블루투스의 보안 취약성과 공격

이인범* · 류대현*

*한세대학교 IT학부

Vulnerability and Attacks of Bluetooth System

In-Baum Rhee* · Dae-Hyun Ryu*

*Hansei University

E-mail : dhryu@hansei.ac.kr

요 약

본 논문에서는 먼저 블루투스 시스템과 블루투스 정보보호에 대해 설명하였고, 또한 블루투스 규격에서 정의하고 있는 정보보호 구조를 분석하고 그 취약성을 제시하고, 다양한 블루투스 해킹 기법들을 소개하였다. 또한 CarWhisperer를 이용하여 휴대폰에 사용하는 핸즈프리에 적용하여 핸즈프리에 임의의 음성 메시지를 주입하는 공격과 핸즈프리를 통해 대화하는 내용을 녹음하여 파일로 저장하는 공격 과정을 수행하였다.

ABSTRACT

In this paper, we describe Bluetooth system and Bluetooth security. And we analyze the structure of information security and vulnerability, introduced one of Bluetooth hacking techniques. We show a demo of the attack process to inject arbitrary hands-free voice messages and save the file information, recording a conversation through hands-free device.

키워드

블루투스, 보안, 취약성, 공격, CarWhisperer, 핸즈프리

Ⅰ. 서 론

블루투스의 다양한 응용 분야, 특히 전자 상거래 등에서 응용을 고려 할 때 보안 문제에 대한 연구는 매우 중요하다고 생각된다. 예를 들어 독일의 Siemens사는, CeBit2000에서 블루투스를 사용한 전자 결제의 데모를 선보였다. 이는 블루투스를 탑재한 휴대 전화기 등과, 자동판매기 등 점포의 단말과의 사이로, 구입하는 상품 정보와, 휴대 기기에 내장되고 있는 유저 정보를 주고받는 것. 유저로부터 얻은 ID를 기초로, 점포 측의 시스템이 과금 및 정산 처리를 하는 구조이다.

실제로 블루투스는 효과적인 암호화와 인증기술을 사용하여 개발되어 있다. 그러나 블루투스의 다양한 응용분야를 고려 할 때 블루투스에서 제공되는 정보보호 구조가 모든 경우에 안전하다고 보기는 어렵다. 예를 들어 블루투스는 링크레벨에서의 인증과 암호화를 제공하지만 링크레벨에서 적용하는 것은, 명함교환 같은 보다 공공적인 적용 모델에 대해 친숙한 사용자 접근이 어렵게 할 수도 있다. 특히, 높은 보안 수준이 요구되는 특수한 응용 분야에 적용할 경우, 블루투스에서 제공되는 보안 구조의 파악과 문제점 분석은 매우 중요하다.

본 논문에서는 먼저 블루투스 시스템과 블루투스 정보보호에 대해 설명하였고, 또한 블루투스 규격에서 정의하고 있는 정보보호 구조를 분석하고 그 취약성을 제시하고, 다양한 블루투스 해킹 기법들을 소개하였다. 본 연구에서는 CarWhisperer를 이용하여 휴대폰에 사용하는 핸즈프리에 적용하여 핸즈프리에 임의의 음성 메시지를 주입하는 공격과 핸즈프리를 통해 대화하는 내용을 녹음하여 파일로 저장하는 공격 과정을 수행하였다.

Ⅱ. 블루투스 보안 개요

블루투스 기술은 짧은 거리에서 peer-to-peer 통신을 지원하는데 다른 무선 기술처럼 무선 채널의 특성상 다른 사람도 통신에 자유롭게 참여할 수 있기 때문에 블루투스에서는 사용자의 정

보의 신뢰성유지와 보호를 위해 응용 계층(application layer)과 링크 계층(link layer)에서 보안구조를 제시하고 있다.

암호는 각각의 링크를 보호하고 인증은 원하지 않는 디바이스에 의한 엑세스를 방지하여 데이터와 응용 기능(application function)을 보호하며 주파수 호핑 방식(frequency hopping schem)과 짧은 통신 거리 또한 보안을 유지하는 한 방법이다.

보안의 유지가 철저해 질수록 사용자는 서비스를 이용하는데 불편을 감수해야 하는데 블루투스는 이러한 불편을 최소화하기 위해서 서비스의 종류에 따라 보안 수준의 정도를 선택 할 수 있도록 정의하고 있으며 이를 세 가지의 보안 모드(security mode)로 나누고 있다.

Mode 1 : 보안이 없는 모드로 이 모드는 비교적 중요성이 떨어지는 데이터에 사용되며 링크 레벨 보안 기능을 그냥 통과하며 명함이나 달력 등을 교환하는 경우가 이 모드를 사용하는 대표적인 예이다.
Mode 2 : 서비스 레벨의 보안이 제공되는 모드로 L2CAP에서 채널이 형성되기 전까지는 보안이 적용되지 않으며 다양한 접근 절차(access procedure)가 제공될 뿐만 아니라 각각의 어플리케이션들은 독립적으로 서로 다른 보안 레벨을 가지고 동작할 수 있다.
Mode 3 : 링크 레벨 보안이 제공되는 모드로 LMP에서 링크가 형성되기 전에 LM에 의해 보안 절차(security procedure)가 동작하게 되고 모드 2의 경우보다는 엑세스가 자유롭지 못하지만 보다 높은 보안 레벨을 유지 할 수 있는 모드이다.

블루투스는 사용자 보호와 정보 비밀성을 위해 응용계층과 링크 계층에서 보안 수단을 제공한다. 각각의 블루투스 유닛(unit)에서는 인증과 암호화 루틴이 동일한 방식으로 구현된다. 링크 계층에서 보안 유지를 위해 사용되는 4개의 개체는 BD_ADDR(Bluetooth Device Address), 링크키, 암호키, 난수이다.

BD_ADDR은 각 블루투스 유닛에 대해 유일한 48 비트의 IEEE 주소이다. BD_ADDR은 공개적으로 알려져 있고 블루투스 유닛의 조회(inquiry) 루틴을 통해 얻을 수 있다. 링크키는 초기화 과정에서 생성되는 128비트의 비밀 키이며, 유닛 키, 조합 키(combination key), 마스터 키, 초기화 키 등이 링크 키로 사용된다.

암호 키는 8~128 비트의 크기를 가지며 인증 과정에서 링크 키로 부터 생성된다. 암호 키의 크기는 다음 두 가지 이유로 인하여 고정되어 있지 않다. 첫째 이유는 프라이버시에 대한 정부기관의 정책과 수출규제 등 암호 알고리즘에 부과된 여러 요구사항과 관계가 있다. 둘째 이유는 알고리즘과 암호화 하드웨어를 재설계할 필요 없이 보안 업그레이드를 손쉽게 하고자 함이다. 키의 크기를 늘리는 것은 공격자의 증가하는 컴퓨팅 파워에 대항하는 가장 간단한 방법이다. 현재 64비트 암호 키는 대부분의 응용에 대해 만족할 만한 비밀성 보호를 제공한다. RAND는 블루투스 유닛 내의 난수 또는 의사 난수 프로세스에서 생성되는 난수이며, 링크키와 암호 키 생성에 사용된다.

그러나 블루투스의 다양한 응용분야를 고려 할 때 블루투스에서 제공되는 정보보호 구조가 모든 경우에 안전하다고 보기는 어렵다. 예를 들어 블루투스는 링크레벨에서의 인증과 암호화를 제공하지만 링크 레벨에서 적용하는 것은 명함 교환 같은 보다 공적인 적용 모델에 대해 친숙한 사용자 접근이 어렵게 할 수도 있다. 특히, 높은 보안 수준이 요구되는 특수한 응용 분야에 적용할 경우, 블루투스에서 제공되는 보안 구조의 파악과 문제점 분석은 매우 중요하다.

Ⅲ. 블루투스 보안 취약성

블루투스는 무선으로 기기 간에 정보를 교환하므로 정보보호 측면에서 무선 방식이 갖는 취약점을 갖고 있다. 본 연구에서는 먼저 블루투스 시스템에 대해 설명하고 블루투스 규격에서 정의하고 있는 정보보호 구조를 분석하고 그 취약성을 조사 하였다.

블루투스의 암호화 방식은 약간의 취약성을 갖고 있다. 키 길이가 128 비트인 E_0 스트림 암호화기는 어떤 환경에서는 O(2^64)로 깨질 수 있다고 알려져 있다. 간단히 말하면 주어진 키 수열의 길이가 E_0에서 키 수열 생성 시 가장 짧은 LFSR 사용자의 주기보다 길다면 divide-and-conquer 형태의 공격이 가능하다. 그러나 이러한 문제는 블루투스 규격에 이미 고려되어 있다. 즉, divide-and-conquer 공격은 부분 입력에 해당하는 키 수열을 필요로 하는데 블루투스는 매우 큰 재동기 주파수(re-synchronization frequency)를 갖고 있다. 그런데 각 프레임을 암호화하기 위하여 생성되는 키 수열은 독립적이고 충분히 짧기 때문에 그러한 방법으로 공격하기는 어렵다.

또한 두 블루투스 장치의 초기화 과정에서 PIN 코드의 사용은 사용자를 불편하게 한다. 즉, 두 장치를 연결할 때마다 매번 PIN코드를 두 번 입력시키는 것은 짧은 코드라 할지라도 짜증나는 일이다. 만약 블루투스 장치가 ad hoc 네트워크로 구성되어 있고 각각 초기화되어야 한다면 사용자를 참기 힘들게 하고 보안을 유지하기는 쉽지 않다. 따라서 규격에서는 긴(16바이트 이상) PIN코드를 갖는 응용 계층의 키 동의 소프트웨어를 사용할 것을 권고하고 있다. 그렇게 한다면 연결된 각 장치에 PIN코드를 물리적으로 입력시킬 필요는 없지만 Diffie-Hellman 키 동의(key agreement)와 같은 방법이 필요하다.

그리고 초기 키를 어떻게 생성할 것인가도 중요하다. 초기 키의 강도는 순전히 PIN코드에 달려있다. E22 초기화 키 생성 알고리즘은 키를 PIN 코드로부터 유도하는데 PIN 코드의 길이는 난수

이며 무선으로 전송된다. 이 경우, 안전성은 순전히 PIN 코드에 달려있으며 4자리 PIN 코드를 사용할 때 10.000개의 서로 다른 가능성이 있다. 기사용된 PIN의 50%가 "0000"이라는 사실을 고려한다면 유효한 초기화 키는 매우 적다.

유닛 키 방식에도 문제가 있다. 인증과 암호화는 링크 키를 통해 참여자가 비밀을 나누고 있다는 가정에 근거한다. 이 과정에서 사용되는 다른 정보는 공개되어 있다. 장치 A와 장치 B가 링크 키로 A의 유닛 키를 사용한다고 가정하자. 이 때 장치 C가 장치 A와 통신할 수 있고 A의 유닛 키를 링크 키로 사용할 수 있다. 이것은 A의 유닛 키를 먼저 획득한 장치 B가 위조된 장치 주소를 갖는 유닛 키를 사용하여 암호화 키를 계산하고 트래픽을 모니터할 수 있다. 이것은 자신을 장치 A에 C인 것처럼 또 장치 C에 A인 것처럼 인증할 수 있다.

모든 블루투스 장치에 대해 유일한 블루투스 장치 주소는 또 다른 문제를 제기한다. 어떤 사람이 갖고 있는 어떤 블루투스 장치에 연결이 이루어졌을 때 이 사람의 행동이 쉽게 모니터 되고 추적될 수 있다. 즉 블루투스를 이용한 모든 거래가 기록되고 결국 개인의 프라이버시가 침해될 수 있게 된다.

인증의 경우에도 사용자 인증은 이루지지 않으며 단지 장치의 인증만이 이루어진다. 만일 사용자 인증이 필요하다면 응용 계층의 보안에서 이루어져야 한다. 또한 블루투스는 각 서비스에 대하여 허가과정을 분리하여 정의하지 않는다. 이렇게 함으로서 블루투스 구조에서 프로토콜 스택을 바꾸지 않고 적용될 수 있지만 보안 관리부의 변경과 등록과정이 필요하게 된다.

Ⅳ. 블루투스 시스템의 공격

블루투스는 보안기능을 제공하고 있지만 위에서 설명한 취약점 외에도 Dos공격, 도청, MITM 공격, 메시지 변조 등과 같은 공격에 여전히 취약하며 블루투스 특성을 이용하여 발생되는 공격도 존재한다.

본 연구에서는 CarWhisperer를 이용하여 휴대폰에 사용하는 핸즈프리에 적용하여 핸즈프리에 임의의 음성 메시지를 주입하는 공격과 핸즈프리를 통해 대화하는 내용을 녹음하여 파일로 저장하는 공격 과정을 수행하였다.

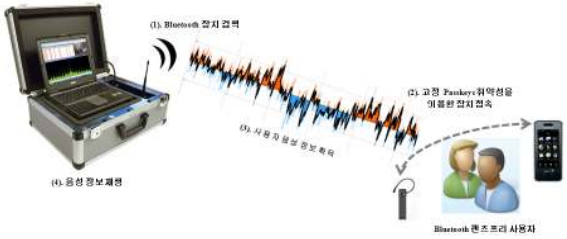

그림 1. CarWhisperer를 이용한 블루투스 시스템 공격

1. 실험 대상 장비 및 도구
- ASUS USB-BT21 mini Bluetooth v2.0 + EDR
- Samsung HM1600
- CarWhisperer : 이 도구를 통해 Bluetooth 핸즈프리의 취약점을 이용하여 본 연구의 실험을 수행한다. http://trifinite.org/trifinite_stuff_carwhisperer.html 에서 다운로드 가능하다.
- SOX : 이 도구는 raw Format의 오디오 파일을 wav Format의 오디오 파일로 변환해주는 도구로써 해당 실험에서 사용된다. http://sox.sourceforge.net 에서 다운로드 가능하다.

2. 환경 설정

가상 머신인 VMware 환경에 Ubuntu OS를 설치한 후 해당 Bluetooth Dongle을 Connecting하여 CarWhisperer와 SOX를 이용해 위에서 소개한 상용 Bluetooth 핸즈프리(Samsung HM1800과 LG HMB-585)의 취약성을 이용한 실험을 수행 하였다.

표 1. 실험 환경

설치 환경	Ubuntu-10.04.1-desktop-
OS	VMware 7.1.2 build-301548
Bluetooth Dongle	Connect
Bluetooth HansFree	Listen

3. 실험 수행 방법 및 내용

위와 같은 실험환경을 셋팅한 후, VMware의 UbuntuOS 터미널에서 다음과 같은 순서의 Command를 통해 실험을 수행한다.

- step 1: 연결된 블루투스의 hcid.conf 파일을 편집. sudo gedit /etc/bluetooth/hcid.conf
- step 2: hcid.conf 파일에 passkey 부분을 0000의 암호로 변경하여 저장
- Step 3: hcd.conf 파일을 저장과 종료 후 다운로드 받은 cawwhisperer을 압축 해제 후 해당 파일로 이동 / 확인.

cd Desktop/carwhisperper-0.2 dir
- step 4: carwhisperer 설치. sudo make
- step 5: 설치를 완료하기 위해서 먼저 Makefile을 수정한다. sudo gedit Makefile
- step 6: Makefile 내의 모든 cw_pin.sh파일을 cw_pin.pl 파일로 수정한 후 저장한다.
- step 7: 설치 완료. sudo make install
- step 8: 블루투스 장치가 실행되고 있는지 확

인. hciconfig hci0
- step 9: 실행되지 않는다면 실행되도록 전원을 킨다. sudo hciconfig hci0 up
- step 10: 블루투스 클래스를 찾는다.
hciconfig -a
- step 11: phone 으로 나열되지 않았으면, 장치 클래스를 변경한다.
sudo hciconfig hci0 class 0×500204

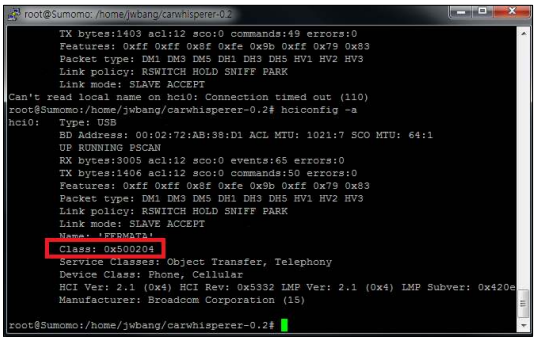

그림 2. Bluetooth 휴대폰 클래스로 변경

: 0x500204는 휴대폰의 클래스를 나타낸다.

- step 12: 범위 내에 있는 블루투스 장치를 스캔한다. hcitool scan hci0

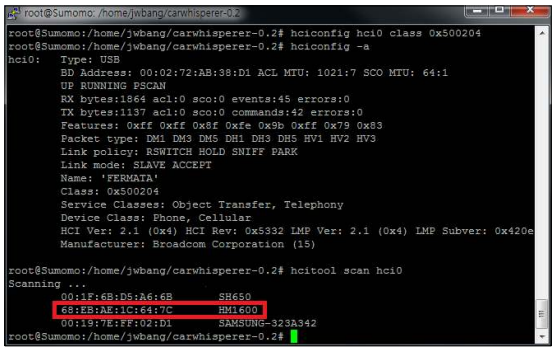

그림 3. 주변 Bluetooth Scan 내용

- step 13: 12단계에서 확인된 주소를 사용하여 해킹 실행. carwhisperer hci0 message.raw out.raw [전 단계에서 확인된 주소]
: Samsung HM1600 MAC주소 68:EB:AE:1C:64:7C
: 위 command를 통해 message.raw의 음성파일의 내용이 해당 핸드프리를 통해 방송되고, 방송 중 핸즈프리를 통해 대화한 내용들은 핸드프리의 마이크를 통해 녹음되어 out.raw에 저장된다.
- step 14: 종료하려면 "Ctrl c"을 누른다.
- step 15: out.raw 오디오 파일을 변환하는 삭스 설치. sudo apt-get install sox
- step 16: carwhisperer 디렉토리에 아직도 있는지 확인하는 동안, raw 파일을 wav 파일로 변환하는 커맨드 실행. sox -t wav recv0.wav -c 1 -r 8000 -s -w recv0.raw
- end

위와 같은 방법을 통해서 Buletooth 2.1 기반의 상용 도구를 대상으로 취약성을 분석하고 실험을 수행하였다. 실험의 수행결과처럼 핸즈프리 상용 제품의 경우 고정된 표준 passkeys를 이용하는 취약점을 가지고 있었으며, 이와 같은 취약점을 이용하여 보다 넓은 스캔 범위를 가질 수 있는 안테나와 함께 동일한 실험을 수행한다면 스캔 범위 내의 모든 핸즈프리 사용자에게 자신이 원하는 방송을 임의적으로 주입할 수 있는 상황을 발생시키거나 반대로 스캔 범위 내 핸즈프리 사용자의 통화 내역을 취득할 수 있는 결과를 얻을 수 있을 것이다.

V. 결 론

블루투스의 다양한 응용분야를 고려 할 때 블루투스에서 제공되는 정보보호 구조가 모든 경우에 안전하다고 보기는 어렵다. 예를 들어 블루투스는 링크레벨에서의 인증과 암호화를 제공하지만 링크레벨에서 적용하는 것은 명함교환 같은 보다 공공적인 적용 모델에 대해 친숙한 사용자 접근이 어렵게 할 수도 있다. 특히, 높은 보안 수준이 요구되는 특수한 응용 분야에 적용할 경우, 블루투스에서 제공되는 보안 구조의 파악과 문제점 분석은 매우 중요하다. 본 보고서에서는 먼저 블루투스 시스템과 블루투스 정보보호에 대해 설명하였고, 또한 블루투스 규격에서 정의하고 있는 정보보호 구조를 분석하고 그 취약성을 제시하고, 다양한 블루투스 해킹 기법들을 소개하였다. 본 연구에서는 CarWhisperer를 이용하여 휴대폰에 사용하는 핸즈프리에 적용하여 핸즈프리에 임의의 음성 메시지를 주입하는 공격과 핸즈프리를 통해 대화하는 내용을 녹음하여 파일로 저장하는 공격 과정을 수행하였다.

참고문헌

[1] Specification of the Bluetooth System, volume 1B, December 1st 1999
[2] Security of Bluetooth: An overview of Bluetooth Security Marjaana Trakbak
[3] Thomas Muller, Bluetooth WHITE PAPER: Bluetooth Security Architecture, Version 1.0, 15 July 1999
[4] Bluetooth Security, Juha T. Vainio, http://www.niksula.cs.hut.fi/~jiitv/bluesec.html#chap1 2000-05-25