개인식별번호 입력 방식들에 대한 사용편의성 비교

Usability Comparison between PIN entry schemes

김창순, Chang Soon Kim*, 송정은, Jeong Eun Song**, 이문규, Mun-Kyu Lee***

요약

현금 인출기를 통해 돈을 인출할 때나 핸드폰의 잠금 설정을 할 때 사용하는 네 자리 숫자를 이용한 비밀 번호 또는 개인 식별번호 입력 방법은 일상생활에서 널리 사용되고 있다. 하지만 숫자를 직접 입력하는 현재의 방법은 shoulder surfing attack(SSA)에 안전하지 않다. 본 논문에서는 SSA에 안전하면서도 누구나 쉽게 사용할 수 있는 새로운 PIN(Personal Identification Number) 입력방법들을 제안하고, 이들 방법과 기존 방법의 안전성과 편의성을 비교한다.

Abstract

Four-digit PIN(Personal Identification Number) is a well-known user authentication method used for many applications including ATMs and mobile phones. However, it is vulnerable to shoulder surfing attacks(SSAs). In this paper, we present new PIN entry methods which are secure against SSA and easy to use. We compare the usability and security of these methods with those of the existing methods.

핵심어: shoulder surfing attack, Graphical password, Personal Identification Number(PIN)

본 연구는 지식경제부 및 정보통신연구진흥원의 IT핵심기술개발사업의 일환으로 수행하였음.[2008-F-045-01, 장애인 및 고령자를 위한 Digital Guardian 기술개발]

*주저자 : 인하대학교 컴퓨터 정보 공학부 석사과정 e-mail: oncelover@gmail.com

**공동저자 : 인하대학교 컴퓨터 정보 공학부 석사과정 e-mail: aboutucs@gmail.com

***교신저자 : 인하대학교 컴퓨터 정보 공학부 조교수; e-mail: mklee@inha.ac.kr

1. 서론

인터넷 등 정보통신기술의 발달로 정보 사회가 도래하면서 개인 정보의 유출과 오남용의 문제가 대두되고 있다. 따라서 정보 보호는 정보 사회에서 필수불가결한 요소로 자리잡았다. 현재 개인 정보를 보호하기 위해 널리 사용되고 있는 암호 방식 중 하나는 숫자 기반의 개인식별번호(Personal Identification Number:PIN)이다. PIN을 사용하는 대표적인 예로는 숫자를 비밀 번호로 사용하는 ATM(Automatic Teller Machine,현금 자동 인출기)이나 휴대 전화의 잠금장치, 디지털 도어락 시스템 등이 있다. 하지만 이러한 PIN 입력방식의 경우 사용자가 비밀 번호에 해당하는 숫자를 입력할 때 타인이 뒤에서 엿보거나 소형 카메라 등을 이용하여 입력하는 모습을 촬영한다면 비밀 번호가 쉽게 누출되는 단점이 있다[1,2]. 이와 같이 사용자의 정보를 어깨 너머로 훔쳐보는 공격을 Shoulder Surfing Attack(SSA)이라 한다. 본 논문에서는 기존의 PIN 입력방식의 약점을 보완하고 사용자의 편의성을 보장해주는 새로운 PIN 입력 방식을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 SSA에 강한 암호 입력 방법에 대해 기술한다, 3장에서는 본 논문에서 제안하는 SSA에 강한 새로운 PIN 입력 기법에 대해 설명하고 4장에서는 새롭게 제안하는 PIN 입력 기법에 대한 사용자 평가에 대해 기술한다. 마지막으로 5장에서는 결론을 맺고 향후 연구 방향에 대해 논의하도록 한다.

2. 관련 연구

본 장에서는 SSA에 강한 기존 암호에 대해 기술한다.

2.1 바이오 인식(Biometrics)

바이오 인식이란 특정 개인이 지닌 신체적 특징과 습관을 이용해 인증하는 방법이다. 흔히 우리가 알고 있는 지문, 홍채, 얼굴, 정맥 인식 등이 이에 속한다. 바이오 인식은 분실이나 도난의 위험이 적고 SSA에 강하다는 장점이 있지만 일반적으로 사용하는 문자나 숫자 기반의 암호보다 비용이 많이 든다는 단점이 있다. 또한 바이오 정보가 유출될 경우 더 이상 사용이 불가능하다는 치명적인 단점이 있다[3, 4].

2.2 그래픽 암호(Graphical Password)

사진이나 그림 등 이미지를 기반으로 한 암호들을 Graphical Password라고 한다[5]. Graphical Password들은 텍스트 기반의 암호에 비해 스파이웨어(spyware)나 키 로거(key logger)와 같은 공격에 강하다. Valentine이 제안한 PASS FACE scheme은 Graphical Password 중 하나의 예로 사람은 글이나 숫자보다 사람의 얼굴을 더 기억하기 쉽다는 기본 아이디어를 이용하여 만든 암호이다[6]. 사용자는 인증을 위해 사용될 얼굴 이미지들을 등록하고 자신이 등록한 이미지를 선택함으로써 합법적인 사용자인지 여부를 인증받을 수 있다. 하지만 이는 SSA에 취약하고 인증을 위해 모든 사용자들의 이미지를 저장하고 접근하기가 수월하지 않기 때문에 실생활에 적용하기 힘들다. 이처럼 기존의 Graphical Password를 이용하는 방법 중에서 SSA에 취약한 점을 보완하기 위해 새로운 방법들이 제안되었다.

Sobrado와 Birget는 2002년 SSA에 강한 Graphical Password scheme을 제안했다[5]. Sobrado등이 제안한 방법을 사용하기 위해 사용자는 먼저 인증에서 사용될 몇 가지 pass-object를 선택한다. 여기서 pass-object란 사용자가 임시로 선택한 객체를 의미한다. 그림 1은 Sobrado등이 제안한 Graphical Password 입력을 위한 화면을 나타낸다. 동그라미로 표시된 세 가지 이미지는 사용자가 등록 시 선택했던 pass-object를 의미하고, pass-object를 연결하여 얻어진 삼각형으로 표시된 영역은 인증을 위해 입력할 수 있는 영역을 의미한다. 사용자는 인증을 위해서 이 영역 안에 있는 임의의 pass-object를 선택하면 된다. 이 방법은 인증을 시도할 때마다 pass-object의 위치가 바뀌므로 입력하는 pass-object가 달라지기 때문에 SSA에 강하다. 하지만 인증을 위해 사용되는 pass-object들이 너무 많아 구별하기 힘들고 사용하기에 복잡하기 때문에 사용자가 인증을 위해 입력하는 시간이 오래 걸린다는 단점이 있다.

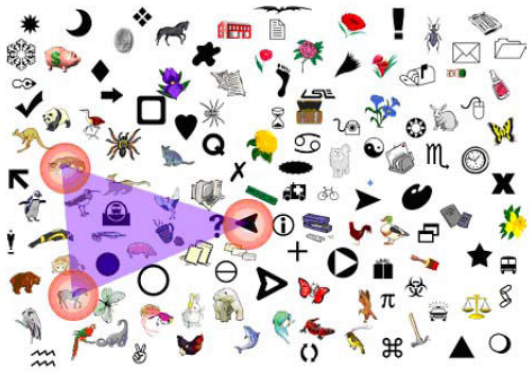

그림 1. Sobrado등이 제안한 SSA에 강한 Graphical Password

이와 비슷하게 2004년 Hong등은 SSA에 강한 방법을 제안하였다[7]. 그림 2는 Hong등이 제안한 Graphical Password 입력을 위한 화면을 나타낸다. 먼저 사용자는 인증을 위해 사용할 각 pass-object마다 고유의 문자 또는 숫자를 부여한다. 인증을 위해서는 그림 2와 같이 자신의 pass-object를 클릭하고 pass-object에 해당되는 고유 문자나 숫자를 오른쪽 아래 입력란에 입력한다. 예를 들어 사용자가 pass-object로 상자 그림, 스마일 그림, 핀 그림, 스프링 그림을 선택했다고 하자. 그리고 각 pass-object에 따라 상자 그림에는 문자열 a12를, 스마일 그림에는 문자열

c2를, 핀 그림에는 문자열 b2를, 스프링 그림에는 문자열 d32를 부여했다고 하자. 그러면 사용자는 인증을 위해 상자, 스마일, 핀, 스프링 그림을 차례대로 선택한 뒤 선택한 그림에 대응되는 문자열 즉 a12c2b2d32를 오른쪽 아래 입력란에 입력하면 된다. 하지만 이 방법은 사용자가 인증을 위해 기억해야할 정보들이 많고, spy ware와 key logger같은 기존의 text 기반의 암호가 갖는 약점을 갖는다는 단점이 있다.

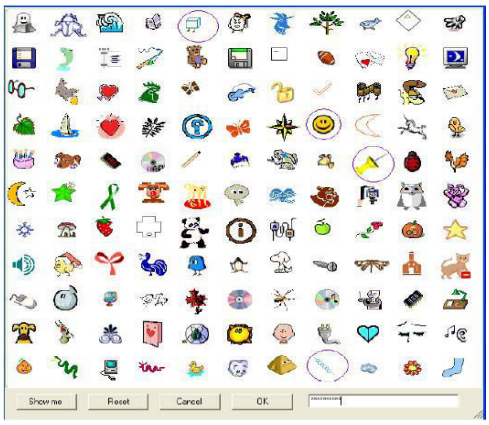

그림 2. Hong 등이 제안한 SSA에 강한 Graphical Password

Sobrado 등과 Hong 등이 제안한 방법들은 SSA에는 강하지만 인증을 위해 너무 많은 이미지들을 사용함으로써 실제 생활에 적용하기에 복잡하고 사용자의 편의성이 떨어진다는 문제점을 갖는다.

3. 새로운 PIN 입력 기법

2장에서는 SSA에 강한 텍스트 기반이 아닌 다른 암호들에 대해 기술하였다. 본 장에서는 현재 가장 일반적으로 사용되고 있는 텍스트 기반 암호 중에서도 특히 숫자를 이용하는 암호를 SSA에 강하면서도 편리하게 사용할 수 있도록 하는 새로운 입력 방법을 제안한다.

3.1 SIMPLE PIN ENTRY

본 절에서는 본 논문에서 제안하는 새로운 숫자 기반 암호의 입력 방법 중 첫 번째 방법인 SIMPLE PIN ENTRY에 대해 기술하도록 한다. 암호를 사용하기 위해 등록하는 절차는 기존의 숫자를 사용하는 암호의 등록 방법과 동일하게 사용하고자 하는 비밀 번호를 등록하면 된다. 설명의 편의를 위해 본 논문에서는 비밀 번호가 네 자리라고 가정하도록 한다. 그림 3은 비밀 번호를 입력하기 위한 화면을 나타낸다. 몇 번째 비밀 번호를 입력하는지 나타내는 단계표시가 있으며, 0부터 9까지 10개의 숫자와 10개의 pass-object가 있다. 여기서 pass-object란 사용자가 임시로 선택한 객체를 의미하며 본 논문에서는 간단한 도형으로 나타내었다. 또한 왼쪽과 오른쪽 버튼을 이용하여 pass-object를 이동시킬 수 있으며 확인 버튼을 통해 입력한다.

그림 3. SIMPLE PIN ENTRY

비밀 번호 입력으로 사용자를 인증하는 단계는 다음과 같다.

① 사용자는 10개의 pass-object 중 임의로 하나의 pass-object를 선택한다.

② 사용자는 왼쪽 혹은 오른쪽 버튼을 통해 자신의 비밀 번호의 첫 번째 숫자 밑으로 선택한 pass-object가 위치하도록 한 후 확인 버튼을 누른다.

③ 두 번째 단계에서는 첫 번째 단계에서 선택하였던 pass-object가 자신의 비밀 번호의 두 번째 숫자 밑으로 위치할 수 있도록 이동한 후 확인 버튼을 누른다.

④ 동일한 방법으로 세 번째, 네 번째 단계에서는 각각 자신의 비밀 번호의 세 번째, 네 번째 숫자 밑에 선택한 pass-object가 위치하도록 한다.

⑤ 사용자의 비밀 번호 밑에 동일한 pass-object가 위치하였을 경우 인증에 성공하고 그렇지 않은 경우 인증에 실패한다.

예를 들어, 사용자의 비밀 번호가 1234이고 사용자가 선택한 pass-object가 ♤라 하면, 인증과정은 그림 4와 같다. 사용자는 선택한 ♤가 비밀 번호의 첫 번째 자리 숫자인 1의 밑에 위치하도록 오른쪽 버튼을 두 번 누른다. 1 밑에 ♤가 위치하면 확인 버튼을 눌러 다음 단계로 이동한다. 이 과정을 공격자가 뒤에서 어깨 너머로 보거나 카메라를 이용해 촬영하더라도 사용자가 선택한 pass-object가 ♤라는 것은 알 수가 없다. 사용자는 두 번째 비밀 번호인 2를 입력하기 위해 새롭게 배치된 pass-object의 ♤가 2의 아래에 놓이도록 왼쪽 버튼을 두 번 누르고 확인 버튼을 누른다. 마찬가지로 세 번째 비밀 번호 3을 입력하기 위해 ♤가 3 아래에 놓이도록 왼쪽 버튼을 두 번 누르고 확인 버튼을 누른다. 마지

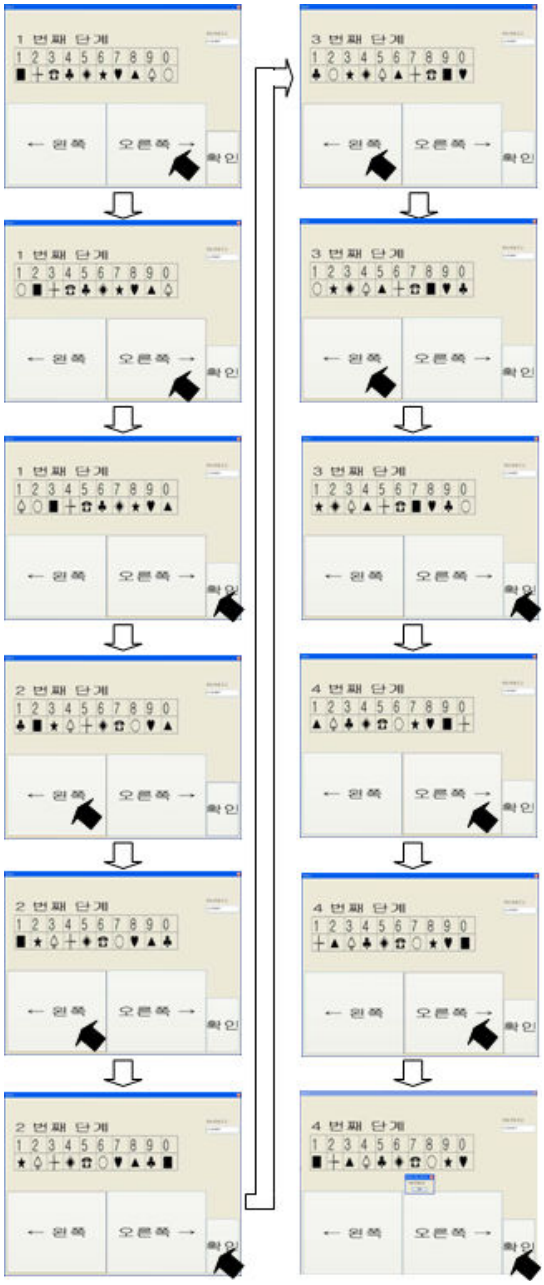

그림 4 인증 과정 예시

막으로 네 번째 비밀 번호 4를 입력하기 위해 오른쪽 버튼을 두 번 눌러 ♤가 4의 아래에 위치하게 이동시켜 확인 버튼을 눌러 인증을 종료한다.

본 논문에서 제안하는 SIMPLE PIN ENTRY 방법은 기존에 숫자를 입력하는 시스템에 적용이 가능하며 SSA에 강하다. 하지만 기존의 숫자를 입력하는 방법은 전수 조사 공격에 대해 10^4의 안전성을 갖는 반면 SIMPLE PIN ENTRY의 경우 10^3의 안전성을 갖는다. 따라서 3.2절에서는 보다 나은 안전성을 제공하기 위하여 SIMPLE PIN ENTRY을 변형시킨 MATRIX PIN ENTRY를 제시한다.

3.2 MATRIX PIN ENTRY

MATRIX PIN ENTRY는 SIMPLE PIN ENTRY의 첫 번째 단계에서 사용자가 임의로 pass-object를 선택함으로써 안전성이 낮아지는 문제를 보안한 방법이다. 그림 5는 MATRIX PIN ENTRY에서 사용할 pass-object들을 나타낸다. 행렬로 나타나는 pass-object들 중에서 사용자의 비밀번호의 첫 번째 숫자에 해당하는 행과 두 번째 숫자에 해당하는 열이 만나는 도형이 입력에서 사용될 pass-object가 된다. 인증을 위한 단계는 SIMPLE PIN ENTRY와 동일하게 pass-object를 비밀 번호의 각 자리 아래에 놓이도록 함으로써 진행된다. 예를 들어, 사용자의 비밀 번호가 1234라고 가정하면 사용자의 pass-object는 그림 5에 의해 ┼가 된다. 사용자는 인증을 위해 그림 4와 유사하게 첫 번째 단계에서는 ┼가 첫 번째 비밀 번호인 1의 아래에 위치하도록 버튼을 이용해 pass-object를 이동시킨다. 동일한 방식으로 각 단계에서 비밀 번호의 각 자리 수에 맞는 숫자 아래에 ┼가 놓이도록 이동시켜 비밀 번호를 입력하게 된다.

MATRIX PIN ENTRY는 SIMPLE PIN ENTRY와 달리 사용자의 비밀 번호에 따라 처음에 주어진 행렬에 의해 결정되는 pass-object를 사용하기 때문에 전수 조사 공격에 대해 10^4의 안전성을 갖는다.

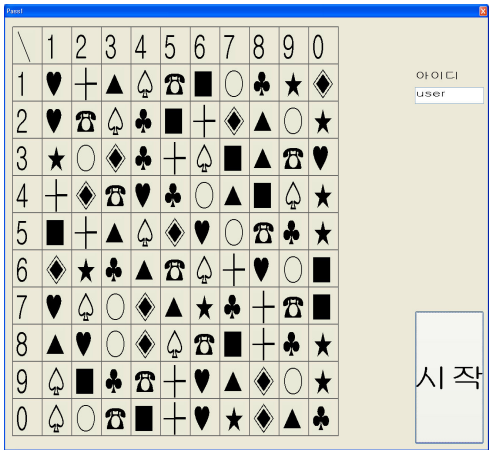

그림 5. MATRIX PIN ENTRY

4. 사용자 평가

4.1 평가 방법

본 논문에서 제안하는 PIN 입력기법을 평가하기 위해 모의실험 및 설문 조사를 하였다. 우리가 제안한 방법은 보편적인 사용을 목표로 하고 있다. 대체로 젊은 사람들보다 고령자들이 새로운 방식에 적응하기 어렵다고 예상하였기 때문에 61~80세 노인 38명을 대상으로 실험을 실시하였다. 이 중 10명은 경한 기억 장애나 인지 기능 장애를 갖고 있

는 경증 치매 환자를 대상으로 실험하였다. 평가를 위해 기존의 숫자를 직접 입력하는 방법과 그래픽 기반 방법인 PASS FACE[6], 그리고 본 논문에서 제안하는 SIMPLE PIN ENTRY, MATRIX PIN ENTRY 네 가지 방법을 실험하였다. PASS FACE의 경우 그림 6과 같이 미리 등록된 15명 중 4명을 선택하여 비밀 번호로 사용하도록 하였다. 실험 절차는 다음과 같다.

① 사용자에게 먼저 각 입력 방법에 대해서 설명한다.

② 사용자가 각각의 방법으로 비밀 번호를 입력해 본다.

③ 각 입력 방법에 대한 설문에 응답한다.

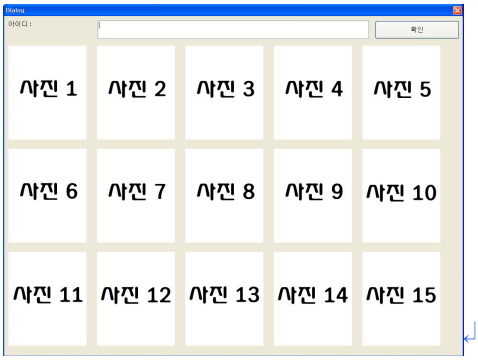

그림 6. 변형된 PASS FACE Scheme.

4.2 결과 분석

설문은 기존의 숫자를 직접 입력하는 방법의 안전성에 대한 질문과 기존 숫자를 입력하는 방법, PASS FACE, SIMPLE PIN ENTRY , MATRIX PIN ENTRY 등 네 가지 입력 방법에 대한 안전성 및 실생활에서의 적용 가능성 여부를 묻는 질문으로 구성되어 있다. 표 1은 실험 대상을 환자군, 정상군, 전체로 나눠 설문 결과를 분석한 결과로 대상군에 따른 각 Scheme별 만족도를 나타낸다.

4.2.1 정상군

정상군에 속하는 실험 참가자 중 약 71.4%의 사람들이 기존의 숫자를 입력하는 암호보다 좀 더 안전성이 높은 패스워드 시스템이 필요하다고 응답했다. 설문 결과 각 Scheme들 중 가장 안전하다고 생각되는 암호는 SIMPLE PIN ENTRY로 약 85.8%의 사람들이 안전하거나 매우 안전하다고 응답하였고 92.9%의 사람들이 이 Scheme이 편리하였다. 하지만 사람들이 가장 선호하는 방법은 MATRIX PIN ENTRY scheme으로 안전하면서도 편이성을 보장해주기 때문이라고 대답하였다. MATRIX PIN ENTRY scheme을 선호하는 이유에 대한 기타 의견으로는 실험 시 로그인 시간이 길어서 편이성이 떨어져 보이지만 반복적인 훈련을 통해 빈번히 사용하게 되면 실생활에서 편리하게 사용가능 할 것 같다고 대답하였다.

4.2.2 환자군

환자군에 속하는 실험 참가자 중 약 70%의 사람들이 기존의 암호보다 좀 더 안전성이 높은 패스워드 시스템이 필요하다고 응답했다. 설문 결과 각 Scheme들 중 가장 안전하다고 생각되는 암호는 MATRIX PIN ENTRY와 SIMPLE PIN ENTRY 두 개로 모두 약 80%의 사람들이 안전하거나 매우 안전하다고 응답하였고 SIMPLE PIN ENTRY은 90%의 사람들이 편리하다고 응답을 하였다. 그에 비해서 MATRIX PIN ENTRY는 50%의 사람들만이 편리하다고 답하였다. 본 논문에서 제안하는 새로운 Scheme에 대한 전반적인 평가에 대해 현재 사용하고 있는 숫자를 입력하는 방법과 달라 익숙하지 않고 복잡하여 실생활로의 적용이 힘들 것이라는 의견이 있었다. 기타 의견으로 안전성 측면에서 볼 때 MATRIX PIN ENTRY가 더 안전해 보이지만 편의성을 고려하였을 때 SIMPLE PIN ENTRY가 좀 더 편리하면서도 안전하다고 응답하였고 50% 이상의 사용자들이 전체적인 안전성과 편리성을 고려하였을 때 SIMPLE PIN ENTRY 방법이 가장 좋다고 대답하였다.

4.2.3 전체

정상군과 환자군을 포함하는 전체 실험 참가자 중 약 71%의 사람들이 기존의 암호보다 좀 더 안전성이 높은 패스워드 시스템이 필요하다고 응답했다. 각 Scheme들 중 가장 안전하다고 생각되는 암호는 SIMPLE PIN ENTRY로 약 84.2%의 사람들이 안전하거나 매우 안전하다고 응답했고 92.1%의 사람들이 편리하다고 응답을 하였다. 그리고 가장 사람들이 가장 선호하는 Scheme은 SIMPLE PIN ENTRY로 36.8%의 사람들이 가장 좋다고 대답하였고, MATRIX PIN ENTRY는 34.2%의 사람들이 좋다고 대답하였다. 결과적으로 안전성과 편리성을 고려하였을 때 70%의 사람들이 본 논문에서 제안하는 방법을 선호하고 있음을 알 수 있다.

표 1. 각 Scheme의 안전성에 대한 만족도 (단위 %)

		5 (매우그렇다)	4	3	2	1 (전혀 아니다)
안전한 방법 필요성	정상군	**71.4**	**0**	14.3	0	14.3
	환자군	**70**	**0**	0	0	30
	전체	**71**	**0**	19.4	0	9.6
PASS FACE	정상군	**3.6**	**50**	14.3	28.5	3.6
	환자군	**0**	**50**	30	20	0
	전체	**2.6**	**50**	18.5	26.3	2.6
SIMPLE PIN ENTRY	정상군	**57.1**	**28.7**	0	7.1	7.1
	환자군	**60**	**20**	10	10	0
	전체	**57.9**	**26.3**	2.6	7.9	5.3
MATRIX PIN ENTRY	정상군	**46.4**	**39.3**	0	10.7	3.6
	환자군	**60**	**20**	10	10	0
	전체	**50**	**34.3**	2.6	10.5	2.6

표 2. 각 Scheme의 편의성에 대한 만족도 (단위 %)

		Yes	모르겠다	No
PASS FACE	정상군	**64.3**	3.6	32.1
	환자군	**50**	10	40
	전체	**60.5**	5.3	34.2
SIMPLE PIN ENTRY	정상군	**92.9**	0	7.1
	환자군	**90**	0	10
	전체	**92.1**	0	7.9
MATRIX PIN ENTRY	정상군	**78.6**	17.8	3.6
	환자군	**50**	10	40
	전체	**71.1**	5.3	23.6

표 3. 각 Scheme에 대한 선호도 (단위 %)

대상군	정상군	환자군	전체
PASS FACE	25	30	26.4
SIMPLE PIN ENTRY	32.1	50	36.8
MATRIX PIN ENTRY	39.3	20	34.2
모르겠다	3.6	0	2.6

5. 결론

본 논문에서는 숫자 기반의 암호시스템에서 좀 더 안전하게 비밀 번호를 입력할 수 있는 SSA에 강한 PIN 입력기법을 제안하였다. 사용자 평가를 통해 사용자들이 기존의 숫자를 직접 입력하는 방법보다 안전한 새로운 입력 방법의 필요성을 인식하고 있다는 것을 알 수 있었고 본 논문에서 제안하는 SIMPLE PIN ENTRY , MATRIX PIN ENTRY가 실제 생활에도 적용 가능함을 확인하였다.

본 논문에서는 고령자만을 대상으로 사용자 평가를 실시하였지만 이후에는 연령대 별로 사용자 평가를 확대 실시하여 결과를 반영할 것이다.

참고문헌

[1] R. Anderson, "Why cryptosystems fail" In proc. 1st ACM Computers and Communications Security Conference. Nov, 1993.

[2] C. Weinstrock, “ATM fraud,” May 1987 http://catless.ncl.ac.uk/Risks/4.86.html#subj1.1

[3] K. Gilhooly, "Biometrics: Getting Back to Business," Computerworld, May 9, 2005.

[4] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 33, pp. 168–176, 2000.

[5] X. Suo, Y.Zhu, G.S.Owen "Graphical Passwords:A Survey", Annual Computer Security Applications Conference 2005.

[6] T. Valentine, "An evaluation of the passface personal authentication system," Technical Report, Goldsmiths College, University of London 1998.

[7] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware,"in Proceedings of International conference on security and management. Las Vegas, NV, 2004.