자동차 내부망 통신네트워크 해킹범죄예방을 위한 융합보안적 대응방안: Bluetooth 활용사례를 중심으로

최관* · 김민지**

요 약

이 연구의 목적은 Bluetooth를 활용한 자동차의 내부망 통신네트워크를 해킹공격으로부터 예방하기 위한 대응방안을 제시하기 위함이다. 이를 위해 2장에서는 자동차 통신네트워크의 정의와 내부망 통신네트워크의 종류에 대해서 살펴보았다. 3장에서는 자동차 내부망 통신네트워크 해킹위험성을 분석하기 위해 Bluetooth에 의한 해킹범죄사례를 살펴보았다. 4장에서는 본 연구의 결과로서 첫째, 『자동차안전기준에 관한 규칙』 개정이 이루어져야 한다. 동법에서는 전자제어시스템의 정의 및 기준사항과 안전운행을 위한 제작 및 정비를 규정해 놓았음에도 불구하고 전자제어시스템을 대상으로 한 해킹범죄 예방 및 방어와 관련된 보안프로그램 혹은 펌웨어 등의 제작과 관련된 규정이 없는 실정이다. 둘째, 자동차의 전자제어시스템 기술의 복잡성에 기인된 자동차 통신네트워크를 보호하고자 자동차 통신네트워크 보호 법률이 신설되어야 한다.

Convergence Security Approach for Motor Vehicle Communication Network Hacking Attack Prevention: Focus on Bluetooth Cases

Choi Kwan* · Kim Minchi**

ABSTRACT

The purpose of this study is to analyse motor vehicle communication network hacking attacks and to provide its prevention. First, the definition of motor vehicle communication network was provided and types of in-vehicle communication network were discussed. Also, bluetooth hacking attack cases were analysed in order to illustrate dangers of hacking attacks. Based on the analysis, two preventive measures were provided. First, Motor Vehicle Safety Standard Law should be revised. Although the law provides the definition of electronic control system and its standards as well as manufacturing and maintenance for safe driving standards, the law does not have standards for electronic control system hacking prevention and defensive security programs or firmware. Second, to protect motor vehicle communication network, it is necessary to create new laws for motor vehicle communication network protection.

Key words : In Vehicle Network, Preventing Hacking Attacks, Bluetooth, Hi-Tech Crime, Convergence Security

접수일(2016년 9월 29일), 수정일(1차: 2016년 10월 30일), 게재확정일(2016년 10월 31일)

* 삼성교통안전문화연구소 책임연구위원, (주저자)
** 숙명여자대학교 사회심리학과 교수 (교신저자)

1. 서 론

오늘날 현대사회는 IT(Information Technology: 이하 IT)기기를 통하지 않고서는 업무가 이루어지지 않는 세상이 되었다. 자동차 역시 마찬가지로 단순히 달리는 존재에서 오늘날에는 운전자의 상황에 맞추어 교통안전과 관련된 모든 정보들을 제공하고 첨단기술들을 통해 운전자를 지원하는 소위 '개방된 네트워크에 기초한 지능형 운송수단'의 개념으로 탈바꿈하였다. 그 결과, 고가의 IT장치들이 자동차에 설치되면서 이에 대한 여러 가지 보안상의 문제들이 발생하는 역기능들이 나타나고 있다.

2016년 9월 22일 중국의 긴보안연구소는 자율주행 전기차를 생산하는 테슬라의 S모델 시리즈를 해킹을 통해 원격 조정하는 모습을 선보였다. 구체적으로, 주행 중인 차를 급제동시키는 모습을 선보이기 위해, 차량의 19km 떨어진 곳에서 노트북을 이용해 자동차 내부망에 접속 후 조작하여 브레이크를 걸었고, 차선 변경 때 백미러를 접거나 방향지시등을 켜고 트렁크를 열기도 하였다. 또한 테슬라의 신형모델인 S75D를 주차모드에서 조정하여 문을 열거나 좌석을 앞뒤로 움직이는가 하면, 차량에 탑재된 인터넷 브라우저 터치스크린을 무용지물로 만드는 것을 선보임으로써 자동차 내부망을 통한 통신네트워크 해킹범죄의 심각성을 잘 보여주었다[14].

구체적으로, Bluetooth와 같은 기능에 기초한 통신네트워크시스템이 자동차에 설치되면서 원격에 의한 자동차구동이 가능해지면서 범죄자들에 의한 악의적인 조작과 공격이 가능해졌기에 심각한 문제가 아닐 수 없다. Bluetooth는 IEEE 802.15.1에서 표준화된 무선 통신 기기 간에 가까운 거리에서 낮은 전력으로 무선 통신을 하기 위한 표준. 10m 이내의 거리에서 3 Mbps 정도의 데이터를 전송하는 기술로 복잡한 설정 없이도 Bluetooth호환 기기라면 곧바로 인식 가능하다. Bluetooth의 적용 범위는 휴대 전화나 노트북, MP3를 비롯한 휴대용 IT 기기에서 자동차나 TV, 냉장고, 운동 기구, 의료 기기까지 확대되고 있다. 1998년 노키아, 소니, 에릭슨, 인텔, 마이크로소프트, 도시바, 레노버, 7개 회사가 표준화 기구인 Bluetooth SIG를 결성한 것이 시초이며, 현재 삼성전자와 LG전자를 포함한 1만 개 회사가 회원으로 가입해 장비끼리 서로 운용을 보장하기 위해 협력하고 있다. Bluetooth는 1999년 버전 1.0 발표 뒤 지속으로 성능을 개선하여 2009년에는 전송 속도를 3Mbps에서 20~100Mbps까지 끌어올린 버전 3.0을, 2010년에는 낮은 전력 기술을 구현할 수 있는 버전 4.0이 상용화되었다. 이러한 기술의 발전과 함께 역기능 또한 발생하고 있는데 이미 영국과 호주에서는 Bluetooth를 활용한 해킹범죄들이 발생하고 있다. 그러므로 IT강국인 한국 역시 거시적 측면에서 사이버위기관리를 위해 대응방안을 고려할 필요성이 제기된다. 이에 본 연구의 목적은 자동차 통신네트워크의 개념에 대해서 살펴보고, Bluetooth에 의한 자동차내부망 해킹에 대한 위험성을 사례분석을 통해 살펴보고 대응방안을 제시하는 것이다.

2. 이론적 배경

2.1 자동차 통신네트워크

전자제어시스템(Electronic Control Unit: 이하 전자제어시스템)이란 자동차의 전기시스템 혹은 서브시스템 중에서 하나 이상을 통제하는 임베디드 시스템인 엔진제어장치로서 엔진구동을 총체적으로 통제하는 시스템이다. 이 시스템의 기술발전은 자동차 통신네트워크의 등장을 불러왔는데, 최초로 도입된 시기는 1988년 보쉬(Bosch)사에서 처음 개발한 계측제어통신망(Controller Area Network; CAN)으로부터 시작되었다. 계측제어통신망은 기존의 자동차부품들이 유선방식으로 연결되어 있던 것을 모두 무선연결화하여 궁극적으로 자동차의 무게를 덜 나가게 만들고 연비를 절감하는데 기여하였으며, 배기가스배출을 대폭 감소시킴으로서 자동차성능을 크게 향상시켰다[3].

자동차통신네트워크는 크게 내부망(In Vehicle Network)과 외부망(Vehicular Ad-hoc Network)으로 구분된다. 첫째, 내부망은 차량 내 감지기나 전자장치 간 유무선 통신 네트워크, 차량본체 및 섀시 부분과의 접속을 통해 제어하는 계측 제어기 통신망(CAN), 오디오, 앰프, 콤팩트디스크 플레이어 등 멀티미디어 접속을 위한 차량 네트워크 시스템(MOST), 그리고 브레이크나 조향 장치와 연결이 이루어지고 통제하는 X

-by-Wire(Flexray) 등으로 이루어져 있다. 둘째, 외부망은 자동차의 외부통신네트워크를 원활히 지원하는 무선통신시스템으로서 일반적으로 텔레매틱스 서비스를 중점적으로 지원하는데 활용된다.

먼저 자동차 내부망은 자동차 내 센서나 개인들을 위한 컴퓨터 하드웨어를 구성하는 한 부분으로서 컴퓨터와 연결이 이루어진 주변기기와 전자부품의 기능들을 확장시키기 위하여 컴퓨터에 연결된 일체의 장치파일과 장치드라이버 인터페이스인 전자장치 디바이스(Device)를 연결하는 역할과 자동차의 전자제어시스템으로 제어정보데이터를 보내는 역할을 하며 구체적인 종류는 아래 <표 1>과 같다[8].

<표 1> 내부망 통신네트워크 종류

구 분	내 용
계측제어 통신망 (CAN)	자동차의 바디나 미터·엔진부분과 연결 그리고 관리하는 통신네트워크
자동차 네트워크 시스템 (MOST)	자동차의 내비게이션, 오디오, 앰프, CDP와 같은 멀티미디어 기기들을 서로 이어주는 통신네트워크
전기신호 제어장치 (FLEX RAY)	엔진 및 브레이크나 조향장치를 서로 이어주고 관리하는 통신네트워크
근거리 연결통신망 (LIN)	바디계의 도어미러나 윈도우를 관리하는 통신네트워크
지능형교통 시스템 인터페이스 (IDB-1394)	오디오나 자동차용 카메라 등과 연결서비스를 통해 제어하는 통신네트워크

출처: 조아람, 조효진, 손영동, 이동훈, 2012.

그리고 추가적으로 자동차 통신네트워크와 관련된 외부망 역시 크게 2가지로 구분가능하며, 자세한 내용은 아래 <표 2>에 정리되었다.

<표 2> 외부망 통신네트워크 종류

구 분	내 용
자동차 대 자동차 통신네트워크 (V2V)	정보전달 과정에서 인프라 없이 자동차 대 자동차의 통신망을 통해 자동차추돌경고 서비스 혹은 그룹통신제공 등을 지원하는 통신네트워크
자동차 대 인프라 통신네트워크 (V2I)	자동차와 유선 혹은 무선통신의 인프라망과 연결되어 단말기 그리고 서버스 사이의 통신지원을 통해 자동차 IP를 통한 교통정보, 안전지원, 다운로드와 같은 서비스를 지원하는 자동차와 인프라 통신망

출처: 김광조, 이동수, 2014

2.2 내부망 통신네트워크 종류

상기의 <표 1>과 같이, 내부망 통신네트워크의 종류는 크게 5가지로 구분가능하다.

2.2.1 계측제어통신망 (Controller Area Network: CAN)

계측제어통신망은 자동차 내부의 컨트롤러와 시스템구동 및 제어에 필요한 기계장치를 지칭하며 전기 혹은 유압 그리고 압축공기를 수단으로 하는 원동구동장치로서, 통상적으로 전류 그리고 작동유압 및 기력압 형태로 이루어진 에너지원으로 작동이 이루어지고 기존의 에너지를 다른 형태의 움직임으로 전환시키는 역할을 담당하는 센서·액추에이터(Actuator: 이하 액추에이터) 그리고 오디오시스템과 Bluetooth를 추가적으로 전자제어시스템에 이어주기 위해 만들어진 통신 프로토콜이다. 계측제어통신망의 장점은 데이터 전송률이 높고 또한 다수의 전자제어장치들을 서로 연결하여 실시간으로 효율적으로 제어가 가능한 분산제어 네트워크이다[1].

그러므로 자동차 진단 및 유지관리, 도난방지와 같은 서비스는 일반적으로 텔레매틱스 소프트웨어 플랫폼에 의해 기술실현이 이루어지는데, 계측제어통신망 드라이버와 액서스 스택에 근거하여 Bluetooth와 USB 드라이버 스택구현 또한 가능하다[7].

계측제어통신망의 통신규격은 메시지에 포함된 ID의 길이에 따라 크게 두 가지 형태로 분류된다. 첫째, 동급버전에 의해 송신된 메시지만 수신하는 표준 계측제어통신망과 계측제어통신망 2.0A와 2.0B Controller를 통해 송신된 메시지 전부를 수신하는 확장 계측제어통신망으로 나누어진다[5]. 또한, 프레임은 모두 4가지 형태로 구현가능하고 아래 <표 3>의 형태를 띤다.

<표 3> 내부망 통신네트워크 종류

구 분	내 용
Data Frame	데이터 전송기능 담당
Remote Frame	데이터 프레임의 전송요구 담당
Error Frame	지역적으로 감지된 에러의 전역적인 신호역할 담당
Overload Frame	데이터 프레임과 리모트 프레임들의 앞·뒤에서 메시지간의 전송간격조절

결론적으로, 계측제어통신망은 자동차 네트워크 분야를 기본으로 철도나 선박 그리고 의료 및 산업네트워크 분야까지 다양하게 활용되고 있다. 뿐만 아니라, 계측제어통신망 확장 규약에 의거하여 비행기 혹은 제트기 조종석 그리고 항법장치에도 널리 사용된다.

2.2.2 자동차네트워크시스템 (Media Oriented System Transport: MOST)

자동차네트워크시스템은 일반적으로, 자동차에 설치된 오디오나 내비게이션과 같은 멀티미디어 기능들 사이의 구동을 위해 만들어진 전자제어시스템이다. 또한, 자동차 통신네트워크 디지털장치를 통합시켜 구현이 가능하도록 지원하는 정보계열의 통신네트워크이다[10].

자동차네트워크시스템은 대용량 멀티미디어 데이터들 사이의 실시간 전송과 제어 그리고 최적화 과정을 통해 이를 제공하는 스트리밍 그리고 패킷기반의 정보전송을 기본으로 하고 있다[12]. 특히, 스트리밍은 컴퓨팅에서 데이터 요소의 시퀀스를 참조하는 대부분의 경우에 시간경과에 따라 다양한 방법으로 활용된다. 이는 스트리밍 항목이 크게 배치함에 비해 한 번에 하나씩 처리되는 것을 원칙으로 하고 있다. 또한, 자동차에 부착된 오디오 혹은 내비게이션과 같은 디지털기기를 보유하고 있는 내부컴퓨터의 멀티미디어 네트워크에 최적화되어 있다는 장점이 있지만, 다른 통신시스템과 비교하여 상대적으로 복잡한 인터페이스를 기반으로 구축되어 있다는 단점이 있다.

2.2.3 전기신호제어장치(Flex Ray)

2016년 현재 자동차의 높은 안전성과 편리성이 중요시 되면서 전자제어시스템의 데이터량 또한 늘어나고 있다. 이에 기존의 계측제어통신망으로는 모든 데이터들을 효과적으로 관리하기가 불가능하다는 문제점이 발생되었고 이를 보완하는 목적을 위해 고안된 것이 바로 '전기신호제어장치'이다[6]. 전기신호제어장치는 기계 혹은 유압으로 제어하던 스티어링 휠 혹은 브레이크와 같은 장치들을 통신네트워크 기술에 기반을 두어 전자적으로 관리하는 기술로 계측제어통신망의 통신 속도보다 빠르면서 신뢰성이 높은 것이 장점이다. 일반적으로 자동차 그리고 해당 운전자안전과 직접적으로 관련된 브레이크 제어시스템에 필수적인 전기신호제어장치는 비트전송률이 최대 20Mbps로 계측제어통신망의 최고 1Mbps인 전송속도와 비교하여 20배 더 빠른 속도를 지니고 있다[9].

2.2.4 근거리 연결통신망 (Local Inter connect Network: LIN)

근거리연결통신망은 계측제어통신망 이후에 탄생한 직렬 통신 프로토콜이며 자동차의 내부 분산시스템을 위해 만들어진 저비용 싱글마스터 통신방식을 기본으로 하고 있다. 본 통신망의 데이터 최대속도는

20Kbps 이며 저속 계측제어통신망의 6분의 1 수준으로 자동차의 썬루프나 도어 미러 그리고 후방주차보조시스템 및 시트제어를 관리하는 Body System에만 한정되어 사용되는 단점이 있다. 또한, 자동차와 해당 운전자안전과 관련된 분야에는 사용이 어렵다는 단점이 있다[2].

근거리연결통신망시스템은 통신 관리를 목적으로 단일마스터인 LinBus를 가지고, 최대 15개로 구성되어진 Multiple Slave노드를 구축하고 있다. 또한 일반적으로 계측제어통신망 프로토콜과 함께 사용된다[4]. 근거리연결통신망-계측제어통신망 Gateway를 통해 계측제어통신망 네트워크에 다양한 감지기들로부터 전달받은 데이터를 재전달하는 역할을 주로 담당한다.

2.2.5 지능형 교통시스템인터페이스(ITS Data Bus-1394: IDB-1394)

지능형 교통시스템인터페이스는 원래 가전제품을 중심으로 개발되었던 IEEE 1394(In Stitue of Electrical and Eletronics Engineers 1394; 1394 표준전자기술)를 바탕으로 데이터버스정보전송시스템방식에 기초하여 자동차 멀티미디어 그리고 텔레매틱스를 목적으로 개발되었다. 지능형 교통시스템인터페이스는 자동차 내 DVD, PC, 후방 카메라, 오디오, 내비게이션 등에 적용되고 있고 통신속도는 최소 400Mbps ~ 최대800Mbps이상으로 다른 내부망 통신네트워크(계측제어통신망, 자동차네크워크시스템, 전기신호제어장치, 근거리연결통신망)들의 정보전달 속도와 비교하여 훨씬 빠르고 최대 63개의 노드를 지원가능하다[6]. 이러한 지능형 교통시스템인터페이스는 자동차 내 멀티미디어나 관련 콘텐츠를 지원함에 있어 서로 상이한 채널에 의해 동시에 여러 전송이 가능하다는 장점이 있지만, 지능형 교통시스템인터페이스만으로는 사용이 불가능한 단점이 있다.

3. 자동차 내부망 통신네트워크 해킹 위험성 분석

3.1 해킹범죄와 Bluetooth 관계

자동차의 내부에 적용 가능한 Bluetooth 기술은 일상에서 통상적으로 사용이 되고 있는 Bluetooth의 성능과 큰 차이가 없다. 2016년 현재 한국의 경우, 차량에 Bluetooth 연결을 위한 포트는 카오디오, 즉 계측제어통신망 시스템에 연결되어 작동하도록 되어 있다. 일반 자동차에서 종종 Bluetooth 기능서비스를 활용하였던 운전자들이 자동차시동을 걸게 되면 자동적으로 페어링 과정으로 나아갈 수 있도록 스캔준비 상태가 이어지는데, 이와 같은 Bluetooth 서비스 기능을 악용한 사례들이 나타나고 있다.

Bluetooth 서비스는 근거리에서의 무선데이터에 의한 통신이지만 자동차 전자제어시스템과 쌍방으로 데이터 송 ·수신이 이루어지기에 서로 간 상호연결을 기반으로 한 PAN(Personal AreaNet Work;개인통신망, 이하 PAN) 구성이 가능해지는 것이다. Bluetooth 서비스는 모바일기기와의 접속을 통해 핸즈프리 장치연결 및 MP3 감상 역시 가능하다. 그러나 상기의 기능 역시 범죄자들에 의해 자동차 안에서 이루어지는 대화 및 통화내용을 녹음할 수 있어 사생활 노출의 문제가 발생한다[11].

일반적으로, Bluetooth를 해킹범죄에 이용하려는 시도는 공중에 존재하는 전파를 스캐닝 하는 단계부터 출발한다. 그 이유는 보안과 관련된 어떠한 추가사항들이 존재하지 않으므로 Bluetooth의 기초적인 PIN 코드를 활용해 목표물과 연결을 시도하게 되는 것이다. 사업용 그리고 비사업용 자동차의 Bluetooth는 계측제어통신망을 기본으로 무선통신을 시도하게 되며, 내부가 아닌 외부로부터 Bluetooth가 확인이 되면 자동차에 내재된 초음파센서 혹은 적외선센서를 활용하게 된다[13].

자동차 내부망 통신네트워크 해킹을 위한 가장 첫 번째 단계는 '스캔과정'이라 할 수 있다. 범죄자의 Bluetooth가 해킹범죄의 목표인 자동차의 Bluetooth과 연결되기 위해 접속가능한 장치를 찾아가는 과정으로 규정할 수 있고, 일반적으로 휴대 전화에 장착하여 전화기를 손에 들지 않고도 상대방과 통화 가능하도록 지원하는 장치인 Hands Free 혹은 음향재생을 두 계통의 회로로 좌우를 분리하여 입체감 있는 음향을 만들어내는 장치인 Audio의 Stereo 장치들 위주로 탐색하게 되며, 이렇게 탐색과정이 끝나면 연결과정으로

넘어간다.

두 번째, '연결단계'에서는 PIN 번호를 입력하게 된다. PIN번호는 일반적으로 자동차의 Bluetooth 공장에서 제조 및 출하할 때 기본적으로 설정된 PIN번호는 단순한 숫자조합으로 이루어져 있다. 국내의 00자동차의 경우 '1234'로 설정하는 실정이다.

한국의 경우 자동차를 구매하는 구매자들은 보통 설정되어 있는 PIN 번호를 변경 없이 사용하는 경우가 대부분의 경우를 차지한다. 셋째, 자동차주변기기에 대한 Bluetooth 연결은 페어링 단계에서 상대방의 PIN번호 요구 및 입력과정을 통해 다시 한 번 상대방의 연결허가를 요구하고 최종적으로 Bluetooth 연결이 성공적으로 이루어지게 된다. 하지만 Bluetooth가 장착된 카 오디오에 연결하여 음악이나 송수신하고 있는 전송 내용 등을 빼낼 수 있는 카위스퍼(Carwhisperer)등과 같은 소프트웨어를 이용하여 상기의 장상적인 연결과정 역시 쉽게 우회가 가능하다[7].

자동차보안과 관련된 해킹범죄를 시도할 때, 해킹범죄 목표인 자동차의 오디오화면에 이러한 불법적 시도가 인지되지 않기 때문에 해당 자동차 운전자는 자신의 자동차에서 블루투스 연결에 의한 해킹문제가 발생한다는 것을 인지하지 못한다. 이러한 현실적 문제로 인해 Bluetooth가 연결된 장치들을 활용하여 해당 운전자의 개인적인 정보를 불법적으로 습득이 가능하며 이는 다시 2차 범죄로 악용된 소지가 빈번하다. 예를 들어, Bluetooth를 통한 1차 정보를 기반으로 전자제어시스템의 송수신 관련 데이터를 조작하여 자동차의 오작동을 인위적으로 발생시킬 수 있고 자동차 자체를 원격제어 역시 가능하다. 21세기 첨단 자동차는 도난 등의 물리적인 측면의 보안에서부터 원격제어, 브레이크, 열선에 이르기까지 대부분의 주변기기들이 차량 내부통신과 연결되어 있어 Bluetooth에 기반을 둔 해킹범죄에 취약하다. 스마트폰의 경우 해킹범죄 예방을 위해 전원을 끄는 방법도 있지만 일반 자동차의 경우는 이러한 방법이 불가능하다. 그 이유는 자동차는 그 사용자가 운전을 위해 시동을 구동하는 동시에 자동차 주변시스템들이 일제히 구동을 하게 되므로 계측제어통신망과 기타 여러 시스템들이 함께 동작하기 때문이다[3].

결론적으로, 이러한 Bluetooth의 단점을 활용하여 해킹범죄를 성사시키려는 노력은 출퇴근이 복잡한 시간대 혹은 자동차극장과 같은 곳에서 자주 발생한다. 특히, 자동차극장의 경우 라디오 주파수를 통해 영화감상이 이루어지는 형태여서 라디오 기능 혹은 자동차의 오디오 시스템을 구동하여야 설정이 이루어지므로 해당 운전자가 의식적으로 Bluetooth 기능을 하거나 꺼놓지 않은 이상 스캔가능 상태에 놓이므로 작동이 가능하게 된다. 자동차의 오디오시스템은 작동하지만 Bluetooth는 페어링이 안 된 상태에서 스캔 대기상태가 이어지므로 해커와 같은 사이버범죄자들이 Bluetooth를 기반으로 하여 자동차해킹 시도 시 범죄성공을 위한 최적의 요건이 완성되는 것이다.

3.2 Bluetooth 활용한 해킹사례 및 위험성 분석

3.2.1 해킹사례

"2015년 호주에서는 컴퓨터를 활용한 자동차 신종범죄들이 급증하면서 경찰, 검찰, 법원, 교정기관, 보호관찰소 등의 형사사법기관(Criminal Justice Agencies)들을 당혹스럽게 만들고 있는데, 자동차 문을 무단으로 열어 자동차안의 귀중품 등을 불법적으로 훔치는 사례는 있었지만, 컴퓨터를 활용하여 자동차의 잠금장치와 경보장치를 무력화시켜 자동차절도를 일삼는 수법의 대중화는 처음이었기 때문이다. 적외선 포트가 내장된 초소형 휴대 컴퓨터인 팜톱 PC를 이용해 원격조종장치가 설치된 자동차의 잠금장치 암호를 해독하는 수법으로 차의 문을 여는데 10초라는 시간 밖에 소요되지 않았다.

또한 침입흔적 역시 남지 않아 용의자를 추적하기에 어려움이 따랐다. 그러나 호주자동차협회에서는 원격잠금장치시스템은 사용할 때마다 암호변경으로 인해 안전과 보안에 문제가 없다고 발표하였지만 최신형 승용차의 원격잠금장치 암호까지 해독하여 그 피해가 증가하였다. 이에 호주자동차보험수리연구센터가 적외선을 이용한 원격조종장치를 장착하고 있는 약 4백만 대의 자동차가 이 신종수법 범죄의 피해를 입을 위험에 처할 것으로 예측하였고, 자동차보험협회는 자동차에 명백한 침입흔적이 없는 경우 도난 사실 확인이 불가능해 보상을 둘러싼 분쟁 또한 빈번하게 발생할 것으로 예측하여 신종범죄수법으로 인해 사회적으로 많은 문제점을 낳는 계기가 되었다."

3.2.2 위험성 분석

상기의 근거리 무선통신망을 활용한 자동차 해킹 피해사례는 자동차잠금장치의 통신데이터 주파수를 맞추어 그 기능을 해제시킨 사례로서 Bluetooth기술에도 접목 가능한 범죄수법이다. 자동차잠금장치를 무선리모콘으로 통제가능하다는 사실을 악용해 범행을 저지른 경우로서 무선리모콘 역시 근거리 통신 데이터의 일종에 속하기 때문이다[11]. 우리가 일상에서 사용하는 TV 리모콘의 원리를 적용한 근거리 적외선 통신프로토콜로서 자동차 해킹의 경우 다른 범죄와는 달리 범죄행위에 대한 흔적을 찾기가 거의 불가능하므로 보험적용이 어려워 민사소송으로까지 이어질 수 있고 보험사기범죄에도 악용될 수 있다. 그리고 Bluetooth기술에 기반을 둔 자동차해킹의 경우와 유사해 Bluetooth를 해킹하여 자동차의 오류나 원격제어 발생 등으로 예기치 않은 문제로 이어질 수 있기에 더욱 심각하다.

적외선 포트에 기반을 둔 기법은 기술적인 측면에서 Bluetooth기술보다 매우 제한적일 수 있다. 즉, 적외선 포트의 통신거리는 최대 1m로 매우 좁은 근거리 내에서 30도라는 일정한 각도 유지와 방해물이 없어야만 통신이 가능하다. 하지만 Bluetooth의 경우 적외선 포트보다 훨씬 넓은 적용범위와 데이터 전송속도 또한 보다 빠른 무선 통신프로토콜로서 해당 범죄발생피해가 심각할 것으로 예상된다.

이처럼 1998년 Bluetooth가 만들어진 이래로 사용자 정보암호화를 위해 E 알고리즘에 기반을 둔 4개의 선형 귀환 이동 레지스터를 갖는 합산수열 발생기를 사용해오고 있다. 합산 수열 발생기는 일정한 클럭을 갖는 이진 LFSRs((Non-linear Feedback Shift Register): 이하 LFSRs)를 활용하여 왔고 보다 빠른 암호속도와 복호속도가 지원되어 스트림 암호에 일반적으로 활용된다[6]. LFSRs는 간단한 전기역학이나 전자회로로 쉽게 구성할 수 있고, 긴 주기와 매우 균일한 분포 출력을 얻을 수 있다는 장점으로 스트림 암호로 군대 암호학 분야에서 의사난수생성기로 오랫동안 사용되어 왔다. 하지만 LFSRs의 출력은 암호을 상당히 단순하게 하는 완전한 선형이라는 문제점이 있다. LFSRs 상태로부터 몇 비트의 비선형 조합·두개 이상 LFSRs 출력의 비선형 조합·LFSRs의 불규칙적인 클록 주기라는 세 가지를 LFSRs 기반의 스트림 암호의 단점을 해결하기 위해 쓰이고 있다. LFSRs 기반의 스트림 암호는 A5/1,A5/2,E0과 시링크 생성기가 포함된다.

또한, LFSRs는 일정한 유형의 선형성으로 출력 수열로부터 어렵지 않게 암호해독이 가능하다는 특징이 있어 도리어 그 취약성에 노출될 수 있다. 결국 보안이 가미된 합산 수열 발생기 형태의 E 알고리즘을 개선하여 선형 LFSRs 중 일부를 비선형 NFSR로 교체시켜 클럭을 랜덤화한 후 순환클럭을 조정함으로써 출력되는 키 수열의 안전성을 높일 필요가 있다.

4. 대응방안 및 결론

상기의 Bluetooth기술에 의한 자동차 내부망 통신네트워크 해킹문제를 예방하기 위해 2가지 대응방안을 제시하고자 한다. 첫째, 『자동차안전기준에 관한 규칙』을 개정할 필요가 있다. 동 규칙은 자동차의 중량이나 규격, 제동장치, 조향장치 및 부품의 규격사항들을 규정해 놓음으로서 전자제어시스템에 관한 제동사항 역시 함께 규정되어 있다. 하지만 전자제어시스템의 정의 및 기준사항과 안전운행을 위한 제작 및 정비를 규정해 놓았음에도 불구하고 전자제어시스템의 사이버보안을 위해 보안프로그램 혹은 펌웨어 제조 및 제작과 관련된 규정이 없으며, 무엇보다도 안전한 자동차운행 그리고 정비목적의 규정에서도 사이버보안과 관련된 내용들을 찾아볼 수 없다. 자동차 통신네트워크 해킹으로 인해 자동차의 전자제어시스템에서 예기치 않은 원격제어나 오류 등이 발생할 것을 감안하여 자동차 통신네트워크 및 전자제어시스템을 보호하기 위한 보안프로그램이나 펌웨어 등의 제작 및 보호규정사항이 의무적으로 추가될 필요가 있다.

둘째, 자동차 통신네트워크 보호 법률을 신설할 필요가 있다. 2016년 오늘날의 자동차는 전자제어시스템에 의해 작동되고 있다. 자동차 통신네트워크를 통하여 텔레매틱스 및 원격제어 서비스 지원이 가능해짐에 따라 해킹으로부터 보안취약성이 날로 증가하고 있다. 이에 정보통신기술 그리고 물리적 기술이 융합된 융합기술로 이루어진 해킹범죄위험을 사전예방하

기 위해 독립된 법률이 필요하다.

오늘날 많은 국민들이 자동차를 이용한다는 점에서 개인의 생명과 신체 및 재산을 위협하는 범죄에서부터 국가적 위기를 촉발시킬 수 있는 신종범죄 및 테러범죄까지 자동차 해킹피해는 다양하게 발생가능하기 때문이다. 그리고 자동차의 경우, 일반통신네트워크에서 발생할 개연성이 높은 해킹과 유사한 유형으로 이는 자동차 통신네트워크에 침투하여 위험을 발생시키기가 보다 용이하기에 해킹 발생이 더욱 빈번할 것이다. 그러하기에 이러한 자동차의 전자제어시스템 기술의 복잡성에 기인된 자동차 통신네트워크를 보호하고자 단독법령이 필요하며, 이를 통해 Bluetooth기술에 의한 자동차 내부망 통신네트워크 해킹문제를 예방하고 국민안전, 나아가 국가안보까지 확보하기 위한 노력이 선행되어야 한다.

참고문헌

[1] 강동주, 이종주, 이영, 이임섭, 김휘강, “전력 SCADA 시스템의 사이버 보안위험평가를 위한 정량적 방법론에 관한 연구”, 정보보호학회논문지, 23(3), pp. 445-457, 2013.

[2] 강영두, ‘원전 계측제어 시스템 사이버보안성 평가 방법 연구’, 전북대학교 대학원 박사학위 논문, 2011.

[3] 김광조, 이동수, “escar회의 등을 통한 각국의 자동차 보안기술 연구동향”, 정보보호학회지, 24(2), pp. 7-20, 2014.

[4] 김진우, 한태만, “차량 내 인포테인먼트를 위한 표준 오픈 플랫폼 동향 및 GENIVI기반의 휴먼 머신 인터페이스”, 정보과학회 논문지, 29(6), pp. 444-452, 2012.

[5] 고종빈, 이석준, 손태식, “스마트그리드 제어시스템 보안 위협 평가방안 연구”, 정보보호학회논문지, 23(5), pp. 873-883, 2013.

[6] 이동훈, "자동차 보안 이슈와 표준화 동향", OSIA Standards & Technology Review, 27(2), pp. 56-64, 2014.

[7] 이혜련, 김경진, 정기현 ,최경희, 박승규, 권도근, “자동차용 ECU의 CAN메시지를 통한 자동차 공격 방법연구”, 한국컴퓨터정보학회논문지, 18(11), pp. 39-49, 2013.

[8] 조아람, 조효진, 손영동, 이동훈, “CAN버스 공격에 안전한 메시지 인증 및 키 분배 메커니즘”, 정보보호학회논문지, 22(5), pp. 1057-1068, 2012.

[9] 조아람, ‘CAN버스 공격에 안전한 메시지 인증 및 키 분배 메커니즘’, 고려대학교 대학원 석사학위 논문, 2013.

[10] 최병주, 서주영, 양승완, 오정석, “동적 임베디드 소프트웨어 테스트와 카인포테인먼트 시스템 테스트 적용 성과”, 정보과학회논문지, 18(5), pp. 369-379, 2012.

[11] Brooks, R. R., Sander, S., Deng, J., Taiber, J., "Automobile security concerns", IEEE Vehicular Technology Magazine, 4(2), pp. 52-64, 2009.

[12] Hahn, A., Govindarasu, M., "Cyber attack exposure evaluation framework for the smart grid", IEEE Transactions on Smart, 2(4), pp. 835-843, 2011.

[13] Koscher, K., Czeskis, A., Roesner, F., Patel, S. ,Kohno, T., “Experimental security analysis of a modern automobile,” 2010 IEEE Symposium on Security and Privacy, pp. 447-462, 2010.

[14] 경찰신문, 자율주행 전기차, 해킹에 ‘원격조정’ 당했다, 2016. 9. 22.

[저 자 소 개]

최 관 (Kwan Choi)

호주 국립모나쉬대학교
범죄학·형사사법학 박사
한세대학교 인문사회학부 교수
現) 삼성교통안전문화연구소
책임연구위원
(산업보안업무 담당)

email : schgosi@daum.net

김 민 지 (Minchi Kim)

미국 뉴욕시립대학교
법심리학 박사
한국형사정책연구원
부연구위원
現) 숙명여자대학교 사회심리학과
교수

email : mkim76@sm.ac.kr