情 報 保 護 學 會 誌
第 11 券 第 4 號, 2001. 8

Bluetooth Security에 관한 고찰

서 대 희*, 이 임 영*, 김 해 숙**, 김 영 백**

요 약

무선 인터넷 서비스가 국내외적으로 크게 발전하고 있으며 머지않아 무선 통신이 일반화될 것이라는 전망이 나오고 있다. 그러나 무선 인터넷이 보다 활성화되고 이를 활용하기 위해서는 보안기술의 적용이 필수적이다.

본 고에서는 자유롭고, 안전하며, 신뢰성 있는 무선통신의 기술에서 필수적인 근거리 무선 통신 기술의 표준으로 자리잡고 있는 Bluetooth에 대한 표준화 동향 및 자체 제공되고 있는 보안 서비스에 대한 취약점을 분석하였다.

이는 보안 서비스의 취약점을 제시함으로써 국내 무선 인터넷 기술의 발전과 Bluetooth 응용 서비스를 활성화시키는데 기여하기 위함이다.

Ⅰ. 서 론

무선통신 기술이 급속도로 발전하는 가운데 휴대폰을 통한 인터넷 접속 기술은 완성 단계에 이르렀으나, 컴퓨터와 컴퓨터 주변기기 그리고 PC와 PC의 연결을 위한 단거리 무선 통신 기술이 필요하게 되었다. 그러나 무선 통신 기술은 무선이라는 통신 환경이기 때문에 얻은 장점이 있는 반면에 유선에 비해 보안상으로 매우 취약한 면을 보이고 있다.

본 연구에서는 최근 근거리 무선 통신의 표준으로 주목을 받고 있는 Bluetooth의 개요와 표준안에 대해 알아보고, 제공하고 있는 보안에 대해 검토하고자 한다. 또한, Bluetooth가 제공하고 있는 보안 서비스를 실제로 Ad-hoc네트워크나 홈네트워크에 적용하였을 경우 많은 취약점이 문제시 되고 있다. 이에 따라서 본 연구에서는 Bluetooth가 가지는 자체적인 보안 서비스의 취약점과 실제 다른 네트워크에 적용했을 때 나타나는 취약점도 함께 분석하고자 한다.

Ⅱ. Bluetooth 개요

최근 Bluetooth라는 말을 자주 듣게 된다. 우리나라말로 해석하면 '푸른 이빨'이란 뜻으로 해석되는 Bluetooth는 스칸디나비아 국가인 덴마크와 노르웨이를 통일한 바이킹 해럴드에서 유래되었다.

Bluetooth는 최초 스웨덴의 에릭슨이라는 회사에서 무선 근거리 통신을 위해 저전력, 저비용으로 무선 인터페이스를 가능하게 하기 위한 기술로서 시작된 프로젝트 이름이었다. 후에 이러한 프로젝트명을 바꿀려고도 하였으나 프로젝트의 이름이 현재의 이름으로 굳어졌다. 이에 따라 Bluetooth에 관심을 갖는 회사들은 1998년 5월에 무선 근거리 통신을 위한 하나의 프로젝트 개발을 위해 결성되었다. 이러한 그룹은 기존 케이블로 연결된 셀룰러 전화기를 통해서 셀룰러 망에 연결된 다중 통신을 조사하고자 하였으며 이것이 SIG(Special Interest Group)라는 이름으로 시작된 최초의 모임이다.[1][2]

Bluetooth 이전에도 IrDA, IEEE802.11, SWAP와 같은 무선 근거리 무선통신들이 많이 등장하였다. 그러나 Bluetooth가 주목받고 있는 이유는 여러 가지 들 수 있는데 우선 기업 측면에서는 대량 출하수량을 통해 전세계적으로 판매할 수 있다는 점을 들 수 있으며 저가격으로 제조할 수 있다는 장점을 가지고 서로의 상호작용을 일으켜 부품에 대한 저가격화가 가능하고 이에 따라 출하수량이 늘어

본 연구는 한국정보보호진흥원의 정보보호 기반구축 지원 사업의 일환으로 수행하였습니다.
* 순천향대학교 정보기술공학부 (patima@sec-cse.sch.ac.kr)
** 한국 정보보호 진흥원

나는 상승효과를 가져다주고 있다. 또한 사용자 측면에서는 적은 소모 전력으로 휴대폰이나 기타 주변 장치들의 무선 연결을 통해 선이 없는 인터페이스를 이루므로 보다 간편하고 효율적인 측면에서 사용자에게 다가서고 있다. 전체적으로 살펴보았을 때 Bluetooth가 주목받는 이유를 살펴보자면 정보통신 산업이 무엇을 위해 발전하였는가를 살펴보면 쉽게 알아볼 수 있다. 이는 보다 자유롭고, 안전하며, 신뢰성과 최근 급부상하고 있는 인터넷의 확장과 더불어 발전하고 있는 것이며 이를 만족하기 위해 제안된 기술이 Bluetooth라 볼 수 있다. Bluetooth를 간단히 정의한다면 근거리 무선 통신을 위한 하나의 기술이다. 중요한 것은 사용자의 요구에서 발생한 기술이라는 점이다. 이는 Bluetooth가 가져야 하는 여러 가지 특징 중에서 어쩌면 가장 중요한 특징이라고 할 수 있다.

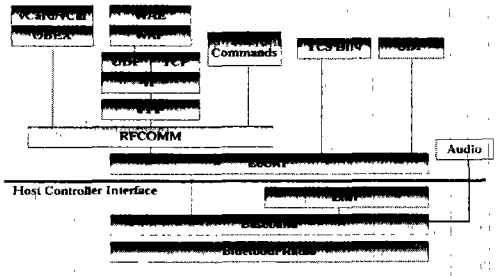
Bluetooth는 전 세계적으로 사용이 가능하며 허가가 필요 없는 무선 대역인 2.4GHz~2.5GHz 대역에서 운용되고 있으며 특징을 정리하면 다음과 같다.

- 1Mbps의 전송속도 (실제 723kbps)
- 대기상태 0.3mA, 송수신시 최대 30mA
- 전송거리 10M(2003년까지 100M까지 확장)
- 각 상태별 송신전력의 구분
- GFSK (Guassian Frequency Shift Keying) 변조방식
- FHSS (Frequency Hop Spread Spectrum) 사용

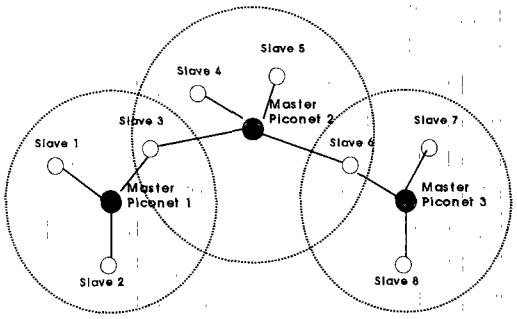
또한, Bluetooth는 자체적으로 보안 서비스를 제공해주고 있다. 이러한 보안 서비스는 각 장치에 적당한 보안 기능을 제공하며 주요 기능은 다음과 같다.

- 인증을 위한 Challenge-Response
- 암호화를 위한 스트림 암호
- 임의의 시간에 변경이 가능한 세션키의 생성

Bluetooth의 또 다른 특징의 하나는 하나의 작은 네트워크의 구성이 가능하다는 것이다. 이는 피코넷이라 불리우며 하나의 피코넷에는 2개에서 최대 7개까지의 슬레이브가 가능하다. 이러한 피코넷이 여러개가 모여 서로 연결되어 있을 때 이를 스카터넷(Scatternet)이라 한다. 결국 이러한 피코넷은 여러 통신장비를 하나의 통신 네트워크로 묶을 수 있다는 장점이 된다. 그림 1은 일반적인 Bluetooth 구조를 나타내는 그림이며 그림 2는 Bluetooth의 피코넷과 스카터넷의 관계를 잘 보여주고 있다.[1][2][3]



〔그림 1〕 Bluetooth 구조



〔그림 2〕 피코넷과 스카터넷

Ⅲ. Bluetooth 표준안 요약

1. Bluetooth SIG

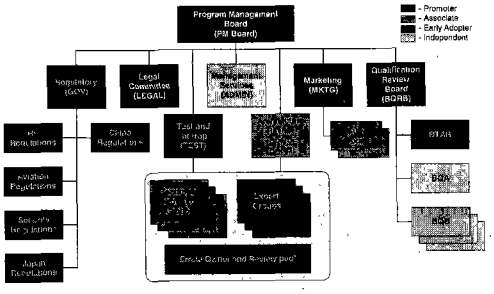
Bluetooth Special Interest Group은 Bluetooth 개발을 이끌 통신과 컴퓨터 산업분야의 회사들간의 컨소시엄이다. 1998년 5월 Bluetooth 기술 개발을 위해 결성된 Bluetooth SIG는 에릭슨, 인텔, IBM, 노키아, 도시바 등 5개사로 시작한 후 1999년 12월에 모토로라, 마이크로소프트, 루슨트테크놀로지, 3COM등 4개사가 추가로 프로모터 그룹에 가입하였다.

이 컨소시엄은 Bluetooth 기술을 하나의 규격으로 발전시키기 위해 각자의 핵심역량을 연계시켰다. 현재 9개사가 Bluetooth SIG에 소속되어 있으며 전체 회원사의 숫자는 2천개 이상에 달한다. 지금까

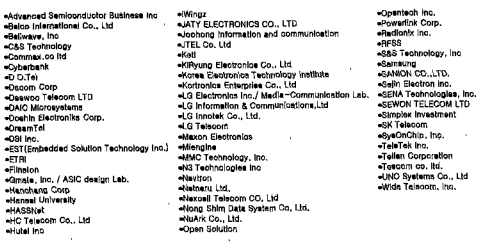
지 참여 업체는 지속적으로 확산되고 있는 추세이며, 특히 99년 마이크로소프트의 SIG 가입은 특별한 의미를 가지고 있다. 유사한 근거리 무선 데이터 통신 기술인 IrDA가 마이크로소프트의 윈도우95에 탑재됨으로써 급속한 사용확산을 이룬 사례를 염두에 둘 필요가 있다. 세계 OS 시장의 대부분을 점유하고 있는 MS의 영향력을 통해 Bluetooth가 세계 표준으로 자리잡을 가능성이 한층 높아진 것이다.

현재 Bluetooth 기술을 적용하는데 관심이 있는 조직이나 업체는 Bluetooth 어댑터(Bluetooth adopter)합의서에 사인을 함으로써 회원사로 참여할 수 있다. SIG의 회원사(adopter 또는 non-founding SIG회원사)는 Bluetooth 기술을 기반으로 하는 제품 개발에 로열티 없는 라이센스의 자격을 갖게 되며, Bluetooth 관련 제품을 개발한 회사는 Bluetooth SIG의 인증을 받아 Bluetooth 마크를 부착함으로써 세계적으로 공인된 Bluetooth 제품으로 판매할 수 있다.

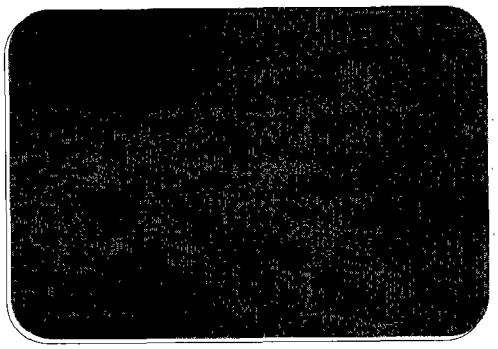
현재까지는 이러한 인증에 대한 정확한 절차나 기준이 정해져 있지 않은 상태이지만 올해 말까지는 인증 제도에 대한 사항이 결정될 것으로 예상된다. 국내에서 Bluetooth SIG에 가입한 회사는 3월 현재 46개사나 된다. 정부기관으로 ETRI, KETI 등이, 대기업으로는 LG, 삼성, 현대, 대우 그리고 정보통신기기 관련 업체 및 대학교들이다.



〔그림 3〕 현재 Bluetooth SIG 구성



〔그림 4〕 국내 Bluetooth 관련 개발 업체



〔그림 5〕 Bluetooth 응용분야 프로파일 워킹 그룹

또한, SIG에서는 Bluetooth를 기초로 해서 새로운 응용 분야를 위한 프로파일을 만들기 위해 다음과 같은 12개의 새로운 워킹 그룹이 만들어 졌다.[1][4]

2. SIG그룹의 Bluetooth 표준화 동향 고찰

SIG는 3Com, Ericsson, IBM, Intel, Lucent, Microsoft, Motorola, Nokia 및 Toshiba와 같은 각 분야의 선두 업체들과 188.2 채택/연관 업체들로 구성되어 있는데, 98년 10월말 200개 회원사에서 회원사 수가 현재 2,800여 개로 계속 증가 추세에 있다. 99년 8월에 Bluetooth 스펙 버전 1.0 규격이 발표되어 사실상 표준으로서, 관련 업체들은 핵심 부품을 비롯한 소프트웨어 개발 키트 등의 제품 출시 등을 통해 지속적인 증가 추세를 보이고 있을 뿐만 아니라 2000년 12월에 발표된 1.1는 99년 8월에 발표된 1.0 규격을 보안하였으며 12월에는 이를 업그레이드한 1.0B 버전을 추가로 공개했다. 현재는 2000년 12월에 공개한 1.1 버전이 스펙으로 제시되고 있으며 올해 중반경에 버전 2.0을 공개할 예정이다.

Bluetooth 관련 국제적인 공식 표준을 정하는 단체는 IEEE 802 LAN/MAN Standards Committee이다. 현재 IEEE 802.15에서는 Bluetooth를 이용하여 물리 계층 및 데이터링크 계층을 통한 PAN의 표준화 작업이 진행중에 있으며, 현재 Bluetooth 표준화의 쟁점은 다음과 같이 3가지로 요약된다.

- IEEE 802.15 Working group의 표준화 영역은 물리계층 및 MAC계층에 국한되지만, SIG는 SAPs(Service Access Points) 및 PICS(Protocol Implementation Conformance)를 포함해야 한다고 논의되고 있다.

- 802.11 WLAN과 같이 2.4GHz 대역에서 작동하는 IEEE802 표준 계열과 Bluetooth 또는 근거리무선네트웍이 공존할 수 있는 바람직한 방법에 대하여 논의되고 있다.
- 화상정보의 고속 통신이 가능한 차세대 고속 Bluetooth 표준에 대하여 논의되고 있다.
- 차세대 고속 Bluetooth 표준은 2.4GHz 대역에서 Bluetooth1.1 기술과 호환되는 2-10 Mbps급 Bluetooth2 기술 개발 및 2.4 또는 5GHz 대역에서 Bluetooth1 및 Bluetooth2 기술들과 호환되는 20Mbps급 Bluetooth3 기반 기술 개발이 진행되고 있다.

Bluetooth 표준은 Bluetooth의 기술개발, 시장 형성을 위해 구성된 통신, 컴퓨터, 네트웍 관련 유수 회사들의 협력체 SIG(Special Interest Group)에 의해 사실상 표준안 마련되었고 SIG와 IEEE802.15의 협력으로 국제 표준을 정하고 있다.

Bluetooth의 특징은 SIG 가입 회사간에는 Bluetooth 기술이 open license이어서 가입 회사수가 급증하고 있어 그 기술 발전 속도가 매우 빠르며, 시장 형성 속도도 빠르다는 것이다. 이는 사용자의 현재 욕구인 양방향 실시간 근거리무선통신을 가장 빠른 시일내에, 가장 저렴하게 제공할 수 있다는 Bluetooth의 장점에 기인한다. 즉, Bluetooth 사용자의 현재 욕구를 사실상표준에 근거하여 저렴하게 만족시킬 수 있을 뿐만 아니라, 가까운 미래의 사용자 요구에 비추어 성능 및 가격 측면에서도 큰 장점을 가지고 있다.[1][4][5]

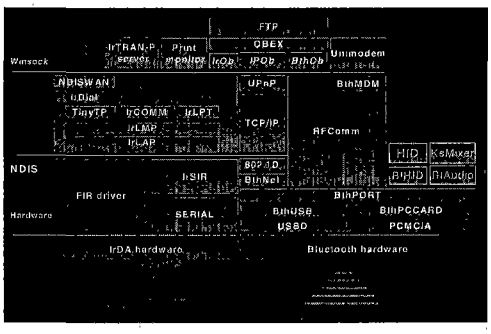
3. IrDA, 무선 LAN, Bluetooth간의 비교

근거리 무선 통신에서 사용되는 대표적인 기술은 Bluetooth를 비롯해 IEEE802.11, 홈RF 및 IrDA 등이 있으나, 특히 Bluetooth가 주목받고 있는 이유는 다음과 같다.

첫째, 대량 생산을 기대할 수 있다는 점이다. 이것은 세계적인 휴대전화 메이커들이 모두 채용을 포명하고 있다는 것이 크게 작용하는데, 특히 세계 휴대시장의 40% 이상을 장악하고 있는 에릭슨과 노키아가 적극적으로 탑재할 것임을 밝혀 Bluetooth 관련 부품 메이커 입장에서는 단기간에 수천만 대 규모의 시장을 기대할 수 있다. IEEE802.11이나 홈RF의 경우는 이와 많은 차이를 보이는데, 예를 들어 홈RF는 가정내의 PC나 무선 전화 등으로 방향을 잡고 있기 때문에 Bluetooth가 목표로 하는 시장과 분명히 달라 홈RF가 휴대전화기에 탑재되는 일은 있을 수 없다고 사료된다.

둘째로, 전세계를 대상으로 판매가 가능하다. 이것은 2.4GHz대의 ISM를 사용함으로써 거의 전세계 공통으로 사용할 수 있는 송수신 모듈을 제조할 수 있기 때문이다.

셋째, 저가격으로 제조할 수 있다. 이것은 Bluetooth 인터페이스를 2001년에는 CMOS LSI로 한 개의 칩화를 실현할 수 있다는 뜻이다. 그 이유는 Bluetooth 인터페이스 LSI의 설계 조건이 IEEE802.11이나 홈RF만큼 엄격하지 않아 전송 거리를 10m로 할 경우 IEEE802.11이나 홈RF에서는 필수적인 전력 공급 기기가 Bluetooth에서는 필요 없으며 이로 인해 저소비 전력화가 가능하다. 그림 6은 Bluetooth의 Architecture를 비교한 그림이며, 표 1은 Bluetooth 경쟁 대안간의 비교를 나타낸 것이다.[1][2][5][6]



〔그림 6〕 IrDA/Bluetooth Architecture

〔표 1〕 IrDA/무선 LAN/Bluetooth의 비교

비교 \ 무선	Bluetooth	IEEE802.11	SWAP	IrDA
최대 전송속도	1Mbps	2Mbps	0.8Mbps, 1.6Mbps	4Mbps
이용대역	2.4GHz	2.4GHz	2.4GHz	2.4GHz
변조방식	FHSS (호핑횟수:1600회/초)	DS 및 FHSS	FHSS (호핑횟수: 50회/초)	4단계 PPM/16단계 PPM)
음성채널	있다	없다	있다	없다
트래픽	음성, 데이터	데이터	음성,데이터	데이터
모듈 가격	5달러(예정)	미정	25달러(예정)	200~300엔
최대전송 거리	10m(1mW, 0dBm) 100m(100mW+ 20dBm)	100m(802.11의 경우에는 30m)	50m	3.8m
최대 소비전력	데이터 송신 30mA 대기 0.3mA	최대1W정도	미공개	수 mA
1차 변조방식	GFSK	BPSK/QPSK 및 GFSK	GFSK	상기
접속 제어방식	없다	CSMA/CA	CSMA/CA TDMA	없다
보안	표준(검증,암호화)	선택	표준(암호화)	없다

Ⅳ. Bluetooth Security 검토

이 장에서는 Bluetooth에서 자체 제공되고 있는 보안 서비스에 대한 개요를 살펴보고 분석하고자 한다.

1. Bluetooth 보안 개요

사용자 보호와 정보 보안을 위해 시스템은 쌍방 환경에 적당한 보안 기능을 제공해야 한다. 즉, Bluetooth에서 각 유닛은 인증과 보안 알고리즘을 같은 방식으로 구현해야 한다.

기본적 수준의 보안이 정의되어 칩 구현에 적당하도록 될 것이고 인증 알고리즘은 처리 기능에 있어서 장치에 무리가 가지 않는 수준에서 제공될 것이다. 암호화 알고리즘에 대한 앞으로의 지원계획은 후방향 호환성(Backward Compatibilty)을 지원할 것이며, 제공되는 주요 보안 기능은 다음과 같다.[7]

- Challenge response routine for authentication
- Stream cipher for encryption
- Session key generation - session keys can be changed at any time during a connection

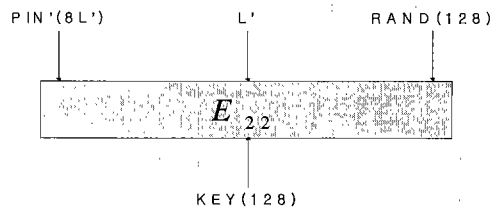
2. Bluetooth Security 분석

Bluetooth에서의 보안 서비스는 정보의 비밀성을 위해 응용 계층과 링크 계층에서 보안 수단을 제공한다. 일반적으로 응용 계층과 링크 계층에서의 보안 수단은 인증과 암호화가 이루어지며 동일한 루틴으로 이루어진다. 링크 계층의 보안 요소는 BD_ADDR, 링크 키, 암호 키, 난수로 이루어진다.

BD_ADDR은 48비트로 이루어지며 공개적으로 알려져 있는 주소이다. 링크키는 초기화 과정에서 생성되는 128비트 비밀키로서 Unit 키, 조합 키, 마스터 키, 초기화키로 이루어져 있으며, 암호 키는 8~128비트의 유동적인 크기를 가지게 된다. 이는 프라이버시에 대한 정부 및 정책에 따라서 유동성을 제공하기 위해서 이며 보안 업그레이드를 위해 유동적인 환경을 제공하는 이유이기도 한다. 마지막으로 난수가 발생되는데 이는 Bluetooth Unit내의 의사 난수 프로세서에 의해 생성되는데 이러한 난수는 링크키와 암호키 생성에 사용되어 진다.

링크 키는 인증과 암호키 생성시 비밀키로 사용되어지며 반영구적이거나 임시적으로 사용되어 진다. 반영구적으로 사용될 경우에는 비활성 메모리에 저장되어 현 세션이 끝나도 계속되어 사용되어지는 반면 임시적으로 사용될 경우에는 현 세션에서만 사용하게 된다. 링크 키의 종류에는 조합키 K_{AB}, Unit 키 K_A, 마스터 키 K_{master}, 초기화 키 K_{init} 등이 있다.

Unit 키 K_A는 각 Unit들이 소유하며 Unit에서 만들어지며 Unit 최초 동작시 생성되고 이후 거의 변화되지 않는다.



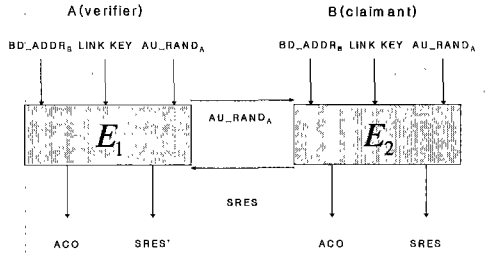
〔그림 7〕 초기화 키 생성

조합키 K_{AB}는 서로 다른 두 Unit의 정보로부터 생성되며 특성에 따라 링크키가 반영구적으로 사용할 수 있다. Master 키 K_{master}는 현 세션에서 사용되는 일시적인 링크키로서 Point-to-Multipoint 통신시에 사용 가능하며 초기화 키 K_{init}는 초기화 과정동안 링크키로 사용되며 두 Unit가 처음으로 링크를 설정할 때 수행되는 과정으로 인증과 링크키의 전송에 사용된다.

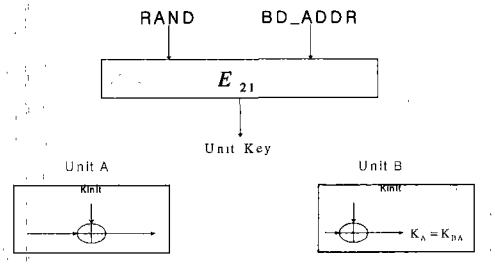
링크키 외의 보안 변수는 암호키 K_C와 PIN이 사용되어 지는데 암호키는 현재 링크키로부터 파생되며 매 세션마다 생성된다. PIN은 Bluetooth Unit내에 제공되는 고유번호로서 사용자가 임의 선택하거나 초기에 Unit에 주입되어진다. 처음 링크 설정시 두 Unit는 동일 PIN을 공유하게 되며 한쪽 Unit의 PIN을 다른쪽 Unit에 주입하거나 두 Unit에 새로운 PIN을 주입할 수 있으며, PIN은 보통 1~16 바이트로 선택할 수 있으며 보다 긴 길이의 PIN 코드로 변경이 가능하다. 이러한 보안 요소들을 분배하기 위해 Bluetooth는 응용 계층에서 Diffie-Hellman 방식을 이용해서 제공된다. 프로토콜이 생성되는 초기화에서는 초기화키를 생성한 후 인증을 거쳐 링크키를 생성하고 링크키를 교환 후 암호키를 생성하는 과정으로 이루어진다. 초기화 키 생성에서는 일시적으로 사용되는 링크키로서 입력값은 신청 Unit의 BD_ADDR, PIN code, PIN 길이 입력,

검증 Unit 난수로 입력되어 진다. 생성되는 초기화 키는 이후 생성되는 링크키의 교환과 두 Unit에 링크키가 없을 때 인증에 사용되며 키의 교환이 끝나면 폐기된다.

Challenge-Response방식을 이용해서 이루어지는 인증은 서로 공유하고 있는 비밀키를 실제로 알고 있는지 확인하는 것을 이야기한다. 인증에서 사용되는 키는 링크키를 사용 두 Unit가 처음 접속하는 경우에 사용되며 인증키로 초기화키가 사용되어 진다. 인증의 검증 Unit에서는 자신이 생성하는 난수 AU_RAND를 신청 Unit에 전송하면 신청 Unit에서는 응답값인 SRES(Signed Response)를 전송하게 된다. 이는 마스터가 결정하게 되는데 마스터의 결정은 양자간 아무가 가능하며, 응용에 따라 결정하게 된다. 이러한 응용에 따라 일방향 또는 상호 인증 수행하게 되는데 상호 인증인 경우에는 양자 모두 난수를 생성하고 교류하여 확인한다. ACO(Authenticated Ciphering Offset)는 암호키 생성에 사용되기 위해 저장된다.



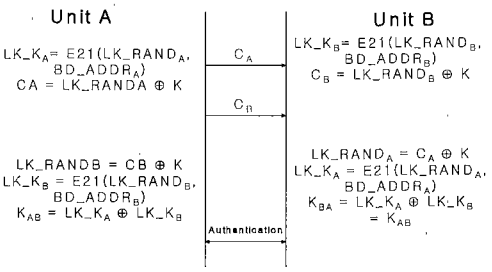
〔그림 8〕 인증 절차



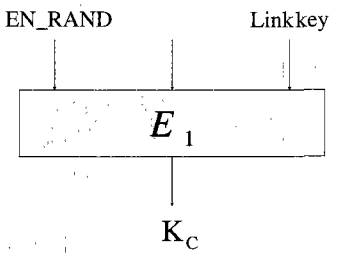
〔그림 9〕 Unit 키 생성과 분배

Unit 키는 Unit가 처음 동작할 때 생성되며 E21 알고리즘에 의해 생성되며 한번 생성되면 비활성 메모리에 저장되어 반영구 비밀키로 사용된다. 두 Unit 중 어느 Unit의 키를 링크키로 사용할 것인지를 결정하게 되는데 일반적으로 제한된 메모리 용량일 지닌 Unit의 Unit 키가 사용된다.

조합키는 링크키로 조합키의 사용이 요구될 경우 초기화 절차중에 생성되며 Unit A와 Unit B에서 생성되는 난수의 조합으로 되며 E21 알고리즘을 이용하여 두 개의 난수가 생성되면 Unit A와 Unit B에 이를 전송하고 랜덤수를 확인 후 동일한 조합키를 생성하게 된다. 암호키는 현재의 링크키, 96비트 COF(Cipher Offset Number), 128비트 난수를 이용하여 E3 알고리즘으로 암호키를 생성한다. COF 생성은 현재 링크키가 마스터키이면 마스터의 BD_ADDR로부터 생성되며 그렇지 않을 경우에는 인증 절차에서 계산되는 ACO값으로 설정되며 암호키는 암호 모드 사용시 매번 자동적으로 바뀌게 된다.



〔그림 10〕 조합키 생성 절차

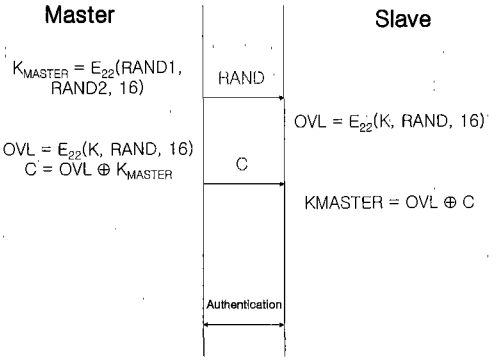


〔그림 11〕 암호키 생성

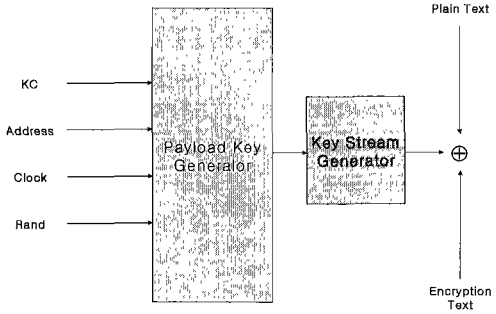
마스터키 생성은 E22 알고리즘을 사용하여 생성된다 마스터는 새로운 난수를 생성하여 슬레이브로 전송하며 마스터와 슬레이브는 E22 알고리즘을 이용하여 128비트 OVR을 생성하게 된다. 이때 마스터는 K_{master}와 OVR을 XOR한 다음 이 값을 슬레이브로 전송하게 되며 슬레이브는 전송된 값과 OVR을 XOR하여 K_{master}를 생성하게 된다. 암호키는 K_C 생성후 메시지 암호화를 통해 인증된다.

Bluetooth에서 암호화는 E0라는 스트림 암호를 사용하게 되는데 3부분으로 구성되어 있으며 키 생

성 부분, 키 스트림 비트 생성, 암호화 및 복호화로 이루어져 있다.[7][8][9]



〔그림 12〕 마스터키 생성 절차



〔그림 13〕 암호화 알고리즘 E0의 구조

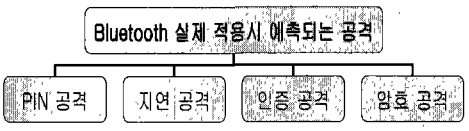
V. Bluetooth 취약점 분석

Bluetooth가 가지는 취약점은 기술내역서 자체가 가지는 취약점과 실제 Bluetooth를 적용하였을 때 나타나는 취약점으로 구분하여 볼 수 있으며, 기술내역서에서 나타나는 자체 취약성은 다음과 같다.

〔그림 14〕 Security Weakness in Bluetooth

1. Bluetooth를 실제 적용시 예측되는 공격

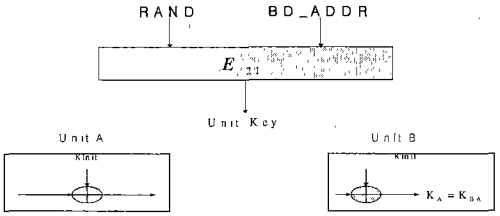
Bluetooth를 실제 적용 하였을때 그림 15와 같은 4가지의 예측되는 공격이 이루어 질 수 있다.



〔그림 15〕 실제 공격시 예측되는 공격

1.1 암호화된 디바이스간의 통신을 도청하거나 PIN의 공격을 통한 공격

일반적으로 Bluetooth를 통해 당사자들이 중요한 통신을 하기 위해 상호간이 동의하에 암호화된 통신이 이루어진다. Bluetooth의 취약점은 디바이스들이 한 쌍이 되는 동안에 교환된 메시지들에 대한 도청을 할 수 있다는 것이다. 즉, Bluetooth 계층에서 응용 프로그램 계층에서의 암호화가 수행되지 않으면 공격자는 Man-in-the-middle-attack이 가능하다는 것이다.



〔그림 16〕 유닛 키 생성과정

Bluetooth 디바이스들 사이에 이루어지는 첫 번째 프로토콜은 중요한 정보의 교환을 이루는데 만약 첫 번째 프로토콜에서 사용될 정보를 얻지 못할 경우 두 번째 프로토콜이 실행된다. 첫 번째 프로토콜의 목적은 키들을 한정된 메모리의 자원을 가진 디바이스에 저장하기 위해서이다. 첫 번째 프로토콜의 목적이 이루어지지 않을 때 두 번째 프로토콜이 실시된다. 두 번째 프로토콜은 장치들 사이에 서로 다른 링크키로 첫 번째 과정을 재 실시하는데 이는 PIN 번호와 번지를 생성하여 이루어진다. 그러나 PIN의 코드가 8~128비트로 이루어짐에도 불구하고 사용하지 않는 값을 0으로 채우는 것에 대한 취약점을 보이고 있다.

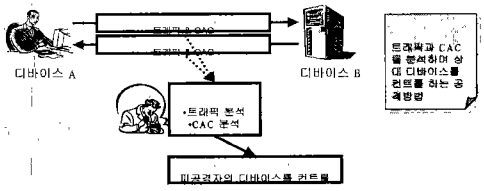
첫 번째로 K_a를 이용하여 A-B 간의 연결을 위한 링크키로 사용하게 되며 유닛 A로 K_a를 전성하게 되며 유닛 B는 K_a를 링크키로 K_{BA}로 저장하게 된다. 이때 초기화 키 K_{ini}는 K_a보호용으로 사용되고

폐기된다.

일단 공격자는 디바이스가 생성할만한 난수를 임의로 생성하여 링크 키를 계산한다. 이는 공격자가 디바이스 사이에 이루어지는 정보를 도청하게 된다면 송신 디바이스와 수신 디바이스 어느 것이든 위장이 가능하다. 만약, 공격자가 디바이스의 유닛 키를 알고 있다면 이것 역시 공격자의 위장이 가능하다고 추정할 수 있다.

1.2 지역 공격

공격자가 Bluetooth 디바이스를 이용하여 모든 디바이스간의 통신이 가능한 공격을 이야기한다. 즉, 공격자가 피공격자의 디바이스를 컨트롤하는 것이다. 이것은 피공격자의 디바이스가 일단 응답하면 공격자는 그 디바이스를 자신이 만든 임의의 디바이스를 통해 컨트롤을 할 수 있다는 것이다. 이러한 공격을 지역 공격이라고 볼 수 있는데 이는 디바이스간의 관계성에 기반을 두고 네트워크 트래픽을 가로채거나 CAC을 가로채는 공격이 이루어질 수 있다. 실제적으로는 주로 피코넷의 디바이스를 식별하기 위하여 공격자는 이러한 공격을 실시한다. 지역 공격은 보통 응용계층에서 이루어지며 적당하지 않는 소프트웨어를 컨트롤하여 Bluetooth의 디바이스를 공격하는 공격으로 중요하게 이루어진다.



〔그림 17〕 지역 공격

1.3 인 증

Bluetooth는 Challenge-Response 인증 방식을 이용하는데 이는 서로 공유하고 있는 비밀키를 실제로 알고 있는지 확인하는 방식으로 Bluetooth에서는 링크키를 사용하게 된다. 두 디바이스는 처음 접속하는 경우에는 인증키로 초기화키를 사용하게 되는데 이는 처음에 검증 유닛은 자신이 생성한 난수를 신청한 유닛에 송신하게 되고 신청한 유닛은 응답값을 전송하게 된다. Bluetooth의 디바이스에서 피코넷에서 마스터를 결정할 때는 양자간에 아무나 가능하지만 이는 응용에 따라 결정하게 된다. 응용이란, 일방향 또는 상호인증을 이야기하며 상호인증의 경우에는 양자 모두 난수를 생성해 교류 및 확인하는 것을 이용한다.

공격자는 Bluetooth 디바이스에 대하여 특정한 일치를 수행하는 것이 아니라 확률론적으로 일치가 될만한 것에 대한 무작위적 공격을 준비한다.

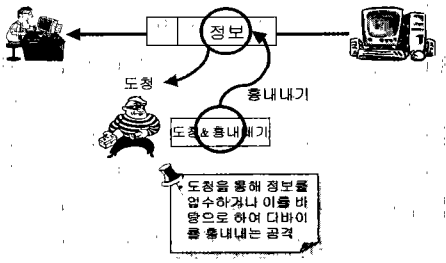
1.4 암 호

암호에 대한 취약성은 단순한 평문은 128비트로 되어 있어 2^{100}의 계산을 요구하는 보안 요소가 사용되는데 이는 이미 공격자로부터 공격당하기 쉬운 취약점을 보이고 있다고 알려져 있다. Bluetooth는 LFSR을 4번 이용하여 계산하는데 이는 결과값으로 가로채 분석하거나 유추하여 해독할 수 있을 뿐만 아니라 생일공격도 가능하다.

2. Bluetooth 기술 내역서 1.1의 취약성 분석

Bluetooth 기술 내역서에서 제공하고 있는 보안 서비스는 그림 18과 같은 취약성을 가지고 있다.

〔그림 18〕 기술내역서 1.1의 취약성 분석



〔그림 19〕 도청과 위장 공격

2.1 도청과 위장 공격

근본적으로 키 생성 프로토콜이나 키 생성에 대한 프로토콜로서 Bluetooth의 키 생성 방식은 난수와 PIN 그리고 Bluetooth 디바이스 주소를 이용하여 계산된다. 만약에, PIN이 유효하지 않거나 유닛간에 전송이 안된다면 공격자는 이를 쉽게 알아낼 수

있다. 이러한 취약점은 PIN의 길이를 충분히 길게 사용한다면 취약점을 보안할 수 있다.

2.2 오프라인 PIN의 취약점

두 디바이스간에 키를 수립하는 결정에 대한 도청적인 공격을 고려해 볼 수 있다. 이는 현재 Bluetooth 버전에서 유닛간의 키 교환 전에 PIN 번호를 결정지을 때 공격자가 공격할 수 있는 여지가 있다고 볼 수 있다. 이렇게 강탈한 PIN 번호에 대한 정보는 피공격자의 키를 유추할 수 있는 토대가 될 수 있다.

예) 도청과 같은 모든 PIN들에 대한 추측을 가정해 볼 수 있다. 키의 검증 단계에서 공격자는 계산되는 추측을 통하여 공격자 자체의 정확도를 검증하여 가장 정확한 예측을 확률론적으로 계산해 낼 수 있다.

공격자는 첫 번째 PIN을 추측하여 수행하고 있는 키에 대한 정보를 얻은 다음 부정하지 않는 정보를 흘려 피공격자의 디바이스가 동작하는 결과를 본 뒤 정확한 PIN에 대한 추측을 행할 수 있다. 이로 인해, 피공격자의 응답이 정확하다면 공격자는 공격자가 원하는 초기화키를 계산할 수 있게 된다. 초기키의 획득에 대한 문제는 검증 알고리즘의 문제이며 우리들은 일단 공격자가 Challenge-Response에 대한 쌍을 얻으면 이러한 공격이 수행되었다고 보는 것이 올바르다고 볼 수 있다.

2.3 지역 공격

Bluetooth가 사용하고 있는 주파수 호핑 방식에서는 다른 디바이스간에 의사 랜덤과 서로 다른 상태에서의 주파수를 사용하게 된다. Bluetooth 구조상으로 슬레이브는 마스터의 주파수를 확인하고 그에 대한 응답을 취하게 되며 그 다음에 슬레이브는 마스터의 시간적인 측면과 일치하는 의사 랜덤적인 주파수 호핑 순차를 확정하고 이것에 대한 일치성에 의해 슬레이브는 결과를 전송한다. 즉, 공격자는 지리적으로 분산되어 있는 디바이스들에 대한 응답에 대한 결과들을 통해 피공격자와 연결되어 있는 디바이스들을 대상으로 공격을 실시한다.

2.4 결합 공격

공격자가 시간적인 딜레이를 이용하여 디바이스를 추정하여 이루어지는 공격이다. 이는 주파수 도약의 순서를 이용하여 찾아 낼 수 있으며 대응 밴드들에 대해 트래픽의 분석이 이루어지면 더 큰 부분을 얻을 수도 있다.

2.5 암호 공격

공격자는 합산 레지스터와 2^{93}의 확률로 결과 값들을 유추해 낼 수 있다. Bluetooth에 대한 공격은 Goloc에 의해 제안된 공격이 이루어질 수도 있다. 이는 암호의 내부 상태들에 대하여 무작위적 선택을 통해 그에 대응하는 출력키를 얻어 key stream과 key stream간에 보안적 관계를 유추해 보는 공격 방법이다.

Ⅵ. 결 론

Bluetooth가 현재 각광 받고 있는 기술임에는 틀림이 없다. 근거리 무선 통신의 표준으로 자리 잡고 있는 Bluetooth는 개인의 무선 단말기를 이용 기존 유/무선망을 활용하는 신기술이다. 또한, 다른 근거리 무선 통신과는 달리 Bluetooth에서 제공되고 있는 자체 보안기능(키 관리, 암호화, 인증)등을 이용하여 높은 보안 기능을 필요로 하는 전자상거래와 같은 서비스와 활용할 수도 있다. 그러나 Bluetooth에서 자체 제공되고 있는 보안 기능은 현재까지 많은 취약성을 보이고 있다. 이러한 취약성이 실제 적용되었을 때 개인 사용자의 보안적인 안전성을 침해할 우려가 있을뿐만 아니라 유/무선을 이용하는 기존 및 새로운 네트워크에 적용시에 많은 보안적 취약점을 발생시킨다. 따라서 새로운 Bluetooth 표준안에서는 기존 표준안에서 가졌던 취약성을 보안하고 보다 안전하고 효율적인 보안 서비스를 제공해야 할 것이며, Bluetooth SIG 그룹에서는 기존 근거리 무선 통신과의 차별화를 위해 계속해서 보완하여 좀더 세분화된 표준을 발표할 것이다. 추후 IEEE802.15에서 추진중인 표준안과 SIG 그룹에서의 표준안이 하나로 통합되고 Chip에 대한 가격인하가 이루어진다면 Bluetooth는 쉽게 근거리 무선 통신의 표준으로 자리잡을 수 있을 것이다. 정책적인 측면에서 우리나라에서는 무선 LAN과 Bluetooth를 근거리 무선 통신의 규격으로 활용하고자 계획중에 있으며 관련 기관들의 연구가 진행중에 있다.

국내에서 개발중인 Bluetooth 제품들은 최근 개

최된 많은 IT 관련 홍보장에서도 단연 많은 관심을 끌었다. 그러나 이러한 국내 제품들은 Bluetooth에서 제공되는 자체 보안 서비스의 요구조건 조차 만족하지 못함으로써 차후 많은 개선할 사항의 여지가 있다. 이를 위해서 국내 실정에 적합한 Bluetooth 국내 규격안 마련과 함께 Bluetooth 보안 제품 개발을 위한 기초가 마련되어야 하겠다. 이를 위해서는 국제 표준안을 기반으로 국내 실정에 맞는 규격안 마련이 시급할 뿐만 아니라 국내 Bluetooth 개발 업체들 중에서 Bluetooth 보안 제품 업체들의 개발 방향을 제시할 수 있는 많은 연구가 진행되어야 할 것이다.

참 고 문 헌

[1] http://www.bluetooth.or.kr
[2] http://maso.zdnet.co.kr
[3] http://www.ketinrl.re.kr
[4] http://time.kotel.co.kr/s-tends/
[5] http://www.freechal.com/ktec/
[6] http://www.iseebank.com/home/start.asp
[7] http://www.bluetooth.com/developer/whitepaper/whitepaper.asp.
[8] http://www.korwin.net/com_lab/morgue.html.
[9] http://www.bluetooth.com/developer/specification/specification.asp.
[10] http://www.cs.hut.fi/Opinnot/Tik-86.174/sectopics.html. (Ullgren T.Security in Bluetooth: Key management in Bluetooth)
[11] http://www.bell-labs.com/user/markusj/bt.html. (Jakobsson M., Wetzel S. Security Weakness in Bluetooth: RSA 2001)
[12] http://www.homerf.org.
[13] http://bluetooth.ericsson.se.
[14] http://www.wireless.com.
[15] http://www.intel.com/mobile/bluetooth.
[16] http://www.irda.org.
[17] Proc. of '00 Bluetooth Developers Conference, San Jose.
[18] 김홍기, "단거리 무선통신 Bluetooth 기술 표준 및 동향분석" 한국 정보처리학회지 제 7권, 제3호, 2000년 5월.
[19] "Bluetooth SIG Conference Technical report" 1999.
[20] 최용락, 소우영, 이재광, 이임영 "통신망 정보 보호", 도서출판 그린, 1997.2.
[21] 이만영, 김지홍, 류재철, 송유진, 염흥렬, 이임영 "전자상거래 보안 기술", 생능출판사 1999.8.
[22] 최용락, 소우영, 이재광, 이임영 "컴퓨터 통신 보안", 도서출판 그린, 2001.2
[23] Alfred J. Menezes, Paul C.van Oorschot, Scott A. Vanstone "HANDBOOK of APPLYED CRYPTOGRAPHY", CRC, 1996.11.

〈著 者 紹 介〉

서 대 희 (Dae-Hee Seo)
학생회원
2001년 2월 : 동신대학교 전기 전자공학부(학사)
2001년 3월~현재 : 순천향대학교 전산학과 석사과정
관심분야 : 암호 이론, 컴퓨터 보안

이 임 영 (Im-Yeong Lee)
정회원
1981년 8월 : 홍익대학교 전자공학과 졸업
1986년 3월 : 오사카대학 통신공학과 석사
1989년 3월 : 오사카대학 통신공학과 박사
1989년 1월~1994년 2월 : 한국전자통신연구원 선임연구원
1994년 3월~현재 : 순천향대학교 정보기술공학부 부교수
2001년 3월~현재 : 순천향대학교 전자상거래 S/W 연구센터 센터장
관심분야 : 암호이론, 정보이론, 컴퓨터 보안

김 해 숙 (Hae-suk Kim) 정회원
1994년 2월 : 경희대학교 수학과 졸업
1996년 2월 : 포항공과대학교 수학과 졸업(석사)
2000년 2월 : 포항공과대학교 수학과 졸업(박사)
2000년 3월~12월 : 포항공과대학교 전산수학연구센터 박사후 연구원

2000년 12월~현재 : 한국정보보호진흥원 선임연구원
관심분야 : 정보보호

김 영 백 (Young-Baek Kim)
정회원

1995년 2월 : 순천향대학교 정보통신공학과 졸업
1997년 2월 : 순천향대학교 정보통신공학과 석사
1996년 12월~2000년 3월 : 한전KDN
2000년 4월~현재 : 한국정보보호진흥원
관심분야 : 정보보호