Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.3, Jun. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.3.501

난수생성기를 이용한 멀티채널 보안카드 설계*

서 화 정,† 석 선 희, 김 경 훈, 김 호 원‡
부산대학교

A Multi-Channel Security Card based on Cryptographically Secure Pseudo-Random Number Generator*

Hwa-jeong Seo,† Seon-hee Seok, Kyoung-hoon Kim, Ho-won Kim‡
Pusan National University

요 약

온라인 뱅킹 서비스는 금전과 관련된 업무를 처리함으로 정보교환에 있어서 안전한 보안이 제공되어야 한다. 현재 안전한 전자 금융 거래 서비스를 위해 공인인증서와 비밀번호, 보안카드, 일회용 비밀번호생성기(OTP) 와 같이 여러 가지 사용자 인증 방법이 존재한다. 특히 보안카드는 금융거래를 진행함에 있어서 모든 비밀정보를 포함하는 가장 중요한 비밀 매체이고 한 번 노출이 되고 나면 보안카드로써의 기능을 상실할 뿐 아니라 공격자는 획득하기 가장 어려운 비밀정보를 가지게 되므로 보다 높은 확률로 공격을 성공할 수 있다. 본 논문에서는 물리적인 보안카드가 가지는 비밀정보를 다른 채널에 분할하여 저장하는 기법을 통해 정보 유출의 위험성을 줄이는 방안을 제시한다. 제안하는 멀티채널 보안카드는 표시되는 비밀 정보의 양을 줄이고, 동적으로 생성하는 방법을 이용하여 비밀 정보 노출의 취약성을 줄이고 피싱 공격을 예방하는 기능을 가진다.

ABSTRACT

The online banking service handles a banking business over the internet, it is necessary to ensure that all financial transactions are processed securely. So, there are various authentication technique for e-banking service : a certificate, a personal identification number(PIN), a security card and a one-time password(OTP). Especially, the security card is most important means including secret information. If the secret information of card is leaked, it means not only loss of security but also easy to attack because security card is a difficult method to get. In this paper, we propose that a multi-channel security card saves an secret information in distributed channel. Proposed multi-channel security card reduces vulnerability of the exposed and has a function to prevent phishing attacks through decreasing the amount of information displayed and generating secret number randomly.

Keywords: Card, Security Card Application, Multi-Chanel Authentication

접수일(2014년 12월 30일), 수정일(2015년 3월 24일), 게재확정일(2015년 4월 9일)
* 본 연구는 2015년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원(No.10043907, 개방형 고성능 표준 IoT 디바이스 및 지능형 SW 개발)과 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음" (IITP-2015-H8501-15-1017)
† 주저자, hwajeong@pusan.ac.kr
‡ 교신저자, howonkim@pusan.ac.kr(Corresponding author)

I. 서 론

인터넷 뱅킹에서 사용되는 보안 솔루션으로는 공인인증서, 일회용 비밀번호, 보안카드, 가상키보드 등이 있다. 이러한 보안 솔루션의 안전성은 수학적으로 풀기 어려운 계산문제에 기반을 두고 있기 때문에 암호 해독 시도나 전사적 공격과 같이 암호에 대한 전통적인 기법의 성공률은 매우 낮다. 따라서 최근

공격자들은 금융거래정보를 수집하기위해 피해자들의 심리적인 마음을 잘 이해하고 그들이 자신의 정보를 순순히 제시하도록 하는 사회 공학적 기법을 통해 공격 대상과 관련된 비밀정보를 획득하고 이를 악용하여 금전적 이득을 취하고 있다 [1]. 피싱 및 파밍 공격자들은 택배배송정보, 온라인 청첩장 등을 가장한 URL이 포함된 SMS를 전송하여 악성 어플리케이션 다운로드를 유도하거나 인터넷 접속 정보를 수정한 뒤 대형 포털을 가장하여 금융 비밀정보를 요청하기도 한다.

본 논문에서는 보안카드의 기존 디자인을 변경하여 피싱 및 파밍사이트를 구분할 수 있는 기능을 제공하고 비밀정보를 일부만 표시함으로 보안카드의 정보 유출 가능성을 줄이는 방법을 제안한다. 더 나아가 보안카드의 비밀정보가 정적으로 제공되는 것이 아닌 금융거래시점마다 실시간으로 비밀정보가 생성되는 새로운 보안카드를 제안한다. 제안 방법은 물리적인 보안카드의 정보와 동적으로 생성되는 다른 채널의 정보를 섞어서 하나의 새로운 보안카드를 만들어 내는 방식이다. 본 논문의 구성은 다음과 같다. 2장에서는 관련연구에 대해 알아본다. 3장에서는 제시하는 보안카드의 알고리즘을 설명한다. 4장에서는 해당 기법에 대한 평가를 하며 5장에서는 논문의 결론을 기술한다.

II. 관련 연구

전자금융 이용이 가능한 매체는 PC뿐 아니라 스마트 폰과 태블릿과 같이 다양한 기기를 이용할 수 있게 되고, 그에 따른 전자통신금융사기 수법의 발전으로 인해 안전한 전자금융거래를 위한 관한 연구가 활발히 진행되고 있다. 본 장에서는 최근 제안된 금융사기 방지 기법들에 대해 확인해 보도록 한다.

2.1 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 통해 입력방식의 안전성을 높이는 효율적인 방안이 제시되었다 [2]. PC화면에 숫자 키패드를 무작위로 배치하고 각 숫자에 마다 4자리 난수를 생성하여 스마트 폰 키보드에 전송한다. 사용자는 PC 키보드로부터 키보드 배열 정보를 얻게 되고 아무것도 표시되지 않는 스마트폰 키보드를 통해 비밀번호를 입력한다. 이렇게 비밀정보의 입, 출력 채널을 다르게 설정하므로 금융 거래 시 보안성이 향상된다. 하지만 비밀정보가 난수 값 형태로 전송되더라도 특정 난수가 2번 이상 반복되는 경우 비밀번호의 패턴이 공격자에 노출될 수 있는 문제점을 가지고 있다.

2.2 스마트폰을 활용한 안전한 온라인 승인시스템

현재 전자금융거래에서 사용되고 있는 보안솔루션의 보안기능이 강화됨에 따라 사용자의 세션은 안전하게 보호되지만 다양한 환경 상에서의 편의성 저하로 인해 효율적인 적용이 어렵다. 이를 해결하기 위해 단말기에 설치된 OS 또는 브라우저에 종속되지 않는 보안기술을 제안하였다 [3]. 제안된 보안기술은 이미지를 이용한 인증기술로서 인증 서버로부터 생성되는 이미지 정보를 통해서 결제가 수행되는 기법이다.

이는 간편하게 사용이 가능한 보안 기술로써 그 효용성이 높게 평가되지만 보안에 취약한 Wi-Fi를 통해 이미지를 전송하게 되면 중간자에 의해 이미지가 조작될 수 있는 문제점(Man In The Middle attack, MITM)을 가진다.

2.3 전자금융거래 환경에서 보안카드 실수입력방지 기법 적용을 통한 피싱/파밍 사고 방지 방안

전자금융사기 사고 예방을 위한 사용자의 보안카드의 디자인과 입력 인덱스 값을 수정하여 사용자가 사이트에 대한 진의여부를 판단하는 기법이 제안되었다 [4]. 기본적으로 세로로 정렬이 되어 공격자가 사용자의 보안카드를 쉽게 묘사하는 것이 가능하다. 하지만 제안된 기법에서는 보안카드 지시번호의 배열 형식과 순서, 일부 보안 카드 번호에 마스킹 적용 등을 통해 보안카드를 사용자마다 상이한 형식으로 발급한다. 이를 통해 사용자가 피싱 웹사이트 상 보안카드 번호 입력 화면과 본인이 가진 실물 보안카드가 상이함을 인지하도록 하여 보안카드 번호의 입력 가능성을 낮추도록 하였다. 하지만 사용자가 미처 상이점을 알아채지 못하는 경우에는 공격이 가능한 문제점을 가진다.

III. 난수 생성기 기반의 멀티채널 보안카드

보안카드는 거래 은행으로부터 발행되는 물리적인 비밀 정보저장 장치로써 사용자가 기억하기 힘든 불규칙한 숫자 조합을 적어 놓은 비밀번호 코드 북이라고 할 수 있다. 보안카드의 비밀정보는 사용자에 의해 보호되어야 하며 금융거래 시점에서 물리적 카드를 소지하고 있어야 금융거래 진행이 가능하다. 보안카드를 사용하는데 있어서 소지에 대한 번거로움으로 인해 사용자들은 보안카드를 사진으로 찍어 스마트폰에 저장하거나 메일로 보관하는 경우가 발생하였고, 이러한 보안카드의 비밀정보를 보관해주는 스마트폰 어플리케이션도 개발되었다. 사용자들은 편의성을 위해 보안카드 비밀정보를 접근하기 쉬운 곳에 저장하였으나 이로 인해 보안카드 유출로 인한 보안의 위협은 더 커졌다. 물리적인 보안카드의 비밀정보는 분실하게 경우 모든 비밀정보가 한 번에 노출되기 때문이다. 본 논문에서는 기존 보안카드의 비밀정보를 디자인을 변경한 물리적인 보안카드와 다른 채널과의 결합을 통해 비밀정보를 동적으로 생성할 수 있는 보안카드 설계 방안을 제시한다.

3.1 멀티채널 보안카드 설계

3.1.1 제안하는 물리적 보안카드

보안카드의 비밀정보를 저장하기위한 첫 번째 채널은 물리적으로 제공되는 보안카드이다. 기존과 동일하게 보안카드의 비밀정보를 물리적인 카드를 이용하여 제공하게 되는데, 이때 물리적인 카드를 통해 저장되는 비밀정보의 양은 Fig.1.과 같이 기존의 비밀정보의 약 50%만 제공하게 된다. 기존 보안카드 형태에서 무작위로 선택된 반 정도의 비밀 번호는 카드에 표시 되지 않고 구멍이 뚫린 형태로 보안카드를 생성한다. 또한 제안하는 멀티채널 보안카드를 이용하여 금융 서비스를 제공할 경우 은행에서 사용자마다 다른 형태로 비밀정보가 숨겨진 보안카드를 제공함으로 악의적인 이용자가 보안카드 디자인을 유추하기 어렵게 한다. 이는 또 다른 채널인 동적 비밀번호 생성기에서 비밀번호 생성 시 사용자가 가지고 있는 물리적 보안카드의 공백부분에만 비밀번호를 생성하게 하므로 피싱, 파밍공격에 대해 강인한 특성을 가지게 된다.

Fig. 1. Proposed secure card design

이후 과정은 기존과 동일하게 사용자가 직접 전자금융을 이용하기위해 멀티채널 보안카드 중 물리적 보안카드의 일련번호를 등록하므로 온라인 뱅킹 서버는 미리 약속된 비밀번호 생성 프로세스와 일련번호를 이용하여 계산해 낼 수 있게 된다. 즉, 온라인 뱅킹 수행 시점에 사용자를 통해 입력되는 물리적 비밀카드 번호를 인터넷뱅킹서버가 계산을 통해 산출해 낸 보안카드 비밀 정보를 확인하여 입력 값을 검증하게 된다.

3.1.2 난수 생성기를 이용한 비밀번호 생성기

본 논문에서 제안하는 멀티채널 보안카드의 두 번째 채널은 사용자가 항상 휴대하고 있는 스마트폰이며 비밀정보를 제공하기위해서 비밀번호 생성 어플리케이션을 이용한다. 휴대폰을 통해 생성되는 보안카드 정보는 온라인 뱅킹 서버와 휴대폰이 초기에 상호간에 분배한 seed값을 통해 난수 값을 생성하는 기법을 취한다. 해당 seed값은 타임스탬프, 카운터 혹은 사전 정의된 비밀 키 값으로써 공격자가 seed값을 알지 못하면 보안카드를 생성할 수 없다. 먼저 보안카드 어플리케이션을 실행하게 되면 스마트폰에 사전에 정의된 사용자의 타임스탬프, 카운터, 비밀 키 값을 확인하게 되고 해당 비밀정보가 암호학적 보안 요건을 만족시키는 유사 난수 생성기 (Cryptographically Secure Pseudo- Random Number Generator)의 시드가 되어 난수 값을 생성하게 된다. 생성된 난수 값은 물리적 보안카드의 비밀번호가 표시되지 않는 위치에 출력되어 나타나도록 설계되었다. 난수생성기를 이용하여 생성된 화면과 물리적 보안카드와 겹쳐서 보안카드 전체정보를 완성하는데 사용되게 된다. 완성된 정보 중 사이트에서 요구하는 2개의 비밀정보는 사이트에 입력하게 되며 이러한 새로운 기법을 통해 인증 과정이 완성되

게 된다.

3.2 멀티채널 보안카드 구현

멀티채널 보안카드를 사용가능성을 시험해 보기위해 물리적 카드와 비밀번호 생성 어플리케이션을 구현해 보았다. 두 채널을 모두 이용하여 온전한 보안카드의 정보를 얻기 위해 물리적 보안카드를 비밀번호 생성 어플리케이션이 실행되어있는 스마트폰의 스크린에 올려서 보안카드와 휴대폰이 겹쳐서 나타나는 비밀정보를 확인할 수 있도록 한다.

3.1.3 대상 장비

해당 기법을 수행하기 위해서는 스마트폰의 스크린과 겹쳐서 정보를 얻어내는 방법으로써 현재의 스마트폰이 보안카드보다 커야 해당 기법이 적용가능하다.

Fig.2.와 같이 일반적인 스크린 크기를 가지는 갤럭시 S3 제품의 경우에도 보안카드에 비해 큰 화면을 제공한다. 따라서 보안카드를 휴대폰에 겹쳐서 새로운 정보를 생성해 내는 제안 기법은 범용적으로 거의 모든 휴대폰에 적용이 가능한 기술이다.

Table 1.은 현재 많은 스마트폰 사용자가 이용할 것이라 예상되는 모델의 스펙을 간략히 분석한 내용으로 모든 스마트폰이 제안하는 보안카드보다 훨씬 큰 스크린을 제공하며 이는 제안 기법의 적용에 문제가 없음을 의미한다.

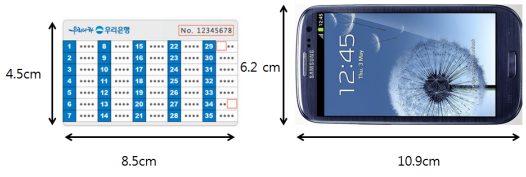

Fig. 2. Comparison of physical secure card and smartphone

Table 1. Specification of target devices

Galaxy S3	Galaxy S4	Galaxy S5	G pro
4.8 inch	5 inch	5.1 inch	5.5 inch

3.1.4 멀티채널 보안카드 구현 상세

제안하는 멀티채널 보안카드에서 물리적 보안카드의 디자인은 비밀정보가 있는 부분에 빈 공간을 만들고 스마트폰의 어플리케이션을 통해 비밀정보가 물리적 보안카드 공간 사이로 비치는 부분을 종합하여 온전한 보안카드를 생성하도록 디자인되었다.

Fig. 3.에서 실제 제작한 카드의 형태를 확인할 수 있는데, 임의의 난수들이 배열된 기존의 보안카드와 비슷한 형태로, 카드 상의 공백은 어플리케이션에서 표시되는 난수를 확인하기 위한 것이다. 기존의 보안카드와 유사하게 6개의 열이 한 묶음으로 앞의 2개의 열은 지시번호이고 뒤의 4개의 열이 난수가 출력되어 있는 부분이다. 구멍이 뚫려있는 부분은 어플리케이션에서 생성된 난수를 확인할 수 있는 일종의 창이다. 이 부분에 어떤 번호가 나타날 것인지는 스마트폰에서 실행되는 비밀번호 생성 어플리케이션에 달려 있으므로, 물리적 보안카드를 분실하여도 전체의 보안카드 비밀정보를 알아내기 어렵다. 현재는 구현 예시로써 적은 수의 비밀정보 공백만이 생성되어있지만 실제 구현에서는 약 50%의 공백이 불규칙적으로 생성되는 형식으로 구현될 것이다. 본 논문의 구현 예에서는 보안성을 보다 향상시키기 위해 보안카드의 값을 포함한 인덱스의 값도 동적으로 생성이 가능하도록 물리적 보안카드에서 공백으로 표현하였다.

Fig.4.은 스마트폰에서 비밀번호 생성 어플리케이션을 나타낸 그림으로 어플리케이션의 동작 모습을 확인할 수 있다. 비밀 번호 어플리케이션은 구동이 된 즉시 난수표의 크기만큼 난수를 생성하는데, 이 구현 예시에서는 난수표의 크기를 40으로 정했다. 40개의 인덱스는 Fig.4.의 좌측 두 개의 열과 같이 임의의 자리로 배치가 된다. 공백 배치된 부분에 따라서 난수가 생성되며, 새로이 난수를 생성하고 배치

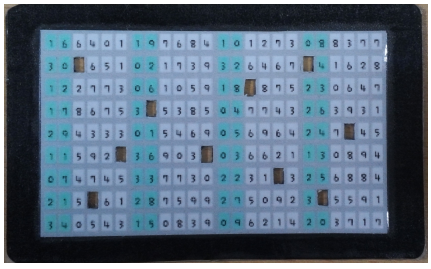

Fig. 3. Proposed phisical card

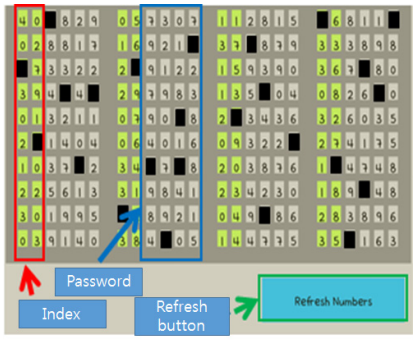

Fig. 4. Application working process

하고자 한다면 화면 하단에 'Refresh Numbers'를 눌러서 새로운 난수를 수행할 수 있다. 난수가 표시되는 위치는 물리적 보안카드의 공백부분과 동일한 위치이며 물리적 보안카드의 숫자가 표시되는 부분은 비밀번호 생성 어플리케이션에서 공백으로 표시된다. 이렇게 비밀번호 생성 어플리케이션에서 비밀번호가 공백으로 표시 부분은 물리적 보안카드의 비밀정보 표시부분과 일치하게 됨으로 사용자들은 동적 비밀번호 표시 패턴을 확인함으로 현재 진행 중인 전자금융 거래사이트가 진짜인지 공격자에 의해 위조된 사이트인지 확인 할 수 있다. Fig.5.에서는 실제로 제작한 또 다른 물리적 카드와 비밀번호 생성 애플리케이션 동작 모습을 나타낸다. 물리적 보안카드의 임의로 만들어진 공백을 통해 사용자가 비밀번호 생성 어플리케이션을 실행시켜 겹치게 되는 경우 해당 공백을 통해 어플리케이션의 난수 값이 나타나게 된다.

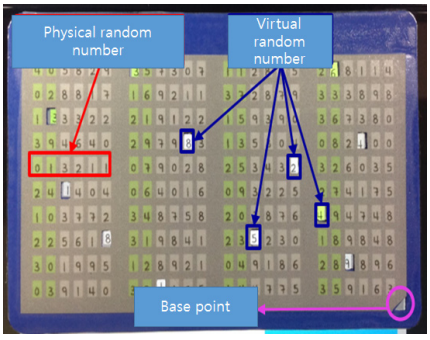

Fig. 5. Proposed secure card

IV. 평가

본 논문에서 제안한 난수생성기를 이용한 멀티채널 보안 카드를 평가하기 위해 금융보안연구원의 전자금융 신 인증기술 연구보고서 [5]에서 사용된 인증기술검토방법을 이용하며 검토항목은 보안성과 편의성, 적용성의 측면에서 제안 모델을 평가한다.

4.1 보안성

제안하는 알고리즘의 가장 큰 이점은 기존 물리적 보안카드에 집중되어 있던 비밀정보를 다른 채널로 분산시킴으로써 모든 인증 채널을 확인하지 않는 경우에는 공격자가 비밀 번호를 온전히 파악할 수 없다. 제안하는 방법과 같이 두 개의 인증채널 사용하는 경우 물리적 보안카드가 유출되어도 공격자는 물리적 보안카드에 포함된 50%의 정보만을 가지고 사용자의 인증을 시도하게 된다. 하지만 나머지 50%의 정보를 확실하게 알지 못하는 경우에는 공격이 성공할 수 없다. 이와 반대로 다른 채널(스마트폰)이 유출된 경우에도 동일하게 물리적 보안카드의 정보를 확인하지 못하면 공격을 성공하는 것이 불가능하다. 이는 공격자로 하여금 두 개의 보안카드 채널을 모두 확보하는 것을 어렵게 함으로 보안카드 비밀정보를 얻는 것이 어렵기 때문이다. 이러한 특징으로 인해 기존의 기법과 비교해 보안성이 강화되어 보안카드 유출로 인한 문제를 방지할 수 있다. 뿐만 아니라 스마트폰을 이용하는 채널의 경우 보안카드비밀전호 값이 보안카드 입력요구가 발생할 때마다 변경되기 때문에 한번 휴대폰의 가상 보안카드가 노출이 되는 경우에도 해당 정보는 한번만 전자금융 거래에서만 유효하고 그 다음 세션에서는 사용이 불가능하다. 또한 화면에 생성되는 보안카드 비밀번호 표시 패턴은 사용자마다 다르게 표시되므로 피싱 및 파밍 수법에 강인한 특성을 가지게 된다. 따라서 기존에 비해 높은 보안성 제공이 가능한 동적 보안 카드 모델 구현이 가능하다.

4.2 편의성

기존의 보안카드는 지갑이나 자신이 생각하는 안전한 장소에 보관하여 온라인 결제 상황 발생 시 꺼내어 보게 되는 방식을 취한다. 제안하는 기법의 경우 보안카드를 꺼내어 다른 채널(스마트폰)에 보안카드의 비밀정보와 동시에 확인하는 과정이 추가적으로 수행되게 된다. 따라서 제안하는 방법은 기존의 기법에 비해 다른 채널을 통한 확인과정의 부하가 발생하게 되지

만 인증에 필요한 시간이 약 10~15초정도이므로 사용상의 편의성을 최대한 확보한 방법이다.

4.3 적용성

제안하는 난수생성기를 이용한 멀티채널 보안카드를 기존의 온라인 뱅킹 및 모바일 뱅킹에 적용하기 위해서는 물리적 보안카드 디자인 변경과 기존 프로세스에서 스마트폰을 이용하는 비밀번호 확인 채널에 대한 개발이 필요하다. 하지만 제안하는 방법의 경우 기존 전자금융거래 절차에서 보안카드를 확인하는 부분만 변경되므로 전체 시스템에서 수정해야할 부분이 많지 않다. 또한 새로운 시스템을 적용할 때 사용자가 부담해야하는 비용은 발생하지 않으며, 보안카드 비밀번호 생성 어플리케이션 개발 및 기존 시스템 수정에 필요한 금액만 발생하며 유지보수에도 큰 비용이 들지 않으므로 적은 비용으로 보안성이 향상된 새로운 인증방법을 도입할 수 있다.

4.4 SMS를 통한 멀티채널 인증과의 비교

SMS를 통한 멀티채널 인증기법은 사용자가 원하는 서비스에 대한 인증 요청 시 자신의 핸드폰을 통해 인증코드를 전송받게 되고 이를 다른 기기의 인증란에 입력함으로써 인증이 완료되는 기법이다. 해당 기법은 새로운 채널을 통한 암호화를 위해 SMS 혹은 다른 네트워크 채널을 사용해야하는 문제점이 발생하며 이는 새로운 보안취약점을 야기한다. 현재 SMS 전송 시 메시지에 대한 수취인과 송신자 정보 변조가 가능하다. 이와는 달리 제안하는 기법은 SMS 혹은 다른 통신 채널을 사용하지 않으므로 보안취약성의 범위가 줄어드는 장점을 가진다. 또한 SMS를 통한 멀티 채널 인증 시 기본적으로 최대 3분 정도의 시간 동안 인증코드를 기다리게 된다. 이는 사용자에게 멀티채널을 통한 인증 시 대기시간을 증가시켜 인증에 걸리는 전체 시간을 증가시키는 문제점을 가진다. 이와는 달리 제안하는 기법은 서비스 사용을 위해 접속한 사이트 혹은 앱 상에서 멀티인증이 되는 형식으로써 보다 빠르고 직관적으로 안전성을 향상시키는 장점을 가진다.

V. 결 론

본 논문에서는 기존의 물리적 보안카드를 분실하여 노출될 수 있는 비밀정보의 양을 50%로 줄이는 기법을 제안한다. 본 제안은 누구나 가지고 있는 스마트폰을 통한 가상의 보안카드 매칭 정보를 생성하여 물리적 정보와 같이 제공함으로써 보다 복잡도가 높은 보안카드의 설계가 가능하다. 또한 정적인 기존 보안카드와는 달리 동적으로 보안카드 구성이 가능한 장점을 가진다. 이는 동적 보안정보는 노출되더라도 해당 세션이 지나면 사용이 불가능하다는 것을 의미한다. 본 제안기법은 실제로 구현 및 테스트되어 실용도 측면에서 높은 편의성과 보안 강도가 제공됨을 확인하였다.

References

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

[2] Park Younglok, Son Jinwoo, Shin Seonho and Yoon Myungkeun, ″Methods for Multi-channel based Financial Input,″ Review of KIISC, Vol.23 no.1, pp. 9-17, Feb 2013.

[3] Jin Seungman, ″Online Authentication System with Smartphone Technology,″ Review of KIISC, Vol.23 no.1, pp 18-27, Feb. 2013.

[4] Park Jinkyu and Lee Jungho, “Miss-type-proof based Techniques to Prevent from Phising and Phaming,” Review of KIISC, Vol.23 NO.6, Dec. 2013.

[5] Financial Security Agency, “Online Banking Reports on Authentication,” 2011.

〈저자소개〉

서 화 정 (Hwa-jeong Seo) 종신회원
2010년 2월: 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월: 부산대학교 컴퓨터공학과 석사 졸업
2012년 3월~현재: 부산대학교 컴퓨터공학과 박사과정
〈관심분야〉 정보보호, 암호화 구현, IoT

석 선 희 (Seon-hee Seok) 학생회원
2011년 2월: 부산대학교 컴퓨터공학과 학사 졸업
2011년 8월~2014년 1월: 삼성전자 근무
2014년 3월~현재: 부산대학교 컴퓨터공학과 석사과정

김 경 훈 (Kyoung-hoon Kim) 학생회원
2014년 2월: 부산대학교 컴퓨터공학과 학사 졸업
2014년 3월~현재: 부산대학교 컴퓨터공학과 석사과정

김 호 원 (Ho-won Kim) 종신회원
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