모바일 환경에서 블루투스를 위한 비대칭 암호기반의 개선된 상호인증 기법

이대섭*, 박태성**, 전문석*
*숭실대학교 컴퓨터학과
glittering87@naver.com

Improved Mutual Authentication Scheme based on Asymmetric Encryption under Mobile Environments

Dae-seop Lee *, Tae-Sung Park**, Moon-Seog Jun*
*Dept of Computer Science, Soongsil University

요 약

블루투스(Bluetooth)는 별도의 인증 기관 없이 각 디바이스간의 독립적인 인증과정을 통해 데이터를 서로 전송하는 기술을 사용하고 있다. 바로 이러한 특징 때문에 인증 기반 기관을 이용한 네트워크에서 발생하는 문제점과는 다른 특징을 가진 문제점들이 나타날 수 있으며, 그 외에도 부인방지나 무결성이 제공되지 않아 스마트단말기의 경우 많은 취약점이 될 수가 있다. 본 논문에서는 이러한 블루투스 암호화 인증과정의 취약점을 보완하고자 비대칭키 암호화기법을 활용한 전자서명기법과 대칭키 암호화기법을 사용하여 향상된 블루투스 암호화 인증과정을 제안한다.

1. 서론

무선통신 기술이 급속도로 발전하는 가운데 휴대폰을 통한 인터넷 접속 기술은 완성단계에 이르렀다 할 수 있으나, 컴퓨터와 컴퓨터 주변기기 그리고 PC와 PC의 견결을 위한 단거리 무선 통신 기술이 필요하게 되었다. 그러나 무선 통신 기술은 무선이라는 통신 환경이기 때문에 장점이 있는 반면에 유선에 비해 보안상으로 매우 취약한 면을 보이고 있다.

본 연구에서는 최근 근거리 무선 통신의 표준으로 주목을 받고 있는 블루투스의 개요 대해 알아보고 제안하고자 하는 블루투스의 취약점을 보완한 기법에 대해 알아보고자 한다.

블루투스(Bluetooth)란 이동전화, PDA같은 이동가능한 소형 장치들간의 양방향 근거리 통신을 가능하게 해주는 기술이자 근거리에 놓여 있는 컴퓨터와 이동단말기, 가전제품 등을 무선으로 연결하여 쌍방간에 실시간 통신을 가능하게 해주는 규격을 말하거나 그 규격에 맞는 제품을 이르는 말이다. 그러나 이 블루투스는 별도의 인증 기관 없이 각 디바이스간의 독립적인 인증에만 너무 치중한 나머지 기존 인증 기반 기관을 이용한 네트워크에서 발생하는 문제점과는 다른 특징의 문제점들이 나타난다.

블루투스 표준에는 다음과 같은 세 가지 기본 보안 서비스를 명시한다.

1)인증 : 의사소통할 장비의 신원을 확인, 사용자 인증은 기본적으로 블루투스에 제공되지 않는다.

2)기밀 : 오직 보내는 사람과 받는 사람만이 승인된 유일한 장치에 액세스하여 데이터를 열람할 수 있다.

3)권한부여 : 장치가 허용되기 전에 이 서비스를 사용할 권한을 보장하여 자원의 통제를 제공한다.

블루투스 감사 및 부인방지 같은 다른 보안 서비스가 제공되지 않는다. 이 외에도 여러 가지 취약점으로 인하여 블루투스의 향상된 보안이 필요하다. 본 논문에서는 이러한 블루투스의 취약점을 보완하기 위해 비대칭키 암호화 기법을 이용한 전자서명기법을 적용해 현 블루투스 통신에 보다 강력한 보안적 기법을 적용하고자 한다. 본 논문의 2장에서는 블루투스의 개요 및 관련연구, 3장에서는 제안하고자 하는 기법, 마지막으로 4장에서는 결론을 맺고자 한다.

2. 관련연구

2.1 블루투스의 개요

현재 무선 멀티미디어 시장에서 가장 주목을 받고 있는 것이 블루투스이다. 블루투스가 기존의 무선 통신장비에 비해서 더욱 곽광받는 이유는 통신기능이 없는 디바이스에 간단하고 작은 모듈을 첨가함으로써 서로 무선 네트워크로 연결을 할 수 있다는 점이다. 또한 연결 시 서로 무선통신을 할 수 있는 범위 안에만 있으면 연결이 쉽게 되므로 사용상의 간편함을 들 수 있다. 그러나 블루투스는 해결해야할 많은 문제점이 있다. 간단한 데이터 전송과 음성 전송만을 할 수 있지만, 화상회의 등 고속의 데이터

전송량을 필요로 하는 장소에서 사용하기 위해서는 데이터 전송량을 늘릴 수 있는 방법이 개발되어야 한다. 현재 많이 사용되고 있는 블루투스가 사용자 중심의 네트워크를 형성할 경우 여러 네트워크로의 확장이 가능하지만 이로 인해 발생되는 보안적인 문제점을 해결하지 않을 경우 새로운 형태로의 네트워크 환경에 적용하기엔 많은 어려움이 따른다.

본 논문에서는 블루투스의 보안적 취약점을 보완하고자 한다. 이러한 블루투스는 사양과 버전에 따라 총 4가지 보안모드를 정의한다. 전혀 안전하지 않은 보안 모드 1, 서비스 레벨 보안을 강화한 보안 모드 2,보안 모드 3은 링크 레벨 적용 보안모드이며, 보안 모드 4는 보안 절차를 링크한 후에 시작하는 보안 모드를 강제로 실행한다.

또한 보안 단순 페어링(SSP)는 ECDH 공개 키 암호화의 추가를 통해 수동 도청과 페어링 과정중 중간자 공격에 대한 보호를 위한 보안을 향상시킨다.[1]

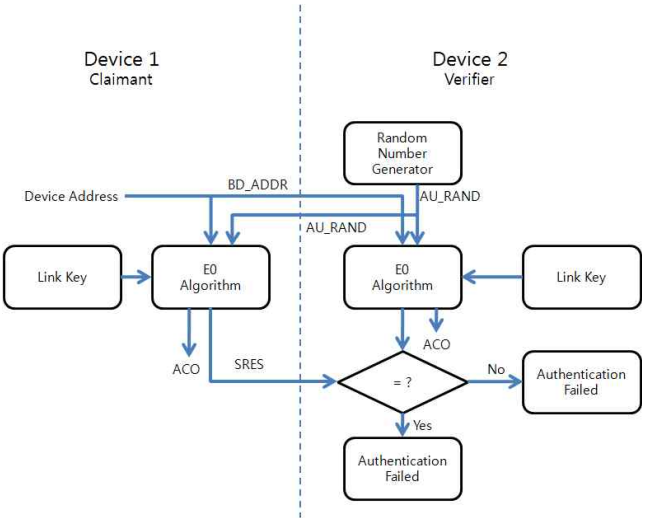
블루투스 디바이스는 숫자 비교 6자리 숫자를 표시하고 사용자가 “예” 또는 “아니오” 응답을 입력할 수 있게 설계되어있다. 페어링하는 동안, 사용자가 각 디스플레이에 6자리 숫자로 표시된다. 그리고 각 장치에 “예”라고 응답을 하면 제공하는 번호가 일치하는 경우, 그렇지 않으면 “아니오”와 페어링에 실패를 한다. 이 경우에도 표시되는 값이 링크 또는 암호화 키를 결정하기 위해 사용되지는 않는다. 또한 보안 모드는 4개의 블루투스 서비스가 요청 될 때, 보안이 전혀 인증이 안 된 링크키, 인증된 링크키 를 요구해야 한다.

2.2 인증

블루투스 장치 인증 절차는 challenge-response방식의 형태로 되어 있다. 각 장치가 인증 절차에 상호작용을 언급하는대로 수신자는 장치를 증명하는 시도는 장치 요청자의 신원을 확인한다.

Challenge-response 체계는 [그림 1]에 그려져 있다.

SK	Private Key
PK	Public Key
K	Secret Key
BD_ADDR	Device address
AU_RAND	Authentication randum number
SRES	Signed Response



[그림 1]

인증 프로세스의 단계는 다음과 같다.

1 단계 : Verifier가 128비트 임의의 요청을 (AU_RAND)한다

2 단계 : 자신의 고유한 48비트 블루투스 장치 주소 (BD_ADDR)를 사용하여 계산하는데 사용하는 링크 키인 AU_RAND 입력한다.

3 단계 : E1알고리즘을 통하여 Verifire로 계산된 32비트값을 산출한다.

4 단계 : Verifire가 그것이 계산된 값으로 Claimant의 SRES을 비교한다.

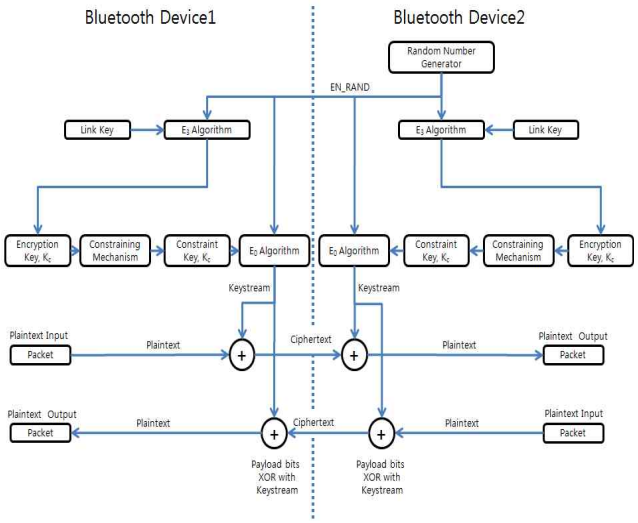
5 단계 : 이 두 32비트 값이 같은 경우에는 인증이 성공적으로 간주된다. 2개의 32비트 값이 동일하지 않으면 인증이 실패한다.

이와 같은 단계를 수행하면 단방향 인증을 수행, 블루투스 표준은 모두 편도와 상호 인증을 수행할 수 있다.

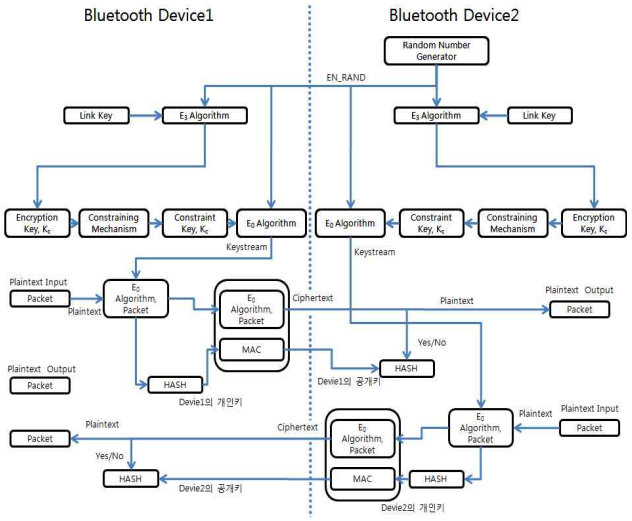
3. 제안

3.1 기존 블루투스 암호화 과정

아래 [그림 2]은 기존의 블루투스 암호화 과정을 그린 것이다. [그림 2]에 표시된 바와 같이, 암호화 키는 암호화 알고리즘으로 내부 키 생성기를 사용하여 생산한다. ACO 값의 스트림 암호 키는 비밀로되는 블루투스 장치, 128비트 난수와 96비트 ACO값에서 개최되는 128비트 링크 키를 기반으로 생산한다. [그림 1]에서 보는 바와 같이 ACO는 인증 절차 중에 생성되어 있다.



[그림 2]



[그림 3]

블루투스 암호화 절차는 스트림 암호에 E0를 기반으로 한다. 키 스트림 출력 단독 또는 페이로드 비트를 수신 장치로 전송하고 이 키는 스트림 암호화 알고리즘을 선형 피드백 쉬프트 레지스터를 기반으로 사용하여 생산한다. 암호화 함수는 입력으로 아래로 이동한다. 마스터ID(BD_ADDR), 128비트 난수(EN_RAND), 슬롯 번호, 그리고 결합된 각 패킷의 전송 전에 LFSRs를 초기화 암호화키, 암호화가 활성화되어 있는지 확인한다. 슬롯번호는 각 패킷과 스트림 암호 변경에 사용하고, 나머지 변수는 정적 유지하고 있다가 암호엔진 또한 각 패킷으로 초기화 된다.

3.2 제안하는 블루투스 인증 과정

기존의 블루투스는 서로 상호인증만을 전적으로 신뢰할 뿐만 아니라 처음에 상호인증이 이루어지면 재연결을 할 경우 재인증과정이 이루어지지 않는다. 또한 부인방지나 무결성에 관한 보안인증이 이루어지지 않는다. 본 논문에서는 블루투스의 부인방지와 무결성의 문제를 해결하고자 한다.

아래의 [그림 3]은 앞서 설명한 기존의 블루투스 암호화 인증과정의 취약점을 보완하고자 본 논문에서 제안하는 블루투스에서 비대칭 암호기법의 전자서명을 활용한 개선된 상호인증 기법이다.

[그림 3]을 보면 E0 Algorithm 까진 기존 블루투스의 흐름도와 같다. 허나 패킷과 같이 캡슐화 되어 전송이 될 때 E0 Altorithm, Packet을 해쉬한 값에 Device1의 개인키로 암호화 하여 E0 Algorithm, Packet을 같이 동봉하여 Device2에 보낸다. Device2는 E0 Algorithm, Packet을 해쉬한 값과 MAC 값을 Device1의 공개키로 복호화한 값과 비교하여 같을 경우 E0 Algorithm을 제외한 Packet만을 산출하여 Deivce2에 전달해준다. 값이 다를 경우에는 Device2에 전송해주지 않고 폐기한다.

Device2에서 Device1에 전송해 줄 때도 같은 과정을 거친다.

이러한 과정을 거침으로써 Device2에선 Device1을, Device1에선 Device2를 각각 상호 인증 할 수 있고 해쉬라는 무결성 검사와 자신의 개인키로 암호화하고 공개키로 복호화하는 전자서명기법으로 인해 부인방지도 제공한다.

4. 결론

블루투스가 현재 각광 받고 있는 기술임에는 틀림이 없다. 근거리 무선 통신의 표준으로 자리 잡고 있는 블루투스는 개인의 무선 단말기를 이용하여 기존 유/무선망을 활용하는 기술이다. 또한, 다른 근거리 무선 통신과는 달리 블루투스에서 제공되고 있는 자체 보안기능 등을 이용하여 높은 보안 기능을 필요로 하는 전자상거래와 같은 서비스와 활용할 수도 있다. 그러나 블루투스에서 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 적용할 때 많은 보안적 취약점을 발생시킨다 따라서 새로운 블루투스 표준안이나 기술에서는 기존의 블루투스의 표준안이나 기술에서 가졌던 취약성을 보완하고 보다 안전하고 효율적인 보안 서비스를 제공해야 할 것이다.

본 논문에서는 기존의 블루투스의 인증기법엔 제공하지 않는 무결성과 부인방지를 보완하는 기법을 제안하였지만 이 뿐만 아니라 블루투스는 현재도 많이 취약한 것을 고찰하고 꼭 빠른 개발만이 아닌 보안적인 면에도 소홀하지 않은 제품이나 기술개발이 필요하다.

참고문헌

[1] Karen Scarfone. John Padgette, "Guide to Bluetooth Security", NIST, September 2008에트리

[2] Dr.GrEen, "Bluetooth Tutorial", 1월, 2008

[3] 박희진, “블루투스 모바일 폰을 위한 보안인증 시스템”, 과학기술학회, pp.261-263, 4월, 2007

[4] 최유미, “블루투스 단거리 무선 네트워크 상에서 보안과 인증 메커니즘”, 정보학회, Vol.5, No.1, 2004

[5] 김형락, “ 순환 클럭 조절된 비선형 알고리즘을 이용한 블루투스 암호화시스템의 안전성 개선”, 한국통신학회, pp.640-648, 7월 2009

[6] Bluetooth Specification Version 1.1, "Core", Specification of the Bluetooth System volume1, Feb 2001

[7] 박천교, “Bluetooth의 개요 및 어플리케이션”, 정보통신연구진흥원, 2000