JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 4 : 855~863 Apr. 2015

금융보안을 위한 물리적 보안 카드의 설계 및 구현

서화정 · 김호원*

Design and Implementation of Physical Secure Card for Financial Security

Hwa-jeong Seo · Ho-won Kim*

Department of Computer Engineering, Pusan National University, Pusan, Korea

요 약

본 논문에서는 전자금융 신종 사기 수법에 의한 사용자의 비밀정보 유출을 방지하기 위하여 자신이 가진 보안카드와 스마트 폰을 이용하여 금융거래 사이트를 검증하는 새로운 기법을 제안한다. 이를 위해 보안카드를 새롭게 디자인하여 공정한 사이트에 접속하는 경우에만 보안카드와 스마트폰을 통해 사이트의 인증이 가능하도록 하였다. 또한 기존의 OTP를 통한 보안 인증에서는 방어할 수 없었던 중간자 공격을 사용자의 거래 내역에 따른 보안카드 값 생성을 통해 효과적으로 방어하는 방안도 제안한다. 본 논문에서 제시하는 기법은 보안카드와 스마트폰을 통한 새로운 사이트 인증 기법으로써 사용자가 직접 피싱, 파밍 사이트를 판단할 수 있을 뿐 아니라 중간자 공격에 대한 대처방안으로도 매우 효과적인 기법이다.

ABSTRACT

In this paper, we present a novel method to verify the financial site and prevent sensitive information disclosure with financial security card and smart phone. This method allows homepage access when user accesses to the valid site with right security card and smart phone. Furthermore, traditional OTP method cannot be secure against to Man in the middle attack, but out method presents the countermeasure of this. User can readily recognize the phishing and pharming sites and even avoid Man in the middle attack by malicious users.

키워드 : 물리적 보안카드, 금융 보안, 설계 및 구현

Key word : Physical Security Card, Financial Security, Design and Implementation

Received 24 December 2014, **Revised** 22 January 2015, **Accepted** 11 February 2015

* **Corresponding Author** Ho-won Kim(E-mail: howonkim@pusan.ac.kr, Tel:+82-51-510-1010)
Department of Computer Engineering Pusan National University, Pusan, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2015.19.4.855 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

온라인을 통한 금융서비스의 제공은 사용자가 언제 어디서나 금융 서비스에 접근 가능하게 함으로써 오프라인 서비스의 문제점인 접근성과 가용성을 동시에 해결하는 솔루션이다. 서비스의 편리함으로 인해 2014년 3월말 인터넷 뱅킹 서비스 등록 고객 수는 9,775만 명으로 전분기말대비 2.4% 증가하였다[1]. 스마트폰 뱅킹 등록 고객 수(4,034만 명)는 빠른 증가세를 지속하여 서비스개시(2009년 12월)이후 최초로 4천만 명을 돌파했다. 2014년 1/4분기 중 인터넷 뱅킹 이용건수 및 금액(일평균 기준)은 6,369만 건, 36조 1,394억 원으로 전 분기 대비 각각 14.7, 3.9 % 증가했다. 스마트폰 뱅킹의 경우 이용건수 및 금액은 2,737만 건, 1조 6,276억 원으로 전 분기 대비 각각 14.5, 6.7 % 증가했다. 하지만 온라인 금융서비스의 확대는 금융사기에 대한 위험에 보다 쉽게 노출되게 되는 결과를 초래하게 되었다. 경찰대학 치안정책 연구소 “치안 전망 2014”에 따르면 2013년 1월에서 10월까지 스미싱, 파밍, 메신저 피싱 등 금융 보안사기는 연간 3만 1천건, 메모리 해킹은 2013년 6월부터 10월까지 426건으로 나타났다. 전체 해킹 피해액은 233억 2천만 원에 달하는 것으로 나타났다[2]. 사용자들의 안전한 온라인 금융서비스는 선택적 요건이 아닌 필수적인 요인으로써 그 중요성이 점차 강조되고 있다. 현재 인터넷 뱅킹에서 사용되는 보안 솔루션으로는 공인인증서, 일회용 비밀번호, 보안카드, 가상키보드 등이 있다. 이러한 보안 솔루션의 안전성은 수학적 불가능성에 기반을 두고 있기 때문에 공격자가 암호에 대한 전통적인 기법으로 공격을 시도하는 경우는 매우 드물다. 공격자들은 피해자들의 심리를 잘 이해하고 그들이 자신의 정보를 순순히 제시하도록 하는 사회 공학적 기법을 통해 확보한 계좌와 관련된 비밀정보를 통해 보다 쉽게 금전적 이득을 취하고 있다[3]. 특히 최근에 발생하는 피싱, 파밍은 사용자의 실수를 통해 비밀정보를 취하는 방식을 사용한다. 최근에는 피싱 및 파밍 사이트를 통해 사용자의 보안카드 정보를 알아내는 공격을 방어하기 위해 보안카드의 배치 및 인쇄 값을 변경하여 사용자가 사이트의 상이점을 알아채도록 도와주는 방법이 제시되었다[4]. 하지만 해당 기법은 사용자에게 적극적인 피드백을 주기 보다는 사용자가 상이점을 통해 판단해서 결정하도록 하여 사용자의 부주의로 인한 피해 발생 가능성이 존재한다. 이와 더불어 공격자가 사이트와 사용자 중간에 위치하며 거래를 조작하는 중간자 공격에 대해서는 효과적으로 방어하지 못하는 문제점을 가진다.

본 논문에서는 보안카드의 기존 디자인을 변경하여 사용자에게 보다 적극적인 피드백을 줌으로써 피싱과 파밍공격을 방지할 수 있는 기법을 제시한다. 또한 해당 기법은 기존의 OTP 기술에서는 방어하기 힘들었던 MITM에 대해서도 방어가 가능하다[5]. 마지막으로 보안카드의 정렬을 불규칙하게 변경한 새로운 레이아웃 디자인을 통해 실수로 발생하는 정보입력을 방지하는 기법을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 관련된 연구에 대해 살펴본다. 3장에서는 제시하는 보안카드의 알고리즘을 설명한다. 4장에서는 해당 기법에 대한 평가를 하며 마지막으로 5장에서는 논문을 마무리 한다.

Ⅱ. 관련 연구

2.1. 보안카드를 통한 금융 보안

보안카드는 온라인상에서 고객들의 재산 보호 및 투자거래 시의 안전을 보장하기 위한 장치로, 다수의 난수와 기타 일련번호 등이 적혀있는 일종의 난수표로서 사용자에게 각 금융사당 1매씩 발급된다. 주로 공인인증서를 새로 발급받을 때나, 공인인증서를 통한 온라인 금융 거래 시 사용되며, 공인인증서를 통해 금융사 홈페이지에 접속한 후 금융서비스 요청 시 보안 카드의 난수를 요구받은 대로 입력하고, 마지막으로 다시 공인인증서와 이의 비밀번호를 입력하면 금융 거래를 할 수 있다. 은행에서는 보안카드와 동일한 숫자들을 저장하고 있는 형태가 아니라, 사용자가 입력한 번호가 맞는지 확인하는 시스템으로 되어 있다[6,7].

2.2. 신종 금융사기: 피싱, 파밍

금융감독원의 2011년 9월 ~ 2013년 12월까지 주요 금융 사기 경로조사에 따르면, 보이스피싱이 60.6%를 차지하고 피싱, 파밍이 39.4%를 차지한다. 하지만, 최근 피싱, 파밍 방식의 신, 변종 수법이 증가함으로 2013년도 통계 자료만 본다면 과반수 이상이 피싱, 파밍임을 확인할 수 있다. 여기서 피싱(Phishing) 이란 개인정

보(Private data)와 낚는다(Fishing)의 합성어로 전화, 문자, 메신저, 가짜사이트 등의 수단으로 피해자를 기망 및 협박을 해서 개인정보 및 금융거래 정보를 요구하거나 피해자의 금전을 이체하도록 하는 수법이다. 악의적 공격자는 사용자에게 문자나 이메일을 통해 피싱사이트 주소를 전송하고, 피싱사이트 주소임을 인지하지 못한 사용자는 피싱사이트에 접속하게 되고 자신의 비밀정보를 입력하게 됨으로써 공격이 성공하게 된다.

파밍(Pharming) 이란 피싱(Phishing)과 조작(Farming)의 합성어로, 악성프로그램에 감염된 PC를 조작하여 피해자가 정상 사이트로 접속하더라도 가짜 은행사이트로 접속을 유도하여 금융거래정보를 빼낸 후 금전적인 피해를 입히는 수법을 말한다. 공격자는 악성코드를 사용자에게 전송하게 되고 사용자는 이를 자신의 컴퓨터 혹은 스마트폰에 깔게 됨으로써 적합한 사이트의 주소가 변경되어 악의적 사이트에 접속되게 된다. 사용자는 의심 없이 자신의 정보를 입력함으로써 공격이 성공하게 된다.

2.3. 신종 금융사기: 중간자 공격

중간자 공격이란 피싱 공격을 응용한 것으로 공격자는 피해자를 가짜 웹 사이트로 유인하여 정보를 입력하도록 하고, 공격자는 실제 웹사이트로 접속하여 피해자가 입력한 정보를 이용하여 정상 사용자인 것처럼 금융거래를 진행하는 수법이다. MITM 방법이 더욱 위험한 이유는 공격자가 실제 웹사이트에서 수신인 정보만 자신의 정보로 변경하고, OTP나 2채널 인증을 위한 인증코드는 가짜 웹사이트로부터 실시간에 가까운 시간으로 중계 받으므로 사용자를 속이는 동시에 탈취와 악용을 할 수 있다[8]. 뿐만 아니라 기존 피싱 또는 파밍 수법에서 보안카드 전체 입력 요구가 많았다면, MITM 기법에서는 피해자가 정상 금융거래를 진행한다고 생각하고, 보안카드를 정상적으로 두 개만 입력하여도 공격자의 공격이 성공할 때까지 피해자가 해킹사실을 인지하기 어렵다.

2.4. 기존 금융사기 방어 기법

최근 발표된 금융보안 공모전 수상작들은 신 금융사기 기법에 대한 방어 기법들을 많이 제안하고 있다. 본 장에서는 2012, 2013년도에 제안된 금융사기 방지 기법들에 대해 확인해 보도록 한다.

2.5. 다중채널 기반의 안전한 금융거래 입력방식

PC 혹은 스마트폰만을 이용한 거래는 공격자에게 단말기가 해킹당한 경우 사용자가 단말기에 입력하는 정보는 공격자에게 유출될 수 있는 문제점을 가진다. 이러한 정보유출을 방지하기 위하여 다중 채널을 이용하여 입력과 출력을 분리하는 새로운 접근 방법을 제안하여 입력방식의 안전성을 높이는 효율적인 방안이 제시되었다[9]. PC에서 대응되는 스마트폰의 키보드 값을 랜덤하게 생성하여 해당 값을 전송하도록 하며 이는 공격자가 키보드의 배치를 알 수 없게 하는 특징을 가진다. 하지만 해당 기법은 입력에만 국한된 기법으로써 MITM을 통해 중간자 공격이 수행되게 될 경우 거짓된 세션을 공격자의 의도에 의해 처리하게 될 우려가 있을 뿐 아니라 난수의 값이 전송되더라도 특정 난수가 2번 이상 반복되는 경우 비밀번호의 패턴이 노출될 수 있는 문제점을 가진다.

Ⅲ. 제안하는 기법

3.1. 싱글채널

싱글채널을 통한 거래 사이트 인증 기법은 휴대폰 혹은 컴퓨터 하나만을 이용한 인증기법이다. 이는 기존의 사이트에서 사용자가 금융거래 사이트에 접근하게 될 시에 사이트에서 접속한 사용자의 신원을 확인하고 사용자에 특화된 인증화면을 보여주는 것이다. 사용자는 인증화면이 자신의 조건과 만족하는 경우 해당 사이트가 피싱/파밍 사이트가 아님을 확인할 수 있다. 하지만 하나의 채널을 이용한 인증기법은 공격자가 하나의 채널을 점령하게 될 경우 인증화면의 정보를 지속적으로 수집하여 사용자의 비밀정보를 빼내어 갈 수 있는 문제를 가진다. 이를 보완하기 위해 멀티채널을 통한 인증기법이 요구되어 진다.

3.2. 멀티채널

멀티채널을 통한 인증기법의 경우 하나의 채널이 점령당하는 경우에도 남아 있는 채널이 안전한 경우 공격자에게 정보가 노출되지 않는 장점을 가진다. 멀티채널을 통한 사이트 인증 프로토콜에서 사용자는 금융서비스 홈페이지에 접근하여 공인인증서로 홈페이지에 접근하게 된다.

이때 자신이 가진 스마트폰을 열어 인증요청을 하게 되면 해당 어플리케이션에서는 홈페이지에 암호화된 인증 요청 메시지를 보내게 된다. 사이트에서는 해당 어플리케이션이 적합한 어플리케이션인지 메시지를 복호화하여 포함된 서명값을 확인하여 적합한 경우에 인증화면을 생성할 때 필요한 시드 정보를 암호화하여 스마트폰에 전송하게 된다.

해당 시드정보는 사용자의 보안카드로 인증이 가능한 정보를 포함하게 되며 해당 정보를 통해 인증 화면을 휴대폰에 보여주게 된다. 따라서 악의적인 어플리케이션은 사이트에서 전송되는 암호화된 정보를 복호화하는 것이 불가능하므로 시드를 통해 인증화면을 구성하는 것은 불가능하다. 만약 사이트에 접근한 컴퓨터가 점령된 경우에는 휴대폰에서의 적합한 인증 화면 시드 제공이 불가능하다. 그 이유는 적합한 시드정보를 사이트에서 보내주지 않으면 사용자는 적합한 인증 화면을 휴대폰에서 확인하는 것이 불가능하기 때문이다. 휴대폰이 점령된 경우에는 사이트에 인증 요청을 적합하게 할 수 없기 때문에 안전하다. 상세 수행순서는 알고리즘 2에 명시되어 있다.

3.3. 중간자 공격에 안전한 보안카드/스마트폰 기반 인증 기법

중간자 공격은 기존의 공격과는 달리 공격자가 사용자가 신뢰하는 사이트의 중간에 위치하면서 사용자가 원하는 서비스에 접근할 때 중간에서 해당 세션을 가로채어 자신이 원하는 요청으로 바꾸어 공격하는 기법이다. 이를 방지하지 위해 멀티채널 간의 연결이 서로 되지 않는 환경으로 구성하였다. 사용자는 온라인 거래를 수행할 사이트에 접근하여 원하는 서비스에 대한 모든 정보를 입력하고 자신의 휴대폰에 방금 전 사이트에 입력한 거래에서 중요한 정보(은행, 계좌, 금액)를 입력하도록 한다. 해당 입력정보는 보안카드를 통한 인증을 수행할 때 생성되는 화면의 구성에 대한 시드값으로써 휴대폰에 내장된 카운터, 타임스탬프와 같은 비밀정보와 함께 OTP 생성에 사용되게 된다. 여기서 내장된 카운터와 타임스탬프는 상호간에 연결이 없는 경우에도 사이트와 초기에 공유된 값으로써 상호간에 동일한 값을 가지게 된다. 만약 휴대폰이 해킹되어 사용자의 거래와 다른 거래에 대한 보안카드 화면이 생성되는 경우에도 정당한 사이트에서 요구하는 보안카드 값과 상이하기 때문에 거래가 성립되지 않는다. 사이트가 해킹된 경우에도 휴대폰 상에서의 보안카드 생성 규칙에는 영향을 미칠 수 없으므로 기존의 MITM 공격에 따른 보안사기를 방지할 수 있다. 자세한 프로세스는 알고리즘 3에 명시되어 있다.

3.4. 피싱/파밍 사이트 인증을 위한 보안카드 디자인

본 장에서는 보안카드를 통한 인증을 위해 새롭게 디자인한 보안카드를 제시한다. <그림 1>에서와 같이 기존의 보안카드는 상, 하단 그리고 좌우편에 어느 정도의 여백이 존재함을 확인할 수 있다. 본 논문에서는 사용되지 않는 여백부분을 피드백에 필요한 하나의 도구로 사용함으로써 사용자가 간단한 테스트를 통해 피싱 혹은 파밍 사이트를 구별 가능하도록 한다.

그림 1. 기존 보안카드의 여유공간
Fig. 1 Traditional Security Card with Margin

<그림 2>에서와 같이 새롭게 제작된 보안카드는 상하의 홈을 만들어 스마트폰의 화면과 겹쳐서 홈 사이로 나타나는 정보를 확인하여 적합한 값이 도출되는지 검증하게 된다. 해당 기법은 스마트폰의 스크린과 겹쳐서 정보를 얻어내는 것이므로 현재의 스마트폰이 보안카드보다 커야지 해당 기법이 적용가능하다. <그림 3>에서와 같이 현재 판매되는 거의 모든 스마트폰은 보안카드보다 훨씬 큰 스크린을 제공하며 이는 제안 기법이 큰 어려움 없이 적용 가능함을 의미한다.

일반적인 스크린 크기를 가지는 갤럭시 S3 제품의 경우에도 보안카드에 비해 큰 화면을 제공한다. 따라서 보안카드를 휴대폰에 겹쳐서 새로운 정보를 생성하는 것이 가능하다.

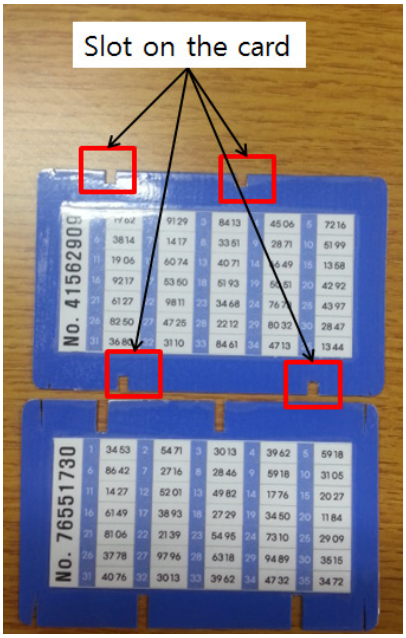

그림 2. 제작된 새로운 보안카드 디자인
Fig. 2 New Security Card Design

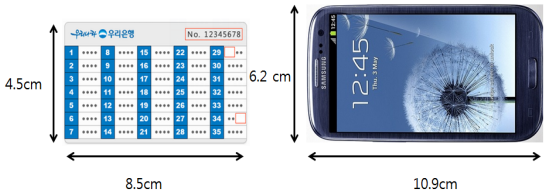

그림 3. 보안카드의 크기와 휴대폰의 크기 비교
Fig. 3 Comparison of Size of Security Card and Smartphone

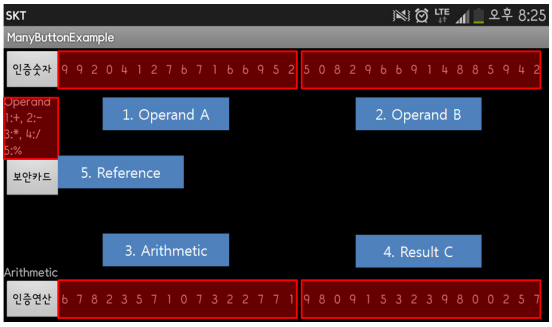

그림 4. 제안하는 보안카드 인증 화면 구성
Fig. 4 Authentication Screen of Proposed Security Card

<그림 4>에서는 스마트폰에서 생성되는 인증화면의 구성이 설명되어 있다. 해당 화면은 총 5가지의 영역으로 구분된다. 먼저 1, 2는 사칙연산의 두 개의 입력 인자를 의미하며 3번은 사칙연산 그리고 4번은 계산 결과값을 나타낸다. 5번에는 3번 연산에 대한 설명을 제시하였다. 예를 들어 카드를 대었을 때 보이는 공간의 숫자가 1, 4, 1, 5인 경우 1+4=5로써 결과값이 맞음을 의미한다. 계산 결과를 간단하게 하고 보안성을 높이기 위해 모든 결과값은 모듈러 10을 한 일의 자리 수만을 4번 결과 칸에 나타나도록 하였다.

<그림 5>는 초기화면을 나타내며 해당 화면에서는 아무런 문자가 표기되지 않는다. 이제 버튼을 눌러 인증숫자와 인증연산을 차례대로 생성해보도록 한다. 인증 숫자를 누르게 되면 위에 위치하는 칸에 난수 값들이 일제히 채워지게 된다. 인증숫자가 채워진 화면은 <그림 6>와 같다.

그림 5. 보안카드 인증 화면 초기 상태
Fig. 5 Initialization Status of Security Card

그림 6. 보안카드 인증 검증 숫자 생성
Fig. 6 Generation of Authentication Number

그림 7. 보안카드 인증 검증 연산 및 결과 생성
Fig. 7 Generation of Authentication Arithmetic and Results

가장 아래의 인증연산 버튼을 누르게 되면 <그림 7>과 같이 사칙연산과 최종 결과값이 아래 줄에 표기되게 된다. 해당 화면이 표기되면 새롭게 디자인된 보안카드를 휴대폰의 스크린에 올려서 생성된 인증 화면이 적합한지를 확인할 수 있다. 지금부터는 실제로 구현된 보안카드 앱과 보안카드 실물 디자인을 통해 피싱 혹은 파밍 사이트를 구분하는 기법을 시연하고자 한다. <그림 8>에서는 보안카드와 스마트폰이 나타나 있다. 실험에 사용된 휴대폰은 G Pro 휴대폰으로써 넓은 스크린을 가지고 있다. 앞에서 명시된 바와 같이 현재 출시되는 대부분의 휴대폰이 넓은 스크린을 제공함으로 본 기법을 문제없이 구현할 수 있다. 현재 프로세스는 <그림 13>의 인증화면 요청이 끝난 후 사이트로부터 시드값을 획득한 이후 스마트폰에서 인증화면을 출력하는 프로세스를 나타낸다.

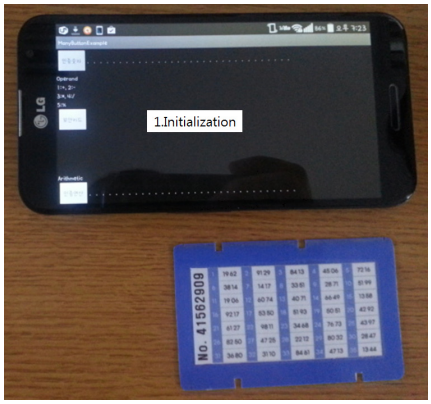

그림 8. 보안카드 인증 초기 상태
Fig. 8 Initialization of Security Card

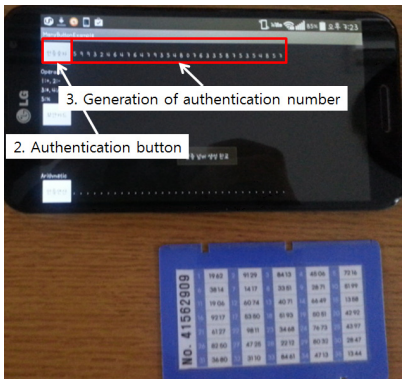

그림 9. 보안카드 인증 숫자 생성
Fig. 9 Generation of Authentication Number

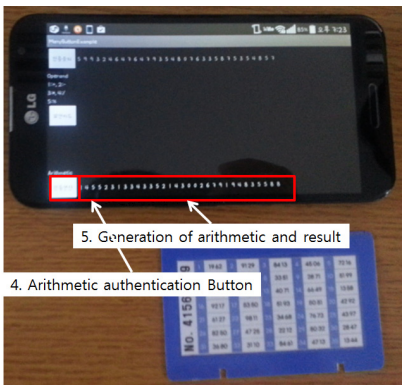

그림 10. 보안카드 인증 연산 생성
Fig. 10 Generation of Authentication Arithmetic

<그림 10>에서는 인증 버튼을 누르게 될 때 인증 숫자 쌍들이 표기되는 화면을 나타난다. 해당 인증 숫자 쌍들은 구현에 따라 매우 긴 쌍으로 표기를 하여 사용자가 특정한 규칙에 따라 고르도록 하는 방식으로도 구현이 가능하다. <그림 11>에서는 생성된 인증 화면에 보안카드를 매칭하여 올바른 결과값이 도출되는지를 확인하는 과정이다. 먼저 상단의 숫자가 4, 4이고 아래 숫자가 1, 8임을 확인할 수 있다. 첫 번째 홈은 첫 번째 인자이고 두 번째 홈은 두 번째 인자이다. 그리고 세 번째 홈은 인증 연산이고 마지막으로 네 번째 홈은 결과값이다. 따라서 이를 종합하여 하나의 식을 세워보면 4+4=8 이 되므로 결과값이 맞게 되어 해당 사이트는 적합한 사이트임을 확인할 수 있다. 여기서 결과값이 10을 초과하는 경우에는 모듈러 10 연산을 통해 첫 번째 자리의 수만을 확인하도록 한다.

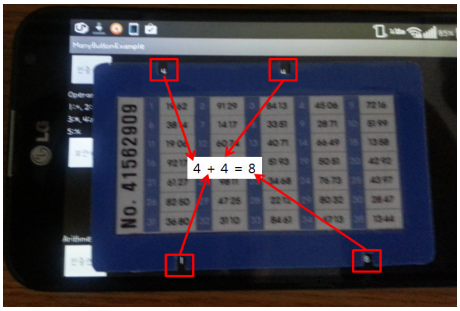

그림 11. 보안카드 인증 수행
Fig. 11 Authentication of Security Card

숫자를 이용한 방식은 사용자에게 계산을 요구함으로써 불편함이 발생할 수 있다. 따라서 <그림 12>와 같이 색상만을 이용하는 인증기법을 동일한 보안카드 인증 기법에 적용가능하다. 해당 기법은 빈칸에 나타나는 색상이 모두 동일하면 인증이 되는 경우라고 생각하면 된다. 여기서 홈페이지와 디바이스를 이용한 멀티채널 인증이 적용되기 위해서는 사이트에 현재 빈칸에 보이게 될 색상을 표기해 주고 사용자는 휴대폰을 열어서 그 색상만으로 마스킹되어 보이는지를 확인하는 방식으로 사이트를 인증할 수 있다.

<그림 13>에서는 보안카드를 통해 마스킹 기법을 시도한 경우의 결과화면을 나타낸다. 실험에서와 같이 사용자는 자신의 보안카드로 해당 색상을 확인하는 방식을 통해 올바른 사이트인지 확인할 수 있다. 해당 그림에서는 모두 녹색을 표기함으로써 사이트가 인증이 됨을 확인할 수 있다. MITM에 강인한 기법을 제안하기 위해서는 멀티채널을 사용하되 사이트와 휴대폰간의 정보 공유가 일어나지 않는 방식을 취해야 중간자 공격에 안전할 수 있다. 그 이유는 중간자 공격은 사이트와 휴대폰 간의 정보가 교환될 때 발생하기 때문이다.

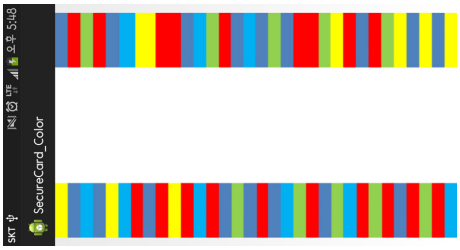

그림 12. 색상을 통한 인증화면 구성
Fig. 12 Authentication Screen with Color

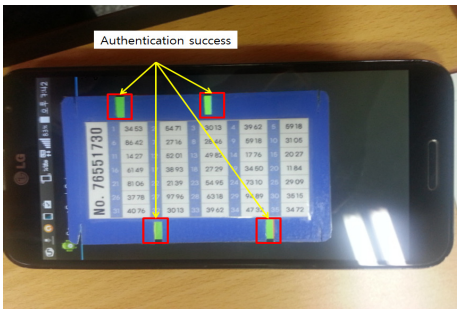

그림 13. 실제 테스트한 색상 인증 화면
Fig. 13 Authentication Test

따라서 본 논문에서는 거래에 필요한 핵심정보의 부분을 휴대폰에 입력하여 사이트와 사전에 공유된 비밀정보를 조합하여 생성된 보안카드 번호값을 생성함으로써 중간자 공격에 대한 위험을 방지할 수 있다. 사용자가 계좌이체를 하는 경우 상대방의 은행과 계좌번호 그리고 송금금액을 스마트 폰에 입력하게 되면 스마트 폰에서는 해당 정보를 포함하여 사이트와 공유하는 타임스탬프, 카운터 값을 이용하여 보안카드 인증 화면을 생성하게 된다. 여기서 생성되는 임의의 값은 보안카드의 인덱스를 나타내는 값이다.

Ⅳ. 평 가

본 장에서는 제안한 기법에 대한 보안성과 효율성에 대해 확인해 보도록 한다.

4.1. 보안성

새로운 보안 카드 기법 적용 시 기존의 피싱과 파밍 그리고 MITM 공격에 대한 방어 가능성과 기존의 실수 입력 방지 보안 카드와의 보안성에 대해 확인해 본다. 제안된 기법은 피싱/파밍을 위한 인증을 위해 인증 페이지를 보안카드로 확인해 보는 방식을 통해 사이트의 진위여부를 확인하게 된다. 숫자를 이용한 방식을 사용할 경우 나올 수 있는 숫자의 개수는 0~9으로 총 10개이며 이는 0.1의 확률로 올바른 값을 공격자가 임의로 맞출 수 있다는 것을 의미한다. 10%의 확률은 공격 성공률이 매우 높지만 해당 인증과정을 여러 차례 사용자가 수행하게 될 경우 확률은 지속적으로 줄어들게 된다. 만약 공격자에 의해 인증화면이 노출되는 경우에도 보

안성을 높이기 위해서는 결과 값을 멀티채널을 이용하여 규칙을 변경하면 화면 노출로 인한 보안 취약성을 방어 할 수 있다. <그림 14>에서와 같이 이전에는 사칙연산을 수행했다면 보안성이 강화된 버전에서는 모든 홈에 있는 값을 더해서 나오는 값을 사이트에서 출력하도록 하는 것이다. 이는 스마트폰 화면만을 통해서는 보안카드의 공백에 위치한 곳을 정확히 확인하는 것이 불가능하다. 이와 더불어 결과 값을 마스킹하여 올바른 결과 값이 나오지 않도록 하는 방법을 취할 수 있다. 예를 들어 결과 값이 2인 경우 마스킹 값을 적용하여 곱하기 8이 늘 수행되도록 하여 결과가 6이 도출되도록 하는 것이다. 해당 마스킹 값은 주기적으로 바뀌도록 하여 화면이 노출되는 경우에도 공격이 쉽게 이루어지지 않도록 할 수 있다. 색상의 경우에는 총 4개의 홈이 있고 총 경우(색상)의 수가 n일 경우 모든 색상이 같을 확률은 약 (1/n)^4 가 되게 된다. 색상보안카드의 경우에도 화면 노출의 위험성을 <그림 15>와 같이 사이트에 특정 색상 정보를 표기함으로써 방어할 수 있다. 여기서는 화면에 나타나는 색상의 수를 나타내어 실제로 보안카드를 통한 마스킹 시에 휴대폰에 나타나는 값을 확인하는 방식으로 화면의 노출로 인한 보안 취약성을 방어할 수 있다.

그림 14. 페이지 노출에 강인한 보안카드 화면 설계 ver. 1
Fig. 14 Design of Security Card Screen against Page Disclosure ver. 1

그림 15. 페이지 노출에 강인한 보안카드 화면 설계 ver. 2
Fig. 15 Design of Security Card Screen against Page Disclosure ver. 2

MIMT를 방어하기 위한 보안카드 기법의 경우에는 공격자가 두 개의 디바이스를 점령하는 경우를 제외하고는 공격자가 의도한 거래를 성립시키는 것을 막을 수 있다. 그 이유는 기존의 기법과는 달리 두 개의 디바이스를 온라인으로 연결시키지 않아 중간자가 거래에 개입하는 것이 불가능하며 모든 거래는 사용자가 직접 거래의 중요정보를 입력하고 이를 통해 도출된 보안카드 입력화면이 도출되도록 하였기 때문이다. 여기서 보안카드의 인덱스 또한 보안카드의 홈을 통해서만 확인 가능하므로 공격자는 입력되는 보안카드의 정보를 얻는 것이 불가능하다.

4.2. 효율성

새로운 보안카드를 이용한 안전한 금융서비스를 위해서는 실용적인 사용 용이성 또한 같이 살펴보아야 한다. 본 장에서는 제안 알고리즘의 효율성에 대해 살펴보도록 한다. 제안하는 알고리즘 적용 시 기존에 없던 사이트 인증 절차를 중간에 포함함으로써 사용자의 시간적 손해가 발생한다. 따라서 사용자는 보다 원활한 서비스 제공면에서 불만을 제기할 수 있다. 하지만 해당 서비스는 기존에 불가능했던 피싱/파밍 사이트를 구분할 수 있는 알고리즘을 제공한다. MITM 방어 기법의 경우 스마트폰에서 계좌 정보를 입력하는 시간이 소모되게 된다. 하지만 이 또한 지금까지 방어하지 못했던 MITM공격을 방어할 수 있다는 장점을 가지므로 약간의 시간적 손해보다 보안 안정성에 따른 이득이 더 크다고 할 수 있다.

Ⅴ. 결 론

본 논문에서는 피싱, 파밍 그리고 MITM과 같은 최근 문제가 되고 있는 금융사기 기법들에 대해 확인해보고 이를 효과적으로 방어하기 위한 보안 카드 인증 메커니즘을 설계 및 구현해 보았다. 해당 기법은 지금까지 제시된 기법들과는 달리 사용자가 능동적으로 피싱, 파밍 사이트를 구분할 수 있을 뿐 아니라 현재 제시되는 기술로는 방어가 어려운 MITM을 효과적으로 방어하기 위한 새로운 패러다임을 제시한다. 해당 기법은 현 금융 시스템에 바로 적용이 가능한 실용적인 구조를 가지며 쉽게 구현이 가능한 장점을 가진다.

감사의 글

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발사업 [10043907, 개방형 고성능 표준 IoT 디바이스 및 지능형 SW 개발]과 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음(IITP-2015-H8501-15-1017)

REFERENCES

[1] The bank of Korea, “2014 third quarter Reports on Domestic Internet Banking Services,” 2014.

[2] Research Center on Security Policy of Police University, “Future of Security 2014,” 2014.

[3] AhnLab. Social engineering method [Internet] Available: http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=3&seq=9761

[4] J. K. Park and J. H. Lee, “Miss-type-proof based Techniques to Prevent from Phising and Phaming,” *Review of KIISC*, vol.23 no. 6, pp. 9-17, Dec. 2013.

[5] ZDNET. New Financial Phishing Attack [Internet]. Available:http://www.zdnet.co.kr/news/news_view.asp?article_id=20130702122904

[6] Wikipedia. Personal identification number [Internet]. Available: http://en.wikipedia.org/wiki/Personal_identification_number

[7] Wikipedia. ISO 9564 [Internet]. Available: http://en.wikipedia.org/wiki/ISO_9564#PIN_ entry_devices

[8] Wikipedia. One-time password [Internet]. Available: http://en.wikipedia.org/wiki/One-time _password

[9] Y. L. Park, J. W. Son, S. H. Shin and M. K. Yoon, "Methods for Multi-channel based Financial Input", *Review of KIISC*, vol.23 no.1, pp. 9-17, Feb 2013.

서화정(Hwa-jeong Seo)

2010년 2월: 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월: 부산대학교 컴퓨터공학과 석사 졸업
2012년 3월 ~ 현재: 부산대학교 컴퓨터공학과 박사과정
※관심분야 : 정보보호, 암호화 구현, IoT

김호원(Ho-won Kim)

1993년 2월: 경북대학교 전자공학과 학사 졸업
1995년 2월: 포항공과대학교 전자전기공학과 석사 졸업
1999년 2월: 포항공과대학교 전자전기공학과 박사 졸업
2008년 2월: 한국전자통신연구원 정보보호연구단 선임연구원/팀장
2008년 3월 ~ 현재: 부산대학교 정보컴퓨터공학부 부교수
※관심분야 : 스마트그리드 보안, RFID/USN 정보보호 기술, PKC 암호, VLSI 설계, embedded system 보안, IoT