차량용 스마트키 취약점 분석과 해킹공격 대응방안

김승우* · 박대우*†

*호서대학교 벤처대학원

Vulnerability analysis of smart key for vehicle and countermeasure against hacking attack

Seung-woo Kim* · Dea-woo Park**

*Hoseo Graduate School of Venture

E-mail : tearmoa@naver.com · prof_pdw@naver.com

요 약

ICT 신기술의 발달과 함께, 자동차에도 신기술이 적용되고 있다. 차량용 스마트키도 ICT 신기술이 적용된 단말기이다. 따라서 차량용 스마트키에 대한 사이버 해킹공격이 가능하다. 스마트키에 대한 사이버 공격으로 차량제어에 이상이 생길 수 있다. 차량제어는 차량 탈취 및 차량 통제권의 위협을 가져다 줄 수 있다. 본 논문에서는 차량용 스마트키에 대한 취약점을 분석한다. 차량용 스마트키에 대한 사이버공격 사례를 분석한다. 그리고, 차량용 스마트키에 대한 실제 해킹공격을 실시하고, 대응방안을 제안한다. 대응방안을 강구한 차량용 스마트키에 대한 해킹공격을 실시하고, 사이버공격 보안에 대한 대응방안을 분석한다. 본 논문은 차량 탈취 예방과 안전한 국민생활에 기여할 것이다.

ABSTRACT

With the development of new ICT technology, new technologies are being applied to automobiles. The smart key for vehicles is also a device to which ICT new technology is applied. Therefore, a cyber-hacking attack against a smart key of a vehicle is possible. The cyber attack on the smart key can cause an abnormal control of the vehicle. Vehicle control can lead to vehicle hijacking and vehicle control risks. In this paper, we analyze the vulnerability of smart key for vehicle. Analyze cyber attacks against smart keys in vehicles. Then, we conduct real hacking attacks on smart keys for vehicles and propose countermeasures. We conduct a hacking attack against the smart key for vehicle that has devised countermeasures and analyze countermeasures against cyber attack security. This paper will contribute to the prevention of vehicle deodorization and to the safety of the people.

키워드

차량용 스마트키, 취약점, 해킹공격, 사이버보안

Ⅰ. 서 론

ICT 컴퓨팅 기술은 일상생활 환경뿐만 아니라 교육, 의료, 국방, 환경, 행정 등 다양한 인간 활동 영역에 활용되고 있다. 최근에 자동차 도난방지장치를 스마트키 시스템이라고 불리는 전자인증방식으로 대체하려는 필요성이 커지고 있고 그 응용기술로써 범용성이 뛰어난 RFID 시스템이 각광을 받고 있다.

최근에 등장하는 자동차들은 소형차까지 스마트키가 대중화된 상태다. 키를 주머니에 넣고 손잡이를 잡거나 버튼을 누르면 문이 열리고 시동도 걸 수 있어 놓치기 힘든 편의장비로 꼽힌다.

그러나 이면엔 '보안 취약'이라는 약점이 존재한다. 지난해부터 이 취약점을 이용한 자동차 도난 사건이 유럽을 중심으로 부쩍 늘어 사회적 문제가 되고 있다.

주머니에서 키를 꺼내지 않고 도어 손잡이를 당기거나 검정 버튼을 터치하는 것만으로도 잠금장치를 해제하기 위해선 키를 소지한 운전자가 차에 접근했다는 걸 인식해야 한다. 이를 위해 스마트키는 단거리 전파를 지속적으로 낸다. 혹은

그 반대로 차에서 단파를 쏘는 경우도 있다. 이를 모두 PKE(Passive Keyless Entry) 시스템이라고 한다.

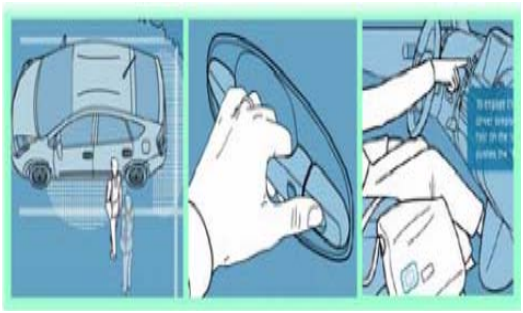

그림 1. 스마트키 작동순서[1]

① 스마트키 소지 후 차량 접근
② 도어 핸들 접촉
③ 무선통신에 의한 ID 인증 후 도어락 해제
④ 탑승 후 Start/Stop 푸시버튼 작동
⑤ 무선통신에 의한 ID 인증 후 스티어링락 해제 및 엔진시동[2]

그림 2. 스마트키 전파(인식)[3]

II. 관련연구

자동차 키, 돌리는 방식에서 버튼 하나로 1940년대 후반 미국 자동차 업체 크라이슬러는 키를 돌려 문을 열고 시동을 거는 '턴키 스타터' 기술을 처음 개발했다.

이후 1980년대 초 키를 꽂아 돌리지 않아도 문을 여닫을 수 있고, 시동도 걸 수 있는 '버튼식 무선 키(Remote Keyless Entry)' 기술이 등장했다. 버튼식 무선 키는 1990년대 '이모빌라이저(immobilizer)' 기술과 결합된다. 이모빌라이저를 탑재하면 키와 차량 간 고유 암호가 맞아야 시동을 걸 수 있다.

최근 신차에 탑재되는 스마트 키는 'PASE (Passive Start and Entry)' 기술을 적용했다. 운전자가 키를 꺼내 버튼을 눌러야 하는 기존 버튼식 무선 키와 달리 스마트 키는 주머니에서 키를 꺼내지 않고 문을 열 수 있다. 또 시동을 위해 키를 돌리는 대신 버튼을 누르면 바로 출발할 수 있게 됐다.

스마트 키는 운전석 근처에 허가된 키가 없으면 시동이 걸리지 않고 스티어링 휠도 움직이지 않아 차량 도난을 방지해준다.

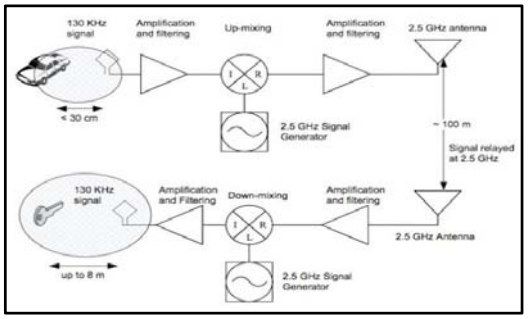

그림 3. PKE(Passive Keyless Entry) 시스템[3]

2. 1 차량용 스마트키

차량의 양방향 통신에 의해 키를 몸에 지니는 것만으로도 잠금장치를 해지할 수 있고 시동까지 걸 수 있는 최첨단 시스템이다. 벤츠 S클래스에서 처음으로 적용됐고, BMW, 아우디, 렉서스 등의 고급차종을 위주로 적용되기 시작했다. 현재는 현대, 기아차 등 국산 자동차를 포함한 대부분의 브랜드가 기본 사양으로 채택하는 추세이다.

스마트ECU, Receiver, 실내 안테나, 실외 안테나로 구성되어 있으며, 많은 기능과 접목하여 소비자가 선택할 수 있도록 개발하고 있다.

추가 복제가 불가능해 분실 시 서비스센터를 방문해 새 스마트 키에 고유 암호를 등록해야 하는 등 절차가 복잡하고 비용이 많이 드는 만큼 주의가 필요하다.

2. 2 스마트 키 주요 기능

① 전자키를 꺼내지 않고, 도어핸들의 터치에 의해서 잠금 혹은 잠금을 해제할 수 있는 기능
② 열쇠를 넣지 않고 버튼을 누르거나 돌려서 엔진 시동을 할 수 있는 스타트 기능
③ 엔진에 설정된 암호가 일치해야 시동이 걸리는 이모빌라이저(immobilizer)를 장착하여 가짜 키 혹은 단순조작으로 엔진 시동을 할 수 없게 하는 도난방지기능
④ 차량 주인이 차량 곁으로 오면 자동으로 라이트를 켜서 운전석 앞을 비추는 웰컴 기능
⑤ 문을 잠그지 않고 차량을 이탈하였을 때 일정 시간 후 문을 잠그는 오토락 기능

Ⅲ. 차량용 스마트키 취약점 분석

3. 1 차량용 스마트키 취약점 분석

PKE 시스템은 1~3m의 짧은 거리에만 전파가 도달하는데 도둑들이 이를 증폭해 300m까지 떨어진 곳에서도 작동할 수 있도록 하는 수법을 쓰고 있다.

3. 2 차량용 스마트키 공격분석(사례)

차량을 탈취하기 위해 팀플레이(2인 1조)가 필요하다. 작은 증폭기를 가방에 넣은 한명이 쇼핑을 즐기는 운전자 근처에 붙고, 나머지(수신자)는 주차장의 자동차에 접근한다. 증폭된 스마트키의 전파를 그대로 받기 때문에 자동차는 차주의 스마트키를 사용한 것으로 인식하게 된다.

그림 4. 가해자1이 운전자 접근, 전파를 수신[4]

그림 5. 가해자1이 운전자의 차량신호를 가해자2에게 전송[4]

그림 6. 운전자 차량을 가해자2가 탈취(1분 소요)[4]

덕분에 도둑은 손쉽게 차의 문을 열거나 시동을 걸 수 있다. 한번 걸린 시동은 스마트키가 없어도 꺼지지 않는다. 물론, 다시 시동을 걸 순 없지만 이동해 자동차를 분해하거나 귀중품을 훔치면 그만이다.

또, 고도의 해킹이 필요 없어 특별하지 않은 보통 사람도 범죄에 뛰어들 수 있다. 최근 중국의 한 해커 그룹이 20달러 정도에 구입할 수 있는 장치(신호 증폭기와 수신기)를 이용해 차를 훔치는 장면을 연출한 바 있다.

사실, PKE 기술이 보안에 취약하지만 현재까지 이를 완전히 막을 뾰족한 방법이 없다는 것이며 최근 네덜란드 암스테르담에서 개최된 보안 관련 컨퍼런스 'HITBSecConf2017'에서도 비슷한 문제가 제기된바 있다.[5]

Ⅳ. 차량용 스마트키 공격 대응 방안

4. 1 스마트키 보안위협 요소

최근 외제차량의 고급화에 따른 보안과 편의성을 위한 시스템이 차량에 보급 및 확산되고 있는 실정이다. 도난에 따른 피해 사례가 증가되면서 도난을 근본적으로 차단하는 대책 마련이 시급한 상태이다. 이러한 도난에 따른 보안 장치 수요는 국내외에서 꾸준하게 증가하고 있는 실정이지만 도난방지를 위한 자물쇠의 역할은 단순히 물리적인 고정 장치로만 사용되고 있다. 이러한 물리적 해체 및 분리를 원천적으로 방지할 수 있는 시스템과 IoT기반의 무선통신을 이용한 보안인증 방법을 이용하여 구현하도록 제안한다.

4. 2 스마트키의 NFC 보안 기술

NFC는 RFID(Radio Frequency ID) 및 IC 카드에서 축적 된 정보를 바탕으로 한 기술로 AES(advanced encryption standard)로 암호용 표준화가 되어 있으므로 본 이륜차의 이동제안장치 무선키로 사용한 NFC에 적용된 암호표준은 AES을 적용하였다. 본 표준은 민감하지만 비밀로 분류되지는 않은 자료들에 대해 보안을 유지하기 위해 군사용으로 사용되었던 암호화 알고리즘이며 그에 따라 민간 부문의 상업 거래용으로서 사실상의 암호화 표준으로 널리 활용되고 있는 실정이다.

제안된 이동제한 장치에서는 NFC를 적용하였다. 이것은 개인 정보인 개인 정보를 안전하게 교환할 수 있을 뿐만 아니라 기존의 자물쇠와 같은 이동제한 장치 및 열쇠를 소지할 필요가 없게 된다.

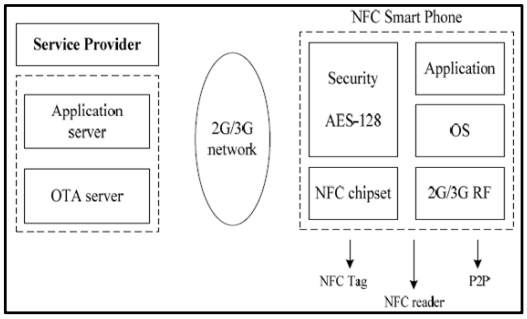

그림 7. NFC 보안인증 구성도[6]

4. 3 호일 / 전자파 차단 파우치로 보안

전자파의 발생원리를 보면 전기장과 자기장의 두가지 파동이 서로 반복하여 대기중에 퍼져 나가기 때문에 전기장이 중간에 소멸된다면 자기장 또한 발생되지 않으며 알루미늄 호일은 전기장이 내외부로 발생되지 않도록 막아준다.

전자파차단(EMF Shield) 스마트폰 파우치는 두개의 전자파 차단 주머니로 구성되어 앞쪽 칸은 한 면만 차단 되고 뒤쪽 칸은 사방이 전자파를 차단한다.

뒤쪽 칸에 스마트폰을 넣으면 RF 신호의 송수신이 거의 제로까지 줄어들기 때문에 벨소리(진동)가 울리지 않게 된다.

그림 8. 알루미늄 호일

그림 9. 전자파차단 스마트폰 파우치

4. 4 공격보안 대응 분석 결과

① 스마트키를 알루미늄(호일) 감싸고 전파 차단 테스트

② 스마트키를 전자파차단 스마트폰 파우치 내 전파 차단 테스트

표 1. 스마트키 전파 차단 테스트 결과

구 분	테스트 결과	비 고
① 알루미늄(호일)	전파 차단 (시동 및 도어락 작동 불가)	방어 성공
② 전자파 스마트폰 차단 파우치	전파 차단 (시동 및 도어락 작동 불가)	방어 성공

Ⅴ. 결 론

본 연구에서는 차량의 스마트키 전파를 복제하여 차량을 탈취하는 취약점을 소개하였으며, 이에 대한 도난방지를 위해 알루미늄 호일 및 전자파 차단 스마트폰 파우치를 이용해 결과를 제시하였다. 테스트 결과, 실제 스마트키를 알루미늄 호일 및 전자파차단 기능 제품에 적용시 보안에 안전한 것으로 결과가 도출되었다. 마지막으로 향후 연구과제로는 NFC의 통신방법과 보안 인증을 위한 암호화 프로그램 방식을 적용한 스마트키 개발이 연구되어야 할 필요가 있다.

참고문헌

[1] 용찬지, 차량 스마트키 시스템을 위한 RFID와 Bluetooth 기반의 사용자 인증 및 제어 모듈 설계 및 구현, pp. 5, 2016년 2월

[2] 이윤섭, 김경섭, 윤정희, 최상방, 교통카드와 같은 범용 RFID를 활용한 자동차용 스마트키 시스템 설계 및 구현, pp. 449, 2009년 7월

[3] 당신의 스마트키를 알루미늄으로 감싸야 하는 이유 http://m.encarmagazine.com/bible/bible1/view/78711

[4] http://tv.naver.com/v/1881764 '제조사 뭐하나' 스마트키 약점 이용해 차량 싹쓸이 영상 공개

[5] 스마트키 차량 "편한만큼 훔치기도 쉽다 http://www.zdnet.co.kr/news/news_view.asp?artice_id=20170504090559&type=det&re=

[6] 진태석, NFC기반의 보안인증을 통한 이륜차 도난방지장치 구현, pp. 167, 2016년 1월