Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.6, Dec. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.6.1045

진동 신호를 이용한 카드 단말기 부채널 공격*

장 수 희,[1†] 하 영 목,[2] 윤 지 원[1‡]
[1]고려대학교 정보보호대학원, [2]한국전자통신연구원

A Side Channel Attack with Vibration Signal on Card Terminal*

Soohee Jang,[1†] Youngmok Ha,[2] Jiwon Yoon[1‡]
[1]Graduate School of Information Security, Korea University, [2]ETRI

요 약

본 논문에서는 카드 단말기로부터 발생할 수 있는 부채널 신호를 통해 금융 중요 정보의 누수가 발생할 수 있다고 가정하고, 실제 적용 가능한 공격 모델을 새로이 제안한다. 논문에서 제안하는 공격 모델은 소형 센서를 카드 단말기에 부착하여 카드 단말기에서 발생하는 진동 신호를 이용한 진동 신호 기반 부채널 공격이다. 이 소형 센서를 통해 카드 결제 승인 단말기의 버튼을 누를 때 발생되는 진동신호를 알아낼 수 있으며, 이러한 정보는 금융 정보를 탈취하는 기반이 된다. 이러한 연구는 기존에 실시된 다른 부채널 연구들과 어느 정도 유사한 면도 있으나, 본 논문은 비언어적 모델을 기반으로 한다는 점에서 그 성격이 다르다. 왜냐하면 금융 결제에 필요한 카드 번호, 비밀번호, 휴대전화 번호 등은 일정한 패턴을 가질 수 없기 때문이다. 또한 소형 카드 단말기를 이용한 연구가 거의 없었다는 점에서 본 연구는 의미를 가진다. 이에 소형 무선 센서를 데이터를 수집하고, 데이터 특성을 고려해 주파수 영역의 스펙트럼 및 주성분 분석 방법을 이용한 통계적 신호처리 및 패턴 인식 알고리즘을 이용해 수집 정보를 분석을 실시한 뒤, 그 실험 결과를 선보인다.

ABSTRACT

In this paper, we assume that the information leakage through side-channel signal may occur from the card payment terminal and newly introduce a real application attack model. The attack model is a side channel attack based on vibration signals, which are detected by a small sensor attached on card terminal by attacker. This study is similar to some other studies regarding side channel attack. However, this paper is different in that it is based on the non-language model. Because the financial transaction information such as a card number, password, mobile phone number and etc cannot have a constant pattern. In addition, there was no study about card terminal. Therefore, this new study is meaningful. We collected vibration signals on card terminal with a small wireless sensor and analyzed signal data with statistical signal processing techniques using spectrum of frequency domain and principal component analysis and pattern recognition algorithms. Finally, we evaluated the performances by using real data from the sensor.

Keywords: Side channel attack, Security, Card terminal, Signal processing

I. 서 론

카드 결제 승인 단말기는 물품 및 서비스 결제 시 대금 지급을 가능하게 돕는 일반적인 장치이다. 사용자가 단말기에 결제에 필요한 정보들을 입력하거나 카드에 있는 마그네틱 혹은 IC칩을 읽히면, 카드 번호, 계좌 번호, 비밀번호, 휴대폰 번호 등의 정보들은 단

접수일(2014년 8월 22일), 수정일(2014년 10월 30일), 게재확정일(2014년 10월 30일)
* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 "2014년도 고용계약형 정보보호 석사과정 사업"의 연구결과로 수행되었음 (과제번호 H2101-14-1001)
† 주저자, hardworker12@korea.ac.kr
‡ 교신저자, jiwon_yoon@korea.ac.kr(Corresponding author)

말기를 거쳐 VAN사와 카드 회사로 가게 된다. 이러한 절차를 걸쳐서 결제 대금 승인 확정되면 카드 거래는 성립한다.

본 논문에서는 이러한 결제 과정에서 카드 결제 승인 단말기로부터 금융 중요 정보의 누수가 발생할 수 있다고 가정하고, 카드 결제 승인 단말기에 발생할 수 있는 정보 누수 위협 요인과 공격 모델을 제안하고자 한다. 특히 결제의 기본이 되는 입력정보들에 대한 부채널 정보 누수에 초점을 두었다.

기존의 카드 결제에 관련된 연구들은 주로 단말기 해킹 내지 암호 알고리즘 및 모듈에 관련한 연구가 주류를 이뤘다. 하지만 이 논문은 기존에 시도되지 않았던 카드 결제 승인 단말기에 발생할 수 있는 물리적 부채널 공격 가능성에 대해 연구해보고자 하였다. 특히 제안하는 공격 모델은 카드 결제 승인 단말기에 부착되어 있는 버튼을 누름으로써 발생되는 신호를 분석하여 금융 정보를 빼내는 방식을 사용한다. 이 공격에서 신호를 수집하기 위해 사용하는 기기는 9축 소형 무선 센서이며, 사용하는 신호 분석 방법은 주파수 영역의 스펙트럼 및 주성분 분석 방법을 이용하는 통계적 신호처리이다. 처리된 신호를 다루기 위해 사용하는 방법은 패턴 인식 알고리즘이며, 해당 공격은 알고리즘의 종류에 제한받지 않는다. 소형 센서를 카드 결제 승인 단말기에 부착하여 카드 결제 승인 단말기에서 발생하는 진동 신호를 이용해 키패드 입력 값을 알아내는 공격에 대한 연구는 아직 진행된 바가 없다.

본 논문은 다음과 같이 구성된다. 먼저 II장에서 부채널 공격에 대한 내용과 기존 연구들에 대해 설명한다. III장에서 카드 단말기에 발생할 수 있는 부채널 공격 위협에 대해 다룬다. 실제 실험과 그 결과는 IV장에서 상세히 다뤄지며, V장에서는 결론으로 마무리한다.

II. 배경 지식 및 관련연구

2.1 부채널 공격

부채널 공격은 Kocher가 1996년과 1999년에 열린 CRYPTO에서 암호 알고리즘에 전력 분석 공격을 발표하면서 처음으로 알려졌다. 그는 암호 알고리즘이 동작할 때 발생하는 시간차를 이용해 암호 시스템을 분석이 가능함을 보였다[1],[2].

우선 부채널이란 전력 신호, 전자기파, 레이저, 소리, 진동 등을 모두 포함한다. 이러한 부채널 정보들을 분석하여 암호를 풀거나 원하는 정보를 얻어내는 것이 부채널 공격이다. 즉, 부채널 공격이란 암호 알고리즘을 직접 건드리지 않고 정보를 처리하는 과정에서 발생하는 측정 가능한 물리량으로부터 공격자가 원하는 정보를 얻어내는 공격이다. 암호 알고리즘이 이론적으로 완벽하게 설계되어 매우 안전하다고 할지라도 부채널 공격에 대한 위험은 여전히 존재할 수 있다. 왜냐하면 부채널 공격은 암호 알고리즘의 이론적 안전성과는 상관없이 구현 환경에 따라 그 가능성이 존재하기 때문이다. 이러한 공격은 주로 암호 알고리즘이나 암호 모듈이 동작할 때 걸리는 전력 소비량, 연산 시간, 전자기파 등을 분석하는 형태로 연구되었다. 또한, 의도적으로 하드웨어나 소프트웨어에 오류를 일으키거나 주파수, 온도 등의 값을 바꾸어 정보가 어떻게 변화하는지 관찰하여 특정 정보를 얻어 내는 방식으로도 연구되었다.

2.2 카드 단말기 관련 연구

본 논문에서는 통계적 신호처리 기법과 패턴 인식 기법을 사용하여 카드 결제 승인 단말기로부터 유출되는 부수적 정보들로 데이터를 유추해 내는 공격과 관련된 연구 내용을 다룬다. 특히 단말기 키패드 입력 시 발생하는 진동을 기반으로 결제 관련 입력 정보를 알아낼 수 있는지 확인해 보고자 한다. 카드 결제 승인 단말기에 이와 같은 공격을 시도한 연구는 없었기에 본 연구가 새롭다고 할 수 있다.

기존에는 결제 시스템 혹은 카드에 직접적인 부채널 공격이 주로 연구되었다. 먼저 [6]는 금융 IC 카드를 대상으로 부채널 분석 및 공격 취약성에 관한 연구이다. 실제 금융 IC 카드에 차분 전력 분석 공격을 수행하였고, 금융 IC 카드의 경우 100개의 전력 신호만으로 카드의 마스터키를 찾을 수 있음을 확인하였다. [7]의 경우 전력 신호의 노이즈 특성을 분석하고 SNR을 모델링하고, 전력 소비 신호 모니터링을 통해 스마트카드보안을 무력화 얼마나 시킬 수 있는지 확인하였다. 이외에도 [8],[9]는 일반적인 스마트카드에 부채널 공격을 수행하였다. [8]은 second-order DPA 공격을 이용하여 마스크 된 AES를 공격하는데 성공하였으며, [9]는 파티셔닝 공격을 통해 SIM 카드의 COMP128 알고리즘을 공격하였다.

카드 결제 승인 단말기와 비슷한 POS 기와 관련한 연구가 있었지만[10],[11], 시스템의 내부적인

접근 및 보안성 평가 측면에서 연구되었으며, 이처럼 소형 카드 단말기를 보안 관점에서 다루는 논문은 현재까지 없었다. 현대 사회에서 카드의 보급과 사용량은 급증하고 있으며, 2015년부터 IC 카드의 전면 의무화 사용이 확정되면서 금융권에서도 부채널 공격에 대한 관심을 갖기 시작했다. 이에 앞으로 다양한 관점에서 카드 단말기에 대한 연구들이 시도될 것으로 기대한다.

2.3 공격 모델 관련 연구

본 논문에서는 부채널 공격에 대해 연구를 진행하였으며, 키패드를 누름으로써 발생되는 진동 신호를 이용해 정보를 유추하는 형태의 공격에 대해 다룬다. 이러한 공격 형태는 정보 보호 분야에서 현재 활발하게 진행되고 있다. 예를 들어, Marquardt는 2011년도에 아이폰에 내장된 가속도 센서를 이용하여 키보드 타이핑을 유추하는 연구를 성공적으로 마쳤다[3]. 이 연구에서는 개별 키보드 타이핑의 진동의 물리적 거리와 위치를 유추하는 데에 스펙트럼, 켑스트럴(cepstral), 제곱근 평균치(root mean square, RMS), 비대칭도, 분산, 첨도 등의 특성을 사용하였고, 추가적으로 언어 모델을 활용하였다. 부가적으로 발생되는 신호를 분석한다는 측면에서 NSA의 도청 사건도 좋은 예시가 될 수 있다[4]. NSA는 건물의 유리창 레이저를 쏴서 그 진동을 통해 대화내용을 도청을 해왔다. 이는 지난 해 크게 이슈가 되었던 NSA 정부 수집 폭로 사태에서 부채널 공격을 이용한 고도의 도청 기술로 이슈가 된 내용이다. 또한 프린터로부터 발생되는 신호를 분석하여 정보를 유추해 내는 방법 또한 연구된 바 있다[5]. [5]는 프린터로부터 발생되는 신호를 분석하기 위해 웨이블릿(wavelet) 특성과 주파수 영역 특성, RMS, 평균, 분산, 비대칭도, kurtosis, crest factor 등을 사용하였고, 원하는 정보를 성공적으로 유추해 내었다.

본 논문에서 다루는 부채널 공격은 기존의 키보드 타이핑에 대한 부채널 공격과 유사하게 보일 수 있다. 하지만, 본 논문은 언어 모델과 같은 부가 기술을 기반으로 사용하지 않는다는 점, 그동안 부채널 공격과 관련된 논문에서 언급되지 않았던 신호처리 방법을 사용했다는 점, 진동을 이용하는 부채널 공격을 카드 단말기에 적용했다는 점에서 그 성격이 다르다고 볼 수 있다. 특히, 기존의 연구들은 언어모델과 같은 부가적인 기술을 기반으로 알아낸 자판 값에 약간의 오류가 있더라도 어느 정도 유추가 가능하였다. 하지만 금융결제에 필요한 카드 번호, 비밀번호, 휴대전화 번호 등은 일정한 패턴을 가질 수 없다. 따라서 기존 연구들이 사용했던 언어 모델과 같은 추가적인 방법을 쓰더라도 큰 효과를 전혀 기대할 수 없으며, 이런 측면에서 기존의 연구들과 차별화 된다.

III. 공격 모델

3.1 공격 가능 요인

먼저 제안하는 공격이 성공하기 위해서는 단말기 사용자가 단말기 패드를 통해 금융 정보를 입력하는 상황이 설정되어야 한다. 이러한 특수한 상황을 가정했을 때 본 논문에서는 다음과 같은 경우에 금융 정보 누수가 발생할 수 있다고 보았다.

- 카드 마그네틱/IC 칩 손상으로 직접 카드번호를 입력하여 거래 할 경우
- 직불카드 거래 시 핀 패드를 이용한 비밀번호 입력 혹은 포인트 조회/사용이 필요한 비밀번호 입력 시 정보
- 카드 결제 승인 단말기를 통한 계좌이체 시 입력하는 금융관련 정보
- 현금 영수증 발급 시 필요한 휴대전화, 사업자 등록 번호 정보

이러한 경우 단말기 사용자는 거래를 위해 반드시 키패드를 통해 금융 거래 정보를 입력해야한다. 그리고 이 때 발생한 입력정보는 단말기에서 발생하는 진동 신호를 이용하여 알아 낼 수 있다고 전제하였다. 왜냐하면 진동 신호는 키패드에서 각 버튼이 눌려질 때마다 미묘하게 다른 차이를 갖는데, 제일 큰 원인은 각 버튼의 위치가 동일하지 않기 때문이다. 따라서 신호가 센서에 전달 될 때 센서와의 거리, 사용자가 누르는 세기 등 여러 요소에 의해 각 버튼은 위치에 따라서 미세하게 차별화된 신호 특성을 갖게 된다.

이러한 특성을 이용하여 본 논문에서는 새로운 공격 시나리오를 구성해보았다. 먼저 단말기에 부착된 진동 센서가 각 키패드라 눌릴 때 발생하는 신호를 감지하게 된다. 이 때, 키패드와 센서 간의 물리적 거리로 인해 센서와 가까운 버튼은 강한 신호로, 멀리 떨어진 버튼은 다소 약한 신호가 전달 될 것이다. 이러한 진동 신호의 차이를 이용하여 버튼 위치(키패

드 입력 값)를 알아내고 궁극적으로는 어떠한 금융 정보가 입력되었는지 유추할 수 있다는 가정을 해보았다.

3.2 공격 개요

우리의 공격 모델은 크게 '데이터 수집', '데이터 분석', '금융 정보 탈취(공격)'인 3단계를 거친다. Fig. 1은 이 모델의 전반적인 흐름을 보여준다. 먼저, 데이터 수집 단계에서는 카드 결제 단말기 사용자가 숫자 입력을 위해 버튼에 압력을 가함으로써 생성되는 신호를 감지하는 센서를 이용한다. 사용자는 계산 또는 계좌이체를 위해 단말기 시스템에 번호를 입력하고, 센서는 그로 인해 발생되는 진동 신호를 포함한 여러 종류의 신호를 감지하여 공격자의 서버에 송신한다. 이러한 과정을 통해 본 논문에서 수집한 정보는 자이로스코프, 가속도계, 지자기계의 각 센서 3축의 정보이다. 이외에 추가적으로 고려할 사항은 센서의 종류, 위치, 주파수 대역 등이 될 수 있다. 우선 공격에 사용할 센서는 적당하게 민감해야 한다. 너무 둔감한 센서는 공격자에게 충분한 정보를 제공하지 못하고, 너무 민감해도 오히려 공격자를 혼란에 빠뜨릴 수 있기 때문이다. 또한, 센서의 존재 여부를 카드 결제 단말기 이용자가 눈치 채지 못하게 위치를 잘 선택하는 것도 중요하다. 주파수 대역은 수신기가 데이터를 받아들일 수 있는 대역이면 충분하다. 센서가 송신한 데이터의 노이즈를 최소화 하며 잘 받으려면 주파수 대역을 주의 깊게 결정해야 하는데, 본 논문에서는 2.4GHz의 주파수를 사용하였다.

다음은 데이터 분석 단계로, 센서에서 수집한 데이터를 분석하여 유의미한 정보를 추려내는 단계이다. 무선 센서를 통해 공격자에게 전해진 신호는 통계적 신호처리 기법을 통해 정제된다. 주어진 신호로부터 목적에 맞는 특성을 추출해 내는 작업은 신호를 다루는 연구에서 매우 중요한 비중을 차지한다. 동일한 데이터를 사용하더라도, 어떤 특성을 사용하는지에 따라 그 성능이 매우 달라지기 때문이다. II장에서 언급했듯, 기존 정보보호 연구들에서는 신호로부터 적절한 특성을 추출하기 위해 웨이블릿(wavelet) 특성, 주파수 영역 스펙트럼(spectrum), 켑스트럴(cepstral), 제곱근 평균치(root mean square), 비대칭도, 분산, 첨도 등을 사용했다. 하지만, 이 특성들은 본 연구에서 만족할만한 결과를 제공하지 못했다. 때문에 이 공격에서는 전송 받은 신호를 분석하기 위하여 다른 방법을 사용 할 것을 제안한다.

먼저, 버튼을 분류하기 위한 분류기(Classifier)에 입력 값으로 이용될 특징들을 추출(Feature Selection)하는 과정이 필요하다. 이 과정은 주파수 영역에서의 파워 스펙트럴 밀도를 계산함으로서 이루어진다. 주파수 영역의 특성을 이용하는 이유는 Fig. 2에서 볼 수 있듯, 시간 영역에서는 버튼 간 차이점을 찾아내기가 쉽지 않았기 때문이다. 더 나아가, 이 논문에서는 이 스펙트럼에 통계적 접근 방식을 접목시킨 특성을 사용한다. Fig. 2는 이 논문에서 사용하는 스펙트럼의 일부분인 1번과 3번 버튼에 해당하는 스펙트럼의 평균, 그리고 표준 편차를 이용하여 그린 상한선과 하한선을 나타낸다. 이 논문에서 이 공격에서 사용하는 특징은 이 상한선과 하한선으로 정의되는 영역에 속하는 데이터의 개수이다. 이렇게 구해진 개수를 각 데이터들은 특징으로 이용한다.

최종적으로 이 공격에서 사용하는 특성은 특성에 주성분 분석(principal component analysis, PCA)이 적용된 데이터이다. 주성분 분석은 투영을 이용하여 서로 선형적으로 의존하거나 중복되는 축들

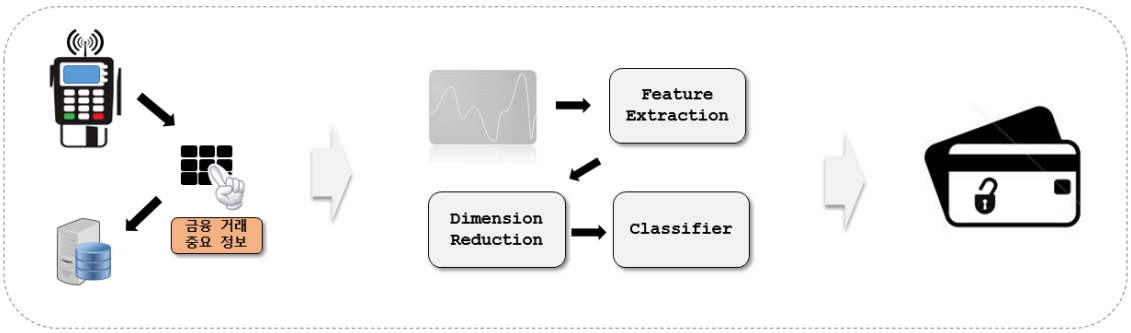
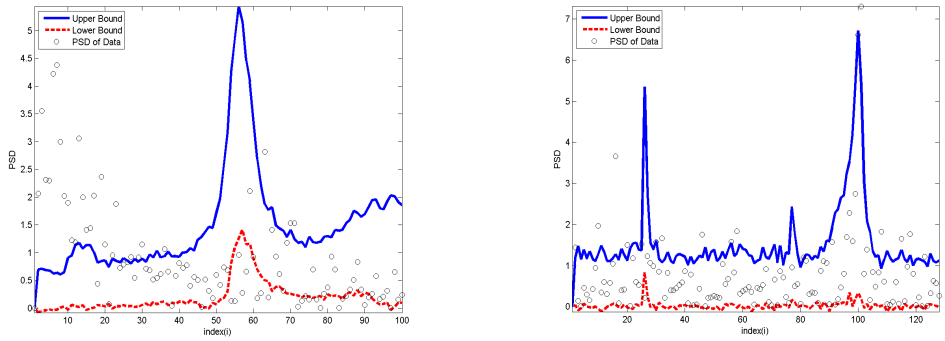


Fig. 1. The overview of attack process



(a) button 1 (b) button 3

Fig. 2. The part of button signal spectrum and the upper/lower bound

을 교차 검증법과 같은 모델 선택 방법에 의해 주어진 기준에 따라 최소화 해주고, 노이즈 또한 동시에 제거해주는 기술이다. 센서의 위치에 따라 스펙트럼의 평균과 그 범위가 달라지겠지만, IV에서 볼 수 있듯, 이러한 특성을 사용하는 이 논문의 공격은 효과적이었다.

정제된 데이터로부터 공격에 의미 있는 데이터를 얻는 마지막 과정은 패턴 인식 분류 알고리즘을 통해 이루어진다. 패턴 인식 커뮤니티에서 가장 많이 자주 사용되는 알고리즘에는 Naive Bayes, k-근접 이웃(nearest neighbor) 분류기, 서포트 벡터 머신(support vector machine), 뉴럴 네트워크(artificial neural network), 가우시안 프로세스 분류기, Dirichlet 혼합 모델, EM(expectation and maximization) 분류기, 로지스틱(logistic) 모델, 히든(hidden) Markov 모델 등이 있다. 이러한 모델들은 교차 엔트로피(cross entropy), Bayesian 접근법, ML(maximum likelihood) 또는 MAP(maximum a posteriori), Newton의 방법과 같은 수치 해석적, 통계적 접근법을 통해 가장 그럴듯한 정보를 제시해준다.

마지막 공격 단계는 앞선 과정을 통해 공격 성공에 충분한 확신이 들었을 때 실행하는 단계이다. 이 단계에서는 앞서 설명한 방법을 통해 유추한 정보를 가지고 카드 결제 단말기에 입력된 정보를 사용한다. 여기서의 확신은 표준 편차의 정도로 알아볼 수 있다. 일반적으로 낮은 표준 편차는 낮은 오류율을 나타낸다.

IV. 실 험

4.1 데이터 수집

우리는 제안하는 공격 모델의 유효성을 검증하기 위해 실제 데이터를 사용하였다. 사용된 장비들은 광우정보통신에서 제작한 2인치 써멀 NICE CHECK 카드 결제 승인 단말기 MIT-5700T, 9축 무선 통신 데이터 송신 지원 센서 EBIMU24G, 그리고 수신기 EBRF24GRCV이다. Fig 3는 MIT-5700T에 센서를 설치한 모습을 보여준다. 카드 결제 단말기에 부착된 무선 통신 센서의 사양은 아래와 같다.

- 2.4GHz 무선 AHRS 모듈
- 임베디드 9 축 MEMS 센서
- 자이로스코프/가속도계/지자기계 각각 3축
- Euler 각, Quaternion, 칼리브레이션 된 원본(raw) 데이터
- 샘플링 주파수 100Hz
- 디지털 저역 통과 필터 : 5Hz~256Hz
- 자이로스코프 민감도 : 250dps~2000dps
- 가속도계 민감도 : 2g~ 16g
- 센서 필터 요소 : 1~50

자이로스코프(gyroscope) 센서로 측정한 데이터, 가속도계(accelerometer)로 측정한 데이터, 지자기계(geo-magnetic)로 측정한 데이터를 제공한다. 자이로스코프는 한 축 또는 여러 축의 회전 움직임의 각 변화량을 측정한다. 또한 자이로스코프는 가속도계와 지자기계와 다르게 중력이나 전자기장과 같은 외부의 힘에 영향을 받지 않고 독자적으로 동작한다.

Fig. 3. The card reader and attached sensor

가속도계는 선형 가속도와 기울임 각도를 측정한다. 단일 혹은 다축의 가속도계는 크기와 선형, 회전, 중력의 가속도 방향들을 합쳐진 상태로 감지한다. 주로 이 센서는 모바일 장비에서 화면을 세로 방향에서 가로 방향으로 돌리는 것과 같은 간단한 혹은 중력과 관련 있는 장비의 방향을 측정하는 용도로 주로 사용된다. 지자기계는 절대적인 방향을 측정하기 위해 사용되며 주로 네비게이션에서 정확한 방향을 알려주기 위해 사용된다. EBIMU24G와 칼리브레이션(calibration) 및 기타 통신 환경에 대해서는 [12]를 통해 더 자세하게 확인할 수 있다.

Fig 3과 같은 환경에서 우리는 샘플링 주파수(sampling frequency)를 100Hz로 설정하고, 일정한 간격으로 모든 버튼을 하나씩 눌러 진동을 생성하였으며, 대상은 '1' 버튼부터 '000' 버튼까지 총 12개의 버튼이다. 버튼을 누른 실험자는 서로 다른 성인 5명이며, 수집한 데이터 중 각 번호별로 151개씩 추출하였다. 따라서 실험에는 총 9060 개의 데이터를 이용하였다.

4.2 데이터 분석

이 논문에서는 수집한 데이터를 기반으로 특징 추출과 일반적인 분류기를 이용하여 자료에서 버튼 정보를 알아 낼 수 있는가를 확인하는 작업을 수행한다. 본 논문에서는 3.2에서 언급된 신호처리 방법, Naïve Bayes, Neural network, Logistic Regression을 사용하였다. 다음은 이 논문에서 사용한 분류기에 대한 간략한 설명이다.

4.2.1 Naïve Bayes 분류기

Naïve Bayes 분류기는 Bayes 정리와 Laplace smoothing, 조건부 독립 개념만으로 분류 문제를 풀어낼 수 있는 기술이다. 이 논문에서는 진동 데이터가 주어졌을 때, 그 데이터가 의미하는 숫자버튼이 무엇인지를 알아내기 위해 이 분류기가 사용되었다. 그 과정은 다음과 같다.

먼저, 훈련을 위한 데이터를 통해, 데이터가 어떤 특성을 가지고 있을 때 몇 번 버튼을 의미했는지에 대한 테이블을 작성한다. 그 후에는, 특정 버튼에 대한 데이터가 주어졌을 때, 데이터가 각 특성을 가지고 있을 확률을 구한다. 여기서 주의해야할 점은 (특정 버튼에 대한) 데이터가 주어졌을 때, 각 특성들은 서로 독립적이라는 것이다. 즉, 각 특성들은 데이터에 대해 조건부 독립이다. 테스트 단계에서는, 앞에서 계산된 결과를 바탕으로 Bayes 정리를 통해 목적하는 '데이터가 주어졌을 때 각 버튼이 될 확률'을 계산한다. 훈련 과정에서 고려되지 못한 특성에 대한 정보는 Laplace 스무딩 기법을 통해 계산되도록 한다.

4.2.2 Neural network

Neural network는 어떠한 문제를 컴퓨터로 해결코자 할 때 그 방식을 인간의 두뇌처럼 문제를 처리하고자 하는 방식이다. 이 모델의 구조는 입력 계층, 숨겨진 계층, 출력 계층으로 구성되어 있다. 주어진 데이터는 이 모델의 입력 계층에 먼저 입력이 되며, 그 후에는 입력 계층과 숨겨진 계층 간의 관계, 숨겨진 계층과 출력 계층 간의 관계를 고려하여 목적하고자 하는 값을 얻어낸다. 이 모델을 사용하기 위해서는 먼저 각 계층 간의 관계를 정의해주는 가중치를 구해야 한다. 이 논문에서는 이를 위해 오차역전파법(back-propagation)을 이용한다. 이는 매 훈련 시 기존의 Neural network에서 출력해 내는 값과 실제 값 간의 차이를 각 계층 간 가중치에 반영하는 방법으로, 보통 반복적 교차 엔트로피 수렴 방법을 통해 이루어진다. 이 실험에서 사용된 Neural network는 초기에 각 계층 간 가중치에 -0.5부터 +0.5 사이의 무작위 값이 설정되며, 자동적 오차 역전파법을 통해 오차가 충분히 작아질 때까지 (5% 미만) 훈련을 한다. 오차 반영 비율은 교차 검증법을 통해 결정한다.

4.2.3 Logistic Regression

로지스틱 회귀 분석 모델은 분석하고자 하는 대상들이 두 집단 혹은 그 이상의 집단 (다변수 데이터)

Table 1. Experimental results

A number of digits	Classifier	Person 1	Person 2	Person 3	Person 4	Person 5	Random
16-digit	Naive Bayes	68.11	64.48	45.57	47.99	65.76	51.52
	Logistic Regression	70.59	65.59	50.00	48.10	66.10	63.08
	Neural Network	67.57	66.11	46.62	46.15	65.97	59.19
4-digit	Naive Bayes	70.52	69.21	48.55	61.57	67.18	62.22
	Logistic Regression	73.87	71.10	51.68	63.44	69.99	65.02
	Neural Network	71.19	68.19	52.71	62.00	66.00	64.98

으로 나누어진 경우에, 개별 관측 값들이 어느 집단으로 분류될 수 있는가를 분석하고 이를 예측하는 모형을 개발하는 데 사용되는 대표적인 통계 알고리즘이다. 이 모델은 확률적 차별화 모델로 여겨지며, 실제 공간에서 다루기 힘든 종속 변수들 간 비선형 영향을 특성 공간에서 다룬다. 이 논문에서는 로지스틱 회기 분석 모델을 사용하기 위해 10가지 클래스에 대한 코딩 스킴, (α를 계수로 하는) 소프트맥스(softmax) 함수, Bayesian 접근 방법을 사용한다. 각 특성에 대한 α는 교차 엔트로피에 대한 Newton의 방법을 통해 구한다.

4.3 실험 결과

공격 모델의 유효성을 알아보기 위해 논문에서는 실제 데이터 및 III장에서 설명한 공격모델을 이용해 카드번호와 비밀번호에 대한 공격을 해보았다. 일반적으로 카드번호는 10진수 16자리로 구성되어 있으며, 계좌 비밀번호 또는 카드 비빌 번호는 10진수 4자리로 구성된다. 즉, 카드 번호를 유추하기 위해서는 16개의 서로 다른 숫자들을 공격 모델로 유추해야 하고, 비밀 번호를 유추하기 위해서는 4개의 서로 다른 숫자들을 유추해야 한다.

또한 본 실험에서는 제안하는 공격 모델이 분류기 종류에 제한받지 않는다는 사실을 확인하기 위해, 세 가지 분류기 Naive Bayes, 로지스틱 모델(logistic regression), 뉴럴 네트워크(neural network)를 제안하는 공격 모델에 적용하고 비교평가를 해보았다. 유추 대상이 될 카드 번호 또는 비밀번호는 무작위로 생성하였다. Table 1에 기재된 결과는 특징 추출 알고리즘인 PCA 및 분류기의 파라미터에 대해 10등분 교차 검증(10-fold cross validation)을 시행하여 찾아낸 가장 좋은 결과들이다. 예를 들면, 카드 번호 유추의 경우(16자리 숫자에 대한 유추), 실험자 1의 로지스틱 모델은 90%의 정보량을 고려하는 PCA와 파워 스펙트럼 표준편차의 1.2배를 오차 한계로 하는 통계적 신호처리 방법으로 처리된 신호를 사용하였다.

실험 결과, 우리는 제안하는 공격 모델이 분류기 종류에 관계없이 카드 단말기를 누름으로써 발생된 진동 데이터를 이용해 목표 번호를 잘 유추한다는 것을 알 수 있었다. 가장 유추가 잘 된 경우는 카드 번호의 경우 실험자 1의 데이터에 로지스틱 모델을 사용한 경우로 그 정확도가 70.59%였다. 비밀 번호(4자리 숫자)에 대한 유추에서는 73.87%의 정확도가 가장 높은 경우였다(실험자 1). 무작위 데이터(모든 데이터를 무작위로 섞어 만든 데이터)에 대한 실험 결과 또한 흥미롭다. 이 실험은 타인의 데이터로 분류를 시도했을 때 이 공격 방법이 유효한 지 알아볼 수 있는 실험이다. 해당 실험에서는 이 논문에서 제안하는 공격이 16자리와 4자리 숫자에 대해 각각 최대 63.08%, 65.02% 정확도를 보였다. 이것은 공격자가 목표 단말기를 사용하는 사람들이 누구라 할지라도 공격하는 데에 큰 구애를 받지 않으며, 심지어 본인이 목표 단말기와 같은 종류의 단말기를 구매 해 공격 모델을 훈련시켜 공격할 수 있다는 것을 의미한다. 무작위로 10진수의 중복된 16개 숫자 또는 4개의 숫자를 유추하는 확률이 $(1/10)^{16}$과 $(1/10)^{4}$라는 것을 생각해봤을 때, 이 실험 결과는, 사용자가 누른 버튼을 유추해야하는 경우 이 논문에서 제안하는 방법을 사용하는 것이 매우 효과적이라는 것을 말해준

다. 또한, 이 결과는 이 논문에서 다루는 공격이 단순한 비선형 회귀모델을 통해 높은 정확도로 이루어질 수 있다는 것을 말해준다. 실험자 4의 경우를 제외하고는, 로지스틱 모델이 가장 좋은 성능을 보였기 때문이다. 로지스틱 모델의 특징은 비선형성을 고려할 수 있는 특성 공간(feature space)에서 선형 회귀 분류를 한다는 것이다. 뉴럴 네트워크 또한 비선형을 고려하지만, 복잡한 계층 구조를 이루고 있다(이 복잡한 계층은 과적합(over fitting) 결과를 초래할 수 있기에, 뉴럴 네트워크를 사용할 때에는 보다 주의 깊은 모델링을 해야 한다). 즉, 이 공격에서 꼭 복잡하고 어려운 모델을 사용할 필요가 없다는 것이다.

V. 결 론

본 논문은 카드 단말기에서 발생하는 진동 신호를 이용한 부채널 공격 시나리오를 새롭게 구성해보고 이를 실험을 통해 검증해보았다. 그 결과 통계적 신호처리와 패턴 인식 분류 알고리즘을 이용하여 카드 결제 단말기의 입력 정보를 유추를 성공하였다.

일반적으로 카드 결제 단말기 사용자가 결제 관련 정보를 위해 사용하는 버튼은 12개이며, 신용 카드 번호는 16개의 숫자로 이루어져 있다. 이러한 사실에 기초하여 단말기에서 수집한 진동 신호로부터 특징을 추출하고, Naïve Bayes, 뉴럴 네트워크, 로지스틱 회귀 알고리즘에 적용해 보았다. 그 결과 최대 73.87%의 정확도로 입력된 카드 번호를 유추할 수 있음을 확인할 수 있었다. 이는 무작위로 입력 정보를 유추해서 정확한 정보를 얻을 확률이 라는 것을 생각했을 때 매우 주목할 만한 결과라고 할 수 있다. 이러한 공격이 실제로 일어난다면 중요 금융 정보로 악용될 소지가 있으므로 이에 대한 보안책이 강구되어야 할 것이다.

References

[1] P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," Advances in Cryptology-CRYPTO'96, LNCS 1109, pp. 104-113, 1996

[2] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," Advances in Cryptology-CRYPTO'99, pp. 388-397, Jan 1999.

[3] P. Marquardt, A. Verma, H. Carter, and P. Traynor, "iPhone: decoding vibrations from nearby keyboards using mobile phone accelerometers," Proceedings of the 18th ACM conference on Computer and communications security, pp. 551-562, Oct. 2011

[4] [saturday FOCUS] NSA has collected wiretap records using vibration on window, MK News, Nov. 1st 2013, http://news.mk.co.kr/newsRead.php?year=2013&no=1070547

[5] M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, and C. Sporleder, "Acoustic side-channel attacks on printers.", USENIX Security Symposium, pp. 307-322, 2010

[6] Chang-Kyun Kim and Il-Hwan Park, "Investigation of Side Channel Analysis Attacks on Financial IC Cards," Journal of the Korea Institute of Information Security and Cryptology, 18(1), pp. 31-39. Feb. 2008

[7] T.S Messerges, E.A Dabbish and R.H. Sloan, "Examining smart-card security under the threat of power analysis attacks," IEEE Transactions on Computers, vol. 51, no. 5, pp. 541-552. May. 2002

[8] E. Oswald, S. Mangard, C. Herbst, and S. Tillich, "Practical second-order DPA attacks for masked smart card implementations of block ciphers," Proceedings of the 2006 The Cryptographers' Track at the RSA Conference on Topics in Cryptology, LNCS 3860, pp. 192-207, 2006.

[9] J.R. Rao, P. Rohatgi, H. Scherzer and S. Tinguely, "Partitioning attacks: or how to rapidly clone some GSM cards," Proceeding of the 2002 IEEE Symposium on Security and Privacy, pp.31-41, 2002

[10] Pedersen, A. Hedegaard and Anders "Security in POS systems," DK-2800,

Technical University of Denmark, 2005
〔11〕 Y.C. ZHOU, Q.Y. CAO, L. GAN, S. FU, and L. GAO, "Embedded POS System Based on Security Module," Information Security and Communications Privacy, 11, 034. 2008
〔12〕 A manual of sensor, http://www.e2box.co.kr/category/기술정보%20및%20자료/EB Motion

〈저 자 소 개〉

장 수 희 (Soohee Jang) 학생회원
2012년 8월: 가톨릭대학교 경제학과 졸업
2013년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 신호처리, 하드웨어, 모바일 보안, 금융보안

하 영 목 (Youngmok Ha) 학생회원
2012년 2월: 고려대학교 정보통신대학 졸업
2014년 8월: 고려대학교 정보보호대학원 석사 졸업
2014년 9월~현재: 한국전자통신연구원 재직
〈관심분야〉 통계신호처리, 전파통신, 임베디드, 차세대 OS

윤 지 원 (Jiwon Yoon) 정회원
2008년 11월: University of Cambridge 전자공학과 박사 졸업
2008년 2월~2009년 5월: University of Oxford 로봇연구소 박사후과정
2009년 5월~2011년 5월: University of Dublin 통계학과 연구원 및 강사
2011년 7월~2012년 8월: IBM 연구소 정규 연구원
2012년 9월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 신호정보처리, 응용통계, 빅데이터 분석 기술, 도감청 탐지기술