JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 20, No. 1 : 81~86 Jan. 2016

다중 채널 인증 기반 보안 카드의 설계 및 구현

서화정 · 김호원*

Multi-Channel Authentication based Security Card Design and Implementation

Hwa-jeong Seo · Ho-won Kim*

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

요 약

본 논문에서는 다중 채널 보안카드 설계 기법을 제공한다. 해당 보안 카드는 투명하게 제작되어 스마트폰의 화면과 합쳐서 나타나는 정보를 통해 비밀값을 도출하게 된다. 이는 기존 보안카드가 가지는 레이아웃의 물리적인 한계를 제거하여 보안카드가 가지는 복잡도를 향상시켰으며 1채널 보안카드의 단점인 물리적 노출에 대한 취약점을 다중 채널로 확장하여 한 번의 물리적 보안카드의 노출이 모든 비밀 정보의 노출로 연결되는 문제점도 해결하였다.

ABSTRACT

In this paper, we present multi-channel authentication based security card design. Since this security card is written on the transparent paper, security information is extracted by overlaying the card with smartphone screen. This method removes the limitations of physical layout in previous security card and improves the security level. Furthermore, our security card is secure when our card is exposed to malicious users.

키워드 : 보안카드, 다중 채널 인증, 레이아웃 설계, 금융보안

Key word : Security Card, Multi-Channel Authentication, Layout Design, Financial Security

접수일자 : 2015. 09. 05 심사완료일자 : 2015. 09. 30 게재확정일자 : 2015. 10. 14

* **Corresponding Author** Ho-won Kim(E-mail:howonkim@pusan.ac.kr, Tel:+82-51-510-3927)
Department of Computer Engineering, Pusan National University, Pusan, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2016.20.1.81 print ISSN: 2234-4772 online ISSN: 2288-4165

ⓒThis is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(http://creativecommons.org/li-censes/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright Ⓒ The Korea Institute of Information and Communication Engineering.

Ⅰ. 서 론

온라인 금융서비스는 언제 어디서나 금융 서비스를 사용 가능하게 함으로써 오프라인 서비스의 문제점인 접근성과 가용성을 해결하였다. 온라인 금융 서비스의 편리함으로 인해 2014년 3월말 인터넷 뱅킹 서비스 등록 고객 수는 9,775만 명으로 전분기말대비 2.4% 증가하였다[1]. 이와 더불어 스마트폰 뱅킹 등록 고객 수(4,034만 명)도 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 금융사기 위험에 보다 취약해지도록 하고 있다. 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 심리적인 마음을 잘 이해하고 그들이 자신의 정보를 순순히 제시하도록 하는 사회 공학적 기법을 통해 확보한 계좌와 관련된 비밀정보를 통해 보다 쉽게 금전적 이득을 취하고 있다. 최근에는 피싱 혹은 파밍과 같이 적법한 사이트를 모방하여 사용자가 실수로 비밀번호를 입력하여 노출시키는 공격이 사용되고 있다. 이를 위해 보안카드의 배치 및 인쇄 값을 변경하여 사용자가 사이트의 상이점을 알아채도록 도와주는 방법이 제시되었다[3]. 하지만 해당 기법 또한 물리적인 입력 값이 한번 노출되게 되는 경우에는 모든 비밀 값이 유출되게 되는 문제점을 가진다.

본 논문에서는 기존의 보안카드에서 확장된 형식으로 정보를 제공할 수 있는 투명한 형태의 보안카드를 제작하였다. 투명한 보안카드의 경우 사용자가 가진 스마트 디바이스의 스크린 상에 겹쳐 보임으로써 보다 많은 정보 제공이 가능하게 된다. 또한 정보 제공 사이트가 적합한 사이트인지 확인하여 피싱 및 파밍 공격에 대처가 가능하도록 하였다. 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. 관련연구

2.1. 보안카드 실수입력방지기법

사용자의 보안카드의 디자인과 입력 위치 값을 수정하여 사용자가 사이트에 대한 진의여부를 판단하는 기법이 제안되었다[3]. 기본적으로 보안카드는 세로로 정렬되어 공격자가 사용자의 보안카드를 쉽게 묘사하는 것이 가능하다. 하지만 해당 논문에서 제안된 기법에서는 보안카드 지시번호의 배열 형식과 순서를 변경하거나 일부 보안 카드 번호에 마스킹을 적용하여 사용자마다 독창적인 보안카드를 발급하여 피싱 웹사이트에 나타나는 보안카드 번호 입력 화면과 본인이 가진 실물 보안카드가 상이함을 인지하도록 하여 보안카드 번호의 입력 가능성을 낮추도록 하였다.

2.2. 오버레이 기반 보안 카드

기존의 보안카드의 복잡도를 향상시키기 위해 스마트폰의 디스플레이를 활용한 오버레이 형태의 보안카드가 설계되었다[4]. 제안된 보안카드는 임의의 난수들을 배열하여 기존의 보안카드와 비슷하지만 레이아웃의 중간에 난수를 확인하기 위해 구멍이 뚫려 있다. 붉은 상자로 표시된 부분은 기존의 보안카드와 같은 형식으로 난수가 출력되는 부분이고, 푸른 부분은 앱에서 생성된 난수를 확인할 수 있도록 하였다. 푸른 부분의 위치에 어떤 번호가 나타날 것인지는 스마트폰에서 실행되는 앱에 달려 있으므로, 해당 보안카드를 분실하여도 정확한 난수를 알아내기 어렵다. 보안카드에는 임의로 공백이 생성되어 사용자가 보안카드와 어플리케이

션 화면이 겹치게 되는 경우 해당 공백을 통해 어플리케이션의 난수값이 나타나게 된다. 휴대폰을 통해 생성되는 보안카드 정보는 온라인 뱅킹 서버와 휴대폰이 초기에 상호간에 분배한 seed값을 통해 난수값을 생성하는 기법을 취한다. 해당 seed값은 타임스탬프, 카운터 혹은 사전 정의된 비밀키 값으로써 공격자가 seed값을 알지 못하면 보안카드를 생성할 수 없다.

Ⅲ. 제안하는 보안카드

기존의 보안카드는 불투명한 플라스틱 수지로 만들어진 것으로, 한쪽 면에는 금융사의 전화번호나 폰뱅킹 관련 코드 번호 등이 기재되어 있으며, 반대쪽 면에는 실제 금융거래 시, 필요한 정보를 입력하기 위한 비밀정보들이 기재되어 있다. 제안하는 보안카드에서는 투명한 소재를 사용하여 보안카드를 제작하였다. 해당 보안카드는 인덱스 정보 없는 비밀정보와 비밀정보 없는 빈칸, 그리고 각 비밀정보를 잇는 희미한 실선으로 구성되도록 한다. 제안하는 보안카드는 스마트폰과 연동하여 사용자가 금융거래를 진행할 때 스마트폰의 화면 위에 카드를 얹어서 실제로 카드 상에 존재하는 물리적인 정보와 스마트폰 상에서 동적으로 구성되는 정보를 종합하여 비밀정보가 생성되도록 하였다.

제안하는 보안카드를 통한 금융거래를 위해서는 먼저 온라인 금융거래 사이트에 접속한다. 그리고 적법한 절차에 따라 로그인을 성공적으로 수행되게 될 경우 자신의 금융거래 페이지로 이동하게 된다. 사용자는 자신이 원하는 서비스를 선택하고 금융거래를 성사시키기 위해 다시 한 번 비밀정보를 입력하게 된다. 이때 제안하는 보안카드를 사용하기 위해서는 스마트폰 상에서 앱을 수행하고 해당 앱을 통해 적법한 비밀정보를 추출하게 된다.

Fig 1에서와 같이 사용자는 보안카드와 스마트폰을 오버랩하여 타원 안에 나타나는 비밀값을 확인할 수 있다. 빨간 타원은 (3, 4), 노란타원은 (6, 5, 6) 그리고 파란 타원은 (9, 2, 7, 8)이란 비밀번호를 나타냄을 확인할 수 있다. 해당 비밀정보는 은행 거래 사이트에 입력하게 될 시에 안전한 거래를 성사하게 된다. 제안하는 보안카드의 경우 기존의 보안카드에 비해 자유롭게 비밀번호의 길이를 선택할 수 있다. 그 이유는 타원을 통해 비밀정보를 묶는 방식에 따라 비밀번호가 유동적으로 변경되기 때문이다. 또한 기존의 보안카드는 몇 번째 행의 몇 번째 열과 같이 원하는 정보의 위치를 제시하지만 제안하는 보안카드의 경우 그림을 통해 직관적으로 비밀정보의 위치를 판단하는 것이 가능한 장점을 가진다.

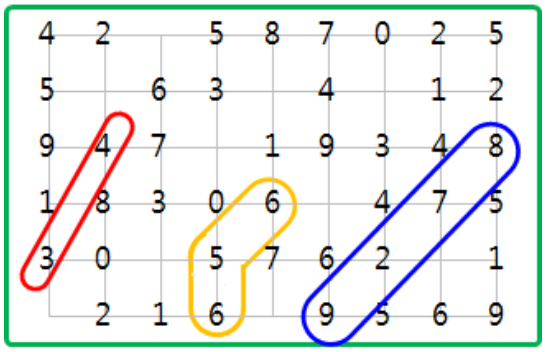

Fig. 1 overlapped screen of security card and application

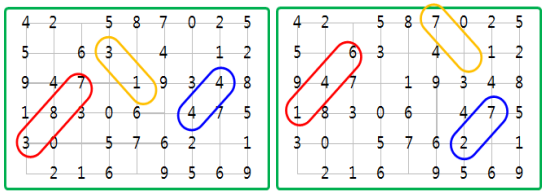

Fig. 2 left: normal site, right: phishing site

제안하는 보안카드의 또 다른 특징은 피싱/파밍 홈페이지를 탐지기능이다. 만약 사용자가 적법한 보안카드를 가지고 올바른 홈페이지에 접속하지 않은 경우에는 사용자가 확인가능 하도록 하고 있다. Fig 2에서는 올바른 사이트와 그렇지 않은 사이트에 접근했을 때의 예시를 보여주고 있다. 왼쪽 그림은 정상적인 사이트에 접속한 경우를 나타낸다. 이는 공백 없이 모든 숫자가 타원 안에 나타나게 된 것을 의미한다. 하지만 오른쪽 화면과 같이 제안하는 보안카드의 타원에는 불규칙인 공백정보가 포함되어 있으며 이는 적법한 사이트가 아님을 확인할 수 있다. 만약 피싱사이트에서 요구하는 정보에 공백정보가 포함되지 않은 경우에는 공백정보를 통한 피싱 탐지는 어려운 점이 있다. 하지만 피싱 사이트가 습득한 정보가 다음 거래 시에 나타날 확률은 n개의 경우의 비밀번호 조합이 있을 때 1/n!이므로 n의 수

가 충분히 큰 경우에는 노출된 정보로 인해 위험해 지는 경우는 발생하지 않는다. 사용자는 공격자가 작성한 피싱 사이트에 유도가 되지만 자신의 비밀정보의 유출을 1차적으로 막고 부분적으로 정보가 유출되더라도 실용적인 공격이 발생하지 않는 특징을 가진다. Fig 3에서는 제안하는 보안카드가 나타나 있다.

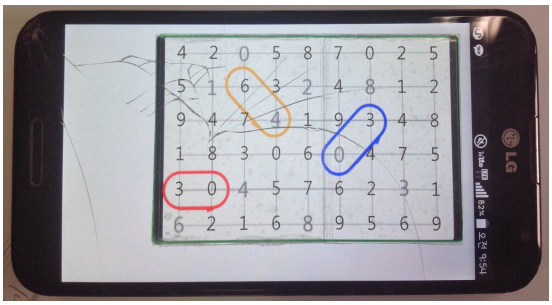

Fig. 3 Working demonstration

Ⅳ. 평 가

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

4.1. 보안성

본 논문에서 제안한 보안카드 기법은 피싱/파밍 탐지, 동적 비밀번호 그리고 비밀번호 확장과 같은 세 가지 보안 기능을 만족하게 된다. 피싱/파밍 탐지 기능은 보안카드의 공백이 타원 안에 나오게 되는 경우 피싱/파밍 탐지 기능을 확인할 수 있다. 따라서 공격자가 보안 카드의 정보를 알아내기 위한 시도를 하는 도중에 사용자는 이를 알아채는 것이 가능하다. 두 번째로 동적 비밀번호 생성이 가능하다. 비밀번호를 공백으로 묶는 방향과 방법에 따라 새로운 비밀번호가 제한적인 숫자들로부터 도출 가능하다. 만약 두 자리의 숫자로 비밀번호를 만드는 경우 전체 숫자의 개수가 n이라면 $\frac{n!}{(n-2)!}$ 이 되게 된다.

이는 기존의 기법들이 n/2개의 경우의 수를 가지는 것과 비교해 많은 동적 비밀번호 생성이 가능하다는 것을 의미한다. 마지막으로 비밀번호 확장의 경우 이전의 보안카드에서는 비밀번호의 길이가 두 자리씩 입력하는 것에 적합하도록 설계되었다. 하지만 제안하는 기법의 경우 비밀번호의 길이가 한 자리부터 보안카드의 길이만큼 확장이 가능하다. 따라서 이를 통해 매우 높은 보안성을 제공하는 보안카드의 제공이 가능하다. Table 1에서는 기존 기법들과의 보안성 기능을 비교하고 있다. 제안하는 기법은 모든 보안 기능에 대해 만족하는 유일한 보안카드 기법이다.

Table. 1 Comparison of security

	Phishing/ Pharming	DynamicP assword	Password Expansion
Basic	×	×	×
Mistake Prevention[4]	○	×	×
Multi Channel[5]	×	○	×
Proposed	○	○	○

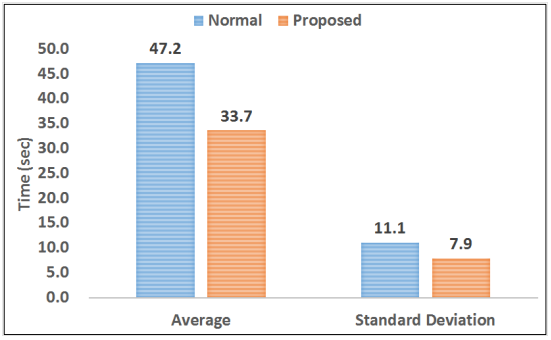

Fig 4 Comparison of typing average speed and standard deviation

4.2. 효율성

새로운 보안카드를 이용한 안전한 금융서비스를 위해서는 실용적인 사용 용이성 또한 같이 살펴보아야 한다. 본 장에서는 제안 알고리즘의 효율성에 대해 확인해 보도록 한다. 제안하는 보안카드는 기본적인 기법과 달리 입력해야하는 값을 찾을 필요가 없다. 그 이유는 화면과 보안카드의 겹쳐보임을 통해 쉽게 입력해야 하는 값을 확인하는 것이 가능하기 때문이다. 6명의 실험자를 통해 기본적인 기법과 제안하는 기법의 성능을 비교한 결과는 다음과 같다. 실수입력방지 혹은 멀티채널 인증 기법을 적용한 보안카드는 기본 기법과 동일한 레이아웃 설계를 사용함으로 기본기법의 성능을 통해 각

각의 기법에 대한 성능을 유추해 볼 수 있다. 제안하는 기법은 전혀 새로운 형식의 보안카드 기법이기 때문에 성능을 측정하는 것이 의미가 있다. 실험을 수행해 본 결과, 기본기법 대비 제안기법에서의 비밀정보 입력 시간은 각 실험자당 최대 46초가 줄어들고, 최소 2초가 줄어들었다. 또한, Fig 4에서 확인할 수 있듯이, 평균적으로도 제안기법의 입력시간이 기본기법보다 약 13초 정도 줄어든 것을 볼 수 있다. 각 실험자의 결과 중 기본기법에서의 최대 소요 시간과 제안기법에서의 최소 소요 시간을 기록한 실험자 5의 결과를 제외하더라도, 평균 입력속도가 기본기법의 경우 42.8초, 제안기법의 경우 35.8초가 소요되므로 제안기법의 입력속도가 더 빠른 것을 확인할 수 있다. 따라서 제안기법을 사용하여 금융거래를 하게 되면 조금 더 효율적이고 빠르게 사용자들이 금융거래를 할 수 있다.

Ⅴ. 결 론

본 논문에서는 안전한 온라인 금융 거래를 위해 사용되는 보안카드에 다중 채널 인증을 적용하여 보다 높은 보안성을 가지는 새로운 보안카드를 설계 및 구현하였다. 해당 기법은 기존의 플라스틱 용지 대신 투명한 용지 (OHP)를 이용하여 스마트폰의 스크린이 용지를 투과해서 나올 수 있는 형식으로 디자인되었다. 이를 통해 기존의 정형적인 비밀번호 입력방식이 아닌 보안카드 상에 나타난 모든 숫자의 쌍에 대한 경우의 수가 적용이 가능하도록 하였다. 또한 피싱과 파밍 홈페이지 방지를 위해 보안카드의 레이아웃을 유추가 불가능한 형식으로 재조정하여 보다 높은 보안성을 가지도록 설계되었다. 해당 기법은 현 금융 시스템에 바로 적용이 가능한 실용적인 구조를 가지며 쉽게 구현이 가능한 장점을 가진다.

ACKNOWLEDGMENTS

This research was partly supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2015-H8501-15-1017) supervised by the IITP(Institute for Information & communications Technology Promotion) and was partly supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No.10043907, Development of high performance IoT device and Open Platform with Intelligent Software) and was partly supported by a grant from the Advanced Technology Center R&D Program funded by the Ministry of Trade, Industry& Energy of Korea(10048537)

REFERENCES

[1] News Wire. 2014 domestic internet services usages, available in http://www.newswire.co.kr/newsRead.php?no=750326.

[2] AhnLab, Social Technology Attack available in http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=3&seq=9761.

[3] Jinkyu Park, Jungho Lee, “Security Card against Phishing and Phaming Attack,” *Journal of The Korea Institute of Information Security and Cryptology*, vol. 23, no. 6, pp. 30-40, Dec. 2013.

[4] Hwajeong Seo, Seonhee Seok, Kyounghoon Kim, Howon Kim. “A Multi-Channel Security Card based on Cryptographically Secure Pseudo-Random Number Generator,” *Journal of The Korea Institute of Information Security and Cryptology*, vol. 25, no. 3, pp. 501-507, June. 2015.

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