BlueTooth Snarfing 공격 및 보안측면

박현욱* 김현수* 김기환* 이훈재**

*동서대학교 정보네트워크학과

*동서대학교 유비쿼터스IT

**동서대학교 컴퓨터정보공학과

BlueTooth Snarfing attacks and security aspects

Hyun Uk Park* Hyun Soo Kim* Ki Hawn Kim* Hoon-jae Lee**

*Dept. of Information Network, Dongseo University

*Dept. of ubiquitous computing, Dongseo University

**Dept. of Information and Communication Engineering, Dongseo University

E-mail : sgparkhyw@naver.com, dong3315@gmail.com, ghksdl90@naver.com, hjlee@dongseo.ac.kr

요 약

현대사회는 많은 디지털 제품을 이용하여 일상생활에 편리함을 주고 있는 가운데, 그 중 하나인 블루투스는 사용자들이 많이 이용하게 된다. 블루투스(IEEE 802.15.1)란 기기 간에 근거리에서 저 전력으로 무선 통신을 사용하기 위한 표준연결 기술이다. 현재는 블루투스 이어폰, 블루투스 스피커, 웨어러블이 탑재된 기기에서도 많이 사용되기 때문에 이를 악용하여 이득을 취하는 사람이 생기게 되었고 그로 인하여 사용자의 피해가 커지고 있는 상황이다. 그래서 사용자의 피해를 줄이고 더 나아가 완전히 막을 수 있는 보안기법에 대해서 연구 하게 되었다. 그 많은 블루투스 해킹 기법 가운데, 블루투스 장치의 펌웨어 취약점을 이용하여 장치 내에 저장된 데이터에 대한 접근을 허용하여 공격하는 BlueTooth Snarfing을 분석 하고자한다.

ABSTRACT

There are many modern societies use the digital products in everyday life in the Middle, convenience, give him plenty of Bluetooth is one of the users. Bluetooth (IEEE 802.15.1) means equipment in the close range between the low-power wireless communication standard for the connection to use the technology. Currently, Bluetooth earphone, Bluetooth speaker, wearable mounted devices also used a lot because it takes people to exploit the benefits had been lifted and thereby increases your damage. So, reducing the damage the user's further research about the security technique that can stop completely. I am sure that many Bluetooth hacking techniques, a Bluetooth device firmware vulnerability within the stored data to allow the approach to attacking the BlueTooth Snarfing and want to analyze.

키워드

BlueTooth, Communication Technology, security, hacking, Attack and Defenses

Ⅰ. 서 론

블루투스는 여러 기기들을 짧은 거리에서 무선으로 쉽게 연결하기 위해 만들어진 기술로 PAN, 즉 '근거리 개인 무선 통신'을 위한 산업 표준이다.

블루투스는 속도를 중요시하는 중장거리의 Wi-Fi(802.11n-2.4GHz, 802.11ac-5GHz)은 달리 적

은 배터리소모와 연결의 편리성에 중심을 둔 근거리 통신기술이다.

이에 본 논문의 구성은 다음과 같다. 블루투스의 소개와 개념을 2장에서 서술하고, 3장에서 블루투스 해킹과 블루스나핑에 대한 개념을 소개하고, 4장에서 블루스나핑의 가상시나리오와 보안측면을 예를 들어 나타낸다. 그리고 마지막으로 5장에서 결론을 낸다.

Ⅱ. 블루투스의 소개와 개념

블루투스라는 이름의 어원은 10세기경 스칸디나비아 반도 지역을 통일한 해럴드 블루투스의 별명에서 따왔다고 한다. 그래서 블루투스의 공식 로고도 해럴드의 H와 블루투스의 B를 뜻하는 스칸디나비아 룬 문자를 이용해서 만들어졌다. 1998년 2월 스웨덴의 통신기기 제조회사 에릭슨을 중심으로 노키아, IBM, 인텔 등의 기술회사로 참여해 현재의 블루투스가 만들어지게 되었다. 그래서 LAN에서 사용되는 이더넷 케이블을 무선 LAN 표준인 와이파이가 대체한다면 블루투스는 주변 기기들을 연결하는 유선 표준인 USB의 역활을 대체한다고 볼 수 있다. 또 와이파이는 여러기기들이 공유기를 통해 데이터를 나누는 개념이라면, 블루투스는 두 기기끼리 “페어링“이라는 직접적인 연결이 있다. 블루투스 4.0부터는 블루투스 기술이 3가지로 나눠져 있다.

클래식 블루투스 (Classic Bluetooth)는 1.0부터 2.1로 이어져온 기존 블루투스 기술들이다. 그리고 고속 블루투스 (Bluetooth High Speed)는 3.0에서 더해진 와이파이를 활용한 HS 고속전송 기술의 연장이며, 저전력 블루투스 (Bluetooth Low Energy)는 전력소모를 최소화하고 배터리 수명을 연장하는데 중점을 둔 새로운 표준이다.

그림 1. 블루투스 로고

Ⅲ. 블루투스 해킹의 개념과 블루 스나핑

블루투스 해킹에는 크게 3가지 방법이 있다. 블루재킹, 블루버깅, 블루스나핑으로 불리우고 있다. 먼저 블루재킹은 모바일기기에 스팸 메시지를 뿌리는 정도이다. 이것은 많이 불편은 하지만 보안상의 위협을 주는 수준은 아니다.

그리고 블루버깅은 휴대폰을 해킹하여 원격 조정 또는 통화내용을 엿듣는 것도 가능하며, 사용자가 눈치 못 채도록 블루투스 기술을 이용하여 휴대 전화에 엑세스가 가능하다. 블루 버깅을 이용하려면 단점이 타겟과 10미터 이내에 있어야 가능하다. 밑의 그림2와 같이 블루투스 대역폭이 미터 단위인 것을 확인 할 수 있다.

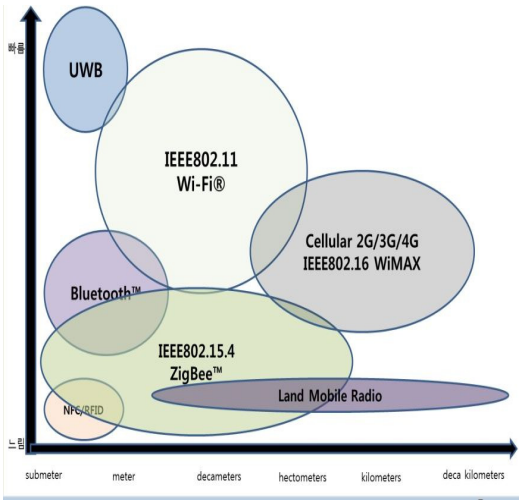

그림 2. 통신망 대역폭[2]

그리고 본 논문에서 주제로 정한 블루스나핑은 스마트폰에 저장된 개인정보, 연락처, 개인 일정표, 문자 메시지에 접근이 가능하다. 이는 사용자가 눈치 못 채도록 블루투스 모바일 기기에 있는 정보를 엑세스 하는 것으로, 사용자가 자신의 기계에 타인의 접근을 눈치 못채도록 하는 non-discovery 모드로 엑세스하게 된다. [1] 밑의 그림3.는 블루투스 동글을 이용한 블루투스 스나핑을 하는 방법을 쉽게 그림으로 나타낸 것이다.

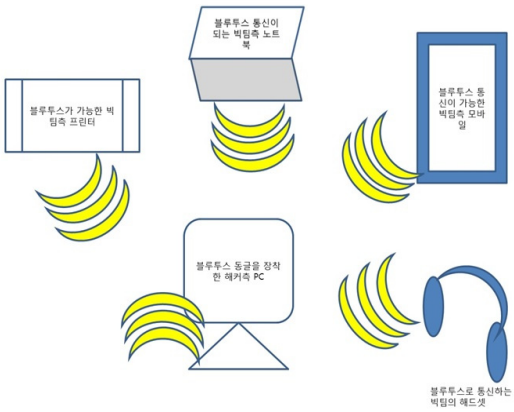

그림 3. 블루투스 동글 사용방법

위 그림은 사용자들이 블루투스를 페어링하여 이용하고 있을 때 해커측에서 사용자의 블루투스 통신을 어디까지 이용할 수 있는지에 대해서 나타낼 수 있는 그림으로써 이와 같이 블루투스 통신에 대한 위험은 매우 크다는 것을 알 수 있다.

Ⅳ. 블루스나핑 가상시나리오와 보안측면

3장에서 블루투스 해킹으로 많은 디바이스들이 보안상 위험에 빠진 것을 알려주었다. 이번 장에서는 블루투스 해킹을 가상시나리오를 설명 하겠다. 우선 일반적인 무선 도청기로는 Bluetooth 신호를 잡을 수가 없다. 문제가 되는 것은 동일한 블루투스 방식의 기기간의 보안이다. [3]

해커가 노트북으로 블루투스를 임의로 켜서 탐지 중에 피해자가 블루투스 장치를 켰을 경우에 해커는 노트북을 스마트폰으로 인식시키기 위해 페이크를 넣고 사용자의 블루투스 장치를 공격을 할 수 있다. 만약 블루투스 디바이스가 음성지원이거나 텍스트가 디스플레이에 나타내지는 디바이스면 해커가 미리 만들어 놓은 가짜 음성 메시지와 텍스트 메시지로 상대방이 이용하는 것을 훔칠 수 있다. 이것을 방지하기 위한 보안대책으로 블루투스의 보안은 3가지 모드가 있다. 첫째, PIN 입력 또는 저장된 링크 키를 이용하여 통신 장치를 식별하는 기능이 있는 인증부분, 그리고 둘째, 도청에 의한 정보 유출을 방지하기 위하여 인증된 장치만 데이터에 대한 접근 허용하는 기밀성이 있다. 또한 통신 장치별로 허용 가능한 서비스만 제공하여 다른 서비스 이용을 차단하는 인가기능이 존재 한다. 그리고 모든 보안관련 처리를 보안 매니저가 담당하기 때문에 유연성 있는 정책 관리 및 구현이 용이하다. 보안 매니저의 주요 기능은 그림4.과 같이 정리가 가능하다.

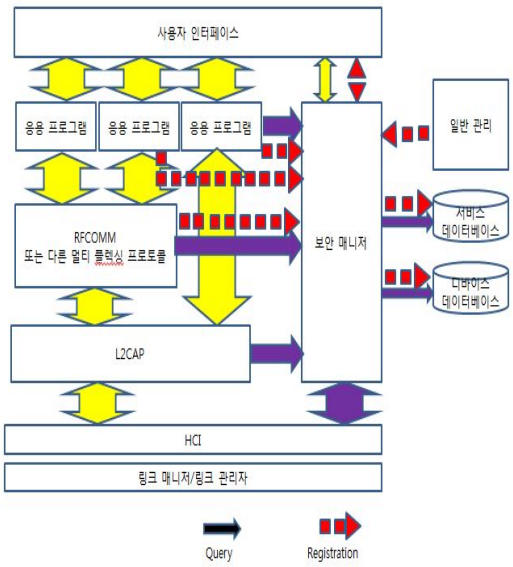

그림 4. 블루투스 보안매니저[1]

보안매니저는 장치관련 보안 정보 관리와 프로토콜 및 응용프로그램의 보안관련 질의응답, 인증 및 암호화를 수행한다. 블루투스의 일반적인 연결 설정 과정 중 보안 관련 절차를 살펴보면 L2CAP이 연결 요청을 받아 보안 매니저에게 접근 허용 여부를 질의하고, 보안 매니저는 서비스 데이터베이스와 디바이스 데이터베이스를 조사하여 필요하면 인증 및 암호화를 수행한다. 보안 매니저가 L2CAP에 접근 승인을 허용하면 L2CAP은 연결설정을 계속 수행하는 것을 보여주고 있다.

Ⅴ. 결 론

본 논문에서는 많이 사용하는 통신기술인 블루투스가 어떤 것인가의 소개와 블루투스 해킹 3가지 방법들 가운데 블루투스 스나핑을 설명하며, 그것에 대한 보안측면을 조사해 보았다. 위와 같이 블루투스 통신은 아직 사용자들이 안심할 정도의 안전이 완벽한 것이 아니며, 블루투스 사용자들의 블루투스를 이용하면서 블루투스 통신에 대해 더 쉽게 이해하고, 그리고 블루투스 통신망의 위험성을 가상시나리오와 함께 알려주었으며, 또한 블루투스의 보안측면에 어떤 것이 있는지 불루투스 이용자들에게 알기 쉽게 말하고 싶은 바이다.

참고문헌

[1] 강동호, 백광호, 김기영, 블루투스 보안기술, 주간기술동향 통권1380호, page 4~5, page 11, 2009.01.21.

[2] JOSE A. GUTIERREZ저, 이원준, 이춘화(공역), 저속WPAN_IEEE_802.15.4센서네트워크, 홍릉과학출판사, chapter1 page5, 2005

[3] blackcon, 블루투스 이어셋(해드폰) 해킹, Hello, Stranger :D, 2013.08.14. , http://blackcon.tistory.com/50