M2M에서 WPA 기반의 인증

*최아름,*이근호
*백석대학교 정보통신학부 정보보호학과
e-mail : godandarum@hanmail.net, root1004@bu.ac.kr

Authentication based on WPA in Machine to Machine

A-Rum Choi' Keun-Ho Lee
Division of Information and Communication, Information security major,
Baekseok University

요 약
본 논문에서는 M2M에서의 WPA 기반의 인증 매커니즘을 제안하였다. 기기 간에 인증서를 배포하고 인증서를 이용하여 하나의 기기만 인증하는 것이 아닌 통신에 참여하는 기기 모두를 인증할 수 있는 매커니즘으로서 위장공격에 대한 위험위협 요소를 방어 할 수 있는 보안을 제공한다.

1. 서론

M2M은 machine to machine, mobile to machine, 그리고 machine to mobile의 통신을 의미한다. M2M은 기계들과 우리의 일상생활 속에 널리 퍼져 있는 기기들의 네트워킹에 관한 개념이다. M2M 통신은 일련의 기구들을 컴퓨터의 본체에서부터 일상의 제품들까지 연결해 사용이 가능하도록 해 줄 것이다. 예를 들면, 가전제품이나 운송수단, 건물 등에서 사용된다. 이 개념은 기계들이나 기기들이 원격지에서 이동통신을 통해서 자신의 데이터를 전송하는 것이 가능하도록 하는 것이다. 현재의 M2M 통신 개념은 GSM망을 넘어 다양한 유무선 네트워크를 활용하는 개념으로 확장되어가고 있다.

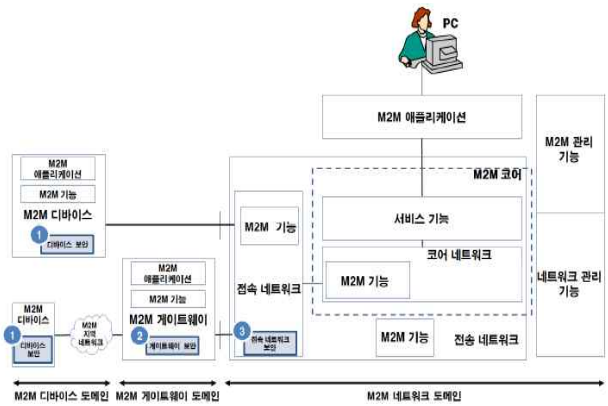
M2M 장치들은 사람과 사물 사이에서 상호작용을 한다. 사람은 데이터를 얻을 수 있고 위치, 건강, 유동적이거나 소모할 수 있는 수준, 온도, 보수 기록, 그리고 생산력의 수준과 같은 기기들의 상태를 한눈에 볼 수 있다. 하나의 기기는 다른 기기들과 연결되어 음악 및 영상과 같은 멀티미디어 정보, 기기의 특정 한계상황에 대한 경고, 그리고 공급 망 정보와 같은 컨텐츠를 공유하여 데이터와 서비스들의 흐름이 지능적이면서도 자동적으로 이루어 질 수 있도록 하는 것이 필요하다[2].

본 논문에서는 M2M에서 발생하는 보안 위협에 대한 분석과 WPA를 이용한 인증 매커니즘을 제안한다.

2. M2M의 보안위협요소와 대응방법

2.1 M2M에서의 보안위협 요소

M2M의 보안 위협에는 네트워크에서 발생하는 보안 위협이 포함된다. 프라이버시(도청, 트래픽분석, 가로채기/방해, 기밀누설, 폐기 정보수집)침해, 변조(가로채기/변경, 부인), 불법 도용/접근(속임수, 권한위배, 물리적 침입, 재사용공격, 중간자 공격), 침투(바이러스, 웜, 악성코드), 서비스마비(자원고갈, 무결성 위배)등 비인가 접근, 비인가 무단 변조의 위험이 있다.



[그림 1] M2M에서의 보안기능

M2M의 보안에는 디바이스 보안, 게이트웨이 보안, 네트워크보안이 있으며 데이터의 기밀성, 무결성, 게이트웨이 및 서버인증, 프라이버시보호 및 추적성, 디바이스인증, 시스템 가용성 등의 보안 조건을 만족해야한다[1][4].

- 데이터노출

M2M 통신 환경에서는 위치, 개인정보, 과금 데이터 등의 민감한 정보를 전송을 하기 때문에 네트워크 어느 지점에 서든 도청에 의해 수집되는 데이터 유출을 예방하기 위해 데이터의 기밀성을 보장해야 한다.

- 데이터 불법 변경 및 삭제

중간자(man-in-the-middle) 공격을 통한 데이터의 불법 변경 및 삭제, 위조된 데이터의 삽입 등에 대응하기 위한 무결성 보장이 필요하다.

- M2M 디바이스 불법 도용 및 용도 변경

M2M 장치는 상대적으로 물리적 보안이 허술한 장소에 배치됨에도 불구하고 자본 절약, 기능성, 유동성 및 개발 용이성의 장점으로 인해 개방형 인터페이스를 지닌 플랫폼에서 구현이 가능하고, 장치에 악성 소프트웨어 삽입 또는 장치 변경으로 인해 악성 디바이스 및 게이트웨이로 용도가 변경될 수 있음으로 M2M 장치의 무결성 검증 메커니즘이 필요하다.

- 서비스 거부공격

서비스 거부공격(DoS)은 시스템의 가용성 및 생산성을 훼손함으로써 시스템 자원과 정보에 대한 접근 능력을 감소시킬 수 있다. 따라서 M2M 통신 환경에서도 주체 또는 디바이스들의 정보 접근 능력을 침해하지 않도록 시스템 가용성을 보장 할 수 있는 보안 메커니즘이 필요하다.

- 사용자의 개인정보 수집 및 도용

M2M 디바이스는 사람의 일상과 밀접하게 연관되어 있으므로 사용자와 관련된 정보를 기록하게 된다. 이러한 사용자 데이터들의 불법적으로 노출 되는 경우, 개인 프라이버시 침해 문제가 발생할 수 있으므로 이를 방지 할 수 있는 보안 메커니즘이 필요하다.

- 위치추적(이동성 제공 디바이스)

이동성을 제공하는 M2M 디바이스의 경우 디바이스의 위치정보 노출로 인해 디바이스 및 디바이스 소유자의 위치나 이동 경로가 노출될 가능성이 존재한다. 따라서 이동성을 제공하면서 추적 불가능성을 제공할 수 있는 보안 메커니즘이 필요하다.

- 위장공격

서버는 전송되는 데이터를 수집하기 전에 데이터가 올바르고 정당한 디바이스 또는 게이트웨이로부터 전송되었는지 확인하는 검증 절차가 필요하다. 반대로 디바이스의 경우에도 수신되는 데이터가 올바르고 정당한 게이트웨이 또는 서버로부터 전송 되었는지 확인하는 검증 절차가 필요하다. 따라서 M2M 환경에서는 자신과 통신하는 상대방 개체에 대한 정당한 개체인지를 검증하는 상호 인증 절차가 반드시 필요하다.

2.2 상호 인증 키 교환 매커니즘

2.2.1 Peer-to-Peer 상호인증 및 키교환 프로토콜

M2M 디바이스와 M2M Server 사이에 상호간에 신뢰된 통신을 제공할 수 있는 개체간 상호인증 및 키 교환 프로토콜로 M2M 통신에 참여하는 개체들 간의 상호인증 절차를 통해 자신과 통신하는 개체의 정당성을 확인할 수 있고, 상호인증 절차를 통해 상호간에 동일한 키를 교환함으로써 이후 세션에서는 안전한 채널 제공을 할 수 있다.

Peer-to-Peer 상호인증 및 키 교환 프로토콜은 사전단계와 상호인증 및 키 교환 단계로 구분할 수 있다. 사전단계에서는 파라미터를 전송하며 상호인증 및 키교환 단계에서는 기기간 인증 및 세션키를 설립하며 이 과 정을 통해 보안채널이 성립되어 신뢰된 통신환경을 제공 받을 수 있다.

이 프로토콜을 통해 재사용 공격, 위장공격을 예방 할 수 있다. 디바이스에서 생성한 랜덤 수를 이용하여 매 세션마다 임시 세션키와 세션키를 새롭게 생성하여 메시지를 암호화 이전에 전송된 메시지를 이후 세션에서 재사용할 수 없다는 점을 이용해 재사용 공격을 예방할 수 있다. 위장공격은 공격자가 서버로 위장하더라도 정당한 서버의 비밀키에 대한 역원값을 알 수 없으므로 올바른 임시 세션키를 생성할 수 없고, 디바이스로 위장하더라도 정당한 디바이스의 패스워드를 알 수 없으므로 서버와 동일한 세션키를 생성할 수 없다는 점을 이용해 예방 할 수

있다.

상호 인증 및 키 교환을 통해 정당한 서버만이 올바른 임시 세션키를 생성할 수 있으므로 디바이스는 동일한 세션키가 설립되었는지 확인을 통해 서버를 인증할 수 있으며 서버 역시 동일한 세션키가 설립되었는지 확인하는 과정을 통해 디바이스의 정당성을 확일 할 수 있다. 이 프로토콜을 통해 프라이버시 문제, 변조, 불법 오용/접근, 바이러스나 악성코드의 침투 등의 문제를 해결 할 수 있다.[1]

2.2.2 원격 사용자를 위한 상호인증 및 키 교환 프로토콜

원격 사용자와 M2M 디바이스 간에 안전한 통신 제공을 위한 상호인증 및 키 교환 프로토콜로 사전 단계에서는 파라미터를 전송하며 상호인증 및 키 교환 단계에서는 원격 사용자가 발급 받은 티켓을 디바이스에게 전송하며 디바이스는 원격 사용자에게 적당한 응답값을 제공하고 이 과정을 통해 보안채널을 형성하며 신뢰할 수 있는 통신환경을 제공한다.

원격 사용자를 위한 상호인증 및 키 교환 프로토콜은 타임스탬프를 이용하여 전달되는 메시지의 재사용 여부를 확인하므로, 재사용 공격에 대해 안전하다. 또한 공격자가 원격 사용자로 위장할 경우, 정당한 원격 사용자의 패스워드를 모르는 공격자는 올바른 MAC 값을 생성할 수 없으므로 원격 사용자로 위장할 수 없으며, 공격자가 디바이스로 위장할 경우, 정당한 디바이스의 비밀키를 모르는 공격자는 올바른 세션키를 획득할 수 없으므로 디바이스로 위장할 수 없어 위장공격에 안전하다. 따라서 이 프로토콜을 통해 디바이스는 올바른 티켓과 MAC 값을 검증함으로써 올바른 원격 사용자임을 인증할 수 있고 원격 사용자는 디바이스로부터 전송된 메시지를 이번 세션에 설립된 세션키를 이용하여 복호하여 동일한 키가 설립되었는지를 확인함으로써, 디바이스의 정당성을 인증할 수 있다[1].

3. 상호 인증 프로토콜

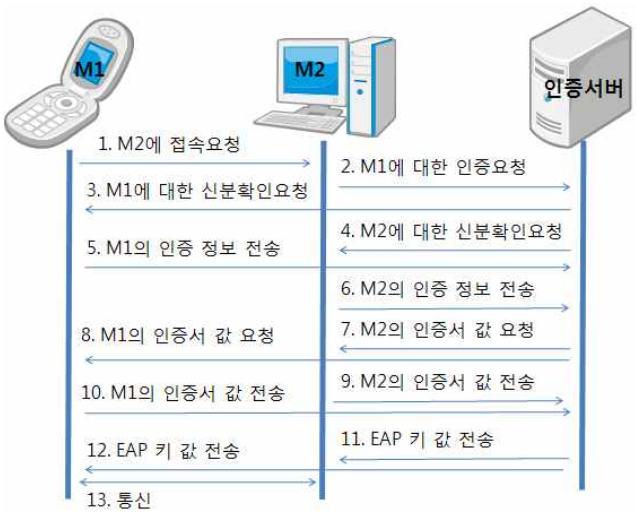
M2M에 WPA 인증과 인증서를 이용한 새로운 인증 프로토콜을 생각해 보았다. M2M의 통신 환경은 대부분 무선으로 이루어져 있고 무선을 이용하기 위해서는 신뢰할 수 있는 기기간의 접속이 필요하며 이 대한 신뢰성 제공을 위해 인증서를 적용하기로 했다.

3.1 시나리오

인증서를 이용한 프로토콜로 위장공격에 안전해야 한다. 위장공격은 공격자가 기기를 위장하여 사용자의 비밀정보를 알아내는 것이다. 즉, 기기로 위장 시 사용자의 비밀 정보를 알아내기 위한 공격을 할 수 있으며 위장된 기기가 정당한 사용자로 위장하여 재전송 공격 등이 가능할 수 있다.

요즘 무선은 사용자가 쉽게 이용 가능하게 되어있고 이에 따라 무선을 사용하는 사용자가 늘어가고 있다. 무선에서의 안전한 인증을 위해 WPA와 인증서를 이용한 방법으로서 인증서버로부터 통신 요청 기기뿐만 아니라 요청에 응하는 기기도 인증 받아 좀 더 신뢰성 있고 안전한 통신이 가능할 것이다.

3.2 WPA와 인증서를 통한 상호 인증



[그림 2] 인증 과정

WPA 프로토콜에 인증서를 도입한 것으로 모든 Machine들은 인증서를 발급 받아 인증서버에 등록을 해야 한다. M1과 M2의 통신을 위해서는 상호 인증이 필요하다.

- 1. M1이 M2 에게 연결을 요청하면 WAP의 모드 중 하나인 EAP가 시작된다.
- 2. 연결 요청을 받은 M2는 서버에 M1에 대한 인증을 요청하게 된다.
- 3,4. 서버는 상호 인증을 위해 M1과 M2 모두에게 신분확인을 요구한다.
- 5,6. M1과 M2는 자신의 인증 정보를 서버에게 보낸다.
- 7,8. 서버는 M1과 M2에게 인증서 값(패스워드)를 요구한다.
- 9,10. M1과 M2는 서버에게 인증서 값을 보낸다.

- 11,12. 서버는 M1과 M2가 정당한 사용자임을 확인하면 확인된 정보와 함께 EAP-TLS를 이용해 통신에 사용될 WEP 키 값을 보낸다.
- 13. 서버에게 받은 WEP 키를 이용해 M1과 M2가 통신을 한다.

이때 보낸 WEP KEY 값은 두 장치의 연결이 종료될 때까지만 사용되며 다음 연결 시에는 새로운 KEY 값을 할당 받아 통신한다.

3.3 검증 결과

[표 1] WPA와 비교

	무결성	인증	위장 공격
WPA	○	○	X
WPA상호인증	○	○	○

기존의 WPA 프로토콜은 TKIP를 통한 무결성 제공과 EAP를 이용한 인증을 제공한다. 인증 서버가 통신을 요청한 기기에 대해서만 인증을 제공을 하고 통신 대상 기기에 대한 인증을 제공하지 않아 위장 공격에 취약하다.

반면 이 논문에서 제안한 WPA 상호인증 매커니즘은 기존의 무결성과 인증을 그대로 유지하되 통신을 요청한 기기와 통신 대상 기기 모두 서버로부터 인증을 받도록 함으로서 요청 기기가 정당한 지와 대상 기기가 정당한 사용자 인지 모두 인증을 받기 때문에 상호 인증을 통한 안전한 통신을 제공할 수 있다.

4. 결론

M2M 간의 통신은 보안에 취약하며 유선과 무선 상에서 나타날 수 있는 보안 취약점이 모두 M2M의 취약점이 될 수 있다. 이에 M2M 간의 안전한 통신을 위해서 기기간의 신뢰할 수 있는 상호 인증이 필요하다. 장치의 종류에 관계없이 서로 안전하게 통신 가능한 다양한 M2M 인증 프로토콜이 필요하며 이 논문에서 제안한 WPA와 인증서를 이용한 상호 인증 프로토콜은 그 중 한 대안으로 볼 수 있다.

참고문헌

[1] 문선기, 전서관, 안재영, 오수연, “안전한 M2M 통신 구축을 위한 상호인증 및 키 교환 프로토콜”, 정보보호학회논문지, 제20권, 제1호, pp. 73-83, 2월, 2010.

[2] “M2M 기술 및 비즈니스 사례”, 21C 지식정보센터(www.inetbook.co.kr)

[3] Dong-Hoon Kim, Jun-Yeob Song, Seuk-Keun Cha, “Introduction of Case Study for M2M Intelligent Machine Tools”, Proceedings of 2009 IEEE International Symposium on Assembly and Manufacturing pp. 17-20, November, 2009

[4] Inhyok Cha, Yogendra Shah, Andreas U. Schmidt, Andreas Leicher, and Michael Victor (Mike) Meyerstein, "Trust in M2M Communication", IEEE VEHICULAR TECHNOLOGY MAGAZINE, pp. 69-75, SEPTEMBER, 2009

[5] “무선 랜의 안전한 사용을 위한 보안대책”, NCSC-TR050021, 국가 사이버 안전센터