자동차 스마트키 증폭 공격을 방어하는 방법

배동기*, 권용규*, 이동헌*, 이대성*
*부산가톨릭대학교

How to defend against car smart key amplification attacks

Dong-ki Bae*, Yong-gyu Kwon*, Dong-hun Lee*, Daesung Lee*
*Catholic University of Pusan
E-mail : willisone@naver.com, dslee@cup.ac.kr

요 약

자동차 스마트키 시스템은 리모컨 형태의 전자식 키를 통해 자동차 문의 잠금 장치를 작동/해제하고, 버튼을 누르는 것으로 시동을 켜고 끌 수 있도록 해주는 기술이다. 스마트키 시스템이 사용자를 편리하게 해주는 것인 만큼 점차 자동차의 필수적인 옵션 중 하나로 꼽히고 있으나, 이에 대한 공격에 대해서는 아직 확실한 대응방안이 나오지 않고 있는 실정이다. 이에 본 논문에서는 스마트키의 공격 방식인 증폭 공격에 대한 분석을 통해 증폭 공격을 막을 수 있는 방안과 증폭 공격으로 인해 자동차의 문이 열렸을 경우 자동차 탈취를 막기 위한 방안을 제시하고자 한다.

ABSTRACT

Car smart key system is a technology that allows you to turn activate / deactivate the auto lock through the contact form of electronic keys on the remote control and turn on the ignition by pressing the button. Smart key system is regarded as one of the essential options of the car as it is increasingly convenient to user, but there is no response yet for an attack to this situation. Therefore, in this paper, through an analysis of the amplification attack of a smart key we propose a way to stop the amplification attack and stop the car seized in case the car door opened due to the amplification attack

키워드

스마트키, 증폭 공격, 레이더, 타임스탬프, 생체 인식

Ⅰ. 서 론

현대 사회에서 자동차는 필수적인 것이 되었고, 사용자들의 편리함을 위해 만들어진 것인 만큼 자동차 시스템에서도 사용자들의 편리성을 증대시키려고 하는 방향으로 계속 발전해 나가고 있다. 자동차의 스마트키 시스템은 리모컨 형태의 전자식 키가 저주파 신호를 발생시키고, 차량 내부에 탑재된 스마트키 컨트롤 유닛에서 스마트키 수신기와 자동차 내장 안테나의 양방향 통신을 조절해 자동차 문을 열고 닫으며, 시동까지 걸 수 있도록 하는 시스템이다. 최초의 스마트키는 1999년 독일의 자동차 회사 벤츠에서 처음 개발해 S 클래스에 세계 최초로 적용시킨 시스템이다. 그 이후 렉서스, 아우디, 포르쉐 등 고급 자동차에 주로 적용되면서 보급이 확대되었다. 우리나라에서는 2004년 기아자동차의 대형 세단 오피러스에 최초로 스마트키 시스템이 적용됐다.[1]

본 논문에서는 스마트키의 신호를 증폭 시켜서 원거리에서 자동차에 인증을 시도하는 신호 증폭 공격에 대한 대비 방안을 제시하고자 한다.

Ⅱ. 본 론

1. 스마트키 신호 증폭 공격

스마트키 신호 증폭 공격이란 스마트키의 신호를 수십 미터로 증폭시켜 차 안에 키가 있는 것으로 인식하게 만들어 차량을 탈취하는 수법이다.[2] 신호증폭 공격에 대한 보안 방안으로는 스마트키를 냉장고에 넣어 신호를 차단하는 것

정도가 방어 방법이라는 지적이 나올 만큼 대책이 쉽지 않은 것이 실정이다.

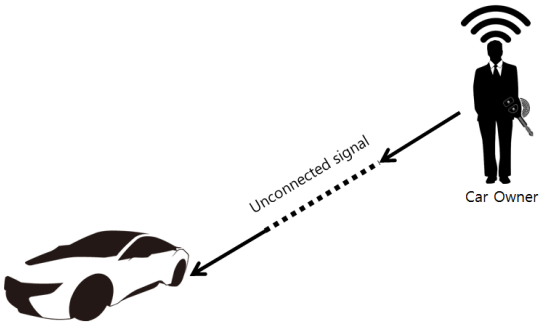

그림 1. 공격받지 않은 상태의 스마트키 통신

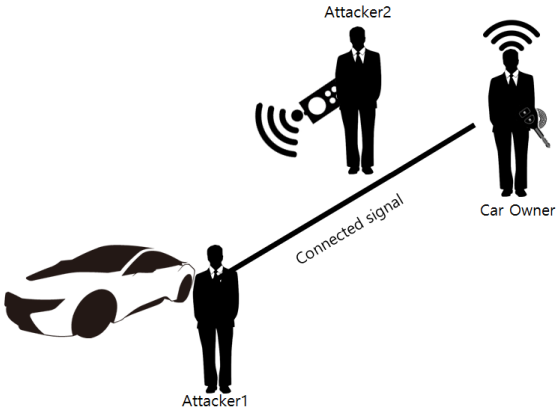

그림 2. 스마트키 신호 증폭 공격을 당했을 때의 통신

2. 레이더를 이용한 스마트키 보안

레이더(RADAR)란 전자파를 대상물을 향해서 발사해 그 반사파를 측정하는 것으로써, 대상물까지의 거리나 형상을 측정하는 장치이다.[3] 고주파 레이더와 저주파 레이더로 나눌 수 있는 데 본 논문에서는 파장이 긴 저주파 형태의 레이더가 전파의 감쇄도 작고, 먼 곳까지 탐지할 수 있어서 스마트키의 사용자를 찾아서 증폭 공격을 막는 방안으로 제안한다.[4]

스마트키의 실 사용자는 원거리에 있으나 공격자가 원거리에서 스마트키의 신호를 증폭시켜서 자동차의 제어권을 탈취하므로 스마트키를 찾는 레이더를 자동차에 부착하여 스마트키를 가진 사용자의 위치를 찾고, 레이더가 스마트키의 신호 범위 안에 사용자가 있는지 사용자 인증 후 증폭 공격 확인 여부를 하여 자동차의 도어 잠금 해제와 시동에 대한 제어권을 보호할 수 있다. 또한 TimeStamp라는 것은 둘 이상의 시각을 비교하거나 기간을 계산할 때 편리하게 사용하기 위해 고안된 것인데, 레이더가 가진 탐지 기능에 스마트키랑 통신을 할 수 있는 기능을 추가하게 된다면 TimeStamp 값을 추가하여 시간적으로 인증 절차를 수행할 수 있으므로 좀 더 철저하게 보안을 할 수 있을 것이다.[5]

3. 지문 인식을 통한 2차 피해 방지

지문인식은 생채 인식의 하나로 각 개인마다 다른 지문 정보를 추출하여 정보화시키는 인증 방식이다. 피부의 진피에서 만들어지기 때문에 진피 부분이 손상되지 않는 한 평생 변하지 않는 특성을 갖기 때문에 지문인식은 개개인을 인식하는 방법이다.[6] 또한 0.5%이내의 에러율이라는 비교적 높은 인식률과 1초 이내에 이루어지는 빠른 검증속도를 가지고 있으며, 다른 생체 인식에 비해 편의성, 신뢰성이 높은 등 장점이 많다. 사용자들은 지문인식을 사용할 때 다른 여러 생체 인식기술과 비교하여 부담감을 적게 나타내며, 지문인식 장비는 매우 적은 공간을 차지한다.[7] 신호 증폭 공격 자체를 예방할 수 있는 방법은 물리적인 방법 밖에 없어서 1차적으로 자동차 도어의 잠금이 해제될 경우 자동차 시동을 걸어서 탈취를 할 수 있는 제어권을 빼앗기지 않기 위해 시동 버튼에 지문 인식 기능을 추가하여 보안을 강화하기 위한 수단으로 이용할 수 있다.[8]

4. 지정맥 인식(dorsal venous)을 통한 2차 피해 방지

지정맥 인식은 적외선을 흡수하는 헤모글로빈과 고유한 혈관의 형태를 활용한 것으로 근적외선을 조사해 혈관의 잔영을 확인해 손가락 내부 정맥패턴을 촬영, 보정하고 템플릿의 특징을 비교해 인증하는 방식으로 혈관 내부를 인증하기 때문에 위,변조가 불가능하다. 죽은 사람의 지정맥 패턴 또한 사용 할 수 없고, 손가락 외부에 이물질이 묻더라도 인증에 영향을 받지 않습니다. 또한, 정맥 고유의 패턴은 중복가능을 찾기 어렵고, 시장에 널리 사용되고 있는 지문인식 방법과 유사해 거부감 없이 사용할 수 있다는 장점이 있다. 또한 유사패턴이 1억명중에 한 명 정도로 나온다. 어려운 기술이긴 하나 생체 인증 수단으로 사용되게 된다면 편리성도 갖출 수 있고, 보안도 강화화며 이용할 수 있다.[7]

III. 결 론

본 논문에서는 스마트키 증폭 공격에 대한 보안 방안을 제시하였다. 레이더를 이용한 방법에서는 레이더에 의한 사용자 위치 파악은 노이즈(주변 차량, 건물, 사람 등)에 영향을 많이 받게 된다면 스마트키 사용자의 위치 파악이 어렵고 레이더 특성상 기후에 따라서 레이더의 성능이 감소하여 탐지 능력이 떨어질 수 있으며, Radio 통신이라서 재전송 공격이 가능할 수 있다. 지문 인식의 경우는 지문이 손상되거나 아예 없어진 경우에는 적용이 불가능 하다는 것인데 우리나라는

전체 인구의 약 5% 정도가 이 경우에 속한다. 잘리거나 메마른 피부, 붕대를 감았거나 추운겨울날 장갑을 끼고 있으면 지문인식기를 사용하기 어렵다는 단점이 있다. 지정맥 인식은 스캐너의 크기가 비교적 크고 모바일 기기 등 대중적으로 사용되기에는 비용이 높다는 점이다.

스마트 키 증폭 공격에 대한 방안을 하나만 선택 할 경우 보안에 문제가 생기면 자동차 제어권을 빼앗길 수 있지만, 2중 3중으로 융합 보안을 한다면 보안이 더 강화되고 제어권을 빼앗길 위험이 줄어든다. 스마트키가 사용자들의 편리성을 추구하기 위해 만들어진 것인 만큼 융합 보안을 하여 불편해지지 않으면서 편리하게 사용할 수 있도록 하는 연구가 추가적으로 더 진행되어야 할 것으로 판단된다.

참고문헌

[1] http://www.driveind.com/205
[2] http://techholic.co.kr/archives/51169
[3] https://ko.wikipedia.org/wiki/%EB%A0%88%EC%9D%B4%EB%8D%94
[4] http://www.nimr.go.kr/subhome/radar/Doc/8th_workshop/classes/11.pdf
[5] https://ko.wikipedia.org/wiki/%ED%83%80%EC9E%84%EC%8A%A4%ED%83%AC%ED%94%84
[6] http://terms.naver.com/entry.nhn?docId=69146&cid=43667&categoryId=43667
[7] http://www.kipo.go.kr/home/portal/nHtml/Data/DataNews85-07.pdf
[8] http://blog.skinfosec.com/220604336899