T-DMB 기반의 TPEG 업데이트 취약점을 이용한 공격 기법

김정훈, 고준영, 이근호
백석대학교 정보통신학부

An Attack Scheme with a T-DMB TPEG Update based Vulnerability

Jung-Hoon Kim, Jun-Young Go, Keun-Ho Lee
Division of Information & Communication, Baekseok University

요 약 다양한 지능형 자동차의 통신 방법의 개발이 편안하고 안전한 정보를 전달해주고 있다. 하지만 이러한 통신 방법의 개발 또한 보안을 생각해야 한다. 지능형 자동차에서 사용될 내비게이션의 업데이트 또한 무선 업데이트 방식을 사용하는데 현재 사용하고 있는 업데이트 방식은 신뢰할만한 보안 방식이 없는 실정이다. 자동차에 사용되는 내비게이션 통신은 국가별로 다양한 방법으로 TTI 서비스를 제공하고 있으며, 우리나라의 경우에는 대부분 T-DMB를 이용하여 TPEG 방식으로 정보를 전송해주고 있다. 내비게이션 무선 업데이트에 대한 특성을 파악하고, 신뢰 할 수 있는 업데이트 정보 전송을 위해 공격 시나리오를 작성 한 뒤 그에 따른 보안 대책을 제안한다.

• Key Words : APT 공격, 지능형 자동차, 텔레매틱스, 지상파디엠비, 티팩

Abstract The development of communication method for a variety of intelligent automobiles are delivering comfortable and safe information. However the development of such communication method must also think about security. Even the update of navigation to be used for intelligent automobiles uses the wireless updating methods but the updating methods currently being used has no reliable security measures. The navigation communications used in the intelligent automobiles are being provided with TTI(Traffic and Travel Information) service using a variety of methods by the countries. In the case of Korea, most are based on T-DMB using the TPEG method for transmitting the information. By identifying the characteristics on the navigation wireless update, a security solution is proposed for delivering the reliable update information after creating the attack scenario.

• Key Words : APT attack, Intelligent Vehicle, Telematics, T-DMB, TPEG

1. 서론

지능형 자동차에 사용되는 내비게이션 통신은 국가별로 다양한 방법으로 TTI(Traffic and Travel Information) 서비스를 제공하고 있으며, 우리나라의 경우에는 전송받은 정보를 실시간으로 업데이트 되어 도로정보 및 도로교통 상황 정보 등 을 운전자에게 보여주는 T-DMB(지상

이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2013R1A1A1A05012348)
*교신저자 : 이근호(root1004@bu.ac.kr)
2014년 7월 5일, 수정일 2014년 9월 16일, 게재확정일 : 2014년 9월 24일

파 DMB) 기반을 이용한 TPEG(Transport Protocol Expert Group) 방식으로 정보를 전송 해 주고 있다. 하지만 TPEG 송신서버에서 보내주는 정보를 내비게이션에서는 별다른 보안기술 없이 받기만 하고 있어 누군가 악의를 가지고 TPEG 송신서버를 해킹하여 내비게이션에 잘못된 정보를 보낸다면 운전자는 즉시 치명적인 사고를 입을 수 있고, 또한 사회적 혼란을 가져 올 수도 있을 것이다.

이렇듯 우리에게 편리함을 제공한다고 생각했던 자동차의 지능형 기술들이 해킹 등의 공격으로 사회적 혼란과 테러를 위한 수단으로 악용될 수 있는 가능성의 시나리오를 알아보고 이를 사전에 예방하기 위한 보안대책을 제안하고자 한다.

2. 관련 연구

2.1 지상파 DMB(T-DMB)

지상파 DMB는 음성, 영상 등 다양한 멀티미디어 신호를 디지털 방식으로 고정, 휴대, 차량용 수신기에 제공하는 방송 서비스이다. 이동 중에도 개인 휴대 정보 단말기(PDA)나 차량용 단말기를 통해 콤팩트디스크(CD)·디지털 비디오 디스크(DVD)급의 고음질, 고화질 방송을 제공하며, 제공 방식은 시스템 A, Dh 및 E의 3개 시스템이 있다. 시스템 A는 디지털 위성 방송과 지상파 디지털 멀티미디어 방송(DMB)의 유럽식 디지털 방송 규격(OFDM:직교 주파수 분할 다중 방식)을 따르고 있고, 시스템 Dh는 지상파 DMB를 기반으로 하되 위성 DMB를 수용하는 혼합 방식을 취하고 있으며, 시스템 E는 부호분할 다중 접속(CDMA) 방식과 거의 동일한 코드 분할 다중(CDM) 방식을 택하고 있다. 지상파 DMB는 T-DMB라고도 표기한다[1].

2.2 TPEG(Transport Protocol Expert Group)

TPEG란 실시간 교통 정보 데이터를 처리하여 국제 표준의 하나인 TPEG XML 형태로 저장 관리하고, 이를 이진 스트림 형태로 DMB를 포함한 디지털 방송망 및 인터넷 등을 통해 제공할 수 있도록 하는 새로운 TTI 시스템이다. TPEG은 RDS-TMC(Radio Data System-Traffic Message Channel)의 한계를 극복하여 높은 데이터 율을 가지며, 아울러 디지털 전송 매체에 적합하도록 개발되었다. 또한 DAB, Internet, DTV, DMB 등 여러 플랫폼 상에서 구현 가능하며, 텔레매틱스 단말, PDA 또는 이동통신 단말을 통하여 TTI 정보를 제공하는 수단으로 이용된다.

현재 TPEG 표준은 Part 1에서 Part 7까지 표준화가 완료되었으며, RTM(Road Traffic Messages), PTI(Public Transport Information), PKI(Parking Information), CTT(Congestion & Travel Time) WEA(Weather Information) 등이 있다[2].

[Fig. 1] TPEG Standard Offer Service

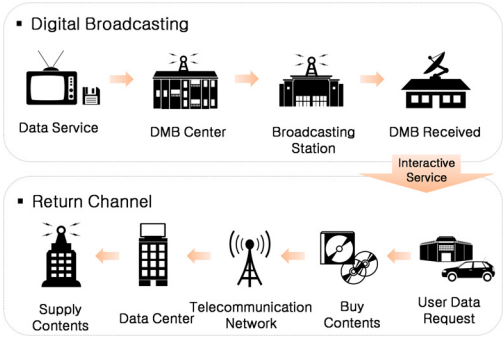
EIA(Environmental Information Alerts) 등이 추가될 예정이며, 우리나라를 비롯하여 독일, 영국, 스웨덴, 일본 등지에서 활발히 구현되고 있다. 특히 우리나라에서는 TPEG-CTT 서비스 표준이 2009년에 국가 표준 제정되었으며, DMB에 적용을 위한 표준도 2009년에 TTA 단체 표준으로 제정되었다.

TPEG 규격은 두 가지 형태로 제공된다. 즉 PC와 같이 인터넷 브라우저를 사용하는 장치를 타겟으로 하는 경우는 tpegML이 사용되며 해당 규격은 CEN/ISO TS 18234이다. 또한 차량 장치와 같이 이동통신망을 통하여 연결되는 장치를 타겟으로 하는 경우는 이진 규격으로 CEN/ISO TS 24530이 해당된다[3,4].

2.3 TPEG를 통한 내비게이션 업데이트 기법

교통정보 수집업체들은 수만 대의 택시, 버스, 물류차량 등에 장비를 설치해 정보를 수집한다. 교차로마다 설치한 위치 발신기 혹은 GPS를 통해 수집 차량들이 지나간 시간을 계산하고 이 자료를 바탕으로 도로 상황을 판

단한다. 여기에 한국도로공사로부터 고속도로와 국도의 정보를 받고, 교통방송으로부터 사고와 공사 정보 등을 받아 최종적으로 T-DMB 사업자에 전달한다.



[Fig. 2] TPEG Updated Principles

T-DMB 사업자들은 수집업체로부터 받은 정보를 변환해 TPEG 송신서버를 통해 내비게이션 단말기로 정보를 전송한다. 이 정보가 내비게이션 맵과 연동해 최종적으로 도로의 교통상황을 화면에 표시해주게 된다.

3. TPEG 취약점을 이용한 시나리오

해커들은 APT공격으로 교통대란을 발생시킬 수 있는 T-DMB 기반의 TPEG 데이터 조작으로 목표를 삼아 TPEG 송신서버의 시스템 취약점을 조사하기 시작한다.

TPEG 서비스를 시행하고 있는 회사들을 공격대상으로 정하고 각 회사에 대한 시스템, 소프트웨어나 하드웨어 등 정보수집을 한다. 또한 C&C 서버 PHP 웹페이지에 백신 솔루션에 탐지되지 않는 악성코드를 심어둔다. TPEG 서비스를 시행하고 있는 회사의 직원들이 자주 접할 수 있는 유명 사이트에 게시판 취약점(XSS 공격)을 이용하여 C&C 서버로 리다이렉트 시킨다. 직원들은 알아채지 못한 채 C&C 서버에서 악성코드를 다운 받게 되어 직원들의 컴퓨터는 해커에게 침투 당하게 된다. 해커들은 회사 내부망을 통해 TPEG 송신서버에 접근한다.

송신서버에서 내비게이션 단말기로 TPEG를 통해 조작된 업데이트 데이터를 보내게 된다. 이 과정을 이용하여 보안이 취약한 TPEG를 통해 조작된 업데이트 항목으로 공격대상의 차량 내비게이션에 접근한다. 공격자는 공격대상의 내비게이션에게 공격 메시지를 보내 잘못된 유가 정보, 잘못된 뉴스 등으로 사용자에게 혼란을 주거나 잘못된 경로 또는 혼잡한 경로로 길 안내를 하여 교통대란을 발생시킨다.

4. 대응방안

4.1 APT공격 대응 기법

4.1.1 관리적 보안대책

① 정보보호 규정 및 지침 강화 : 법률 및 제도의 시행에 다른 적용 대상 여부 및 파급 효과에 대해 종합적으로 검토하여 내부 규정 및 지침 제/개정을 실시한다.

② 임직원 인식제고강화 : 정보보안 교육 대상을 고려하여 일반 과정, 책임자 과정, 실무자 과정으로 구별하여 정보보호 교육 및 훈련 계획을 수립한다.

③ 정보보호 전담 조직의 강화 : 겸용을 자제하고 보안인력의 책임과 역할 등에 대해 충분한 고려를 하여 인력 운영방안을 수립한다.

④ 정보자산 분류 활동 강화 : 정보자산의 중요도 평가 및 보안 등급에 따른 보안 대책 수립한다.

⑤ 정보보안 활동 실시 : 안티바이러스 백신의 주기적 실행, 불법소프트웨어 및 비인가 프로그램의 지속적 관리, 운영체제의 주기적 보안패치, Clean Desk 및 Clean Office 활동을 실시한다.

⑥ 정기적인 대응훈련 : 대응훈련을 정기적으로 실시하여 보안위기 상황을 가정한 조직 내 각 부문 및 담당자의 역할 및 책임, 행동요령 등을 숙지시킴으로써, 능동적인 대응 실습을 통한 역량 강화를 실시한다.

4.1.2 기술적 보안대책

① 단말보안 : 내부정보가 외부로 유출되는 것을 차단하는 PC보안솔루션, 내부망과 외부망의 분리한다.

② 인증요소추가 : 시스템의 로그인시, OTP 또는 휴대폰 인증과 같은 인증 요소를 추가한다.

③ 무선망 통제 : 무분별한 Wi-Fi, Wibro, 비인가 AP 무선기기 사용을 차단한다.

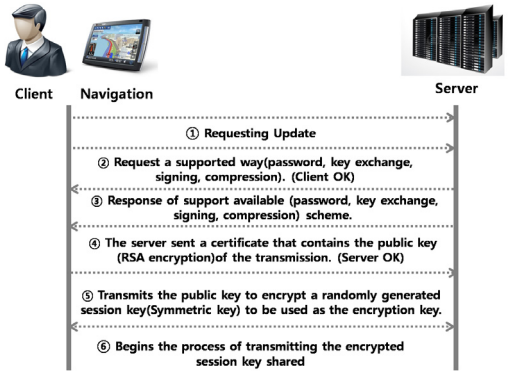
④ 인간 및 정보중심 보안정책 : 접근제어 강화와 암호화 등의 정보중심의 대응방안을 강화한다[5].

4.2 조작된 TPEG 업데이트의 대응 기법

APT 공격을 통한 공격 외에도 교통마비를 발생시킬 장소에 TPEG 송신기를 설치하여 공격할 경우에 대비한 대응 기법 2가지를 제안한다.

4.2.1 암호화 알고리즘 이용 기법

내비게이션이 TPEG을 이용한 업데이트를 할 때 아래와 같이 암호화 알고리즘을 이용하여 데이터를 암호화 한다.



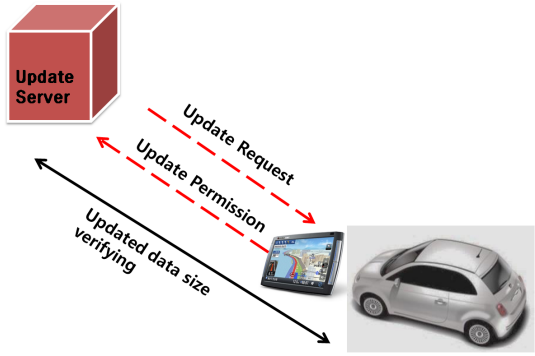
[Fig. 3] Encryption Algorithm

① 내비게이션이 송신서버에 업데이트 요청
② 내비게이션은 송신서버에게 지원 가능한(암호, 키 교환, 서명, 압축)방식을 알려준다.(Client OK)
③ 송신서버는 내비게이션에게 지원 가능한(암호, 키 교환, 서명, 압축)방식을 응답해 준다. (Server OK)
④ 송신서버는 공개키(RSA 암호용)가 포함된 송신서버의 인증서를 내비게이션에게 발송한다.
⑤ 만약 송신서버가 내비게이션의 인증서를 요구할 때 이에 대한 요청도 함께 발송한다.
⑥ Server OK 완료
⑦ 송신서버가 내비게이션의 인증서를 요구할 경우 인증서를 서버로 전송한다.
⑧ 내비게이션은 전송받은 송신서버의 인증서에 대해 내비게이션에 내장된 신뢰 기관으로부터 발급 여부를 확인한 후 암호화키로 사용될 세션 키(대칭키)를 랜덤으로 생성하여 공개키로 암호화해 서버로 전송한다.
⑨ 송신서버는 자신의 개인키로 내비게이션에게 전송받은 세션키를 복호화한다.
⑩ 송신서버는 협상 과정에서 전송된 모든 메시지에 대하여(암호, 키교환, 서명, 압축)방식을 다음부터 적용할 것을 알리는 종결 메시지를 발송한 후 데이터 전송단계로 이동한다.
⑪ 내비게이션은 협상 과정에서 전송된 모든 메시지에 대하여(암호, 키교환, 서명, 압축) 방식을 다음부터 적용할 것을 알리는 종결 메시지를 발송한 후 데이터 전송단계로 이동한다.
⑫ 앞 단계에서 서로 공유된 세션키로 암호화된 전송 과정이 시작된다.

위와 같은 암호화 알고리즘을 이용하여 해커의 악성코드가 삽입된 TPEG 데이터의 업데이트를 막을 수 있다.

4.2.2 업데이트 데이터 크기 비교 알고리즘

해커가 업데이트 데이터에 악성코드를 삽입하여 보내게 된다면 실제 업데이트 데이터 크기와 악성코드에 감염된 업데이트 데이터 크기는 다르게 된다.



[Fig. 4] Updated Data Size Comparison Algorithm

이러한 점을 이용하여 내비게이션은 업데이트 하고자 할 때 업데이트 파일을 송신하는 서버에 업데이트 데이터 크기를 검증하게 한다. 서버에서 알려준 데이터 크기와 수신 받고자 하는 업데이트 데이터 크기가 다를 경우 악성코드에 감염되었다고 판단하여 업데이트를 막는다.

5. 결론

국내 거의 모든 차에는 내비게이션이 장착되어 있다. 지능형자동차가 개발되고 보급화 됨에 따라서 내비게이션의 중요성은 더욱더 커져 갈 것이다. 하지만 현재 내비

게이션 무선 통신을 이용한 업데이트는 지정한 곳이나 신호가 잡히는 곳 아무 장소에서나 할 수 있다. 앞으로 이러한 취약점에 대해 보안 대책을 마련해 두지 않는다면 내비게이션을 장악하여 또 다른 치명적인 피해가 발생할 것이다. 내비게이션 지도의 업데이트를 담당하는 블루투스와 무선 AP 뿐만 아니라 교통 정보를 실시간으로 전송해 주는 TPEG 또한 앞으로 꾸준히 증가할 보안 위협에 대해 대책 마련을 준비해야 할 것이다. 보안 대책 마련을 위해 단순한 내비게이션 회사의 문제뿐만 아니라 방송사, 공공기관에서도 나서서 대규모 보안 위협 공격에 대한 대책을 강구함으로써 지능형 자동차통신 기반의 보안 기술 연구가 활발히 진행될 것으로 기대할 수 있다.

참고문헌

[1] Kil-Nam Oh, Bong-Soo Kim, Wan-Sik Choi, “An Application of T-DMB TPEG to Telematics”, KOCON, Vol. 3, No. 2, pp. 654-658, 2005.

[2] Byung-Soo Kim, Seung-Wook Min, "Design and Implementation of Assisted GPS Navigation Systems Using TPEG Protocol of Terrestrial DMB Data Services", KICS, Vol. 35, No. 11, pp. 1618-1623, 2010.

[3] ISO/TS 18234:2013 Intelligent transport systems -- Traffic and travel information via transport protocol experts group, generation 1 (TPEG1) binary data format, Part 1-6, 2013.

[4] Hwang-Soo Chun, " TPEG service Promotion Trends", ETRI, Vol. 22, No. 6, pp. 170-181, 2007.

[5] Seong-Baek Han, Seong-Gwon Hong, “Countermeasures in the financial sector for the APT attack”, KIISC, Vol. 23, No. 1, pp. 44-53, 2013.

저자소개

김 정 훈(Jung-Hoon kim) [학생회원]

· 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 학생

<관심분야> : M2M, TPEG, 이동통신보안

고 준 영(Jun-Young Go) [학생회원]

· 2009년 3월 ~ 현재 : 백석대학교 정보통신학부 학생

<관심분야> : M2M, TPEG, RFID/USN, 이동통신보안

이 근 호(Keun-Ho Lee) [종신회원]

· 2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)

· 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원

· 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수

<관심분야> : M2M 보안, 이동통신 보안, 융합 보안, 개인정보보호