
Global Report

인터넷 기반 스마트카드 공격시나리오

1. 개요
2. 비접촉식 카드 기술
3. 원격 비접촉식 카드 공격
4. 공격 애플리케이션 분석
5. 결론

1. 개요

1980년대부터 스마트카드 칩(smart card chip)이 내장된 기기를 통해 다양한 작업을 실행하는 데 익숙해졌다. 사용자는 칩에 저장된 정보를 식별하여 권리와 운영을 부여받아 개인화된 독특한 스마트카드 서비스를 제공받을 수 있다. 수년 동안 스마트카드를 사용하기 위해 카드 표면에 부착된 칩을 통해 시스템에 통합된 카드 리더(card reader)에 삽입하여 물리적으로 작동시킨다. 이를 통해 시스템과 칩 간의 물리적 접촉을 설정하고, 전원을 공급하고, 칩 간의 통신을 시작할 수 있다. 이러한 작동은 판매점이나 지불 단말기에서 신용카드를 사용하는 것으로 확산되었다. 이때 스마트카드는 카드소지자가 구매한 상품에 대한 결제거래를 승인하는 데 사용된다. 지난 10년 동안 비접촉식 스마트 카드의 점진적인 도입이 이루어졌다. 이러한 카드의 경우 칩은 코일에 연결되어 있으며, 두 요소는 카드 플라스틱 지지대에 장착되어 보이지 않게 된다. 이 카드는 RF 필드를 방출하는 판독기를 통해 10cm 이내 범위의 커버리지를 갖는다. 이 필드는 코일을 통해 칩에 전원을 공급하고 명령 및 응답을 변조하는 칩과 통신하는 데 사용된다[1]. 이러한 카드는 단순히 비접촉식 카드 또는 RFID(Radio Frequency IDentification) 태그와 유사한 통신특성을 위한 RFID 카드로도 알려져 있다[2], 또는 NFC(Near Field Communication : 근거리 무선통신) 인터페이스가 장착된 장치와 상호작용할 수 있는 기능을 위한 NFC 카드가 있다[3].

비접촉식 카드(contact-less cards)는 카드를 지갑이나 주머니에서 꺼낼 필요 없이 판독기의 근접에서 흔들리기만 하면 된다는 점을 감안할 때 빠르고 쉬운 조작이 가능하기 때문에 관련 시장에서 관심이 집중되고 있다. 또한, 비접촉식 통신은 접촉식 스마트카드가 갖는 마모 및 파손 염려가 없어 매우 효과적이다. 이러한 장점이 있어 비접촉식 카드는 보호시설에서의 환경 액세스 제어를 위한 토큰, 전자신원 문서, 결제카드 등의 목적으로 널리 보급되어 사용되고 있다. 그러나 무선통신 방식(over-the-air communication)으로 인해 비접촉식 카드는 보안문제가 발생하기 쉽다. 특히 카드와 판독기 간에 교환된 메시지는 카드콘텐츠는 칩과의 비접촉 통신 설정을 통해 은밀하게 누출될 수 있다. 이를 액세스하는 경우 카드 콘텐츠를 사용하여 카드 복제본을 만들 수도 있다. 이에 대한 대응으로 비접촉식 카드 통신은 일반적으로 암호화되고 칩 콘텐츠 및 그 기능에 액세스하기 위해 액세스 제어 메커니즘을 채택한다(예 : 카드소지자가 시스템을 통해 코드(PIN번호)를 제공하도록 요청하는 경우 카드와 리더기가 상호작용하도록 되어 있다. 카드 복제 응답 메커니즘이 일반적으로 채택되는 것을 방지하기 위해 판독기는 카드메모리에 안전하게 저장되는 고유한 비밀암호화 키와 함께 카드에 결합된 난수를 전송하여 응답을 생성한다.

그간 여러 문헌에서 스마트카드에 대한 다양한 실제 릴레이 공격방법이 제시되어 이러한 장치에 대한 위협이 어떻게 실질적으로 나타날 수 있는지를 강조한바 있다. 접촉식 스마트카드에 대한 릴레이 공격은 2007년 S. Drimer, S.J. Murdoch에 의해 “Keep your enemies close: distance bounding against smart card relay attacks”에 잘 설명되어 있다[4]. 그러나 접촉식 스마트카드에 대한 릴레이 공격은 프록시 역할과 사용되는 장비 간에 설정된 통신채널이 다르기 때문에 비접촉식 스마트카드에 비해 릴레이 공격이 비교적 용이하다는 것이다.

- 첫 번째 완전한 공격 중 하나는 2005년 G.P. Hancke에 의해 “A practical relay attack on ISO 14443 proximity cards”에서 제시하였다[5]. 두 개의 하드웨어는 전용 RF 채널을 통해 50m의 릴레이 거리를 커버할 수 있도록 통신 프록시를 구현하도록 설계되었다.
- 2009년 G.P. Hancke 등은 “Confidence in smart token proximity: relay attacks revisited” 문헌에서, 2011년 P. Thevenon 등은 “On the weakness of contact-less systems under relay attacks” 문헌에서 비접촉식 시스템의 약점을 설명하였다[6][7].
- 기타 특정 프로그래밍이 가능한 장치가 릴레이와 블루투스 연결을 통해 두 장치 간 프록시로 사용될 수 있는 휴대전화로 구현한 하이브리드 솔루션을 제안한바 있다. 두 개의 휴대전화를 기반으로

한 솔루션이 서로 다른 연구에서 제시되었다.

- 또 다른 하이브리드 솔루션으로 블루투스 연결이나 Wi-Fi 네트워크를 사용하는 (WLAN : Wireless Local Area Networks) 프록시를 통해 수십 미터 거리에서 두 휴대전화 간 릴레이가 가능한 연구 결과를 제시한바 있다.

2. 비접촉식 카드 기술

2.1. 통신 프로토콜

비접촉식 카드 리더 통신을 위한 프로토콜 스택으로 ISO/IEC 14443 표준이 가장 많이 사용되고 있다. 카드의 물리적 특성을 자세히 보면, 카드판독기 통신을 위한 변조와 함께 카드에 전원을 공급하는 데 사용되는 13.56MHz에서 작동하는 RF 필드의 기능을 갖고 있는 점이 특이하다. 이러한 물리적 계층에 따라 표준은 판독기의 근접에서 여러 카드의 존재 가능성, 통신에 사용되는 프레임의 형식 및 프레임을 교환하는 데 사용되는 반이중 프로토콜에 대한 충돌 방지 절차를 명시하고 있다. 비접촉식 카드는 작동하려면 판독기에서 최대 10cm 범위에 배치해야 하므로 상호작용을 설정하려면 물리적 프록시가 필요하다. 카드가 판독기 필드에 배치되면 두 장치는 첫 번째 초기화 및 충돌방지 프레임을 교환하는 통신을 설정하게 된다. 이후 통신방식은 마스터-슬레이브 모드(master-slave mode)로 동작된다. 판독기는 요청을 보내고 카드는 응답으로 회신한다. 이러한 프로세스는 전체 카드 판독기의 상호작용에 걸쳐 반복적으로 이루어진다.

2.2. 보안 메커니즘

일반적으로 비접촉식 카드는 보안인증 제품이다. 이러한 인증을 받으려면 비접촉식 카드의 전체 개발 및 테스트 수명주기가 보안인증 제도의 규칙에 따라 수행되어야 한다. 인증의 결과로, 카드의 하드웨어와 소프트웨어는 카드 칩에 저장된 비밀암호화 자료를 추출하기 위해 측면 채널 공격과 같이 현장에서 공개적으로 알려진 공격에 대응할 수 있어야 한다. 카드 액세스 제어(액세스 제어 코드)를 사용하여 합법적인 카드소지자가 있는 경우에만 카드가 작동되도록 할 수 있다. 코드는 일반적으로 카드소유자만 알고 있는 카드에 저장되는 비밀정보이다. 카드가 판독기 및 그 뒤에 있는 시스템과 상호작용하는 시점에서 사용자는 코드를 제공하도록 지시한다. 이러한 키보드를 통한 입력 자료의 보안 메커니즘을 [그림 1]에 나타낸다. 제공된 코드는 메모리에 저장된 코드(PIN 번호)와 비교하여 카드로 전송되거나, 카드와 판독기 사이의 프로토콜에 사용되는 대칭 암호화 키를 생성하는 파라미터로 사용될 수 있다. 잘못된 코드를 삽입하면 카드는 거래를 중단하게 된다. 카드가 차단되거나 무차별 암호 대입 공격을 방지하기 위해 상호작용이 지연된 후 연속으로 표시할 수 있는 잘못된 코드 수에 대해 임계값을 설정할 수 있다.

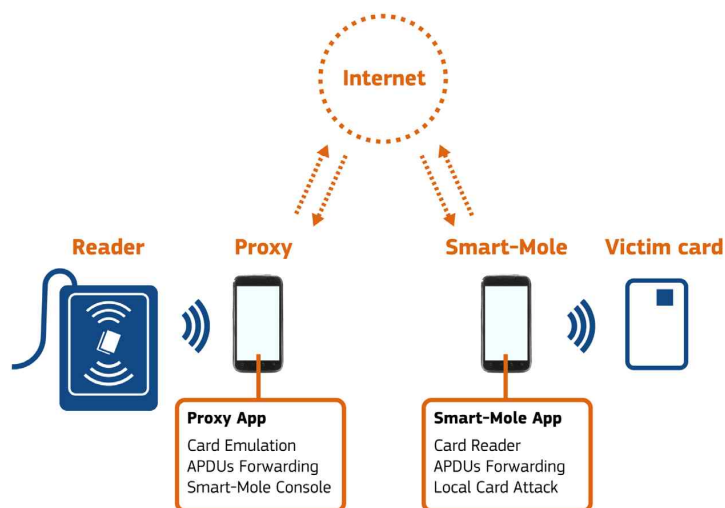


* 자료 : Luigi Sportiello, "Internet of Smart Cards": A pocket attacks scenario", international journal of critical infrastructure protection 26 (2019) 100302, p.5.

[그림 1] 키보드를 통한 입력 자료의 보안 메커니즘

3. 원격 비접촉식 카드 공격

전술한 비접촉식 카드는 보안조건이 충족되지 못하면 공격을 받을 수가 있다. [그림 1]에 나타낸 키보드를 통한 입력 자료의 보안 메커니즘을 기반으로 한 키보드를 통한 입력 자료의 공격구조를 [그림 2]에 나타낸다. 이 아키텍처는 비접촉식 공격 플랫폼으로 활용할 수 있는 일부 비접촉식 카드와 NFC 장착 휴대폰 사용자에게 대한 공격을 실행하는 데 사용될 수 있다[8]. 특히 피해자 호출을 이용하여 공격자에 의해 개발된 악성 응용프로그램에 감염될 경우에는 휴대전화에 인터넷에 연결되어 있어야 한다. 따라서 이동전화 사업자가 제공하는 데이터 네트워크 공격자는 인터넷에 연결된 NFC 장착 휴대전화에 필요하다, 프록시 공격자 자신에 의해 개발된 또 다른 특정 응용프로그램과 함께 설치된 프록시 응용프로그램도 역시 상호작용하는 인터넷 연결을 설정할 수 있다. 이를 위해 응용프로그램은 리더 역할을 하고 근처에 있는 카드와 상호작용이 가능한 휴대전화의 NFC 인터페이스를 사용한다. 프록시 응용프로그램은 NFC 인터페이스를 사용하는 대신 NFC 인터페이스를 이용하여 card emulation mode를 통해 판독기와 상호작용할 수 있다. 이러한 아키텍처를 사용하면 공격자가 다양한 악의적인 공격을 수행할 수 있다.



* 자료 : Luigi Sportiello, “Internet of Smart Cards”: A pocket attacks scenario“, international journal of critical infrastructure protection 26 (2019) 100302, p.6.

[그림 2] 키보드를 통한 입력 자료의 공격 구조

4. 공격 애플리케이션 분석

이 연구에서는 <표 1>에 나타낸 원격 공격자 비용 및 공격자의 이점을 기반으로 공격에 필요한 작업의 방법론을 설명한다. 카드와 판독기 사이에 보안채널이 설정되거나 숨겨진(암호화된) 시스템이 있는 경우 공격자 전략은 채택된 특정 보안조치와 사용가능한 취약점에 따라 달라질 수 있다. 예를 들어, 카드는 단순히 원격으로 사전 플레이 공격을 실행하기 위해 조회될 수 있다. 이는 암호화 메커니즘을 위해 일부 신용카드에 적용될 수 있다.

<표 1> 원격 공격자 비용 및 공격자의 이점

공격자 비용		공격자의 이점	
공격 수행	표준개발 키트로 개발된 소프트웨어가 있는 상용 장치를 이용	피해자 수	NFC 장착 휴대전화와 비접촉식 카드를 가진 모든 잠재적 사용자
공격 확산	다른 앱에 숨겨져 있거나 소셜 엔지니어링을 통해 Malware의 확산	원격	상호작용 원격 활동 피해자 프록시만 상황에 표시됨
취약점 분석	이미 게시된 다른 카드의 약점요인 분석	스텔스 활동	어떤 상황에서는 프록시 대신 운영자의 카드가 표시됨

* 자료 : Luigi Sportiello, “Internet of Smart Cards”: A pocket attacks scenario“, international journal of critical infrastructure protection 26 (2019) 100302, p.10.

이러한 보안 메커니즘은 공격자가 카드와 판독기 간의 통신을 릴레이 함으로써 제외될 수도 있다. 통신을 릴레이 할 수 있지만 BAC(Basic Access Control)를 중단해야 하는 ePassport의 경우 릴레이 공격과 연결하여 카드 액세스 제어를 중단해야 한다. 카드가 권한이 있는 판독기와만 상호작용하도록 제한되는 경우 공격자가 릴레이 공격을 통해 카드를 원격으로 사용하는 것이 유일한 옵션이다. 어쨌든 카드가 액세스제어 측정값에 의해 표시되고 시스템이 사용자에게 카드판독기 상호작용 전에 코드를 삽입하라는 메시지를 표시하는 경우 액세스제어 공격을 사전에 수행해야 한다. 예를 들어, MRZ가 카드판독기 상호작용을 시작하고 첫 번째 데이터집합에 액세스하도록 요구하는 ePassports에서 제공하지만 판독기는 지문과 같은 다른 카드데이터에 액세스하기 위해서는 자체적으로 인증할 수 있어야 한다[9].

5. 결론

비접촉식 스마트카드와 NFC 기능이 장착된 휴대전화가 결합되어 확산되고 있다. 사용자는 서로 상호작용할 수 있는 거리에 있는 주머니와 가방 정도의 접점이 필요하다. 그간 여러 문헌에 알려진 일부 비접촉식 카드 약점이 결합되어 공격자가 신원 도용이나 악의적인 결제거래와 같은 작업을 수행할 수 있음을 확인하였다. 이는 피해자의 카드를 원격으로 사용하여 공격자가 감염된 피해자의 전화를 통해 마음대로 제어할 수 있다는 위험요인이 있다. 이러한 공격들이 이미 적용되고 있다는 증거들이 있는바 상대적 용이성, 가능한 대규모 적용 가능성 및 잠재성 등을 고려하여 악의적인 피해자가 발생하지 않도록 제도적 장치가 필요하다. 이를 위해 개발자 및 규제기관이 비접촉식 카드의 보안을 계속 유지하는 것이 필요하다. 스마트카드는 민감한 데이터를 저장하고 신원 증명 및 결제거래와 같은 중요한 작업을 규제하는 데 사용되는 보안장치이다. 지난 10년 동안 비접촉식 스마트카드가 대규모로 도입하였다. 동시에 비접촉식 스마트카드와 상호작용할 수 있는 NFC 인터페이스가 장착된 이동전화도 증가하였다. 이 연구에서는 비접촉식 카드 분야에서 10년간의 연구 개발 결과를 조사하여 현재의 사회적 맥락과 기술수준에 따른 가능성을 진단하였다. 이 연구결과는 국내 고속도로의 스마트카드 운영 관련 정책에 벤치마킹 자료로 활용할 수 있을 것이다.

[참고문헌]

- [1] ISO/IEC 14443, "Identification cards –contact-less Integrated Circuit Cards –Proximity Cards", 2014.
 - [2] A. Juels, "RFID security and privacy: a research survey"IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp. 381–394, 2006.
 - [3] ISO/IEC 21481, "Information technology –Telecommunications and Information Exchange Between Systems –Near Field Communication Interface and Protocol–2 NFCIP–2", 2012.[4] Common Criteria.
- <<https://www.commoncriteriaportal.org/2016>>
- [4] S. Drimer, S.J. Murdoch, "Keep your enemies close: distance bounding against smartcard relay attacks", in proceedings of the 16th USENIX Security Symposium, pp. 87–102 2007.
 - [5] G.P. Hancke, "A practical relay attack on ISO 14443 proximity cards", Technical Report, University of Cambridge, Computer Laboratory, UK, pp.1–13, 2005.
 - [6] G.P. Hancke, K. Mayes, K. Markantonakis, "Confidence in smart token proximity: relay attacks revisited", Computers & Security, Vol. 28, No. 7, pp.615–627, 2009.
 - [7] P. Thevenon, O. Savry, S. Tedjini, "On the weakness of contact-less systems under relay attacks", in proceedings of the 19th International Conference on Software, Telecommunications and Computer Networks – SoftCOM2011, pp.1–5, 2011.
 - [8] L. Francis, G. Hancke, K. Mayes, K. Markantonakis, "Potential misuse of NFC enabled mobile

phones with embedded security elements as contact-less attack platforms”, in proceedings of International Conference for Internet Technology and Secured Transactions – ICITST 2009, pp.1-8, 2009.

- [9] BSI, “Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token-Part 1”, Ver. 2.20, 2015.

<원문제목> Framework for improving the resilience and recovery of transportation networks under geohazard risks

<원문출처> International Journal of Disaster Risk Reduction 31 (2018) 832-843