카드해킹의 문제점과 대비방안

Problems and countermeasures against card hacking

이진우, 이정훈, 이창엽, 노무승, 오현수

울산대송고등학교 3학년, 울산범서고등학교 3학년, 창원경일고등학교 2학년,
창원중앙고등학교 1학년, 부산진고등학교 1학년

Lee Jinu, Lee Jeonghun, Lee Changyeop, Moo-Seung Rho, Oh Hyensu

Ulsan Daesong High School third grader, Ulsan Beomseo High School third grader, Changwon Gyeongil High School second grader, Changwon Jungang High School first grader ,BUSAN Pusanjin High School first grader

요 약

현재 사용하고 있는 여러 가지 카드들은 자신의 신분을 증명하거나, 혹은 결제, 어떠한 건물에 들어갈 수 있는 권한을 가지고 있는 등, 다양한 용도로 사용 되고 있다. 이러한 카드들이, 다양한 방법으로 복제될 수 있는 문제점이 있어, 이에 저희들은 카드해킹과 관련된 해킹 기법에 대해 조사해보고, 국내에서 어떻게 대응할지, 현 대응방안이 정말로 안전한지, 다시 점검해보고자 한다.

I. 서론

MS카드는 카드 뒷면의 검정 띠 부분이 자기적 성질을 가지거나, 자기 스트라이프라 불리는 자성체를 넣어둔 카드이다. IC 카드와 비교해서, 스키밍 공격에 취약하며, 정보 노출이 쉽고, 외부 자기장의 영향으로 인해, 데이터가 손상되곤 한다. MS카드의 경우 ISO/IEC 7813 규격을 준수하며 Track1, Track2, Track3로 정보를 저장할 수 있는 공간이 나뉘는데, Track1 공간에는 영숫자 79자리까지 저장 가능하며, 주로 부가적인 정보를 남길 때 이 트랙을 사용한다. Track2 공간에는 40자리의 숫자를 저장할 수 있으며, 주로 카드 번호, 결제 금액 등을 저장하는데 사용한다. Track3 공간에는 107자리의 숫자를 저장 할 수 있으며, 주로 긴 숫자 데이터를 처리할 때 사용한다.

RFID란, 사물에 태그를 장비하여, 근거리, 장거리(최대 100m)에서도 사물의 정보를 수집 혹은 저장, 처리함으로써, 원격 카드처리 혹은 관리, 정보의 교환 등 다양한 산업 현장 혹은 일상에서 쓰이고 있다. RFID카드의 종류에는 MIFARE CLASSIC, MIFARE Ultralight, HID, HID iClass, ISO14443a, ISO14443b, ISO1569, SRI512, SRIX4K, Legic, epa, em410Xm Em4x50, Ti, Hitag/Hitag2, indala, T55xx, FlexPass, VeriChip, PCF7931, Kantech ioProx 등이 있다.

IC카드는 반도체 기반으로 제작된 직접회로(IC)칩이 삽입되어 있는 카드를 말하며, MS카드와 달리, 외부 자기장에 의한 데이터 손상이 없을 뿐만 아니라, 개인정보 저장 및 처리가 가능한 양방향 확인이 가능함으로써, MS카드보다 더 나은 보안성을 가지고 있다. 하지만 보안성이 뛰어난 만큼 RFID, MS카드 보다 단가가 비싸 다른 카드에 비해 잘 사용하지 않는 점이 있다.

위와 같이 다양한 산업군, 그리고 우리의 일상 속에 깊이 관여되어 있는 카드 기술들은

우리의 삶을 더욱 편리하게 해주었지만, 이를 이용한 크래커들의 공격으로 인해, 편리 하였던 기술들이 오히려 독이 되어, 문제가 발생하고 있어, 저희[우리]들은 카드 해킹 기법에 대하여 연구를 시작하게 되었다.

II. 본론

2-1 카드 해킹 기법의 이해

MS카드의 경우, 피해자가 MS카드의 자기 테이프를 카드 리더기에 긁게 되면, 자기 테이프에 저장한 값이 나오게 되며, 해당 값을 통해,

그림 1 | 2-1 카드 스키밍 장치

사용자를 식별하거나, 결제를 진행하게 된다. 이를 이용해 크래커는, 리더기에 카드 정보를 빼돌릴 목적으로 흔히 스키밍 장치라 불리는 또 다른 리더기를 덮어씌우는 형태로 설치하여, 피해자가 MS카드를 긁게 되면, 해당 MS카드의 값이 장치에 들어와 저장하게 되고, 추후 해당 값을 다른 MS카드에 저장시켜 카드 복제를 진행하게 되며, 해당 기법을 '오버레이 스키밍'이라 부른다.

RFID카드와 같이, 비접촉식 카드의 경우, RFID의 동작원리를 먼저 파악하면 어떻게 복제가 가능한지 파악할 수 있다. RFID의 경우, 태그에 목적에 맞는 정보를 입력한 후, 부착하게 되는데, 그 후 리더의 안테나를 통해 발사된 무선 주파수가 태그에 접촉하게 되면, 해당 태그가 주파수에 반응하여 입력된 데이터를 안테나로 전송하게 되며, 안테나는 전송 받은 데이터를 디지털 신호로 변조하여 리더에 전달하

그림 2 | Proxmark3

게 되고, 리더는 데이터를 해독하여 컴퓨터 혹은 다른 장치로 전달하는 방식으로 진행된다. 해당 과정에서 크래커는 리더를 준비하여, 피해자에게 접근한 뒤, 리더기를 통해 태그의 값을 알아내며, 해당 태그 값을 다른 RFID카드에 저장시켜, 카드 복제를 진행하게 된다. 이러한 기법을 'RFID 스키밍'이라고 부른다.

그림 3 | 2-1 카드 프린터기 TP-9100

별도로 위와 같은 기법으로 카드 복제 이후, 카드 프린터기를 이용하여 카드의 표면까지 정상 카드로 위조하는 이른바 사회공학기법을 사용해 타인에게 눈속임을 하여 정상적인 카드인 것처럼 보이게 만들 수 있으며, 이는 신분증

위조, 사내 출입증 복제 등 각종 공,사문서 위조에 사용될 수 있다.

2-2 카드 해킹 기법을 이용한 범죄 사례

MS카드는 ATM 카드 출입구와 비슷한 모양의 MS카드 스키머를 정상적인 카드 출입구에 덧붙여 신용카드 정보를 빼가는 방법이 가장 대표적인 사례로, 최근 2018년 11월 4일에 검거된 루마니아인 카드복제 범죄조직원들의 경우 MS카드로도 돈을 인출할 수 있는 Fallback기능이 있는 신용카드가 주로 해외 신용카드인 점을 악용하여 국내 ATM에서 복제된 해외 신용카드로 현금 인출에 성공하였으며, 인터폴과 한국 국제범죄수사대의 협력으로 체포되었다. 이외로 주유소나 편의점에 위장 취업하여 소비자들에게서 카드를 건네어 받을 때 소형 MS카드 스키머를 이용하여 카드정보를 저장하여 복제하는 사례나, 업소에서 복제된 카드를 사용하고 사용한 금액의 일부를 수수료로 업소에 지급하고 나머지를 현금으로 돌려받는 일명 '카드깡'에 이용된 사례가 있다. 심지어 2014년 6월 13일, 선불식 충전카드인 '마이비' 교통카드의 RFID 취약성을 악용해 금액을 변조하여 약 1억 8천만 원 상당의 부당이득을 챙긴 조직이 검거되기까지 하였으며, 2015년 1월 30일 KBS뉴스 현장추적에서 복제한 RFID카드를 이용하여 호텔 도어락을 열거나, 정부청사 출입까지 가능한 것에 대하여 보도한 사례가 있다. 전문적인 카드복제 범죄자들의 경우 사회공학기법을 추가적으로 적용하여 카드 프린트기를 사용해 카드에 이미지와 색을 입히고, 카드 양각기로 카드에 볼록한 번호를 새기며, 티핑기를 이용해 카드 번호에 은박을 입히는 등 진짜 신용카드로 보이게끔 다양한 카드복제 장비를 사용하고 있다.

2-3 IC 카드, 정말 안전한가?

IC카드는 현재, MS, RFID카드의 보안 한계점을 해결하고, 더 많은 데이터를 저장할 수 있는 장점을 통해, 타 방식의 취약한 카드들의 대책 방안 중 하나로 나오고 있다. 하지만, 이 IC카드가 정말로 안전하다고 볼 수 있는지 의심이 갈 수 있다고 생각한다. 이 점을 생각하여 관련 사례를 조사해본 결과, IC 카드의 Chip & PIN이 한 해킹 그룹에 의해 보안이 깨진 사례가 있었다. 해당 사건의 원리는 IC 칩이 개조되고, IC칩에 FUN이라고 각인한 다른 칩을 덮어 납땜한 상태였으며, 일반 IC 칩보다 0.4~0.7mm 두꺼웠다고 한다. 해당 카드를 엑스선을 통해 분석한 결과, 개조 칩에는 배선이 추가되어 회로가 변경되었으며, 이를 이용하여 POS시스템에서 모든 PIN코드를 허용 상태로 바꿔버리는 점을 이용한 것이었다. 하지만, 해당 취약점의 경우, 그 당시, PIN인증이 유럽에서 EMV카드의 거래 확인과 분리되어 있다는 사실을 이용하여, 해킹을 진행하였으며, 현재 이 부분은 해결된 상태이다. 이와 별개로 IC카드와 연계된 실제 피해 사례는 없는 것으로 확인 되었기에, 현존하는 카드 보안 체계 중 가장 안전하다고 볼 수 있다.

2-4 카드해킹의 실질적인 대책 방안

[2-4-1] MS 훼손

MS 카드의 경우, 앞에서 살펴보았듯이, 심각한 보안 문제가 존재하며, 스키머에 상당히 취약한 편이다. 이러한 상황에서 업주들은 가성비 때문에 마그네틱 카드를 채용하고 있지만, 보안상의 이유로 가능하다면, 마그네틱 카드 사용을 중단하고, IC 카드로 새롭게 카드를 발급받거나, 금융권에서는 마그네틱 + IC 카드를 IC 카드로 바꾸는 등의 조치를 취해야할 것이다. 지금으로써는 마그네틱 + IC 카드를 사용하게 되는 경우, 예를 들어, 편의점 혹은 식당에서 해당 카드를 사용하게 될 경우, 종업원이 이 과정에서 따로 준비한 MS 카드 리더기에 읽게 하거나, POS 기기의 보안적 문제, 네트워크의 문제 등의 사유로 카드 보안의 위협이 되기도 하니, 마그네틱 부분에 네오디뮴 자석을 이용하여, MS 부분을 사용할 수 없게 만들어, IC 카드만 사용하는 것을 추천한다.

[2-4-2] POS기의 정기적인 업데이트 및 관리

실제로, 위 사례에서 확인했듯이, POS 기기로 인해, 카드와 관련된 정보가 유출되기도 하였으며, 보안 패치가 지원되지 않는 구 버전의

OS를 사용하는 등의 관리 문제로 인하여, 다량의 카드 정보가 유출되기도 했다. 이 점을 생각한다면, POS 기기를 사용하는 업체에서는 POS 기기의 보안 패치를 정기적으로 적용하고, 지원이 종료된 OS의 경우, 지원이 진행되는 OS로 변경을 하여, 예방 조치를 취해야할 것이다.

[2-4-3] RFID 차폐 필름

RFID 스키밍으로 인해, 외국에서는 많은 카드 복제가 발생하기도 했고, 실제로 사회공학에 활용되어, 보안 사고로 이어지기도 한다. 이를 사전에 방지하기 위해서는, RFID 공격기법의 특징상, 전파만 막아도 이를 예방할 수 있기에, 저렴한 방법으로는 쿠킹호일을 보호하고자 하는 카드에 씌워 전파의 영향을 받지 않도록 하는 방법이 있으며, 해당 원리를 이용하는 차폐 필름 혹은 관련 제품을 사용하는 방법이 있다. [EX] 지갑 / 여권 케이스 / ETC]

III. 결론

본 논문에서는 결론적으로 MS와 RFID가 들어간 카드를 채택하고 있는 카드회사 및 기업은 비용이 조금 더 들더라도 IC카드로 전환해야 될 필요가 있다. 또한 사람들에게 해당 카드가 취약하다는 사실을 알릴 필요가 있으며, 이미 MS, RFID가 들어간 카드를 사용 중인 경우 최대한 카드 복제 예방방법을 숙지하여, 사용에 주의를 해야 된다. 경비원, 주점 종업원과 같이 카드를 검증하는 사람들은 사회공학에 대비하여 카드를 주의 깊게 봐야 되며, 복제된 카드를 사용하여 피해를 보는 쪽은 대부분 업주 측이므로 카드가 조금이라도 일반적인 카드와 다르다면 바로 의심을 하여 조치를 취해야 한다.

[참고문헌]

[1] '멤버십 카드 위조해 현금 빼낸 루마니아인 구속',한겨레신문,2018.11.04.,

http://www.hani.co.kr/arti/society/society_general/868697.html?_fr=mt2

[2] "ATM기 '고품질 스키머'에 고객들은 속수무책", RadioKorea뉴스, 2016.01.09.,

https://www.radiokorea.com/news/article.php?uid=235386

[3] '신용카드 IC칩 보안, 어떻게 뚫었을까'

, TechHolic뉴스, 2015.11.02.,

http://www.techholic.co.kr/news/articleView.html?idxno=42664

[4] "[현장추적] '카드 출입증' 1분이면 복제 정부청사도 뚫려", KBS뉴스, 2015.01.30.,

https://www.yotube.com/watch?v=X7Q3pRRQf7o

[5] "마이비카드 해킹해 잔액 조작 일당, 1억 8천여만원 챙겨", 보안뉴스, 2014.06.13.,

https://www.boannews.com/media/view.asp?idx=41469&kind=1