 있다. 그 결과 실험을 통해 미리 T값을 결정하고 이를 이용하여 Relay Attack을 구분하는 과정을 (그림 13)과 같이 정리할 수 있다. 먼저 POS와 스마트폰 사이에서 정상적인 결제 프로세스를 N번 반복하여 $t_{3G,i}, t_{WiFi,i}$

〈표 3〉 T값으로 고려할 수 있는 값들과 그에 따른 오거부, 오인식 수(단위 : 초, 횟수)

	WiFi			3G		
	Value	False Rejection	False Acceptance	Value	False Rejection	False Acceptance
평균	0.104	12	0	0.597	11	0
중간값	0.063	48	0	0.182	50	0
평균+표준편차	0.3153	5	0	1.9245	10	81
평균+표준편차×2	0.5265	4	0	3.2516	5	86
평균+표준편차/2	0.2097	5	0	1.2609	10	0



(그림 14) 계산된 T값으로 Relay Attack을 구분(WiFi)



(그림 15) 계산된 T값으로 Relay Attack을 구분(3G)

값을 측정한다. 그리고 각각의 평균값과 표준편차 값을 계산한 뒤 이를 이용하여 T_{WiFi}, T_{3G}를 계산한다. 그리고 사용자와 POS의 결제 프로세스를 진행하여 t_{user}를 측정한 뒤 T_{WiFi}, T_{3G}와 비교하여 정상 결제인지 Relay Attack 인지를 판단한다.

T값을 평균+표준편차/2 로 이용한 경우 정상 결제 과정과 Relay Attack을 구분하는 모습은 (그림 14, 15)과 같다. 이 그림은 (그림 11, 12)에서 T값을 추가로 표현한 그림으로 T값에 따라 정상 결제 과정과 Relay Attack을 구분할 수 있다. T값을 평균+표준편차/2 로 한 경우, WiFi는 오거부 된 경우가 5회, 오인식 된 경우가 0회였으며, 3G는 오거부 된 경우가 10회, 오인식 된 경우는 0회로 볼 수 있다. 정상 사용자가 오거부 된 경우에는 다시 시도하여 프로세스를 진행할 수 있지만 공격자가 오인식 되는 경우는 한 번이라도 발생한다면 공격자가 공격에 성공하게 되는 것이기 때문에 오인식 되는 것을 0으로 유지하면서 오거부 되는 것을 최대한 낮출 수 있는 T 값을 설정하는 것이 타당하다 볼 수 있다. 그러나 무선 통신 상태의 불안정성과 사용자 스마트폰의 상태 등에 따라 정상적인 사용자임에도 불구하고 설정된 T값 보다 결제 프로세스가 더 오래 걸리는 경우, Relay Attack으로 판단되어 정상적인 프로세스를 진행하지 못할 수 있다.

5. 결론

이 논문에서는 BLE를 결제를 보조하는 수단으로 활용하는 경우 발생할 수 있는 Relay Attack에 대한 실험을 수행하고 그 대응 방안에 대해 논의하였다. BLE를 이용하여 결제 프로세스를 진행하는 경우 사용자는 별도의 앱을 실행하거나, PIN을 입력하는 절차를 생략하고 진행할 수 있다. 그러나 Beacon 메시지를 이렇게 결제 프로세스에 이용하는 경우 보안 측면에서의 고려가 없다면 공격자가 Beacon 메시지를 복제하거나 위 · 변조하여 사용자에게 전달할 수 있다. 또한 사용자의 결제 관련 정보가 공격자에게 유출될 수 있고 공격자가 사용자처럼 행동하여 결제를 진행할 수도 있다.

이 연구에서는 Relay Attack에 대응하기 위한 방안으로 정상적인 사용자와 Relay Attack인 경우 수행되는 시간에 따라 구분하는 방법을 제안하였다. 정상적인 사용자가 수행하는 시간보다 Relay Attack에서 공격자가 진행하는 시간이 오래 걸리는데 이는 공격자와 FakePOS가 정상적인 결제 프로

세스에 개입하여 정보를 주고받는 과정이 추가되기 때문이다. 이러한 시간의 차이를 이용하여 정상적인 사용자와 Relay Attack을 구분할 수 있다. 다만 공격을 구별하기 위한 값 T가 어느 정도로 정해지느냐에 따라 사용자가 Relay Attack으로 오거부되거나, 공격자를 정상적인 사용자로 판단하는 오인식이 발생할 수 있다. 따라서 T 값을 어떻게 결정하여 사용하는 지가 공격을 구분하는 데 있어서 중요하다고 할 수 있다. 이 연구에서는 T 값을 결정하고 이를 이용하여 Relay Attack을 구분하는 알고리즘을 제안하였다. 또한 이 알고리즘을 이용하여 결정된 T 값을 이용하여 정상적인 결제과정과 Relay Attack을 구별하는 것을 (그림 14, 15)를 통해 보였다.

향후 연구에서는 더 빠른 통신 채널을 이용하여 시간을 이용하여 구분하기 힘든 Relay Attack에 대해서도 대응할 수 있는 방안에 대해 연구해야 할 것이다.

▌참고문헌

〔1〕 Bluetooth.com - http://www.bluetooth.com/Pages/Bluetooth-Home.aspx

〔2〕 정준영, 김대영, "공간적 소셜리티를 인식하기 위한 장치간의 거리 측정", 한국차세대컴퓨팅학회 논문지, 제 10권 제 1호, pp.40-47, 2014. 2.

〔3〕 SK텔레콤, 장소에 맞게 활용 가능한 블루투스 '비콘' 4종 출시 - SK Telecom blog (http://blog.sktworld.co.kr/4793)

〔4〕 bloter.net, '뜨는 '블루투스 비콘', 미래는 어떨까', http://www.bloter.net/archives/198568

〔5〕 bloter.net, '비콘으로 위치 기반 고객 마케팅을', http://www.bloter.net/archives/195795

〔6〕 김진복, 한태윤, 이문규, "스마트폰 사용자를 위한 단계별 복합 인증", 제 7권 제 5호, pp.4-12, 2011. 10.

〔7〕 송정은, 김진복, 이문규, "진동을 이용한 스마트 디바이스 사용자 인증 방법", 제 10권 제 1호, pp.6-21, 2014. 2.

〔8〕 SK텔레콤, 'SK 나이츠 앱' 출시! 좌석위치 안내해주고 실시간 이벤트 참여까지! - SK Telecom blog (http://blog.sktworld.co.kr/4557)

〔9〕 KT, 비콘 활용한 안전 서비스 '세이프존' 출시 - http://news.inews24.com/php/news_view.php?g_serial=891191&g_menu=020310&rrf=nv

〔10〕 ios:iBeacon 이해 - https://support.apple.com/ko-kr/HT202880

〔11〕 PayPal - https://www.paypal.com/webapps/mpp/beacon

〔12〕 Levi, Albert, et al. "Relay attacks on Bluetooth authentication and solutions." Computer and Information Sciences-ISCIS 2004. Springer Berlin Heidelberg, 278-288, 2004.

〔13〕 Ryan, Mike. "Bluetooth: With Low Energy Comes Low Security." WOOT. 2013.

〔14〕 Di Mauro, Alessio, et al. "Detecting and preventing beacon replay attacks in receiver-initiated MAC protocols for energy efficient WSNs." Secure IT Systems. Springer Berlin Heidelberg, 1-16, 2013.

〔15〕 Haataja, Keijo MJ, and Konstantin Hyppönen. "Man-in-the-middle attacks on bluetooth: a comparative analysis, a novel attack, and countermeasures." Communications, Control and Signal Processing, 2008. ISCCSP 2008. 3rd International Symposium on. IEEE, 2008.

〔16〕 Haataja, Keijo, and Pekka Toivanen. "Practical man-in-the-middle attacks against bluetooth secure simple pairing." Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on. IEEE, 2008.

〔17〕 Roland, Michael. "Applying recent secure element relay attack scenarios to the real world: Google Wallet Relay Attack." arXiv preprint arXiv:1209.0875 (2012).

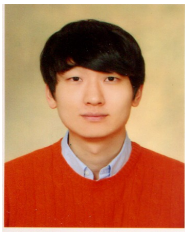
〔18〕 Benchbee - http://www.benchbee.co.kr/
〔19〕 Specification of the Bluetooth System, core version 4.1, pages 2528 - 2529.

저자소개

◆ 최진춘

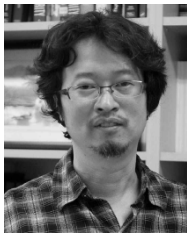
- 2011년 2월 인하대학교 컴퓨터 정보공학과 졸업
- 2014년 2월 인하대학교 컴퓨터 정보공학과 석사
- 2014년 3월~현재 인하대학교컴퓨터정보공학과 박사 과정
- 관심분야: 네트워크 보안, 무선 센서 네트워크 보안

◆ 서승환



- 2014년 2월 인하대학교 컴퓨터 정보공학과 졸업
- 2014년 3월~현재 인하대학교컴퓨터정보공학과 석사 과정
- 관심분야: 네트워크 보안, 포렌식, 무선 인터넷 보안

◆ 양대헌



- 1994년 2월 한국과학기술원 과학기술대학 전기 및 전자공학과 졸업
- 1996년 2월 연세대학교 컴퓨터과학과 석사
- 2000년 8월 연세대학교 컴퓨터과학과 박사
- 2000년 9월~2003년 2월 한국전자통신연구원 정보보호연구본부 선임연구원
- 2003년 2월~현재 인하대학교 컴퓨터정보공학과 교수
- 관심분야: 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안, 네트워크 보안

◆ 이경희

- 1993년 2월 연세대학교 컴퓨터 과학과 학사
- 1998년 8월 연세대학교 컴퓨터 과학과 석사
- 2004년 2월 연세대학교 컴퓨터 과학과 박사
- 1993년 1월~1996년 5. LG 소프트(주) 연구원
- 2000년 12월 ~ 2005년 2월 한국전자통신연구원 선임연구원
- 2005년 3월 ~ 현재 수원대학교 전기공학과 부교수
- 관심분야: 바이오인식, 정보보호, 컴퓨터비전, 인공지능, 패턴인식