블루투스 연결 보안

*신은지, 이아람, 이하준, 이덕규
*서원대학교 정보보안학과
alghk0207@naver.com, sosw3539@naver.com, gkwns0@naver.com

BlueTooth Connection Security

Eun-Ji Shin, A-ram LEE, Ha-Jun Lee, Deok-Gyu Lee
*Dept. of information security, Seo-Won University

요 약

블루투스 취약점을 이용한 공격을 방지하기 위한 블루투스 보안으로 블루투스의 링크키 인증 과정을 OTP 기능과 접목하여 실행하여 블루투스 재연결 인증 과정 취약점(BIAS)에 대해 보안을 강화한다.

1. 서론

1.1 연구의 필요성

블루투스는 디지털 통신 기기를 위한 개인 근거리 무선 통신 산업 표준으로 수 미터에서 수십 미터 정도의 거리를 둔 정보기기 사이에, 전파를 이용해서 간단한 정보를 교환하는데 사용된다.

블루투스의 장점은 무선 랜(와이파이)과 달리 벽이나 장애물 등에 민감하지 않아 데이터 전송율이 높고, 데이터를 여러 주파수로 나눠 전송하기에 보안성이 우수해서 많이 활용되고 있다.

그러나 블루투스의 연결 시 보안 취약점으로는 BIAS(Bluetooth Impersonation)가 발생할 수있다. BIAS는 공격자가 이전에 페어링 된 원격 기기의 주소를 Spoofing 할 수 있고, 이를 통해 링크키 없이도 페어링 된 장비에서 인증 절차를 성공적으로 수행할 수 있게 되는 공격방식이다.

이런 취약점을 이용한 공격을 막기 위해 본 논문에서는 블루투스 기기의 MAC 주소 또는 링크키가 유출되어도 Spoofing 공격을 방지할 수 있는 방법을 연구한다.

2. 관련연구

2.1 OTP (One Time Password)

OTP[2]는 말 그대로 One Time Password의 약자로, 보통의 고정적인 패스워드와는 다르게 매번 다른 패스워드를 만든다. 사용자 인증 방법 중 하나로 사용하기에 편리하며 높은 보안성을 가지고 있다.

OTP 보안성

기존의 ID/PWD를 노출이 되었음에도 2차(사용자 인증 서비스)적인 보인확인을 할 수 있는 보안성을 가지고 있다. 그리고 2차적인 인증서비스(OTP)의 패스워드를 유출했더라도, 우리는 예측할 수 없는 이 특성으로 보안을 유지할 수 있다. OTP는 HASH 함수를 통해서 랜덤의 값(난수)을 추출하므로 역으로 입력 값을 알아내기가 어렵다. 그러므로 악의적인 해커에 의해 패스워드를 Sniffing 당한다 해도 원래의 패스워드를 찾기 어려울 것이다.

OTP 종류

OTP의 종류로는 S/Key방식, 챌린지 리스펀스 방식, 시간 동기화(Time Synchronous) 방식, 이벤트 동기화 방식이 있다. 그 중 시간 동기화 방식은 시간을 일회용 비밀번호의 입력 값으로 사용하여 인증서버와 사용자는 같은 시간을 일회용 비밀번호의 입력 값으로 넣어야 한다.

시간 동기화 과정

① 사용자는 일회용 비밀번호를 생성해 PIN번호(사용자의 패스워드와 비밀키)를 인증서버에 보낸다.

② 인증서버는 PIN을 통해 비밀키를 찾고 생성된 일회용 패스워드가 수신한 것과 일치하는 지를 파악한다.

③ 이때, 인증서버와 사용자 토큰사이에 시간이 일치하지 않으면 사용자 인증은 실패하고 일치하면 인증에 성공한다.

일회용 비밀번호의 입력 값을 서버로부터 받지 않는 장점을 갖고 있으나 서버와 사용자 토큰의 정보를 일치시켜야 하는 단점과 또한 사용자의 수가 많은 경우 여러 개의 시간을 동시에 일치시키는 것도 어렵다. 인증서버와 사용자 토크 간에 시간정보를 일치시켜야 하는 불편함을 가지고 있다.

2.2 HASH FUNCTION

HASH 함수는 임의의 길이를 갖는 메시지를 입력하여 고정된 길이의 HASH 값을 출력하는 함수이다. 현재 사용되고 있는 표준 HASH 함수들은 256비트의 HASH 값을 출력한다. 암호 알고리즘에는 key가 사용되지만, HASH 함수는 key를 사용하지 않으므로 같은 입력에 대해서는 항상 같은 출력이 나온다. 이러한 함수를 사용하는 목적은 메시지의 오류나 변조를 탐지할 수 있는 무결성을 제공하기 위해서다.

HASH 함수의 특성은 아래와 같다.

- 역상 저항성 (Preimage Resistance) :

HASH 값으로 원문을 유추할 수 없음

y = h(x)에서 y로 x를 찾는 것이 어려움

- 제 2 역상 저항성 (Second Preimage Resistance) : 주어진 원문과 같은 HASH 값을 갖는 다른 원문을 찾기 어려움

h(x) = y 인 x와 y가 주어지고, h(w) = y인

w를 찾기 어려움

- 충돌 저항성(Collision Resistance) :

동일한 HASH값을 갖는 다른 두 원문을 찾는 것이 어려움

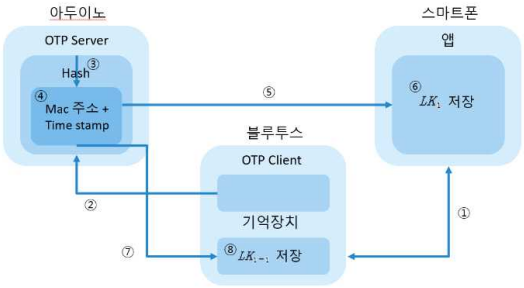
h(x) = h(w)인 x, w를 찾는 것이 어려움

3. 설계

3.1 모듈

스마트폰은 Galaxy S20 FE, 아두이노는 UNO R3 SMD, 블루투스는 HC-06, 기억장치는 EPPROM을 사용한다.

3.2 초기 연결



(그림 1) 초기연결

아두이노에 OTP서버와 HASH 함수를 구현하고, 블루투스에 OTP 클라이언트와 기억장치를 구현한다.

위 그림 1과 같이 구현하고 과정은 다음과 같다.

1. 블루투스와 스마트폰이 페어링 된다.

2. 블루투스가 OTP 서버에 MAC 주소를 전달한다.

3. OTP Server에 링크키 생성을 요청한다 (이하 LK_1)

4. LK_1 생성 후 HASH 함수로 암호화한다.

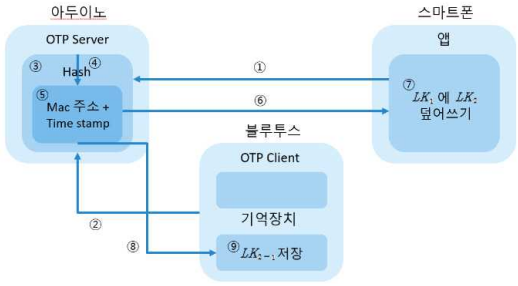
5. 생성된 LK_1을 스마트폰에게 전달한다.

6. 스마트폰은 전달받은 LK_1을 저장/보관한다.

7. 생성된 LK_1의 일부분을 블루투스에게 전달한다. (이하 LK_{1-1})

8. 블루투스는 전달받은 LK_{1-1}을 저장/보관한다.

3.3 재연결



(그림 2) 재연결

위 그림2와 같이 구현하고 과정은 다음과 같다.

1. 스마트폰에서 OTP Server로 LK1을 전달한다.

2. 블루투스에서 OTP Server로 LK_{1-1}을 전달한다.

3. OTP Server에서 LK_1과 LK_{1-1}를 비교한다.

일치하면 인증에 성공하고 그렇지 않으면 인증에 실패한다

4. OTP Server에 링크키 생성을 요청한다 (이하 LK_2)

5. Time Stamp를 이용하여 LK_2 생성 후 HASH 함수로 암호화한다.

6. 생성된 LK_2를 HASH 함수로 한 번 더 암호화하여 스마트폰에게 전달한다.

7. 스마트폰은 전달받은 LK_2을 LK_1에 덮어쓴다.

8. 그 후 이전과 동일하게 재생성된 LK_2의 일부분을 블루투스에게 전달한다. (이하 LK_{2-1})

9. 블루투스는 전달받은 LK_{2-1}을 저장/보관한다.

위 설계로 공격자가 이전에 페어링 된 원격 기기의 주소를 Spoofing 할 수 있고, 이를 통해 링크키 없이도 페어링 된 장비에서 인증 절차를 성공적으로 수행할 수 있게 되는 공격을 블루투스 연결 시 OTP에 블루투스의 MAC 주소뿐만 아니라 시간 정보를 이용하여 링크키를 생성하고 Master와 Slave에 링크키 일부분을 보관하여 MAC 주소 또는 링크키가 유출되어도 Spoofing 공격을 방지한다.

4. 결론

본 논문에서는 아두이노 프로그램을 사용하여 OTP Server를 구축하고, 스마트폰 앱을 이용해 블루투스 동작을 확인하였다.

블루투스 연결 시 OTP에 블루투스의 MAC 주소뿐만 아니라 시간정보를 이용하여 링크키를 생성하고 Master와 Slave에 링크키 일부분을 보관하여 MAC 주소 또는 링크키가 유출되어도 Spoofing 공격을 방지해 안정성을 확보한다.

OTP만 사용하는 것이 아니라 HASH 함수를 추가해 차별성을 두어 사용자가 만족할 수 있는 프로그램을 개발하였다.

참고문헌

[1] 전정훈. 저전력 블루투스의 보안 위협 요인들에 관한 연구. 융합보안 논문지, 17(4), 3-9. (2017)

[2]유환신. 블루투스 4.0 기술을 이용한 차량용 보안 인증 시스템 설계. 한국산학기술학회논문지 18.7 : 325-330.(2017)