신용카드의 안전성 향상을 위한 구조 및 거래절차 개선방법*

이 영 교** · 안 정 희***

A Reform Measure of the Structure and Transaction Process for the Safety Improvement of a Credit Card

Lee, Young Gyo · Ahn, Jeong Hee

〈Abstract〉

Credit cards are more convenient than cash of heavy. Therefore, credit cards are used widely in on_line (internet) and off_line in nowadays. To use credit cards on internet is commonly secure because client identification based security card and authentication certificate. However, to use in off_line as like shop, store, department, restaurant is unsecure because of irregular accident. As client identification is not used in off_line use of credit cards, the irregular use of counterfeit, stolen and lost card have been increasing in number recently. Therefore, client identification is urgently necessary for secure card using in off_line. And the method of client identification must be simple, don't take long time, convenient for client, card affiliate and card company. In this paper, we study a reform measure of the structure and transaction process for the safety improvement of a credit cards. And we propose several authentication method of short-and long-term for client identification. In the proposal, the client authentication method by OTP application of smart-phone is efficient nowadays.

Key Words : Credit Card, Identification, Authentication, Certificate, OTP(One Time Password),

Ⅰ. 서론

신용카드는 1949년 시카고의 사업가인 프랭크 맥나라가 최초로 만듦으로써 사용되기 시작했다. 다량의 현금을 휴대하기 불편했던 사람들은 고액권 화폐 그리고 수표를 사용했으며 결국에는 신용카드를 사용하게 되었으며 현재에는 전세계적으로 광범위하게 사용되고 있는 결제수단이 되었다. 우리나라에는 1970년대에 신용카드가 도입되었으며 2009년 말 기준으로 개인들이 1년동안 신용카드를 사용한 횟수는 45억여건이고 거래금액으로는 334조원에 이른다. 이를 환산해보면 신용카드를 하루 평균 124만번 사용했으며 9,157억원의 금액을 지불했다. 신용카드 발급 건수는 1억 2백만장으로 2004년 카드대란이 발생하기 전의 최고점이던 2002년말 수준을 회복하였다. 경제활동인구가 대략 2,400만명인 것을 감안하면 평균 1

* 본 논문은 2010년 서일대학 학술 연구비에 의해 연구되었음.
** 서일대학교 인터넷정보과 조교수 (교신저자)
*** 두원공과대학교 스마트폰컨텐츠과 부교수

인당 4.2장의 신용카드를 가지고 있는 셈이다[1]. 그러나 이렇게 많이 사용하는 신용카드가 보안상으로는 아주 취약하다. 신용카드는 마그네틱 부분에 저장되어 있는 정보들만 교체하면 타인의 신용카드가 되어 버리는 치명적인 단점을 가지고 있다. 여러 가지 사유로 폐기된 비정상 고객의 신용카드를 사들여 마그네틱 부분을 떼어내고 정상적인 사용자의 정보가 저장된 마그네틱을 붙여 이를 백화점 등에서 사용하는 불법 사용자들이 늘어나고 있다. 특히 신용카드 위조는 외국여행 후에 빈번히 일어나고 있다. 이에 따라 오프라인에서 단순한 절차에 의해 이루어지는 신용카드의 거래방법 및 구조를 개선하여 보다 안전한 거래가 이루어지도록 해야 할 필요성이 대두되고 있다.

따라서 본 연구에서는 그동안 정보보호에 대한 대책이 미비한 오프라인 거래상의 신용카드를 중심으로 안전성을 향상할 수 있도록 신용카드 및 결제단말기의 구조와 거래 절차 등에 대하여 분석하고 이를 바탕으로 최근 관심을 받고 있는 모바일 OTP를 이용한 대안을 제시하고자 한다. 모바일 OTP는 기존의 하드웨어 형태의 OTP (One Time Password)를 스마트폰 등의 모바일 기기에 어플리케이션으로 탑재한 것이다. 논문의 나머지 부분은 다음과 같이 구성되어진다. 2장에서는 관련연구로 신용카드, 결제단말기의 구조 및 사고를 살펴본다. 3장에서는 현재 우리가 사용하고 있는 오프라인 신용카드 결제방법의 보안방법들을 분석하여 문제점을 도출한다. 그리고 4장에서 모바일 OTP를 이용한 해결책을 제안하고 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련연구

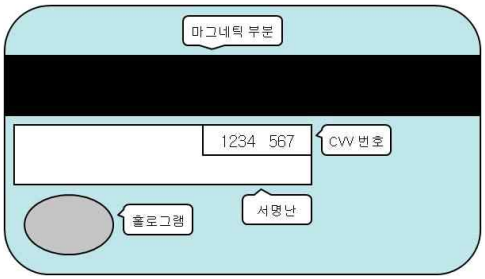
본 장에서는 관련연구로서 먼저 신용카드와 결제단말기를 살펴보고 오프라인에서 신용카드의 사고 발생 유형을 연구하고자 한다.

2.1 신용카드의 구조

우리가 일반적으로 사용하고 있는 마그네틱 카드는 <그림 1>과 같이 공통적으로 앞면에 신용카드번호, 영문 이름, 카드 유효기간이 양각되어 있다. 신용카드번호는 카드 앞면 중간부분에 위치하며 4자리씩 총 16자리의 숫자조합으로 이루어지나 아메리칸 익스프레스(아멕스)카드는 15자리, 다이너스카드는 14자리로 되어 있다.

<그림 1> 신용카드의 앞면 구조

이 중 앞 6자리 숫자를 BIN(Bank Identification Number)이라 하며 카드발급기관을 식별하는데 사용된다. BIN은 카드종류, 국가코드, 발급사의 코드로 조합되어 있어 카드 발급 회사명, 일반・골드・플래티늄 카드의 여부를 확인할 수 있다. 신용카드의 첫 시작번호는 3, 4, 5, 6, 9로 시작되는데 앞 두 자리가 36으로 시작되는 카드는 다이너스카드이며, 37로 시작되는 카드는 아멕스카드이다. 비자에서 발급되는 카드는 4로 시작하며 5는 마스터카드, 6은 중국 은련카드의 시작번호이다. 9는 국내에서만 이용되는 카드의 시작 번호이다. 총 16개의 숫자중에 BIN번호 다음 7번째 숫자부터 15번째 숫자까지는 카드사에서 각 회원에게 부여한 카드발급 일련번호이며, 마지막 자리는 체크번호로 카드 번호의 위조 및 오류를 방지하기 위한 검증번호이다. 카드 유효기간은 총 4자리의 숫자로 표시되는데 앞의 2자리는 월을, 뒤의 2자리는 년도를 표시한다. 그리고 사용자의 영문 이름이 표시되어 있다.



<그림 2> 신용카드의 뒷면 구조

신용카드의 뒷면을 보면 <그림 2>와 같이 검은색의 마그네틱선이 있는데 플라스틱 플레트 위에 1.3㎝의 마그네틱 선을 입힌 것으로 카드 윗면에서 0.5㎝ 아래에 위치한다. 마그네틱 선 안에는 카드번호, 유효기간, 회원정보, 그리고 개별 고객관리를 위한 카드사의 관리정보가 기록된다. 마그네틱 선은 3개의 트랙으로 구분돼 있는데 각 트랙에는 규정된 용량이 있으며, 트랙별로 사용되는 용도가 다르다. 첫 번째 트랙의 용량은 76바이트로 백화점 전용으로 사용된다. 다시 말해 일반 신용카드 업무와 상관없이 개별 백화점 등에서 발급하는 카드를 읽는 데 사용되는 트랙이다. 두 번째 트랙은 카드 결제, 현금서비스 이용 등 신용카드를 이용되며 3개 트랙 중 용량이 가장 적은 37바이트다. 직불카드 역시 신용카드이기 때문에 이 트랙에서 읽게 된다. 마지막 세 번째 트랙은 은행계좌와 관련된 업무를 이용하는 데 사용된다. 이 트랙의 용량은 가장 큰 107바이트다. 통장의 현금 입출금 카드로 겸용해 사용하는 신용카드는 두 번째와 세 번째 트랙을 사용한다. 최근에는 은행에서 직불카드 겸용으로 발급하고 있지만, 과거에 발급된 현금인출카드는 세 번째 트랙만을 사용했다. 지금도 종합금융사, 저축은행, 증권사 등에서 발급하고 있는 현금인출카드, 대출전용카드는 모두 세 번째 트랙만 이용하고 있다. 과거에는 마그네틱 선 안에 기본적인 정보와 함께 비밀번호를 그대로 기록하기도 했지만 보안상의 문제로 현재 발급되는 카드에는 마그네틱 선 안에 비밀번호가 기록되지 않는다.

마그네틱 부분의 아래에 위치한 서명난을 보면 작은 번호가 보인다. 이 숫자는 대개 카드번호 16자리 또는 카드번호 마지막 4자리와 3자리의 숫자의 조합으로 이루어져 있는데 이 끝의 3자리 숫자를 CVV(Card Verification Value) 또는 CVC(Card Verification Code)라고 한다. 인터넷 홈쇼핑 등 온라인 결제에서 상품구매 시 카드없이 카드번호만 가지고 이루어질 수 있는 부정사용을 막기 위해서 사용자가 신용카드를 소지하고 있다는 것을 확인하는 보조수단으로 활용되기도 하였으나 인증서를 통한 결제가 이루어짐에 따라 카드사의 전화상담원이 본인 확인을 위해 물어보는 정도로 이제는 거의 사용되지 않는다. 한 개의 카드에는 2개의 CVV 값이 있는데 서명난에 CVV2가 있고 다른 CVV는 마크네틱선 안에 기록돼 있으며, 카드의 위·변조를 방지하는 역할을 한다. 물론 위조방지용 홀로그램도 서명난의 하단에 위치한다.

카드 표면에 양각되는 카드 번호, 사용자의 영문 이름, 유효기간은 온라인 거래시에 사용되어야 함으로 숨길 수가 없다. 그러나 양각되는 이러한 정보는 한편으로는 공격자에게 카드정보를 제공하게 된다.

- 카드번호 : 백화점 카드, 현금 카드, 신용카드인지의 여부 및 무슨 카드인지 등의 정보를 알려주게 된다.
- 영문이름 : 카드에는 실명이 사용되기 때문에 이를 이용하여 해킹된 다른 정보에서 동일인의 정보를 획득하여 피싱 등에 악용할 수 있다. 카드번호로 고객들을 구분하기 때문에 영문이름은 사실상 표시할 필요가 없다.
- 유효기간 : 카드 분실시에 악의적인 카드 습득자가 사용가능 여부를 판단하도록 한다. 유효기간이 종료되기 전에 카드사에서 이를 통보하고 새로운 카드를 발급해주므로 사실상 사용자가 몰라도 되는 불필요한 정보이다.
- 마그네틱부분 : 불법 사용자가 이를 제거하고 다른 사용자의 정보가 입력된 마그네틱 선을 만들어 붙여 카드를 사용할 수 있다. 따라서 마그네틱 부분을 손상하지 못하도록 하는 기술적인 방법의 도입이 필요하다.

- CVV 번호 : 현재는 거의 사용하지 않는 번호이다.
- 홀로그램 : 불법적으로 제작되거나 복제된 카드인지 여부를 판단하는 데에 사용되지만 이를 확인하는 경우는 거의 발생하지 않는다. 카드 자체를 복제하기보다는 마그네틱 부분만 복사하기 때문이다.

따라서 근본적으로는 온라인과 오프라인에 사용하는 신용카드의 구조가 달라야 한다. 온라인에서 사용되는 신용카드는 유형적인 카드가 없어도 3가지 정보(카드번호, 영문이름, 유효기간)만 있으면 결제가 가능하다. 물론 본인 여부를 확인하기 위하여 공인인증서가 사용되어진다. 오프라인 결제시에는 일일이 3가지 정보를 입력하는 번거로움과 시간을 줄이기 위하여 이 정보들이 담겨있는 카드의 마그네틱 부분을 접촉시켜 결제 단말기에서 읽어들이게 된다. 따라서 오프라인에서 사용하는 신용카드는 이들 정보를 카드 표면에 양각시킬 필요가 없지만 한편으로는 여러 사람의 카드가 섞여 있을 경우 양각된 이름으로 본인 카드를 찾아낼 수 있기도 하다.

<표 1> 신용카드의 분류

종 류	마그네틱형	IC형
양각표시	카드번호, 영문이름, 유효기간	카드번호, 영문이름, 유효기간
기타표시	마그네틱 띠	마그네틱 띠 + IC 칩
결제단말기	IC형 결제단말기를 제외한 모든 단말기	IC형 결제단말기
온라인 노출가능성	높음	낮음
오프라인 노출가능성	높음	높음
장·단점	보안성 요구	결제단말기 확충

이들 정보가 도용되어 불법 카드 사용이 이루어지는 것을 막기 위하여 IC형태의 신용카드가 나와 있다. 이 카드는 이들 정보들이 암호화되어 저장되어 공격자들이 불법적으로 읽어 낼 수 없으며 정식 IC카드결제 단말기에서만 이들 정보를 읽어낼 수 있다. 그러기 위해서는 IC카드결제 단말기의 보급이 이루어져야 하는데 그렇지 못하고 있다. 지난해 말 현재 전국의 신용카드 가맹점은 177만여 곳인데 이들 단말기를 IC단말기로 전환하기는 시간적으로나 경제적으로 어렵기 때문이다. 따라서 현재 IC카드에는 IC칩과 마그네틱 띠가 공존하고 있어 사실상 IC카드의 역할은 하고 있지 못하다. <표 1>은 마그네틱형 및 IC형 신용카드를 비교한 것이다.

2.2 결제단말기

'신용카드 결제단말기'란 신용카드를 소지한 사용자가 신용카드 가맹점에서 결제할 시에 사용자의 고객정보를 해당 카드사에 전송하는 단말기를 지칭하며 '신용카드 조회기'라고도 한다. 일반적으로 신용카드 단말기는 고객의 카드 정보를 전화선이나 인터넷을 통하여 해당 카드사의 호스트 서버에 전달하고 서버는 DB에서 해당 고객의 신용카드의 상태정보 즉, 승인정보를 검색하여 돌려주게 된다. 승인정보가 '한도초과'나 '지불정지' 등이면 더 이상 해당 카드는 사용할 수 없으며 '사용가능'인 경우에만 가맹점에서 입력하는 금액이 '신용카드매출전표'에 찍혀 나오게 된다. 단말기를 판매, 설치해주는 밴(VAN : Value Aided Network) 사업자는 한국신용카드결제(주)-KOCES, 한국정보통신(주), 나이스정보통신, 한국부가통신, 금융결제원-bankpos 등 10여개에 이르고 있다.

단말기는 <표 2>와 같이 일반형, POS형, 무선형 그리고 IC형 등으로 나누며 일반형은 초창기 모델로서 조그만 형태로 전화선으로 승인정보를 받으며 매출전표만을 출력한다. 일반형의 단점을 개선하기 위해 나온 것이 POS 단말기로써 판매시점관리(POS : Point of Sale) 단말기를 지칭하며 개인용 컴퓨터(PC)에 카드 결제 장치를 달아 판매 시점의 상품명이나 가격 등의 데이터를 저장하는 단말기이다. 이 중에는 고객의 카드정보를 함께 저장하는 단말기가 많다. 종합적인 매출관리를 해야 하는 대형 마트는 물론 소형 가맹점에서도 많이 사용하고 있

다. 특히 승인정보를 인터넷으로 주고받기 때문에 신속한 카드결제를 하도록 해준다.

<표 2> 신용카드 결제단말기의 분류

종 류	기 능	장·단점
일반형	승인확인, 전표출력	단순 기능
POS	그 외 매출관리	고객카드정보 저장
무선형	이동성	무선경로의 해킹 가능성
IC형	IC형 카드를 읽을 수 있는 복호화 기능	고객정보의 노출 방지
스마트폰형	스마트폰에 앱과 하드웨어 장착	이동 편리, 간단한 장비

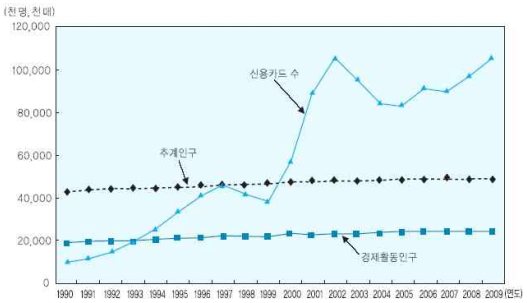
무선형 단말기는 대형 매장, 주유소나 프랜차이즈와 같이 넓은 매장이거나 고객이 자리에서 결제를 하도록 해주는 가맹점에서 편리한 단말기이다. 편리하지만 무선구간에서의 정보보안이 문제가 되고 있다. IC형 단말기는 고객의 카드정보를 아무나 읽을 수 없도록 내장된 메모리칩에 저장된 암호화된 카드정보를 복호화하여 읽을 수 있도록 개발된 장비이다. 개발은 되었으나 보급이 제대로 되고 있지 않다. 그 외에 스마트폰에 어플리케이션과 간단한 장비를 추가하여 사용할 수 있는 단말기도 나와 있다.

문제가 되는 것은 POS 단말기이다. POS 단말기는 2009 년말 기준으로 전국적으로 26만 여대가 보급되어 있으며 전체 카드 대비 결제비율은 30%에 이르고 있다. POS 단말기는 고객의 카드 정보를 저장하고 있기 때문에 해킹으로 인해 정보가 유출, 불법카드가 제작되어 사용되는 사고가 빈번히 발생하고 있다. 고객이 신용카드를 결제할 때 카드번호, 유효기간 등의 카드정보가 자동으로 저장되며 이렇게 남겨진 카드 정보를 시중에서 쉽게 구할 수 있는 카드발급기에 입력하면 복제카드를 만들 수 있다. 카드정보의 용량은 숫자 20~40개에 불과해 단말기 내에 거의 무한정, 무기한 저장할 수 있다. 정부당국은 이런 사실을 알고도 감독 법규를 만들지 않은 채 방치하고 있다. 체인점의 경우 점포마다 POS 단말기가 전산망으로 이어져 있어 이를 해킹하면 대량 복제 사고가 이어질 수 있다. 특히 2010년 4월에는 루마니아의 해커의 대형마트, 주유소 등의 POS 단말기에서 9만 5000여건의 고객 정보를 인터넷을 통해 빼내 국내외에 유통하여 위조카드 제조 등에 악용한 사고가 발생하기도 했다.

가맹점의 POS 단말기에 저장된 고객의 개인정보 유출로 인한 신용카드 복제 등의 2차 피해가 발생함에 따라 뒤늦게 금융감독원과 여신금융협회는 'POS 보안 강화 방안'을 시행하여 2011년 7월부터 보안모듈이 설치되지 않은 POS 단말기의 카드 거래에 대해 카드사가 승인을 거절하도록 하고 있다.

2.3 사고 사례

여행객들이 신용카드를 해외에서 사용하는 과정에서 위·변조 등의 사고발생이 급증한 것으로 나타났다. 2010년 9월 17일, 금융감독원에 따르면 2010년 상반기에 해외에서 발생한 국내 신용카드 사고는 모두 6천150건으로 2009년 전체 해외 사고규모(5천686건)를 넘어섰다. 사고 유형별로는 카드 위·변조가 4천662건으로 가장 많았고 도난이나 분실(535건), 카드정보 도용(495건) 순이었다. 카드 위·변조는 지난 2007년 2천485건, 2008년 3천828건에서 2009년 3천165건으로 다소 줄었지만 올들어 증가세로 돌아섰다. 카드정보 도용은 지난 2007년 439건에서 2008년 532건, 2009년 866건 등으로 꾸준하게 늘어나는 추세다. 금액기준으로는 2010년 상반기에 모두 49억4천600만원의 피해가 발생한 것으로 집계됐다. 해외에서 발생한 신용카드 피해액수는 지난 2007년 54억5천400만원에서 2008년 65억5천100만원, 2009년 73억8천300만원 등으로 늘고 있다. 2010년 상반기의 경우 카드 위·변조로 인한 피해가 41억4천400만원으로 가장 많았고, 도난이나 분실로 인한 피해가 4억2천400만원, 카드정보 도용으로 인한 피해가 1억3천800만원이었다[2].



<그림 3> 최근의 인구 및 신용카드 발급 수

이러한 불법 거래는 카드 표면에 양각되어 있는 카드번호와 출력되는 카드 매출전표상의 카드번호를 비교하면 간단히 알아낼 수 있지만 바쁜 거래에서 이 작은 번호를 확인하기는 쉽지 않다. 특히 외국여행 후에 현지에서 사용한 신용카드가 이러한 방법으로 흔히 불법 사용되는데 이는 거래내역을 확인하는 데에 국내 사용의 경우보다 시간이 더 걸리므로 이를 악용한 사례이다. 신용카드를 이용한 온라인 거래는 공인인증서가 본인 인증의 수단으로 사용되기 때문에 인증서 비밀번호와 보안카드가 노출되지 않는 한 안전성을 확보할 수 있다. 그러나 신용카드를 이용한 오프라인 거래에는 본인을 확인할 대안이 없으며 이러한 불법사용을 막는 연구는 국내외적으로 잘 이루어지지 않고 있는 실정이다.

Ⅲ. 문제점 도출

본장에서는 이를 해결하기 위해 기제안되어 있는 방법들을 소개하고 문제점을 도출하고자 한다.

3.1 근본적인 방법

신용카드의 안전한 사용을 위한 다양한 방법들이 타원곡선이나 공개키 등을 이용하여 제안되었다[3-6]. 특히 최근에는 사용자의 신용카드 정보를 암호화하여 처리하여 유출되지 않도록 해주는 IC 신용카드도 나왔다. 시간과 비용을 투입하여 전국의 모든 가맹점의 단말기를 IC형 단말기로 교체하고 IC 카드도 마그네틱띠가 없는 것으로 대체한다면 신용카드 불법사용을 근절할 수 있다. 그러나 이 방법은 일단 IC 카드 발급 및 IC 단말기 설치에 많은 예산 및 시간이 소요되며 실시된다고 하더라도 결코 근본적인 해결 방법은 되지 않는다. 이들 카드정보들은 결코 패스워드 역할은 하는 것이 아니라 고객을 구분하는 아이디 역할은 하는 정보이기 때문이다. 온라인상의 카드 거래에서는 공인인증서가 본인 확인을 충분히 제공해주기 때문에 불법 사용이 이루어지지 않는다. 반면 오프라인에서는 결제시의 번거로움 및 이로 인한 가맹점의 매출 감소의 우려로 인하여 본인 확인을 제대로 하지 않고 있기 때문이다. 마그네틱 카드라 하더라도 본인확인 방법만 확실하게 구축한다면 충분히 불법 사용을 근절시킬 수 있다. 물론 가맹점에서의 본인확인 방법은 번거롭거나 시간이 많이 소요되지 않는 편리한 방법으로 도입되어야 한다.

3.2 결제후 혹은 결제중의 방법

1) 결제후 SMS 문자통보

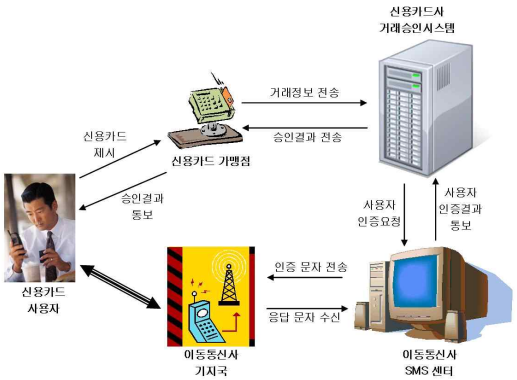
몇 년 전부터 카드사들이 고객이 카드 결제시에 그 결과를 고객의 휴대폰에 SMS(Short Messaging Service) 문자로 보내주는 서비스를 제공하고 있다. 이 서비스는 작은 절차 및 비용으로 큰 효과를 내고 있는 해결 방법으로 판단된다. 고객이 신용카드를 분실했거나 혹은 카드정보를 도용당했더라도 악의적인 사용자의 불법 카드 사용시에 바로 그 결과를 통보받을 수 있기 때문이다. 또한 고객이 신용카드와 휴대폰을 동시에 분실할 가능성이 매우 낮기 때문에 효과적인 방법이라 할 수 있다. 그러나 이 방법은 일부 카드사들이 이 서비스를 유료로 전환하면서 그 효용성이 다소 실종된 상태에 있으며 사후 통보여서 신속한 카드 정지 등의 조치가 이루어져야 더큰 손실을 막을 수 있다.

2) 결제중 비밀번호 요구방법

결제 중에 카드 비밀번호를 입력하도록 요청하는 결제 방법이다. 가맹점에서 직원은 카드 결제시에 고객의 카드 비밀번호를 물어보게 되며 고객이 해당 카드의 비밀번호를 알려주면 입력하는 방법이다. 비밀번호는 본인만이 알고 있어야 하는데도 불구하고 가맹점 직원에게 알려주어야 한다는 것이 이 방법의 첫번째 단점이다. 두번째 단점은 고객이 비밀번호를 기억하지 못하면 결제가 불가능하게 된다는 것이다. 고객입장에서는 신용카드를 발급할 시에 분명히 비밀번호를 신청서에 기입하였지만 한 두장도 아닌 신용카드들의 비밀번호를 일일이 기억하기가 쉽지 않다. 가맹점 입장에서는 그로 인하여 매출이 줄어들게 된다. 이러한 이유들로 인하여 이 방법은 점차 사용되지 않게 되었다. 그나마 기차표 예매창구에서는 아직도 이 방법을 사용하고 있으며 고객의 카드 비밀번호가 노출되는 것을 방지하기 위하여 직원에게 알려주지 않고 창구앞에 위치한 비밀번호 입력패드에 고객이 직접 입력하도록 되어 있다.

3) 결제중 휴대폰을 통한 비밀번호 요청방법

결제 결과를 보내주는 문자 서비스대신 결제중에 사용자에게 양방향 문자 서비스인 MMS(Multimedia Messaging Service) 문자를 보내어 응답에 카드의 비밀번호를 보내도록 요구함으로써 본인인증을 하는 방법이 <그림 4>와 같이 [7]에서 제안되었다. MMS를 이용한 방법은 비밀번호를 직원에게 노출하지 않아도 된다는 장점이 있으며 휴대폰은 우리가 항상 휴대하는 기기이므로 적용하기가 적합한 방법이다. 그러나 고객이 여러 장의 신용카드 비밀번호를 기억하고 있어야 하고 비밀번호가 일치하지 않을 시에 결제가 이루어지지 않게 되는 단점이 있다. 또한 악의적인 공격자에 의해 휴대폰에서 혹은 무선 단계에서 해킹을 당해 비밀번호가 노출될 수 있다. MMS를 이용한 방법이 보다 효력을 가지기 위해서는 동일한 카드 비밀번호 대신 보안카드나 OTP같은 번호를 입력하도록 하여야 한다. 그러나 그럴 경우 사용자는 오프라인 거래를 위해 보안카드나 OTP를 반드시 휴대해야 하는 불편함과 결제시에 번거로움으로 인하여 시간이 더 소용되며 가맹점의 매출에 영향을 줄 수 있게 된다.



<그림 4> 기제안한 MMS를 이용한 결제 개념도

3.3 기존 방법들의 비교

마그네틱형 신용카드로 결제중에 MMS로 동일한 비밀번호를 요구하는 방법을 "결제중 MMS-1 (3)"로 명명하고 비밀번호로 보안카드나 OTP를 요구하는 방법을 "결제중 MMS-2 (4)"로 명명하여 IC카드 및 단말기를 사용하는 방법 (1) 그리고 마그네틱 신용카드를 그대로 사용하며 추후 SMS로 결과를 통보하는 방법 (2)을 비교하면 아래의 표와 같다.

(1)의 방법은 이상적인 방법이지만 이를 위한 인프라 구축에 상당한 비용과 시간이 요구되어진다. 따라서 현실적으로는 적합하지 않은 방법이다. (2)는 간단한 방법이지만 사후 통보에 그치고 있어 원천적인 방지책으로는 부족하다. (3)은 고객이 카드마다 상이한 여러 개의 비밀번호를 기억하고 있어야 하는 불편함이 있고 악의적인공격자에 의해 카드정보 및 비밀번호가 유출되면 지속적으로 불법적인 카드 사용이 이루어질 수 있다. (4)는 고객이 추가적으로 보안카드나 OTP를 휴대해야 하는 불편함

<표 3> 신용카드 보안 방법들의 비교

방법 / 평가유형	(1) IC카드 및 단말기	(2) 결제후 SMS	(3) 결제중 MMS-1	(4) 결제중 MMS-2
소요 비용	아주 높음	아주 낮음	낮음	낮음
변경사항(카드사)	카드 발급, 프로토콜 적용	-	프로토콜 수정	프로토콜 수정
변경사항(가맹점)	IC 단말기 구입	-	프로토콜 수정	프로토콜 수정
변경사항 (사용자)	IC 카드	-	n개의 비밀번호 기억	n개의 보안카드나 OTP 소지
휴대폰번호 등록	-	○	○	○
보안성	높음	사후 통보	과정중 확인	과정중 확인
보안성(비밀번호)	-	-	동일	변화
가맹점의 편리성 (사용자관리 및 통계)	×	○	○	○
가맹점의 매출	-	-	낮음	아주 낮음
결제시 신속성	높음	높음	중간	낮음
사용자 인증성	중간	-	중간	높음

* 신용카드가 n개인 경우

이 있으며 카드마다 보안카드나 OTP가 지급된다면 이들을 모두 휴대하는 것은 더욱 불편한 일이 될 것이다.

따라서 오프라인 신용카드의 안전성을 확보하며 원활한 결제가 이루어지도록 하기 위해서 필요한 요건을 정리해 보면 다음과 같다.

- 인프라 구축을 위해 많은 투자비용 및 시간이 걸려서는 안된다. (전체적으로)
- 고객이 많은 것을 기억하도록 해서는 안된다.
- 고객이 휴대해야 하는 것이 늘어나서는 안된다.
- 신용카드사에서의 비용부담이 늘어서는 안된다. (새로운 신용카드 발급 등)
- 가맹점의 시설투자가 발생해서는 안된다. (단말기 교체 등)
- 가맹점의 매출액이 줄어서는 안된다. (복잡한 결제과정으로)
- 온라인 신용카드 사용시처럼 철저한 본인 인증이 이루어져야 한다.
- 해킹 등으로 고객의 비밀번호 등이 노출되어서는 안된다.

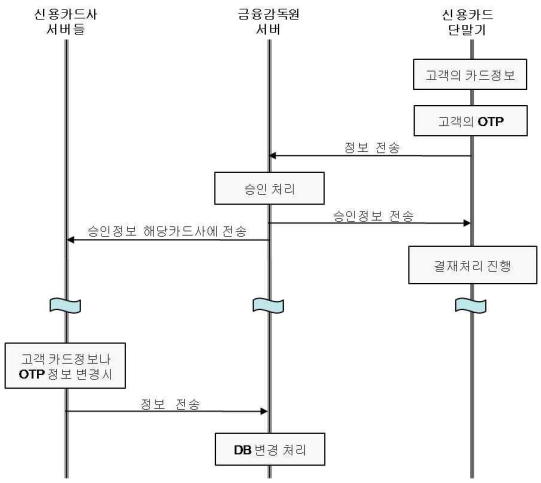
Ⅳ. 해결방안 제안

앞에서 기 제안된 방법들은 장·단기 해결 방법으로 신용카드의 불법 사용을 어느 정도 막을 수 있으며 방법들에 따라 장·단점을 가지고 있다. 최근에는 휴대폰으로 스마트폰이 급격히 보급되고 있다. 본 논문에서는 스마트폰에 어플리케이션을 탑재하여 본인인증을 하는 방법을 제안하고자 한다.

4.1 스마트폰을 이용한 본인인증

온라인 은행거래에서는 인증서와 함께 보안카드가 사용되고 있다. 보안카드는 4자리 숫자가 적힌 카드로써 거래 절차시에 요구되는 순서의 번호를 입력하도록 되어 있다. 고액(천만원 이상) 거래시에는 보안카드보다 더 강력한 OTP를 사용하고 있다. 물론 OTP는 인터넷뱅킹에 가입할 경우나 분실시에 오프라인 은행창구에서 받게 된다. OTP는 작아서 손안에 들어가는 크기이지만 고객이 항상 백화점이나 쇼핑센터 그리고 음식점 등에 OTP를 가지고 다니기는 불편하고 번거로운 일이다. 그러나 휴

대폰은 반드시 가지고 다니게 된다. 따라서 신용카드 발급시에 하드웨어 형태의 OTP대신 소프트웨어형태의 OTP 어플리케이션을 고객의 스마트폰에 다운로드시켜 카드 결제시에 본인인증으로 사용하자는 것이다.



<그림 5> OTP를 이용한 카드결제 처리도

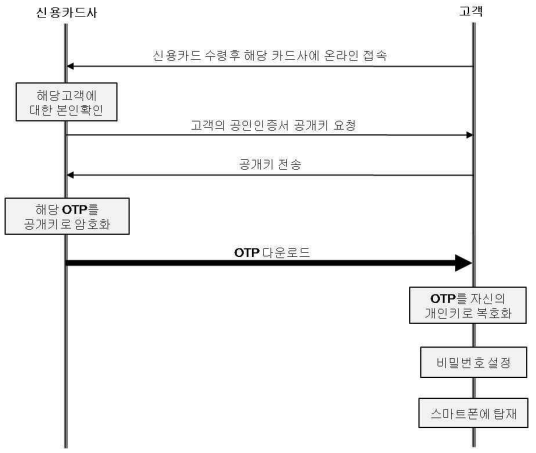
카드결제시 고객은 신용카드를 꺼내어 직원으로 하여금 신용카드 결제단말기에 긋도록 한다. 스마트폰을 꺼내어 해당하는 신용카드의 OTP를 실행시킨다. OTP 비밀번호를 넣어 하나의 OTP를 꺼내어 이를 가맹점 직원에게 불러준다. 결제시 카드의 비밀번호를 넣도록 하는 절차는 이미 개발되어 설치되어 있으나 열차표를 구매하는 등의 일부에서만 사용되고 그 외에서는 번거롭다는 이유로 사용하지 않고 있다. 따라서 본 논문에서 제안하는 방법을 기존의 결재절차에 이용하면 된다. 점원에게 불러주는 OTP는 10진수 6자리이어서 불러주기나 받아 입력하기에 어려움이 없으며 일회용이어서 재사용될 수 없으므로 직원에게 노출되어도 문제가 되지 않는다. 기제안된 방법들보다 더욱 편리하게 결제를 할 수 있다. 스마트폰에 OTP를 탑재하여 본인인증을 수행한다면 스마트폰이 휴대용 PC이므로 마찬가지로 보안카드와 공인인증서를 저장하여 결제시에 이용할 수 있을 것이다. 물론 이러한 경우 보안카드도 디지털화하여 저장 및 관리가 가능하다. 그러나 이러한 방법은 기존의 온라인 결제처럼 안전하지만 결제시에 절차상의 번거로움으로 적용이 쉽지 않다.

인터넷에서는 하나의 OTP로 모든 금융기관을 등록하여 사용하고 있다. 오프라인 신용카드 거래시에 신용카드사별로 별도의 OTP를 배포하여 사용하게 된다면 사용자는 이들 OTP를 관리하고 사용하기 위하여 번거로울 수밖에 없다. 따라서 인터넷 금융거래와 마찬가지로 하나의 OTP로 모든 신용카드 거래시에 사용할 수 있도록 하여야 한다. 이를 위해서는 금융감독원같은 정부기관의 서버에서 통합하여 승인과 본인 인증을 수행해야 한다. 승인은 각 카드사 서버가, 본인 인증은 금융감독원 서버가 수행한다면 별도의 처리로 인하여 카드결제시 시간이 지연되어 불편해질 수 있다. 이를 위해서는 <그림 5>와 같이 카드단말기, 카드사 서버, 금융감독원 서버간의 절차가 일부분 수정되어야 하며 그를 위한 인프라가 구축되어야 한다. 그렇게 되면 <그림 6>의 OTP 다운로드 절차는 한번만 수행하면 된다. 그 대신 추가적인 신용카드 발급시에는 등록하는 절차가 필요하게 된다. 또한 제안하는 OTP는 스마트폰에 앱 형태로 실행되므로 별도의 전원이 필요하지 않아 기존의 OTP에 비해 무한정 사용할 수 있다.

4.2 OTP 다운로드 및 운용

신용카드를 발급받은 고객은 카드수령후 해당 카드사의 홈페이지에 접속한다. 신용카드사는 접속한 고객에 대한 본인인증을 수행한다. 이때 본인인증은 공인인증서를 이용하여 수행하며 본인확인이 이루어지면 고객의 공개키를 요구한다. 고객의 공개키를 수신한 카드사는 해당 고객에 발급할 OTP를 생성하고 고객의 공캐키로 암호화하여 전송한다. 고객은 다운로드된 OTP를 자신의 개인키로 복호화하고 비밀키를 설정한다. 그리고 스마트폰에 OTP를 탑재시키고 사용할 수 있도록 준비한다. 이

렇게 함으로써 인터넷상에서도 OTP에 대한 안전한 다운로드가 이루어지게 된다. 상세한 다운로드 절차는 <그림 6>과 같다.



<그림 6> OTP 다운로드 절차 -초기셋업 과정

OTP 혹은 OTP 발생기(일회용 비밀번호 생성기)는 단 한번만 사용되는 일회용 패스워드를 생성하는 하드웨어 장치로 매번 거래할 때마다 비밀번호를 무작위로 생성하며 1분후에 다시 새로운 비밀번호를 생성한다. 따라서 생성된 비밀번호는 1분간 유효하다. 보안카드는 10진

수 4자리로 이루어진 35개의 번호를 앞뒤로 2개씩 나누어 온라인 금융거래시에 입력하도록 하게 되어 있어 유추가 가능하다. 또한 각 금융기관마다 다른 보안카드를 발급하여 사용하지만 OTP는 1개로 거의 모든 금융기관을 등록하여 사용할 수 있다. 공인인증서와 같이 사용할 경우 금융감독원의 금융보안 인증요소에 따른 보안등급 분류에서 1등급으로 인정받게 된다[8]. 이를 위해 OTP는 다음과 같은 보안요구사항을 만족해야 한다.

- 기밀성(Confidentiality) : 각 객체들 사이의 통신에서 노출되지 말아야할 비밀정보는 허용되지 않은 객체 및 불법적인 제3자에게 노출되지 말아야 한다. 즉, OTP값을 생성하기 전까지 통신되는 정보들은 암호화되어 노출되지 않아야 한다.
- 무결성(Integrity) : 각 객체들 사이의 통신되는 정보들은 변경, 삭제, 재생성되지 않아야 하며 올바른 값이 전달되어야 한다. 즉, OTP를 생성하기 위한 입력값은 불법적인 변조가 없어야 하며 동일한 입력값을통하여 동일한 OTP를 생성하여야 한다.
- 상호인증(Mutual Authentication) : 각 객체들 메커니즘내의 정보들을 이용할 수 있는 정당한 객체인지를 나타낼 수 있어야 하고 정당한 객체가 아님을 부인할 수도 없어야 한다. 즉, 모바일 OTP메커니즘 내에서 OTP를 생성하고 통신하는 객체들은 서로간에 정당한 사용자임이 인증되어야 한다[9].

OTP는 상호인증은 물론 [10]에서 언급한 익명인증의 요건도 만족하고 있다. 아울러 OTP 생성 단말기는 다음과 같은 요구사항을 만족해야 한다[9].

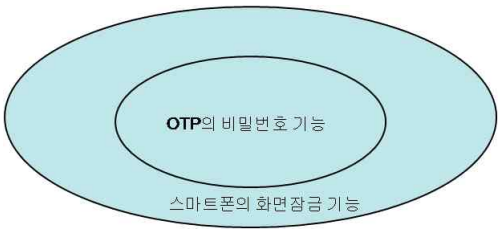
- 보안성(Security) : OTP 단말기에는 허가된 사용자만이 접근이 가능해야 한다.
- 독립성(Independence) : OTP 단말기는 2-Factor 인증을 위해 독립적인 인증매체의 역할을 해야 한다.
- 가용성(Availability) : OTP 단말기는 사용자가 이용하기에 불편함이 없어야 한다.

<표 4> 기존의 OTP 및 제안하는 모델과의 비교

방법 / 항목	제안하는 OTP	기존 OTP
형 태	SW	HW
휴 대	스마트폰에 내장	별도 휴대
실 행	아이콘 클릭	전원 버튼
보 안	비밀번호	-
교체시기	무한정	전원 고갈시
발급형태	온라인	오프라인
해킹 가능성	O	X
결재시간	증가	-

본 논문에서 제안하는 OTP는 기존의 OTP 발생기와는 다음과 같은 차이점 및 장·단점을 가지고 있다.

그동안 사용하던 외장형 하드웨어 OTP를 스마트폰에 탑재하였으므로 해킹의 가능성이 발생할 수 있다. 따라서 앞에서 제안한, 스마트폰에 탑재되는 OTP는 비밀번호를 입력하여야만 일회용 패스워드가 발생하도록 규정하였다. 그러나 추가적으로 스마트폰 자체의 "화면잠금 기능"을 적극 사용하는 것이 바람직하다. 또한 비밀번호 설정 시에도 7자리이상의 영문, 숫자, 특수기호를 혼합하여 사용하도록 하며 1개월마다 정기적으로 비밀번호를 변경하여 OTP의 안전성을 강화시켜야 한다.



<그림 7> OTP 앱의 보안 방법

그러나 한편으로는 이러한 보안조치가 결재시간을 늘이게 되는 단점이 되며 별도의 휴대 OTP와는 달리 해킹의 위험성이 상존하게 된다. 또한 하드웨어 OTP는 분실 시에 신고를 즉시 할 수 있으나 제안하는 OTP는 해킹이 되어 불법 사용자에 의해 사용 중이어도 본인이 이를 인식하지 못할 수도 있다는 단점이 있다.

V. 결론

최근 국회의 경제분야 대정부 질문에서는 카드사 간의 과열 경쟁으로 신용카드 발급과 저신용자의 카드사용이 급증하고 있어 제2의 카드 대란에 대한 우려가 커지고 있어 금융위원회는 신용카드 시장에 대한 감독강화 방안을 내놓기도 했다. 따라서 카드 발급이 늘어나는 만큼 카드 사용에 대한 불법 사고가 발생할 가능성도 커질 것으로 예상된다.

온라인에서 사용되는 신용카드는 공인인증서, 보안카드 혹은 OTP를 이용하여 본인인증을 수행하지만 오프라인에서 사용되는 신용카드는 별다른 본인 인증을 거치지 못하고 있어 불법 사고가 급증하고 있다. 따라서 본 논문에서 오프라인에서 신용카드의 안전한 사용을 위한 구조 및 거래절차에 대한 개선 방법을 장·단기적인 대책으로 나누어 모색하였다. 그리고 스마트폰이 활성화됨에 따라 고객들이 추가적인 장비를 휴대하지 않고 스마트폰으로 본인 인증을 수행하는 방법을 제안하였다.

그러나 한편으로는 제안한 방법이 현재 경제력이 있는 40~60대임에도 불구하고 PC나 스마트폰(앱스토어 및 앱) 등의 컴퓨터 장비 및 소프트웨어를 사용함에 있어 어려움을 겪는 사용자들에게는 불편함을 초래할 수 있고 나아가서는 가맹점의 매출에 영향을 줄 수 있다. 따라서 모든 카드 사용자에게 동시에 적용하기보다는 점차 확대하여 적용하는 것이 바람직할 것으로 사료된다. 본 논문에서 살펴본 대책과 방법은 그동안 연구가 잘 이루어지지 않았던 오프라인 신용카드 거래에서 불법사고를 줄이고 고객과 가맹점 그리고 카드사들을 만족시키는 방법을 제한적인 조건에서 제시했다고 판단한다.

참고문헌

[1] 여신금융협회, "신용카드 업계현황," 2010. 12, pp. 4.
[2] 여신금융협회, "계간 여신금융," 2010. 6, pp. 137.
[3] 장시웅, 신병철, 김광백, "컴퓨터 부착용 신용카드 조화기에 기반한 전자지불 승인시스템의 설계 및 구현," 한국정보처리학회논문지 D, 제 9권, 제 4호, 2002, pp. 723-732.
[4] 유성진, 김성열, 윤천균, 정일용, "타원곡선 암호를 이용한 PDA 기반의 신용카드 결제 프로토콜 설

계," 한국정보처리학회논문지 D, 제 10권, 제 6호, 2003, pp. 1033-1040.

[5] 장시웅, 신병철, 김양곡, "전자상거래 촉진을 위한 공유키 기반 신용카드 조회 시스템," 한국정보처리학회논문지 D, 제 10권, 제 6호, 2003, pp. 1059-1066.

[6] 김해만, 이임영, "안전하고 효율적인 신용카드 기반의 시스템에 관한 연구," 한국멀티미디어학회 춘계학술발표논문집, 제 2권, 제 1호, 1999, pp. 151-155.

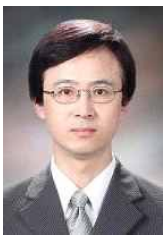
[7] 이영교, 안정희, "휴대폰을 이용한 신용카드의 결제방법," 한국컴퓨터정보학회 하계학술대회 논문집 제18권 제2호, 2010. 7, pp. 181-182.

[8] 윤승구, 박재표, "OTP를 이용한 인터넷뱅킹 시스템의 다중 채널 인증기법," 디지털산업정보학회논문지 제6권 제4호, 2010. 12, pp. 131-142.

[9] 김태형, 이준호, 이동훈, "피싱방지 및 가용성 개선을 위한 PKI기반의 모바일 OTP(One Time Password) 메커니즘에 관한 연구," 정보보호학회회논문집 제21권 제1호, 2011. 2, pp. 18-19.

[10] 이영교, 안정희, "공인인증서를 이용한 익명 인증방법," 디지털산업정보학회논문지 제6권 제1호, 2010. 3, pp. 116-129.

■ 저자소개 ■



이 영 교
Lee, Young Gyo

1986년 2월 한양대학교 전자공학과 (공학학사)
1991년 8월 한양대학교 전자공학과 (공학석사)
1993년 3월~1998년 9월
대우통신종합연구소 선임연구원
1999년 2월~2001년 6월
LG정보통신중앙연구소 선임연구원
2006년 8월 성균관대학교 컴퓨터공학부
(공학박사)
2008년 3월~현재
서일대학교 인터넷정보과 조교수

관심분야 : 정보보안, PKI, 암호이론
E-Mail : younggyo@seoil.ac.kr

안 정 희
Ahn, Jeong Hee

1988년 2월 성균관대학교 정보공학과
(공학학사)
1993년 2월 성균관대학교 대학원 정보공학과
(공학석사)
2000년 2월 성균관대학교 대학원 정보공학과
(공학박사)
1996년 3월~현재
두원공과대학교 스마트폰컨텐츠과
부교수

관심분야 : 정보통신 보안, 전자상거래 보안,
트래픽 제어
E-Mail : jhpro@doowon.ac.kr

논문접수일 : 2011년 7 월 12 일
수 정 일 : 2011년 8 월 17 일(1차), 8 월 22 일(2차)
게재확정일 : 2011년 8 월 25 일