Journal of the Korea Academia-Industrial cooperation Society
Vol. 17, No. 8 pp. 311-317, 2016

http://dx.doi.org/10.5762/KAIS.2016.17.8.311
ISSN 1975-4701 / eISSN 2288-4688

비콘 기반의 이중 보안 기법

박상민, 김철진*
인하공업전문대학 컴퓨터시스템과

A Dual Security Technique based on Beacon

Sang-Min Park, Chul-Jin Kim*
Dept. of Computer Systems and Engineering, Inha Technical College

요 약 사물 인터넷의 활성화로 스마트 디바이스를 기반으로 하는 많은 서비스들이 개발되고 있으며, 이에 디바이스 간의 보안이 강조되고 있다. 현재 사물 인터넷 서비스에 비콘이 상업적 분야에 활용되고 있으며, 일반 가정의 사물 인터넷 서비스에도 적용되고 있다. 그러나 비콘은 블루투스 기반의 서비스로서 보안에 취약하다. 따라서 비콘의 보안을 강화하기 위한 연구가 진행되고 있다. 본 논문에서는 비콘 기반의 서비스 보안을 강화 할 수 있는 이중 보안 기법을 제안한다. 비콘과 인증 서비스를 기반으로 하는 이중 보안 아키텍처와 보안 처리 프로세스를 제안한다. 또한, 제안 기법의 적합성을 증명하기 위해 비콘 기반의 모바일 어플리케이션을 개발하여 검증한다. 검증을 위한 실험 방법는 1차 인증 실패의 인증 실패 사례와 1차 인증 성공와 2차 인증 성공의 인증 성공 사례를 실험한다. 검증 실험의 구성 요소는 2개의 비콘(비콘 ID와 일치, 비콘 ID와 불일치), 1개의 모바일 디바이스 그리고 인증 애플리케이션으로 구성된다. 이중 보안 아키텍처와 1차/2차 인증 프로세스의 적합성을 검증하기 위해 실험한다.

Abstract Many services have been developed that are based on smart devices, and security between devices is emphasized. A beacon on the current IoT(Internet of Things) services has been utilized in the commercial field and is being applied to the services of the home IoT. On the other hand, the beacon is weak to security using Bluetooth-based services. Therefore, it is important to strengthen the security of the beacon. This paper proposes a dual security technique that can enhance the security of beacon-based services. The dual security architecture and security process is proposed based on beacon and authentication service. In addition, mobile application was developed and validated based on the beacon for proving the suitability of the proposed technique. The experimental method for verification are the authentication failure case, such as 1st authentication fail, and authentication success case, such as 1st authentication success and 2nd authentication success. The components of the verification experiments consists of two beacons (matched with Beacon ID, mismatched with Beacon ID), one mobile device and authentication application. This was tested to verify the compatibility of the dual security architecture and 1st/2nd authentication process.

Keywords : Dual Security, Beacon, 1st Authentication, 2nd Authentication, Encryption

1. 서론

스마트폰의 높은 보급률에 따라 어플리케이션이 다양하게 개발되고 있으며, 스마트폰과 호환되는 여러 가지 주변 디바이스들이 연구되고 있다. 모바일 서비스에서 가장 중요한 점은 편리성이며, 사용자가 복잡하게 어떤 행위를 하지 않아도 모바일 디바이스가 인지하고 판단하여 사용자에게 적합한 서비스를 제공해 주는 것이다. 현재 근거리 위치를 기반으로 하는 서비스에는 NFC(Near Field Communication), QR코드(Quick Response Code)가 있으며, 이러한 서비스들은 사용자 인식을 위해 다중 인식에 대한 어려움이 있으며, 복제, 보안등 여러 가지

*Corresponding Author : Chul-Jin Kim(Inha Technical College)
Tel : +82-32-870-2338 email : cjkim@inhatc.ac.kr
Received May 2, 2016 Revised (1st June 20, 2016, 2nd June 22, 2016)
Accepted August 11, 2016 Published August 31, 2016

문제점이 있다[1]. 반면, BLE (Bluetooth Low Energy) 기반인 비콘 서비스는 저전력, 비접촉, 다중호환 방식[2]으로 근거리 서비스를 제공함으로써 기존 인식 서비스를 개선할 수 있는 기술이다. 본 논문에서는 비콘의 여러 요소들을 활용하여 기존의 인식 기술의 편리성 및 보안 이슈를 해결하고자 비콘 기반의 이중 보안 아키텍처를 제안한다.

본 논문의 구성은 2장에서 관련 연구로 비콘을 이용한 보안이 보장되는 근접 서비스 방안 연구 사례에 대해 분석하고, 3장에서는 비콘 서비스를 활용한 이중보안 기법을 제안한다. 4장에서는 본 논문에서 제안한 기법을 이용한 이중보안 어플리케이션에 개발하여 적합성을 검증하고, 5장에서는 결론을 맺는다.

2. 관련연구

2.1 비콘을 이용한 보안이 보장되는 근접 서비스 방안[3]

연구 [3] 에서는 비콘 송신기에서 전송하는 식별자 값이 보안 적으로 취약한 점을 해결하기 위해 제안하는 방법이다. 비콘이 가지고 있는 세 가지 식별자중 Proximity UUID 값은 위치를 확인하기 위해 사용하고, MAJOR나 MINOR 값은 수신한 디바이스의 유효성을 확인하기 위해 사용되는 값 이다. 사용자 디바이스는 비콘 송신기로부터 MAJOR 또는 MINOR 값을 획득후 서버로 전송한 뒤에 서버는 비콘 송신기와 사용자 디바이스에서 수집된 MAJOR 또는 MINOR 값을 비교해서 유효성 검사를 하고 검사가 통과되면 사용자 디바이스에서 특정 서비스가 이용 가능한 보안 기술이다. 또한 본 기술을 지원하기 위해 비콘 송신기에서 유효성 검사를 위해 사용되는 MAJOR 또는 MINOR 값을 변경시켜주어야 하고, 이 값이 변경 된 다음에는 변경된 값을 서버에 전송하여 유효성 검사가 바르게 이루어질 수 있도록 해야 한다. 연구 [3]은 비콘의 MINOR와 MAJOR 값을 이용하여 비콘과 디바이스의 유효성 검사를 한다. 그러나 1차 검증 시 비콘 정보가 누출될 경우 보안에 미흡할 수 있다. 그러나, 본 논문에서는 2차 검증을 요구하기 때문에 정보가 누출될 경우 서비스를 제한하여 보안에 신뢰성을 보장할 수 있다.

2.2 BLE 보안 취약점에 관한 연구[4]

연구 [4] 에서는 BLE의 보안 취약점으로 인해 무선으로 송수신 되는 데이터가 유출될 가능성이 있는 BLE의 문제점을 해결하기 위해 방안을 제안한다. BLE에는 연결을 암호화 하기 위해 사용되는 3가지 키로 임시키인 TK(temporary key), STK(short term key)가 있고 재연결의 암호화를 위해 사용되는 LTK(long term key)가 있다. 이 키들을 생성하기 위해 pairing 프로세스가 3단계에 결쳐 수행된다. pairing 프로세스 2단계 방법중 just works pairing 방법을 사용할 때 생성되는 TK값은 0x00이다. 연결의 암호화를 목적으로 master와 slave가 TK를 포함한 데이터로 STK를 생성하고,생성한뒤에 STK키를 사용해서 AES 암호화 알고리즘으로 링크를 암호화한다. 여기서 BLE 보안의 취약점은 STK를 생성하기 위해 사용할 수 있는 TK의 가짓수가 너무 적다는 것이다. just works인 경우에 TK는 0x00이고 passkey entry는 최대 6자리 숫자이기 때문에 무작위 대입으로 금방 찾을 수 있다. 만약 공격자가 pairing 프로세스의 처음부터 sniffing을 시도하여 transprot specific key distribution 까지의 송수신 된 패킷을 가지고 있다면 무작위 대입 공격하여 실제로 송수신된 값과 비교해서 TK를 구할 수 있다. TK를 구했다면 STK도 계산할 수 있다. 또한 STK로 암호화된 링크도 복호화 할 수 있으므로 LTK도 얻을 수 있다. 하지만 본 논문에서는 사용자 단말기와 블루투스를 사용하여 통신을 할 때 사용자 단말기의 고유값인 디바이스ID와 비콘의 고유값인 MINOR, MAJOR 값을 조합하여 서로 다른 조합법과 암호화로 이중 암호화를 하기 때문에 연구[4]에서 제안한 기법으로 공격자가 공격을 성공하였다 하여도 통신할 때 사용되는 유효 데이터는 이중 암호화되어 전송되기 때문에 공격자가 연구[4]의 공격 기법으로는 유효데이터를 수집하기엔 미흡하다는 점에서 본 연구에서 제안하는 보안 기법은 연구[4]에서 제안한 공격에 대응할 수 있다.

2.3 블루투스 환경에서의 보안 모델 연구[5]

연구 [5] 에서는 블루투스 보안 취약요소를 연구한다. 블루투스 통신에서 나타나는 보안적인 취약성은 주로 유닛키의 사용 문제, 짧은 길이의 PIN 코드의 사용, 암호 알고리즘의 취약성에 의해 나타난다. 블루투스가 보유하고 있는 키는 링크키와 암호키로 구분할 수 있다. 링크키는 블루투스 장치간 인증 단계에서 사용되며, 암호키 생

성 시 사용되는 파라미터이다. 암호키는 두 블루투스 장치간 인증 후에 암호화 통신을 하기 위한 키 이다. 만약, 링크키를 초기키로 사용한다면, 초기키를 생성하고 인증 프로세서에 사용되는 정보의 유일한 비밀 정보인 PIN 코드에 의존하게 된다. 일반적으로 PIN 코드는 네 개의 숫자로 이루어져 있고 10,000개의 서로 다른 값들로 구분된다. 또한 PIN 코드는 코드에 입력되지 않는 부분이 0으로 입력되는 취약점을 가지고 있다. 이로 인해 PIN 코드는 경우의 수가 적으므로 Brute-force 공격에 대한 취약성을 가지고 있다. 마찬가지로 본 연구에서 제안하는 기법에 키로 사용되는 MINOR값과 MAJOR값 또한 다섯 자리로 이루어져 있다. 또한 입력되지 않는 부분이 0으로 입력되는 점도 PIN코드와 같다. 하지만 본 연구에선 MINOR값과 MAJOR값, 사용자 디바이스의 ID를 사용하여 한번 암호화를 하고 보안 검증을 요구한 뒤 다른 암호화 기법을 사용하여 검증을 요구하기 때문에 연구[5]에서 연구한 취약요소를 보완 할 수 있을 것이다.

3. 모바일 이중보안 기법

본 연구는 모바일 디바이스의 블루투스와 비콘을 이용하여 이중보안 기법을 제안하며, iBeacon[6]을 사용하여 인증 시스템의 보안성을 향상 시킬 수 있을 것이다.

3.1 이중보안 아키텍쳐

본 논문에서 제안하는 이중보안 기법을 위한 아키텍쳐는 Fig. 1과 같이 센싱 계층(Sensing Layer), 디바이스 계층(Device Layer), 보안 서비스 계층(Security Service Layer)로 구성된다.

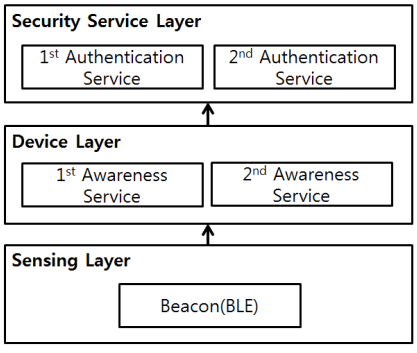


Fig. 1. Dual Security Architecture

디바이스는 센싱 계층을 통하여 비콘이 감지가 되면 RSSI(Received Signal Strength Indication)값을 디바이스로 전송한다. 전송받은 RSSI 값이 특정 값이 되면 등록된 값을 비콘과 디바이스로부터 획득한 값들을 사용하여 이중으로 비교하는 1차, 2차 인식 서비스(1st, 2nd Awareness Service)를 제공한다. 인식 서비스에 의해 제공된 정보는 보안 서비스 계층에서 1차, 2차 인증 서비스(1st, 2nd Authentication Service)를 거쳐 이중 보안 체크를 하게 된다.

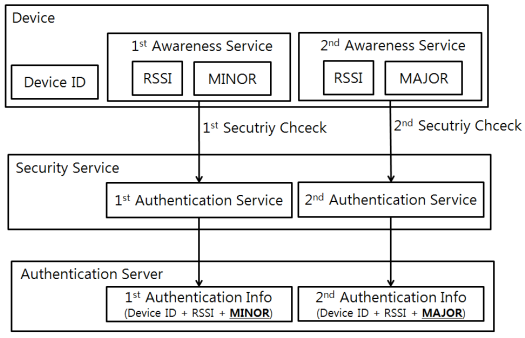


Fig. 2. Security Check Service Architecture

Fig. 2와 같이 사용자가 인식 서비스를 받기 위해 블루투스가 실행중인 사용자 디바이스의 RSSI 값을 전달한다. 1차 인증을 위하여 사용자의 디바이스 ID와 MINOR를 비콘으로 부터 획득하여 1차 인증 정보와 비교하고 값이 일치하면 2차 인증을 위해 사용자 디바이스 ID와 MAJOR를 획득하여 이중으로 인증 서비스를 수행한다.

3.2 이중보안 프로세스

이중보안 프로세스는 백그라운드 프로세스(Background Process)로 실행되며, 블루투스를 통해서 비콘 송신기 위치와 고유 값을 감지한다. 블루투스를 통해 비콘 송신기 위치 감지를 위한 프로세스는 다음과 같다. 블루투스를 사용한 인식을 위해 안드로이드 모바일 플랫폼에서 블루투스를 허용할 수 있도록 AndroidManifest.xml을 설정해야 한다.

1차 인증 절차 구조는 Fig. 3과 같으며 1차인증에 필요한 디바이스 ID와 MINOR 값을 정상적으로 받은 뒤에 서버에 저장된 인증 디바이스의 ID와 MINOR 값과 비교한다. 1차 인증이 허가될 경우, 2차 인증으로 넘어

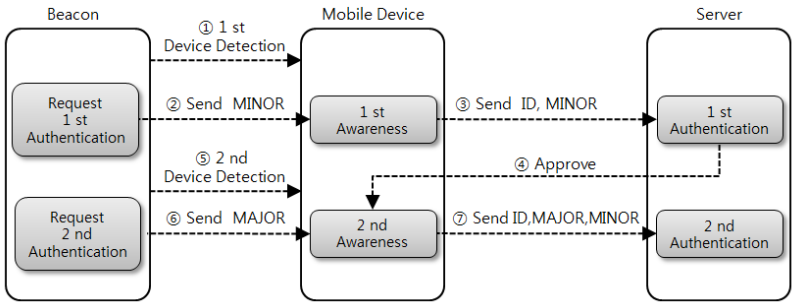


Fig. 3. Dual Authentication Process

가서 ID, MINOR, MAJOR을 모두 가져와서 서버에 저장된 인증 디바이스의 ID와 MINOR, MAOJOR를 비교하여 2차 인증을 수행한다.

비콘이 사용자 디바이스를 감지한 뒤, 이중 보안을 적용하기 위해 사용자 디바이스와 비콘 간에 인증을 실행한다. 블루투스가 비콘 송신기를 감지하면 어플리케이션에서는 주기적으로 RSSI 값으로 거리를 측정한다. 측정한 거리를 확인하기 위해서 IBeacon형 변수인 mIBeacon을 선언 후 IBeacon 모듈인 getRssi()를 사용하여 현재 RSSI 값을 반환 시킨다(Fig. 4). 반환된 값으로 사용자 단말기와 비콘 송신기 거리가 특정 거리가 되고, Proximity[7] (Fig. 5) 까지 조건에 만족하면 인증을 진행한다.

```
/** parsed iBeacon Data */
private IBeacon mIBeacon

&& mIBeacon.getRssi() >= -50
&& (mIBeacon.getProximity() == 1)
```

Fig. 4. Interval Check

```
/**
 * Less than half a meter away
 */

public static final int PROXIMITY_IMMEDIATE = 1

/**
 * More than half a meter away, but less than
 * four meters away
 */

public static final int PROXIMITY_NEAR = 2

/**
 * More than four meters away
 */

public static final int PROXIMITY_FAR = 3
```

Fig. 5. Proximity Definition

Fig. 3과 같이 1차 인증을 위해 사용자 디바이스의 ID와 Beacon의 MINOR 값이 필요하다. 사용자 디바이스의 ID를 얻기 위해 Fig. 6 과 같이 TelephonyManager[8] 클래스를 사용해서 모바일 디바이스 ID를 얻어온다. MINOR값은 IBeacon형 변수인 mIBeacon에 있는 getMinor() 함수를 사용하여 얻어온다.

```
public String getDeviceId(){

TelephonyManager mgr =
(TelephonyManager) getSystemService
(Context.TELEPHONY_SERVICE);

return mgr.getDeviceId();
}

String user_id = getDeviceId();
int minor = 0
minor = mIBeacon.getMinor();
```

Fig. 6. Get ID of Mobile Device

Fig. 7에서와 같이 1차 인증과 2차 인증 과정에서 전달되는 정보에 대해 1차 암호화와 2차 암호화 과정을 통해 보안에 대한 신뢰성을 높일 수 있다. 1차와 2차 암호화 과정에서 사용되는 암호화 방식은 서로 다른 방식을 사용하여 키 누출에 대한 위험을 방지할 수 있다.

서버에서 전달된 데이터를 비교할 때 백그라운드에서 작업을 수행하며, 백그라운드에서 작업을 시켜주는 AsyncTask를 사용한다(Fig. 8). AsyncTask는 메인 Thread와 일반Thread를 가지고 각각의 주기마다 CallBack 메서드를 사용해서 Handler를 사용하여 핸들링하지 않아도 AsyncTask 객체 하나로 편리하게 Background 작업을 진행시켜준다.

AsyncTask 내부는 3가지로 나눠져 있다[9]. onPreExecute는 Background 작업 시작 전에 UI 작업을

진행 하는 역할이다. doInBackground는 Background 작업을 진행 해주는 역할이고, onPostExecute는 Background 작업이 끝난 후 UI 작업을 진행 시켜준다.

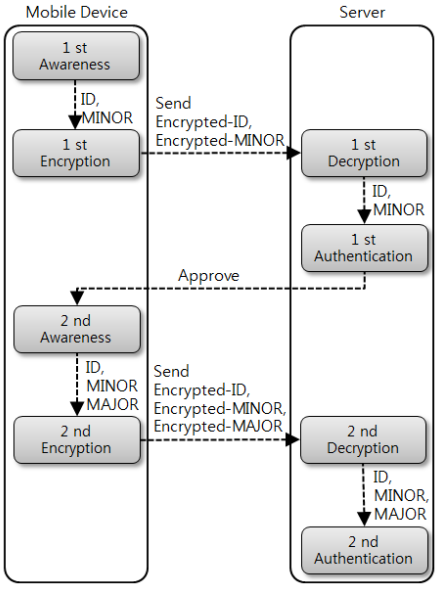


Fig. 7. Encryption/Decryption for Dual Authentication

```
static class TheTask extends AsyncTask<String, String, String> {

protected void onPostExecute(String result) {
super.onPostExecute(result);
editMinor = result
}

@Override
protected void onPreExecute() {
super.onPreExecute();
}
@Override
protected String doInBackground(String... params) {
try {
HttpClient httpclient = new DefaultHttpClient();

HttpGet httpget = new HttpGet(params[0]);
HttpResponse response = httpclient.execute(httpget);
HttpEntity entity = response.getEntity();
if (entity != null) {
return EntityUtils.toString(entity);
} else {
return "No string."
}
  } catch (Exception e) {
return "Network problem"
}}}
```

Fig. 8. AsyncTask Module

AsyncTask를 사용한 백그라운드 작업 과정은 어플리케이션에서 사용자의 ID와 MINOR, MAJOR 값들을 Parameter에다 저장시켜주고, JSP로 그 Parameter들을 받아온다. 그 후에 AsyncTask를 사용하여 백그라운드에서 데이터베이스와의 값 비교작업을 진행한 후 결과 값을 어플리케이션에 전달하는 과정이다.

만약 데이터베이스에 저장된 값과 사용자에 정보가 일치한다면 디바이스 ID값과 MINOR값을 초기화하고, 2차 인증을 위해 디바이스 ID와 MINOR 값, 그리고 MAJOR 값을 한 번 더 획득하여 2차 인증을 진행한다.

데이터베이스와의 비교 값이 True라면 Fig. 9와 같이 'Authentication Success' 이란 음성을 Intent를 사용하여 출력하고, 음성 출력 후에 인증관련 서비스를 종료 시킨다.

```
Intent intentSpeaker =new Intent(ScanService.this, Speaker.class);
intentSpeaker.setFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
startActivity(intentSpeaker);

myTTS.speak("Authentication Success", TextToSpeech.QUEUE_FLUSH, null); //Audio Output

Intent intentSpeaker =new Intent(Speaker.this, SucessActivity.class);
intentSpeaker.setFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
startActivity(intentSpeaker);
endService();
```

Fig. 9. After successful authentication progress

만약, 인증을 실패하였을 경우에는 추가로 3번 인증을 다시 시도하여 총 인증이 3번 실패하였을 경우에는 Intent를 사용하여 '인증실패' 라는 음성을 출력 한다. 그리고 음성 출력과는 다른 Intent를 사용하여 MainActivity에 정의 되어 있는 BroadcastReceiver를 실행시킨다(Fig. 10). myReceiver라는 BroadcastRecevier가 방송이 되면 unregisterReceiver와 finish 메소드를 실행시켜 현재 어플리케이션에서 실행중인 모든 Activity와 Service를 종료시켜 준다.

```
private BroadcastReceiver myReceiver =
 new BroadcastReceiver() {
@Override
public void onReceive(Context context, Intent intent) {
unregisterReceiver(myReceiver);
finish(); }};
```

Fig. 10. BroadcastReceiver

4. 실험 및 평가

본 논문에서는 비콘을 사용한 인증 서비스의 신뢰성 향상을 위한 이중 보안 기법을 제안하였다. 이에 대해 사용자의 인증 상황을 블루투스를 기반으로 이중 보안되는 어플리케이션을 통하여 이중 보안의 적합성을 검증한다. 본 어플리케이션은 사용자 자동 인증 기능, 암호화, 복호화 기능으로 구성된다.

4.1 사용자 자동 인증 기능

사용자 자동 인증 기능은 사용자에게 인증 기능에 대한 편리성을 제공하기 위해 모바일 앱과 비콘, 그리고 서버 간에 자동으로 인증하도록 구현한다. 그러나 1차 인증과 2차 인증 과정을 검증하기 위해 1차, 2차 인증 버튼을 추가하여 확인할 수 있도록 한다.

Fig. 11과 같이 인증 하고자 하는 Beacon 주변에서 이중 보안이 적용될 디바이스를 실행한다. 인증 버튼을 한번만 누르면 앱이 백그라운드 실행으로 자동 전환된다.

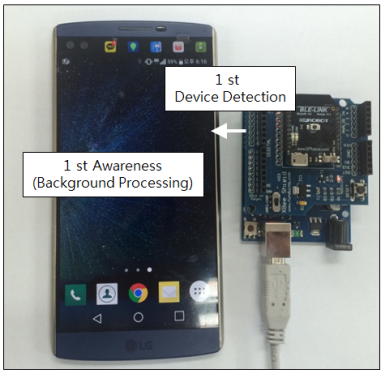


Fig. 11. Detecting Device by Beacon

이 상태에서 통과 하고자 하는 비콘과의 거리가 10~20cm 정도 되면 자동으로 백그라운드에서 블루투스를 통해 비콘 송신기를 감지하게 된다.

사용자의 디바이스가 센싱 거리에 위치하면, 어플리케이션은 사용자 디바이스의 ID와 비콘의 MINOR 값을 서버와 비교하여 1차 인증을 수행한다. 1차 인증이 실패할 경우 Fig. 12와 같이 '인증 실패' 라는 음성과 함께 'FAILED' 메시지를 표시한다.

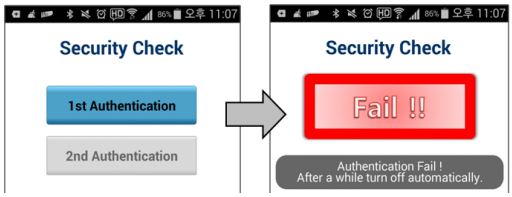


Fig. 12. Fail in 1st Authentication

1차 인증이 통과가 되면 사용자가 아무런 이벤트를 수행하지 않고 2차 인증으로 넘어가며, 1차 인증에서 받아온 디바이스 ID와 MINOR값을 삭제 후 다시 사용자의 디바이스 ID와 비콘의 MINOR, MAJOR 값을 받아온다. 1차 인증과 같이 서버에 저장된 디바이스 관련정보와 비교하는 2차 인증을 수행한다. Fig. 13과 같이 2차 인증에 성공하면 '인증 성공' 이라는 음성과 성공 메시지가 표시된다. 만약 2차 인증에 실패 하였을 경우에는 1차 인증 실패와 마찬가지로 '인증 실패' 라는 음성과 함께 'FAILED' 메시지가 표시된다.

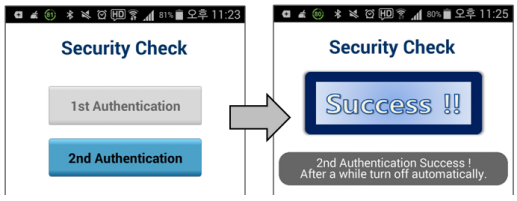


Fig. 13. Success in 2nd Authentication

5. 결론

본 논문에서는 비콘의 MINOR, MAJOR 값과 모바일 디바이스 ID를 이용하여 비콘과 모바일 디바이스 간에 안전한 인증을 위한 이중 보안 기법을 제안한다. 이는 현재 보안성에 이슈가 되고 있는 비콘의 보안성을 향상시켜 주며, 비콘을 기반으로 하는 다양한 서비스를 제공할 수 있는 기반이 될 것이다. 본 논문에서 제시한 이중 보안 기법은 비콘과 블루투스를 연동한 시스템이며, 블루투스 특성상 가까운 거리가 되었을 때 서비스를 해주는 방식이므로 가정의 도어락부터 보안이 요구되는 시설의 물리적 보안 통제에 이용될 수 있다. 향후 연구는 기존 비콘 기반의 모바일 서비스 사례에 적용하여 보안 취약점을 도출하고 적용할 수 있도록 한다.

References

[1] Jong-Kyung Baek, Jae-Pyo Park, “A study of analysis and improvement of security vulnerability in Bluetooth for data transfer”, Journal of the Korea Academia-Industrial cooperation Society, Vol. 12, No. 6 pp. 2801-2806, 2011.
DOI: http://dx.doi.org/10.5762/KAIS.2011.12.6.2801

[2] Bluetooth Smart or Version 4.0+ of the Bluetooth specification, https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics/low-energy.

[3] Jong-Wuk Son, Kook-rae Cho, Bo-Kyu Jang, "Secure Proximity Service Using Beacon", IEEK(Institute of Embedded Engineering of Korea), Preceeding, 2014.

[4] Gi-won Kwon, Sung-hyun Cho, "A Study on the vulnerability of Bluetooth Low Energy Security", KICS(The Korean Institute of Communications and Information Sciences), Winter Preceeding, 2016.

[5] Son-Yong Seung, "A Study of Security Model for Bluetooth Environment", Master's Paper of DongGuk University, 2011.

[6] iBeacon, http://www.ibeacon.com.

[7] Ranging Part of iBeacon, http://en.wikipedia.org/wiki/IBeacon, 2016.

[8] TelephonyManager for telephony services on the device, http://developer.android.com/reference/android/telephony/TelephonyManager.html.

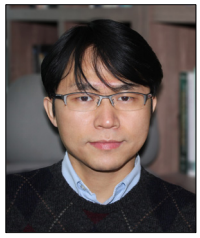
[9] AsyncTask Instructions, http://tigerwoods.tistory.com/28, 2010.

박 상 민(Sang-Min Park) **[준회원]**

- 2014년 3월 ~ 현재 : 인하공전 컴퓨터시스템과 재학

<관심분야>
웹 서비스, 모바일 서비스, 데이터베이스

김 철 진(Chul-Jin Kim) **[종신회원]**



- 2004년 2월 : 숭실대학교 대학원 컴퓨터학과 (공학박사)
- 2004년 3월 ~ 2009년 2월 : 삼성전자 책임연구원
- 2009년 3월 ~ 현재 : 인하공전 컴퓨터시스템과 부교수

<관심분야>
컴포넌트 기반 개발 방법론, 컴포넌트 커스터마이제이션, 모바일 서비스, 클라우드 컴퓨팅