정 보 보 호 학 회 지
제 33 권 제4호, 2023. 8

자동차 스마트키 시스템 보안 연구 동향

주 경 호*, 최 원 석**, 이 동 훈**

요 약

Controller area network (CAN) 네트워크로 대표되는 자동차 내부네트워크와 비교하여 자동차 스마트키 시스템은 상대적으로 소수의 연구가 진행되어오고 있다. 하지만, 현실 세계에서는 스마트키 시스템의 취약점으로 인해 많은 피해사례가 발생하고 있다. 대표적으로, 2010년 NDSS 학회에 소개된 신호 중계 공격 (signal relay attack)은 현재까지도 수많은 자동차 절도 사건들에 악용되고 있다. 이와 같은 문제를 근본적으로 해결하기위해 초광대역 통신 (ultra-wideband communication, UWB)을 사용한 디지털 키 (Digital Key) 기술이 일부 최신 자동차들에 탑재되고 있다. 하지만, 2022년 USENIX Security 학회에서 애플, 삼성과 같은 글로벌 기업이 채택한 high rate pulse repetition frequency (HRP) UWB 측위 시스템에 대한 거리 단축 공격 (distance reduction attack)이 가능함이 소개되었다. 이는 디지털 키 시스템 또한 신호 중계 공격과 같은 보안 위협에 노출될 수 있다는 점을 시사한다.

본 논문에서는 자동차 스마트키 시스템을 대상으로 수행된 공격 연구 사례들을 살펴본다. 먼저, remote keyless entry (RKE) 시스템 및 passive keyless entry and start (PKES) 시스템으로 대표되는 기존 스마트키 시스템을 대상으로 하는 보안 위협에 대해 살펴본다. 다음으로 차세대 스마트키 시스템으로 주목받고 있는 디지털키 시스템을 구성하는 초광대역 통신기술의 동작 원리 및 이에 대한 보안위협 연구 동향을 살펴본다.

Ⅰ. 서 론

자동차 스마트키 시스템 (keyless entry system)은 운전자가 물리적 키 (physical key)를 사용하여 차량을 개폐하는 고전적 시스템을 개선하였다. 스마트키 시스템은 무선 디지털 통신 (wireless digital communication)을 기반으로 운전자가 원거리에서도 차량을 개폐할 수 있도록 편의 기능을 제공한다 (i.e, remote keyless entry (RKE) system). 또한, 합법적인 스마트키를 소지한 운전자가 차량에 접근하면 차량과 스마트키는 사전에 정의된 통신 프로토콜을 기반으로 문을 개폐하는 편의 기능을 제공한다 (i.e., passive keyless entry and start (PKES) system). PKES 시스템을 탑재한 자동차는 radio frequency (RF) 통신을 통해 스마트키가 자동차 실내에 존재하는지 여부를 판단한다. 결과적으로 PKES 시스템이 탑재된 차량에서 운전자는 추가적인 조작 없이도 엔진 구동 버튼을 눌러 차량을 구동할 수 있다.

이와 같은 편의 기능을 구현하기 위해 다양한 통신 기술들이 탑재됨에 따라 스마트키 시스템을 대상으로 하는 보안위협이 최근 십수년간 연구되어오고 있다. 먼저, 스마트키 시스템에 사용되는 암호알고리즘에 대한 암호분석 연구가 다수 진행되어오고 있다. 연구자들은 스마트키 시스템 제조사의 비공개 자산인 암호알고리즘을 역공학을 통해 분석하였으며, 이를 바탕으로 비밀키를 복구할 수 있는 공격 들을 소개하였다. 특히, 2016년 Garcia et al. [1]은 글로벌 자동차 제조 기업인 폭스바겐 (Volkswagen) 그룹에서 제조한 자동차의 스마트키 시스템에 world wide secret key를 사용하고 있음을 소개하였다. 한편, Francillon et al. [2]은 최신 자동차에 탑재된 PKES 시스템에 대한 신호중계 공격을 소개하였다. 공격자는 목표 PKES 시스템에서 사용하는 주파수 대역만 알고 있으면, 어떠한 사전지식 없이도 신호중계 공격을 통해 자동차를 절도할 수 있다. 이와 같은 실용성으로 인해 신호 중계 공격은 2010년 최초로 소개된 이후 현재까지도 수많은 자동차 절도 사건에 악용되고 있다.

이와 같은 보안 위협을 근본적으로 해결하기 위해 자동차 제조사들은 IEEE 802.15.4z 표준에 제정된 초

* 고려대학교 정보보호대학원 정보보호학과 (대학원생, wnrudgh16@korea.ac.kr)
** 고려대학교 정보보호대학원 정보보호학과 (교수, beb0396@korea.ac.kr; 교수, donghlee@korea.ac.kr)

광대역 (ultra-wideband) 기술을 차세대 스마트키 시스템으로 채택하고 있다. 자동차 제조사 및 스마트폰 제조사, 반도체 제조사들로 구성된 Car connectivity consortium (CCC)는 스마트폰을 기반으로한 디지털 키 (Digital Key) 표준을 제정하였다. 해당표준은 near field communication (NFC), Bluetooth low energy (BLE), 그리고 HRP UWB 기술이 탑재된 스마트폰을 이용하여 차세대 자동차 스마트키 시스템을 표준화하였으며, Genesis GV60, BMW iX와 같은 최신 차량들에 해당기능을 탑재하고 있다.

하지만, 2022년 USENIX Security 학회에서는 애플, 삼성과 같은 글로벌 대기업이 채택한 HRP UWB 측위시스템에 대한 거리 단축 공격 (distance reduction attack)이 가능함이 소개되었다 [3]. 공격자는 HRP UWB 표준에서 정의한 scrambled timestamp sequence (STS) 필드에 대한 signal overshadowing 공격을 통해 HRP UWB 장치들이 측정한 거리를 단축시킬 수 있음을 보여주었다. 이는 디지털 키 시스템 또한 신호 중계 공격과 같은 보안위협에 노출될 수 있음을 시사한다.

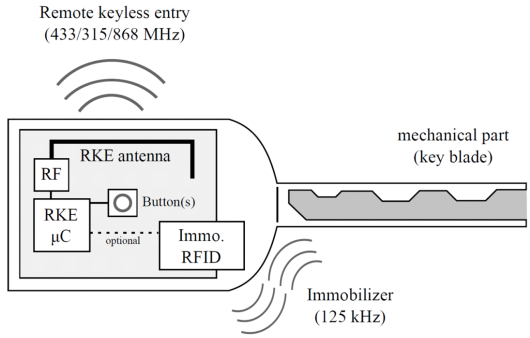
본 논문에서는 현재까지 학계 및 산업계에서 연구된 자동차 스마트키 시스템에 대한 보안 위협 연구를 소개한다. 본 논문은 자동차 도난 방지를 위한 이모빌라이저 시스템부터 초광대역 통신시스템에 대한 최신 보안 위협 연구 사례들을 소개한다.

Ⅱ. 배경지식

본 절에서는 자동차 스마트키 시스템의 대표적인 두가지 형태인 remote keyless entry (RKE) 시스템과 passive keyless entry and start (PKES) 시스템에 대해 살펴본다. 일반적으로 PKES 시스템은 RKE 시스템의 기능을 포함한다. 또한, 차세대 스마트키 시스템에서 사용하는 HRP UWB 통신 기술을 이용한 거리 측정 원리에 대해 살펴본다.

2.1. Remote keyless entry (RKE) 시스템

1995년 European union (EU)는 자동차 도난 범죄를 방지하기 위해 유럽에서 판매되는 모든 자동차들에 이모빌라이저 (immobilizer) 장치를 탑재하도록 강제하였다 [5]. 이모빌라이저는 125kHz 대역인 low frequency (LF) 대역을 통해 자동차의 이모빌라이저

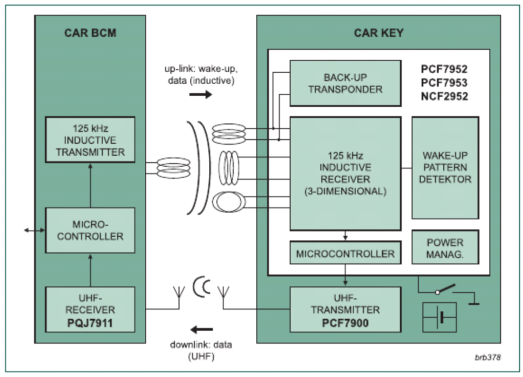


〔그림 1〕 자동차 이모빌라이저 및 RKE 시스템 구조 〔4〕

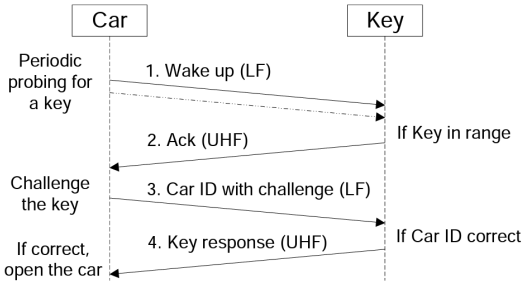
유닛 (immobilizer unit)으로부터 전력을 공급받아 통신을 수행하며, 정당한 이모빌라이저만이 자동차가 전송한 challenge에 대한 response를 생성할 수 있다 ([그림 1]). 이후 운전자 편의를 위해 자동차 제조사들은 remote control 기능이 추가된 remote keyless entry (RKE) 시스템을 출시하였다. 운전자는 스마트키를 조작하여 원거리에서도 차량을 잠금해제 할 수 있다. 이때, 스마트키는 사전에 차량과 교환된 대칭키를 이용하여 명령을 암호화 하며, rolling code 기법을 이용하여 개별 명령의 신규성 (freshness)를 제공한다.

2.2. Passive keyless entry and start (PKES) 시스템

Passive keyless entry and start (PKES) 시스템은 2.1에서 살펴본 RKE 시스템의 원격 잠금해제 기능을 포함하고 있다. 뿐만 아니라, PKES 시스템은 정당한 스마트키를 소유한 사용자가 차량의 문에 부착된 스위치만 누르면 차량의 문을 잠금 해제하며, 구동 버튼을 제어하여 엔진을 구동할 수 있도록 편의를 향상시켰다. 이때, 스마트키는 내장된 배터리로 부터 전력을 공급받아 차량과 상호작용을 수행한다. 이러한 RKE 시스템 및 PKES 시스템은 low frequency (LF, 125~134kHz) 대역 혹은 ultra high frequency (UHF, 433.92 또는 868MHz) 대역을 사용한다. 구체적으로, 차량은 LF 통신을 사용하며, 스마트키는 UHF 대역을 사용한다 ([그림 2], [그림 3]).



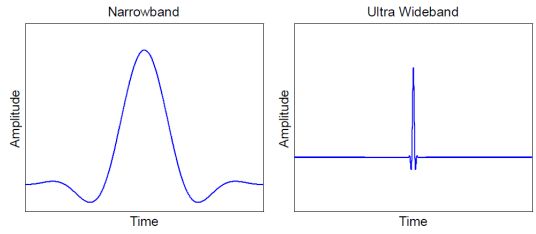
〔그림 2〕 PKES 시스템 구조: 자동차 body control module (BCM)은 LF대역 신호를 송신하고 UHF 대역 신호를 수신한다. 반대로, 스마트키는 LF 대역 신호를 수신하고 UHF 대역 신호를 송신한다〔6〕



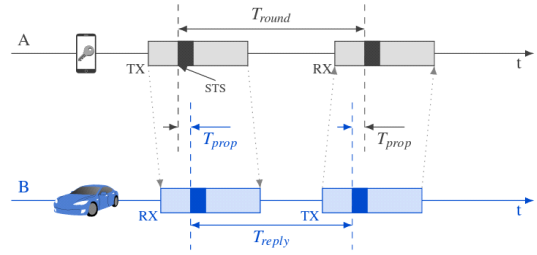
〔그림 3〕 대표적인 PKES 통신 프로토콜 흐름도〔2〕

2.3. 초광대역 통신

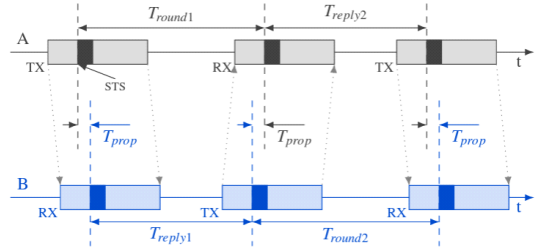
초광대역 (Ultra-wideband, UWB) 통신은 1-2ns 수준의 펄스 신호를 사용하여 넓은 주파수 대역으로 데이터를 송수신하는 근거리 무선통신 기술로, 500MHz 수준의 넓은 주파수 대역폭 및 낮은 출력 에너지를 사용하는 무선통신 기술이다. UWB 기술은 채널 노이즈 및 신호 간섭에 강건한 신호 특성을 기반으로 기존의 협대역 (narrowband) 통신방식인 Wi-Fi, Bluetooth, LTE 통신기술 기반의 측위 기술에 비해 cm 수준의 분해능으로 기기 간의 물리적 거리를 측정할 수 있다 ([그림 4]). 초광대역 통신은 대표적으로 two-way ranging (TWR) 기법을 이용하여 기기간의 거리를 측정한다. TWR 기법은 initiator ([그림 5]의 A)와 responder ([그림 5]의 B)가 송수신하는 프레임에 따라 single-sided two-way ranging (SS-TWR)과 double-sided two-way ranging (DS-TWR)로 구분할 수 있다. DS-TWR은 SS-TWR에 비해 기기 간에 발생



〔그림 4〕 협대역 (narrowband) 신호와 초광대역 (ultra wideband) 물리 레벨 신호〔7〕



〔그림 5〕 SS-TWR 통신 흐름도〔3〕



〔그림 6〕 DS-TWR 통신 흐름도〔3〕

하는 클록 오프셋 (clock offset)에 강건하다는 장점이 있으며, 디지털 키 시스템은 DS-TWR을 채택하여 자동차와 스마트폰 간에 물리적 거리를 측정한다. Initiator와 responder는 수식(1) (SS-TWR) 과 수식(2) (DS-TWR)을 이용하여 기기간의 거리를 계산한다.

$$\widehat{T_{prop}} = \frac{1}{2} \cdot (T_{round} - T_{reply}) \quad (1)$$

$$\widehat{T_{prop}} = \frac{T_{round1} \cdot T_{round2} - T_{reply1} \cdot T_{reply2}}{T_{round1} + T_{round2} + T_{reply1} + T_{reply2}} \quad (2)$$

Ⅲ. 자동차 스마트키 시스템 대상 보안 위협

본 절에서는 스마트키 시스템 대상 사이버 공격 연

구 동향을 살펴본다. 제시된 사이버 공격은 스마트키 시스템의 암호학적 취약점뿐만 아니라 radio frequency (RF) 신호의 물리적 특성 또한 악용하였다.

3.1. 암호분석 (Cryptanalysis)

3.1.1. KeeLoq 알고리즘

Indesteege et al. [8]은 2008년 Eurocrypt 학회에서 자동차 스마트키에 광범위하게 사용되는 KeeLoq 알고리즘을 대상으로 slide attack과 meet-in-the-middle 공격을 소개하였다. 저자들은 2^{16}개의 알려진 평문 (known plaintext)를 사용하여 $2^{44.5}$의 시간복잡도로 KeeLoq 알고리즘의 비밀키를 복구할 수 있음을 보여주었다. Eisenbarth et al. [9]은 KeeLoq 알고리즘의 code hopping scheme에 대한 differential power analysis (DPA)를 통해 비밀키를 복구할 수 있음을 보여주었다. 저자들은 10회의 전력 trace 측정을 통해 수분 내에 비밀키를 복구할 수 있음을 보여주었다. Kasper et al. [10]은 simple power analysis (SPA)를 통해 KeeLoq 알고리즘에 대한 기존 공격들에서 요구되는 비용을 획기적으로 줄이는 공격을 소개하였다. 저자들은 KeeLoq 알고리즘의 복호화 과정에서 발생하는 단일 전력 trace를 측정하여 평문 및 암호문에 대한 어떠한 사전지식 없이도 64bit의 마스터키를 복구할 수 있음을 보여주었다.

3.1.2. Digital signature transponder (DST)

Digital signature transponder (DST) 알고리즘은 Texas Instrument (TI) 에서 제작한 radio-frequency identification (RFID) 장치에서 사용된다. DST 알고리즘은 Ford, Lincoln, Mercury, Toyota, Nissan, Kia, Hyundai, 그리고 Tesla와 차량의 스마트키 시스템과 더불어 약 7백만대의 SpeedPass 결제 시스템에 사용되고 있다. DST 알고리즘은 비밀키의 길이에 따라 40비트 키를 사용하는 DST40 및 80비트 키를 사용하는 DST80으로 분류된다.

Bono et al. [11]은 DST 40알고리즘에 대한 역공학 (reverse engineering), 키 복구 (key recovery)를 수행하여 실제 금융결제 시스템을 통해 공격의 유효성을 보여주었다. 구체적으로, 저자들은 black-box 공격을 통해 DST 알고리즘의 작동 원리를 분석하였으며, 임의의 두 challenge response 쌍과 16개의 FPGA 이용하여 1시간 내로 비밀키를 복구하였다. 이를 이용하여 DST 알고리즘을 사용하는 SpeedPass 결제 시스템을 대상으로 복구된 비밀키가 유효함을 보여주었다.

Wouters et al. [11]은 Tesla model S의 PKES 시스템에 사용된 DST 40 알고리즘을 대상으로 2개의 challenge response 쌍과 5.6TB의 룩업 테이블 (lookup table), 라즈베리파이 3B를 이용하여 2초내에 비밀키를 복구할 수 있음을 보여주었다. 이를 통해 저자들은 정당한 스마트키를 복제하여 목표 차량을 절도할 수 있음을 보여주었다. Wouters et al. [12] DST40의 취약점을 보완하기 위해 키의 길이를 80비트로 증가시킨 DST80에 대한 취약점을 소개하였다. 저자들은 Kia와 Hyundai 차량에서 사용되는 비밀키는 3바이트 수준의 엔트로피를 가지고 있으며, downgrade attack을 통해 키 공간을 2^{80}에서 2^{40}으로 축소할 수 있음을 보여주었다.

3.1.3. Hitag 알고리즘

Hitag 알고리즘은 NXP Semiconductors에서 제작하였으며 48비트의 비밀키를 사용한다. Hitag 알고리즘은 최소 34개 이상의 자동차 제조사에서 판매중인 200여개의 자동차 모델들의 스마트키 시스템들에 광범위하게 사용되고 있다. DST 알고리즘과 마찬가지로, Hitag 알고리즘 또한 초기에는 자동차 이모빌라이저에 탑재되었으나, RKE 시스템 및 PKES 시스템에서도 여전히 사용되고 있다.

Verdult et al. [13] 은 일반적인 하드웨어 장치로 6분 이내로 비밀키를 복구할 수 있는 공격을 소개하였다. 저자들은 Hitag 알고리즘 의사난수 생성기 (pseudo-random number generator) 부재 및 이모빌라이저 시스템의 구현 취약점 등을 소개하였다. 이를 이용하여 공격자는 재전송 공격 및 키 복구 공격을 소개하였다.

Garcia et al. [1]은 Volks wagen(VW) 그룹에서 생산된 자동차 스마트키 시스템에서 사용하는 Hitag 알고리즘들의 취약점을 분석 하였다. 저자들은 무선통신 프레임의 구조에 따라 해당 알고리즘들을 VW-1, VW-2, VW-3, VW-4로 구분하였다. 또한 개별 세대에서 사용된 암호화 알고리즘 및 키 관리, 취약한 차량모

〔표 1〕 RKE 시스템 대상 주요 공격 연구

연도	저자명	대상 알고리즘	공격 방법
2005	Bono et al. 〔11〕	DST	Reverse engineering, time/memory tradeoff attack
2008	Indesteege et al. 〔8〕	KeeLoq	Meet-in-the-middle
2008	Eisenbarth et al. 〔9〕	KeeLoq	Differential power analysis (DPA)
2009	Kasper et al. 〔10〕	KeeLoq	Simple power analysis (SPA)
2012	Verdult et al. 〔13〕	Hitag	Reverse engineering, time/memory tradeoff attack
2013	Verdult et al. 〔15〕	Megamos	Reverse engineering, cryptographic weakness
2016	Garcia et al. 〔1〕	HItag/AUT	Reverse engineering,
2018	Hicks et al. 〔14〕	AUT	Reverse engineering, cryptographic weakness (low entropy)
2019	Wouters et al. 〔11〕	DST	Time/memory tradeoff attack
2020	Wouters et al. 〔12〕	DST	Downgrade attack

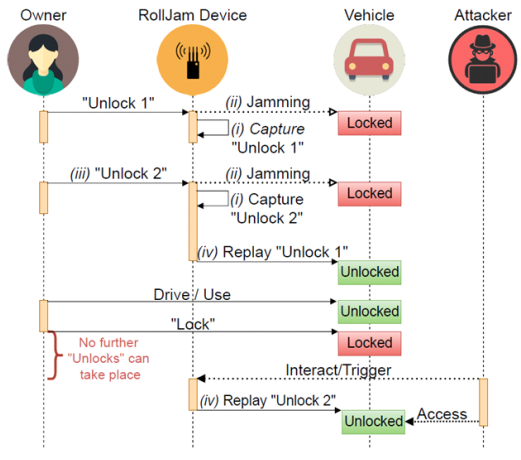
델에 대한 상세한 분석을 수행하였다. 특히, VW-1 이후 VW그룹에서 생산된 차량에 탑재된 스마트키 시스템은 암호학적 키에 기반하여 설계되었다. 그러나 해당 스킴을 사용하는 전세계의 모든 차량이 같은 key를 공유하고 있다는 문제점이 발견되었다. 이러한 취약점에 대응하여 VW 그룹에서는 모든 차량이 개별 비밀키를 가지도록 조치하였다. [표 1]은 현재까지 연구된 스마트키 시스템 대상 암호분석 공격에 대한 주요 연구흐름을 보여준다.

3.2. Rolling code 시스템

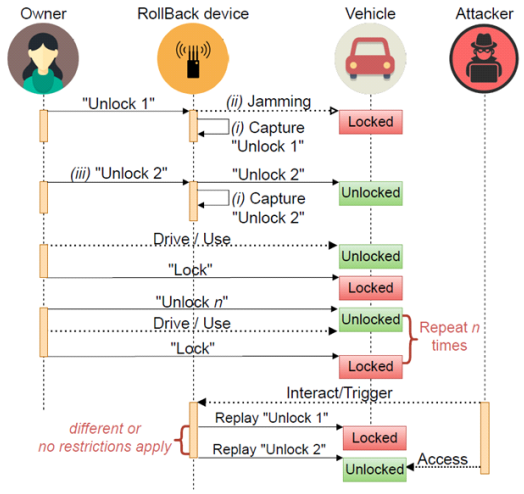
자동차 제조사는 스마트키 시스템에 대한 재전송 공격 (replay attack)을 막기 위해 rolling code system을 도입하였다. Rolling code 시스템은 일반적으로 의사난수 생성기를 사용한다. 송신부는 ‘next code’를 전송하며, 수신부는 자신이 생성한 ‘next code’와 비교하여 해당 code를 검증한다. 이때 자동차와 스마트키는 사전에 카운터를 동기화 하고 있다. 스마트키의 버튼을 누르거나 차량의 문에 부착된 잠금해제 버튼을 누르면 차량과 스마트키는 동기화된 카운터를 증가시킨다. 하지만 실제 사용사례에서는 사전에 설계된 통신반경 밖에서도 스마트키가 동작할 수 있기때문에 수신기는 일반적으로 256개의 ‘next code’와 비교를 수행한다.

Kamkar [16]는 RKE 시스템에 대한 재밍 공격인 rolljam 공격을 소개하였다 ([그림 7]). Rolljam 공격은 rolling code 시스템의 동기화를 인위적을 깨뜨려 카운터를 재사용하는 공격이다. 공격자는 스마트키로부터 전송된 신호를 재밍하여 차량이 Rolling code의 카운터를 증가시키지 않도록 만든다. 이후 공격자는 스마트키가 사용한 카운터를 재사용하여 차량을 잠금해제할 수 있다. 하지만, 재밍 공격을 수행하기 위해서는 공격자가 정당한 운전자의 스마트키로부터 전송되는 신호를 차량이 수신하지 못하도록 해야 한다. 이는 공격자가 운전자가 스마트키의 잠금 버튼을 누르는 순간에 공격을 수행해야 하며, 재밍신호가 스마트키의 신호를 완전히 차단해야한다는 점에서 실제적인 공격이 이루어지기 위해서는 제한사항이 있다고 할 수 있다.

Csikor et al. [17]은 rolling code 시스템의 재동기화(resynchronization) 메커니즘을 악용한 rollback 공격을 소개하였다 ([그림 8]). 저자들은 카운터의 차이가 16보다 클 경우, rolling code 시스템은 이후 수신되는 2개의 연속된 카운터에 재동기화 한다는 점을 악용하였다. 이를 통해 공격자는 기존의 rolljam 공격과



〔그림 7〕 Rolljam 공격흐름도 〔17〕

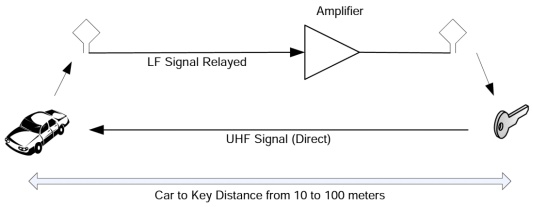


〔그림 8〕 Rollback 공격흐름도〔17〕

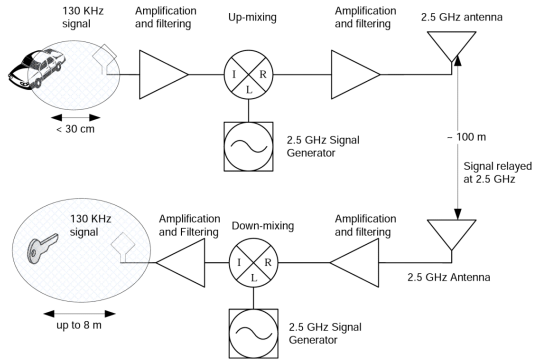
달리 스마트키에서 전송되는 신호를 실시간으로 재밍하지 않고도 자동차를 잠금해제 할 수 있다. 한편, rollback 공격과 유사한 rolling-pwn 공격이 소개되었다. 해당 공격은 Honda 社에서 제조한 다양한 차량 모델들을 대상으로 rollback 공격과 유사하게 연속된 프레임을 전송하여 rolling code 시스템을 재동기화 하는 공격이다. 하지만, 해당 연구의 저자들은 성공적인 공격을 위해 요구되는 프레임의 개수 등과 같은 세부적인 사항을 공개하지 않았다.

3.3. 신호 중계 공격 (Relay attack)

Francillon et al. [2] 은 PKES가 탑재된 차량에 대한 신호 중계 공격을 수행하였다 ([그림 9], [그림 10]). [그림 4]에서 알 수 있듯이 PKES는 정당한 키를 가진 운전자가 차량의 통신 (i.e., LF 대역 통신) 반경 내에 위치하게 되면 challenge response 방식을 통해 인증을 수행한다. 신호 중계 공격은 이와 같은 근접성 (proximity) 기반의 인증을 수행하는 PKES을 대상으로 공격자가 차량과 스마트키의 유효 통신반경을 의도



〔그림 9〕 유선 신호 중계 공격〔2〕



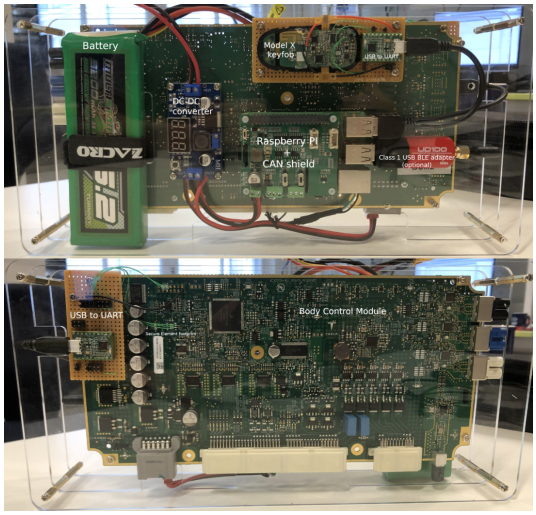
〔그림 10〕 무선 신호 중계 공격〔2〕

적으로 증가시켜 스마트키가 자동차와 멀리 떨어져 있더라도 인증과정을 통과하는 원리이다. 공격자는 목표 PKES 시스템에서 사용하는 주파수 대역만 알고 있다면 자동차에서 전송되는 LF 대역 신호를 정당한 스마트키에 전달하면 된다. 이와 같은 실용적인 특징으로 인해 신호 중개 공격은 실제 차량 도난사건에 악용되고 있다. 한편, Zeng et al. [18] LF 대역 신호와 더불어 스마트키에서 전송되는 UHF 대역 신호를 추가로 중개하여 공격 가능 거리를 증가시킬 수 있음을 보여주었다 ([그림 11]). 저자들은 LF/UHF 대역 신호에서 바이너리 정보를 추출하여 이를 공격자들 간에 중개하여 공격을 수행하였다.

〔그림 11〕 무선 신호중계 공격 장치 (Zeng et al.〔18〕)

3.4. 시스템 취약점 공격

Wouters et al. [19]은 테슬라 Model X의 PKES 시스템의 인증서 검증 부재 취약점을 악용하여 공격자의 스마트키를 목표 자동차에 등록하여 자동차를 절도할



〔그림 12〕 시스템 취약점 공격 장치 (Wouters et al. 〔19〕)

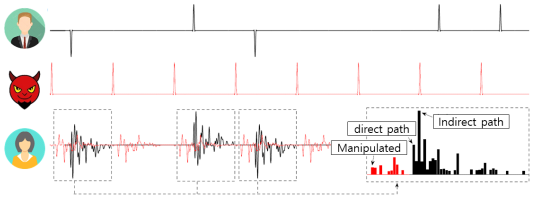
수 있음을 보여주었다. 저자들에 따르면, 테슬라 Model X는 신호중개 공격을 막기 위해 가속도 센서 및 EAL 5+인증을 받은 secure element들을 사용하였으나, 자동차가 새로운 스마트키와의 pairing 과정에서 스마트키의 인증서를 검증하지 않는 점을 악용하였다.

3.5. 초광대역 통신 시스템 대상 거리 단축 공격

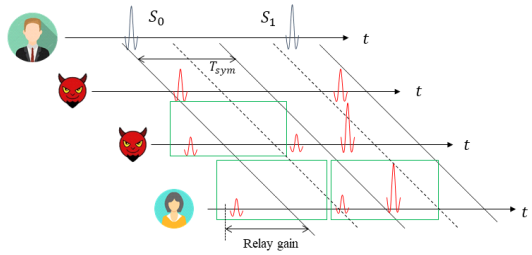
본 절에서는 UWB 시스템의 거리 측정 성능을 저해하거나 distance bounding protocol을 우회하는 공격 기법 연구 사례들을 살펴본다.

3.5.1. Cicada attack

Poturalski et al. [20] 은 UWB 기반 측위 시스템의 성능을 저하하는 cicada attack을 소개하였다 ([그림 13]). 공격자는 정확한 ToF 측정을 위해 사용하는 back-search 알고리즘의 취약점을 악용하여 ToF를 감소 시키거나, 재밍 (jamming)을 통해 denial of service



〔그림 13〕 Cicada attack



〔그림 14〕 PPM 변조기법에 대한 ED/LC 공격

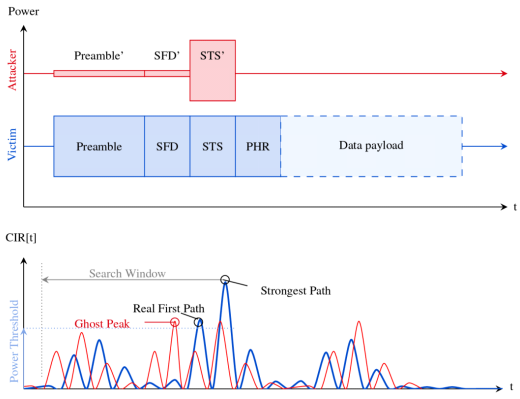
(DoS) 공격을 수행할 수 있다. Back-search 알고리즘은 multi-path 환경에서 복수개의 pulse 신호가 수신될 때 정확한 ToA 측정을 위한 알고리즘으로써, 신호의 중첩으로 인해 indirect 신호의 크기가 direct 신호보다 큰 경우에 발생하는 ToF 측정오류를 방지한다. 공격자는 희생자가 정당한 UWB 펄스를 수신하는 시점에 맞춰 악의적인 UWB 펄스를 주입하여 공격자의 신호를 direct path로 오인하도록 강제한다. ([그림 14]) 결과적으로 이는 작은 ToF 및 단축된 거리 측정 결과를 초래한다.

3.5.2. Early detect/late commit (ED/LC) Attack

Flury et al. [21]은 pulse position modulation (PPM)변조기법을 사용하는 UWB 시스템에 대한 거리 감소 공격인 ED/LC 공격을 제시하였다 [2,3]. ED/LC 공격자는 UWB 시스템의 물리레벨 신호의 결정적 특성을 악용하여, 정당한 신호의 형태를 예측한다. 이를 통해 공격자는 정당한 기기가 송신하는 신호보다 선행하는 공격 신호를 주입하여 ToF를 감소시킬 수 있다. 공격 순서는 아래와 같다.

1. 공격자는 정당한 신호에 선행하는 모조 (dummy) 신호를 주입한다.
2. 공격자는 정당한 신호의 샘플들을 바탕으로 심볼 시간 (T_{sym}) 이전에 수신된 신호의 심볼을 예측한다 (early detect).
3. 공격자는 T_{sym} 이전까지 임의의 UWB 신호를 주입하여(commit signal) 정당한 기기로 하여금 공격자가 예측한 심볼로 복조(demodulation) 하도록 강제한다 (late commit).

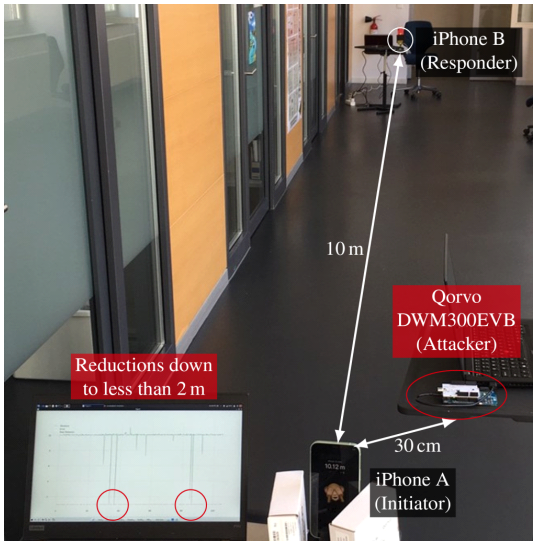
[그림 15]는 PPM 기반의 UWB 시스템에 대한 ED/LC 공격흐름도를 보여준다. 공격자는 정상 신호보



〔그림 15〕 Signal overshadowing 공격 〔3〕

다 t_{realy} 만큼 앞서 모조 신호를 주입하며, 정당한 UWB 신호를 수신하기 시작한 이후 t_{ED} 시점에 심볼의 형태를 예측 후, t_{LC} 시점에 임의의 UWB 를 주입한다. 만약 '0'심볼을 수신한 경우 공격자는 추가적인 신호를 송신하지 않는다. 하지만, '1'심볼을 수신한 경우, 모조 신호의 세기보다 강한 커밋 신호를 주입하여 희생자의 기기가 '1'심볼을 수신하도록 강제한다.

해당 연구에서는 PPM 변조 기반의 UWB 시스템에 대한 공격기법을 제시하였으나, ED/LC 공격 개념은 frequency shift keying (FSK), on-off keying (OOK), phase shift keying (PSK) 기반의 UWB 시스템에도 동일하게 적용될 수 있다.



〔그림 16〕 거리 단축 공격 실험환경 〔3〕

3.5.3. Ghost peak attack

Leu et al. [3]는 디지털 키 시스템에서 채택한 HRP UWB 측위 시스템에 대한 signal overshadowing 공격을 통해 공격자가 기기간에 측정된 거리를 단축할 수 있음을 소개하였다. 공격자는 HRP UWB 측위 시스템의 보안성 향상을 위해 IEEE 802.15.4z 표준에서 새롭게 정의된 STS 필드를 대상으로 signal overshadowing 공격을 수행하였다 ([그림 16) 위). STS 필드는 사전에 교환된 대칭키를 기반으로 생성되는 의사 난수로 구성되어 있으며, 비밀키를 소유한 정당한 기기만이 수신된 STS 필드에서 상호상관 (cross-correlation) 연산을 통해 수신 프레임의 ToA 값을 측정할 수 있다. 하지만 상호상관 연산은 개별 랜덤 비트를 검증할 수 없다는 한계점이 있다. 공격자는 이를 악용하여 비밀키에 대한 어떠한 사전정보 없이도 signal overshadowing 공격을 통해 목표 기기가 측정하는 ToA 측정값을 줄일 수 있으며 ([그림 15] 아래), 이는 기기간 측정 거리 감소로 이어진다. 저자들은 상용 HRP UWB 기기를 대상으로 공격성능을 평가하였으며, 10미터 거리에 있는 물체와의 거리를 2m로 단축할 수 있음을 보여주었다.

Ⅳ. 결 론

본 논문에서는 자동차 스마트키 시스템에 대한 보안 연구 동향을 공격사례 중심으로 살펴보았다. 자동차 스마트키 시스템에서 발생하는 취약점은 수많은 자동차 절도 사건의 원인으로 지목되고 있다. 전통적인 스마트키 시스템의 보안성 향상을 위해 탑재되는 차세대 스마트키 시스템에 대한 사이버 보안 위협이 최근 소개됨에 따라 관심과 연구가 필요하다.

참 고 문 헌

[1] Garcia, Flavio D., et al. "Lock it and still lose it—on the ({In) Security} of automotive remote keyless entry systems." 25th USENIX security symposium (USENIX Security 16). 2016.

[2] Francillon, Aurélien, Boris Danev, and Srdjan Capkun. "Relay attacks on passive keyless entry and start systems in modern cars." Proceedings

of the Network and Distributed System Security Symposium (NDSS). 2011.

[3] Leu, Patrick, et al. "Ghost Peak: Practical Distance Reduction Attacks Against {HRP}{UWB} Ranging." 31st USENIX Security Symposium (USENIX Security 22). 2022.

[4] Garcia, Flavio D., et al. "Lock it and still lose it—on the ({In) Security} of automotive remote keyless entry systems." 25th USENIX security symposium (USENIX Security 16). 2016.

[5] Commission Directive 95/56/EC, Euratom of 8 November 1995 adapting to technical progress Council Directive 74/61/EEC relating to devices to prevent the unauthorized use of motor vehicles

[6] Keyless Entry/Go Leaflet Datasheet by NXP USA Inc.

[7] IEEE 802.15 WPANTM Task Group 4z Enhanced Impulse Radio

[8] Indesteege, Sebastiaan, et al. "A practical attack on KeeLoq." Advances in Cryptology–EUROCRYPT 2008: 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings 27. Springer Berlin Heidelberg, 2008.

[9] Eisenbarth, Thomas, et al. "On the power of power analysis in the real world: A complete break of the KeeLoq code hopping scheme." Advances in Cryptology–CRYPTO 2008: 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings 28. Springer Berlin Heidelberg, 2008.

[10] Kasper, Markus, et al. "Breaking KeeLoq in a flash: on extracting keys at lightning speed." International Conference on Cryptology in Africa. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.

[11] Wouters, Lennert, et al. "Fast, furious and insecure: Passive keyless entry and start systems in modern supercars." IACR Transactions on Cryptographic Hardware and Embedded Systems (2019): 66-85.

[12] Wouters, Lennert, et al. "Dismantling DST80-based immobiliser systems." IACR Transactions on Cryptographic Hardware and Embedded Systems (2020): 99-127.

[13] Verdult, Roel, Flavio D. Garcia, and Josep Balasch. "Gone in 360 seconds: Hijacking with Hitag2." 21st USENIX Security Symposium (USENIX Security 12). 2012.

[14] Hicks, Christopher, Flavio D. Garcia, and David Oswald. "Dismantling the AUT64 automotive cipher." IACR Transactions on Cryptographic Hardware and Embedded Systems (2018): 46-69.

[15] Verdult, Roel, et al. "Dismantling megamos crypto: Wirelessly lockpicking a vehicle immobilizer." 22nd USENIX Security Symposium (USENIX Security 13). 2013.

[16] This Hacker's Tiny Device Unlocks Cars And Opens Garages | WIRED

[17] Csikor, Levente, et al. "RollBack: A New Time-Agnostic Replay Attack Against the Automotive Remote Keyless Entry Systems." arXiv preprint arXiv:2210.11923 (2022).

[18] Chasing Cars: Keyless Entry System Attacks

[19] Wouters, Lennert, Benedikt Gierlichs, and Bart Preneel. "My other car is your car: compromising the Tesla Model X keyless entry system." IACR Transactions on Cryptographic Hardware and Embedded Systems (2021): 149-172.

[20] Poturalski, Marcin, et al. "The cicada attack: degradation and denial of service in IR ranging." 2010 IEEE International Conference on Ultra-Wideband. Vol. 2. IEEE, 2010.

[21] Flury, Manuel, et al. "Effectiveness of distance-decreasing attacks against impulse radio ranging." Proceedings of the third ACM conference on Wireless network security. 2010.

〈저 자 소 개〉

주 경 호 (Kyungho Joo)

2016년 2월 : 고려대학교 컴퓨터통신공학부 졸업
2018년 2월 : 고려대학교 정보보호대학원 정보보호학과 졸업
2018년 3월~현재 : 고려대학교 정보보호대학원 정보보호학과 박사과정

<관심분야> 무선통신보안, 자동차 보안, 무인이동체보안

최 원 석 (Wonsuk Choi)

종신회원

2008년 2월 : 서울시립대학교 수학과 졸업
2013년 2월 : 고려대학교 정보보호대학원 정보보호학과 석사
2018년 8월 : 고려대학교 정보보호대학원 정보보호학과 박사
2018년 9월~2020년 2월 : 고려대학교 정보보호연구원 연구교수
2020년 3월~2023년 2월 : 한성대학교 IT융합공학부 조교수
2023년 3월~현재 : 고려대학교 정보보호대학원 조교수
<관심분야> 자동차 보안, IoT 보안, 암호학

이 동 훈 (Dong Hoon Lee)

종신회원

1983년 8월 : 고려대학교 경제학과 졸업
1987년 12월 : Oklahoma University 전산학과 석사 졸업
1992년 5월 : Oklahoma University 전산학과 박사 졸업
1993년 3월~1997년 2월 : 고려대학교 전산학과 조교수
1997년 3월~2001년 2월 : 고려대학교 전산학과 부교수
2001년 3월~현재 : 고려대학교 정보보호대학원 교수
<관심분야> 암호 프로토콜, 암호이론, USN이론, 키 교환, 익명성 연구, PET 기술