제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

텔레매틱스에서 보안 동향 및 스마트폰 인증

여성권, 이근호
백석대학교 정보통신학부
najarazwi@empal.com, root1004@bu.ac.kr

A Security Survey and SmartPhone Authentication in Telematics

Seong-Gwon Yeo, Keun-Ho Lee
*Dept. of Information Communication, Baekseok University

요 약

IT 기술의 발전으로 M2M 시장이 급부상하고 있는 가운데 M2M 응용분야 중 텔레매틱스의 개념 및 차량 네트워크 보안의 취약성을 알아보았다. 차량 및 IT 기술의 융합과 이동통신망 기술의 발전은 사용자에게 제공되는 서비스의 질은 향상 시켰지만, 이로 인한 보안 위험성은 더 많아지고 다양해졌다. 이에 본 논문에서는 텔레매틱스의 새로운 비즈니스 모델과 이로 인해 발생 될 수 있는 차량 이동통신망 보안의 취약성을 분석하였다. 이 중 발생할 수 있는 위장공격을 예방하기 위해 M2M 기기와 스마트폰의 상호 인증 기법을 제시하였다.

1. 서론

최근 이동통신 기술의 발전으로 많은 사람들이 스마트폰을 이용하고 있다. 급속도로 증가하는 스마트폰 보급률과 활용도로 인해 그동안 국내 사람들에게 잘 알려지지 않았던 M2M(Machine-to-Machine)시장에 대한 관심과 개발이 활발하게 이루어지고 있으며, 다양한 업체의 참여와 함께 M2M 통신에서의 보안 역시 큰 이슈가 되고 있다[6].

M2M은 우리의 주변에서 존재하는 기기간의 통신을 의미한다. M2M 통신은 사용자 및 업체의 컴퓨터와 가전제품, 자동차, 스마트폰과의 연동이 가능하도록 해준다. 이러한 연동으로 인해 각 기기들은 주변에서 수집한 다양한 정보들을 분석하고 분류하여 유무선 네트워크와 이동통신, 전송매체를 이용하여 전송한다.

과거의 M2M 통신에서는 각 기기들 간에 정보 전달만을 수행하였지만, 현재의 M2M 통신은 기기를 넘어서 사람과 기기간의 정보 전달을 하여 사용자가 실시간으로 정보를 확인하는 수준까지 왔다.

본 논문에서는 M2M의 응용분야인 텔레매틱스에 대해 살펴보고, 텔레매틱스의 보안 취약성과 스마트폰으로 텔레매틱스를 이용할 시 발생할 수 있는 취약성에 대해 분석한다. 이러한 분석을 통해 차량 내의 M2M 기기와 스마트폰의 상호 인증에 대한 기법을 제안한다.

2. 관련연구

2.1 텔레매틱스

M2M 시장을 살펴보면 다양한 응용분야가 있음을 알 수 있는데, 주요 응용분야로는 텔레매틱스, 물류관리, 지능검침 시스템, 원격 자산 관리 시스템, 판매 관리 시스템(POS) 및 보안 관련 분야가 있다[1].

M2M 시장을 이끌고 있는 응용분야 중 하나인 텔레매틱스(Telematics)는 통신(telecommunication)과 정보(informaics)의 합성어로, 차량의 위치파악기술, 양방향 통신이 가능한 무선 통신망과 차량 내 단말기를 통해 차량, 운전자, 탑승자에게 다양한 정보 및 서비스를 제공하는 것을 말한다.

즉, 위성위치확인시스템(GPS, Global Positioning System), 지리정보시스템(GIS, Geographic Information System)과 무선통신망을 이용하여 차량 내 모든 탑승자에게 교통정보, 최적경로, 날씨정보, 도난방지, 도난차량 추적, 원격진단, 응급상황에 대한 대처, 인터넷, 전화 등을 제공하는 종합서비스라 할 수 있다[6].

2.2 텔레매틱스 보안 취약성

차량에서 사용하는 대표적인 네트워크로 VANET (Vehicular Ad-hoc Networks)이 알려져 있으며, 차량을 중심으로 차량 간 통신망(V2V Vehicle-To- Vehicle)과 차량과 인프라 통신망(V2I Vehicle-To- Infrastructure)으로 분류된다[3].

VANET도 기본적으로는 기존의 네트워크 기반의 무선 환경을 바탕으로 하고 있기에, 기존의 무선 네트워크 환경이 가지고 있는 보안 취약성을 그대로 가지고 있다[4].
다음은 VANET에서 나타날 수 있는 보안 취약성중 일부

이다.

- The Sybil Attack[5] : 한명의 공격자가 네트워크 상에서 여러 개의 환영노드들로 나타나서 혼란을 가중시키는 공격.

- 위조 공격 : 공격 차량에 의해 차량 간 네트워크 영역 내에서 다른 차량들을 거짓 정보로 오염시키는 공격.

- Jamming Attack : 차량 네트워크 영역 내에서 다른 차량의 통신에 장애를 유발하는 신호를 발생시켜 네트워크 통신을 마비시키는 공격.

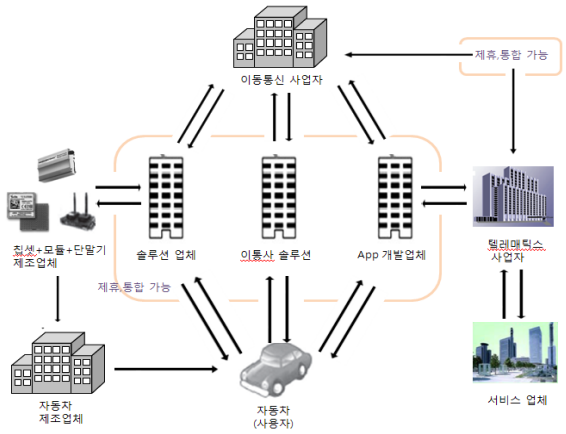
- In-transit Traffic Tampering : 주행 중에 메시지를 전달하는 과정에서 공격 차량에 의한 메시지 삭제·변조를 통해 차량 통신을 방해하는 공격.

이외에도 주변 차량을 자신의 차량으로 오인하게끔 만드는 공격과 차량 내부의 다양한 정보 등을 위변조 하는 공격 등 많은 취약성이 존재하고 있다[6].

2.3 텔레매틱스의 새로운 비즈니스 모델

그림 1을 살펴보면 텔레매틱스 시장은 다수의 하부 업체들이 각각의 독립 분야를 맡아서 참여하는 구조로 되어 있다. 즉, End-User에게 서비스가 제공되는 과정에 있어서 텔레매틱스 서비스 사업자, 칩셋 공급업체, 모듈업체, 단말제조업체, 이동통신사업자, 서비스업체(콘텐츠, 보험회사, 정비회사 등), 솔루션업체 등이 관여한다고 볼 수 있으며, 이외에도 다양한 업체의 참여가 이루어지고 있다.

다수의 업체 중 이동통신 사업자가 텔레매틱스 사업에 참여함으로써 차량 내 M2M 기기와 스마트폰의 통신을 이용하여 사용자는 다양한 정보를 얻을 수 있지만 이로 인한 새로운 보안 취약성이 존재 할 수 있다[6].



(그림 1) 텔레매틱스 비즈니스 모델[6]

2.4 차량 이동통신 기술 및 보안 취약

이동통신은 1세대인 아날로그에서부터 4세대인 IMT-Adcanced까지 진화해 왔으며, 현재는 3세대인 WC-DMA/HSDPA를 주로 사용하고 있다.

이러한 이동통신기술의 발전으로 인해 사용자는 각종 사용자 디바이스(스마트폰, 태블릿PC, PDA, 노트북, 차량용 셋톱박스, PMP 등)로 사용자가 언제, 어디서든 차량의 상태를 파악할 수 있게 되었다. 사용자는 이동통신망을 이용하여 사용자 디바이스와 차량 단말기의 통신을 통해 차량에 대한 각종 정보를 고속의 데이터 전송으로 제공받을 수 있다. 그러나 인터넷 서비스가 스마트폰 환경에서도 구현이 되면서 이동통신망을 이용한 보안 취약성이 존재하게 됐으며, 이러한 취약성은 차량과 통신 중에도 발생 할 수 있다. 다음은 이동통신망을 이용해 사용자와 차량과의 통신 시에 나타날 수 있는 보안 취약성이며, 일부임을 밝혀둔다.

- 모바일 악성코드 : 어플리케이션에 악성코드가 삽입 되어 사용자가 어플리케이션을 다운 받은 후 차량과 디바이스의 통신을 하면 개인정보 및 차량 정보가 유출되는 공격.

- 서비스 거부 공격 : Jamming Attack과 비슷한 공격으로 스마트폰에 다량의 데이터를 전송하여 서비스를 이용하지 못하게 하는 공격. 사용자는 차량 단말기와의 통신도 불가능.

- 무선 인터넷 중계기 공격 : 인터넷에 접속하기 위해 AP(Access Point)에 접속 시 스마트폰과 AP, 차량단말기와 AP가 서로 주고받는 정보가 해커에 의해 해킹되는 공격.

- WiFi Phising : 해커가 자신의 노트북을 AP로 전 환하여 DNS, DHCP, HTTP 등의 서비스를 활성화 시켜 사용자를 유인하는 방법. 사용자 및 차량이 해커의 AP에 접속되어 개인정보가 유출되는 공격.

- 사용자 인증 위장 공격 : 허가받지 않은 사용자가 인증서버로부터 인증을 받아 차량 내 M2M 기기와 통신하여 개인정보 유출 및 차량 오작동을 유발 시키는 공격.

위에서 언급한 바와 같이 차량의 M2M 기기와 스마트폰과의 통신 시 다양한 위험요인이 존재한다. 본 논문에서는 이 중 사용자인척 위장하여 인증을 받아 공격하는 방법에 대한 해결책을 제시한다[6].

3. M2M 기기와 스마트폰 상호 인증

텔레매틱스에서 사용자의 디바이스와 차량 내 기기와의 통신이 상호 인증된 상태로 진행 될 수 있도록 인증 절차

를 제안하였다. 두 기기가 제 3의 기관으로부터 인증을 받아 서로 신뢰된 상태에서 통신을 할 수 있게 하였다.

3.1 시나리오

사용자의 스마트폰 및 차량 내 M2M 기기(이하 MIC)와 신뢰 할 수 있는 제 3기관(이하 TTI)이 있다. 스마트폰은 사용자의 패스워드가 임시로 저장되지 않아야 하며, 패스워드 추측공격을 당하지 않아야 한다. TTI는 사용자 및 MIC의 정보를 보유하고 있으며, 등록 및 키 관리를 담당한다. 또한, 인증 받지 않은 사용자로부터 안전하다고 가정한다.

본 논문에서 사용하는 인증 방법은 스마트폰에서 MIC와의 통신을 위해 접속요청 시 스마트폰 사용자가 정당한 사용자인지 TTI로부터 인증을 받는다. MIC는 TTI로부터 정보를 받아 접속을 요청한 사용자가 TTI로부터 인증을 받은 사용자인지 확인 할 수 있다. 스마트폰 및 MIC가 TTI로부터 인증을 받아 상호 간 신뢰성 있고 안전한 통신이 가능하다.

3.2 상호 인증

사용자가 스마트폰을 이용하여 자신의 차량 내의 MIC에게 연결을 요청할 때 사용자는 TTI로부터 본인 인증을 받아 MIC와 안전하게 통신이 되어야 한다. 사용자가 인증을 위하여 단순히 ID와 패스워드만을 입력하여 인증을 받는 단순한 방식에서 벗어나 좀 더 복잡한 과정을 거쳐 인증을 받는 것이 안전하다.

- 1. 사용자는 자신의 ID와 패스워드를 스마트폰에 입력하면 스마트폰은 사용자의 ID, MAC 주소, 패스워드를 이용하여 만든 비밀 키를 TTI에게 보낸다.
- 2. TTI는 사용자의 패스워드를 기반으로 한 사용자의 마스터 키(UMK)를 찾아서 사용자 정보를 포함하고 있는 TGT-1과 세션 키를 만든다. TTI는 자신의 마스터 키(TMK)를 이용하여 TGT-1을 암호화 하고 TGT-1과 세션 키를 사용자에게 보낸다.
- 3. 사용자는 암호화된 TGT-1과 세션키를 가지며, MIC와 접속할 준비가 됐다.
- 4. 사용자는 TTI에게 TGT-1와 세션키로 암호화한 TimeStamp를 보낸다. TTI는 TMK를 사용하여 TGT-1를 복호화하고 세션 키를 이용하여 TimeSta- mp를 복호화 한다. 사용자가 TTI의 세션 키를 사용할 수 있기 때문에 TTI는 정당한 사용자 인지를 확인 할 수 있다.
- 5. TTI는 사용자와 MIC를 위한 TGT-2를 각각 하나씩 만든다. 각 TGT-2에는 사용자 이름, MIC 이름, TimeStamp를 가지고 있으며 새로운 키인 KAB를 포함한다.
- 6. TTI는 서버의 TGT-2를 MIC의 마스터 키(MK)로 암호화 한다. TTI는 MK로 암호화 된 TGT-2를 사용자와 공유한 세션 키로 다시 암호화 하고 사용자에게 이것을 전송한다.
- 7. 사용자는 세션 키를 이용하여 MK로 암호화 된 TGT-2를 복호화 한다. 복호화로 인해 사용자는 MIC의 TGT-2와 KAB를 알 수 있다. 사용자는 KAB를 사용하여 TimeStamp를 암호화 하고 MIC에게 암호화 된 TimeStamp와 TGT-2를 보낸다. 두 가지를 받은 MIC는 MK를 사용하여 TGT-2를 복호화 하고 KAB를 이용하여 TimeStamp를 복호화 한다.

사용자와 MIC 모두 KAB를 가지고 있으며, 사용자가 TimeStamp를 암호화 하기 위해 KAB를 사용했기 때문에 사용자가 정당한 사용자인지 확인이 가능하다. 사용자 역시 MIC가 TimeStamp를 얻기 위해 KAB를 사용해야만 했기 때문에 MIC가 정당한 기기인지 알 수 있다.

3.3 검증 결과

기존의 인증방법에서는 사용자가 차량 내 M2M 기기와의 접속 요청 시 서버로 자신의 ID와 패스워드만을 이용하여 사용자가 정당한 사용자인지만을 확인하여 M2M 기기와의 접속이 허락됐다.

그러나 본 논문에서는 사용자가 제 3기관과의 암호화 및 키 교환을 통해 정당한 사용자 인지를 확인하고 M2M 기기 역시 제 3기관으로부터 사용자의 정보를 받아 정당한 사용자인지 1차 확인한 후, M2M 기기가 사용자와 키를 교환함으로서 사용자가 정당한 사용자인지 2차 확인을 한다. 이러한 암호화 및 키 교환으로 인해 사용자 역시 M2M 기기가 자신의 기기 맞는지에 대한 여부를 확인 할 수 있다.

4. 결론

본 논문에서는 텔레매틱스를 중심으로 차량 네트워크 보안의 취약성을 알아보고 차량과 이동통신 기술의 융합으로 인해 생성될 수 있는 새로운 비즈니스 모델을 제시해 보았다. 또한, 이동통신망 기술의 발전으로 사용자와 차량의 통신 중에 발생 될 수 있는 보안 취약성을 살펴보고 이 중 사용자와 차량 내 기기의 인증 취약성 공격에 대한 해결책을 제시하였다. 사용자, 차량 내 M2M기기, 제3기관 모두가 상호 인증을 받음으로서 허가받지 않은 사용자로부터의 위장 공격을 예방 할 수 있다.

참고문헌

[1] 김유창, “기기 간 통신(M2M)의 기술 동향과 전망”, 텔릿 코리아, 7월호 pp.66, 2009

[2] 이윤덕, "M2M 산업 현황 및 M2M/IOT 포럼 추진 현황", 2011

[3] 박성일, "이동통신망에서의 M2M 단말 기술", 한국 퀄컴, 2010

[4] 강상우, 박세진, "TPM의 Authenticated Boot를 활용한 VANET의보안 향상 기법 설계", 한국컴 퓨터종합

학술대회 논문집, Vol.36, No.1(D), 2009
[5] Douceur, J.: The Sybil Attack. In: First Intrnational Workshop on Peer-to-Peer Systems, March 2002, pp.251 - 260, 2002
[6] 여성권, 이근호 “텔레매틱스에서의 보안 동향”, 한국융합학회 하계 학술발표논문집, 2011