情報保護學會論文誌
第20卷 第3號, 2010. 6

모바일 환경에서 엿보기 공격에 강한 패스워드 입력방법*

김 창 순,[1†] 윤 선 범,[2] 이 문 규[1‡]
[1]인하대학교, [2]한국과학기술연구원

Shoulder-Surfing Resistant Password Input Method for Mobile Environment*

Chang Soon Kim,[1†] Sun-Bum Youn,[2] Mun-Kyu Lee[1‡]
[1]Inha University, [2]Korea Institute of Science and Technology

요 약

모바일 기기의 보편화와 다양한 종류의 모바일 기기들의 등장에 따라 각종 모바일 서비스들이 제공되고 있다. 이런 모바일 서비스가 늘어나면서 문자메시지, 사진 및 동영상, 주소록, 이메일, 공인인증서 및 기타 각종 개인 정보 등과 같이 단말기에 저장되는 사용자의 정보 또한 다양해지게 되었다. 모바일 기기는 분실 및 도난이 용이하기 때문에 이런 개인정보를 보호하는 사용자 인증이 매우 중요하나, 현재 보편적으로 사용되는 개인식별번호 입력 방법 또는 패스워드 입력 방법은 엿보기 공격(Shoulder Surfing Attack: SSA)에 안전하지 않기 때문에 공격자는 쉽게 사용자의 정보를 얻을 수 있다. 기존에 SSA를 막기 위한 방법들이 제안되어 왔으나 사용 편의성이 떨어지고 모바일 환경에서 사용하기 힘들다. 이에 본 논문에서는 모바일 환경에서 SSA에 안전하면서도 사용자 편의성이 뛰어난 새로운 패스워드 입력 방법을 제안한다. 또한 기존 방법들과의 비교 및 사용자 실험을 통하여 다양한 공격에 대한 안전성 및 사용편의성을 보인다.

ABSTRACT

The advent of various mobile devices and mobile services has caused diversification of information stored in a mobile device, e.g., SMS, photos, movies, addresses, e-mails, digital certificates, and so on. Because mobile devices are lost or stolen easily, user authentication is critical to protect the information stored in mobile devices. However, the current user authentication methods using Personal Identification Numbers (PINs) and passwords are vulnerable to Shoulder Surfing Attacks (SSAs), which enables an attacker to obtain user's information. Although there are already several SSA-resistant authentication methods in the literature, most of these methods lack of usability. Moreover, they are not suitable for use in mobile devices. In this paper, we propose a user friendly password input method for mobile devices which is secure against SSA. We also perform user tests and compare the security and usability of the proposed method with those of the existing password input methods.

Keywords: Password, Personal Identification Number, Shoulder Surfing Attack, Mobile Phone

I. 서 론

모바일 기기 사용자들이 증가함에 따라 사용자 편의를 위해 모바일 기기를 이용한 모바일 뱅킹 서비스, 모바일 웹 브라우저를 이용한 웹 서핑 등 다양한 서비스들이 제공되고 있다.

이런 모바일 기기들에는 사용자의 신상정보, 금융정보, 사진, 동영상과 같은 민감한 정보뿐만 아니라 기업 기밀과 같은 중요한 정보들이 저장되어져 있다. 공격자는 바이러스, 악성 프로그램, 스파이웨어 등과 같은 다양한 위험요소를 이용하여 공격 할 수 있다. 하지만 이러한 위험 요소는 안티 바이러스 프로그램,

접수일(2009년 12월 21일), 게재확정일(2010년 3월 10일)
* 이 논문은 인하대학교의 지원에 의하여 연구되었음.
† 주저자, oncelover@gmail.com
‡ 교신저자, mklee@inha.ac.kr

모바일 데이터 필드의 파일 암/복호화, 코드 사이닝(Code Signing)과 같은 다양한 방법으로 어느 정도 해결될 수 있다.

한편 모바일 기기는 분실 및 도난이 빈번하다는 위험성이 있는데 이때 사용자의 개인정보를 보호하기 위해서 사용자는 사용자 인증을 이용한다. 모바일 기기에서 사용자 인증을 하기 위해 널리 사용되는 방법으로는 텍스트 기반의 패스워드, 숫자 기반의 개인식별번호(Personal Identification Number: PIN), 그 외 지문인식 방법 등이 있다. 그러나 지문인식 방법과 같은 바이오 인식 기법은 별도의 장치가 필요하고 만약 바이오 정보가 노출이 되어도 이 정보를 수정하기 어렵다는 단점이 있다. 텍스트 기반의 패스워드 또는 숫자 기반의 개인식별번호는 손쉽게 인증을 수행할 수 있다는 장점에도 불구하고, 사용자가 패스워드를 입력 할 때 공격자가 어깨 너머로 몰래 엿보거나 소형 카메라 등과 같은 장치를 이용하여 패스워드를 입력하는 모습을 촬영한다면 사용자의 패스워드를 쉽게 얻을 수 있는 치명적인 약점이 있다. 이와 같이 사용자의 정보를 어깨 너머로 훔쳐보는 공격을 Shoulder surfing attack (SSA)이라 하는데, 그래픽적인 요소를 이용하여 이와 같은 공격에 안전하면서도 사용자들에게 편의성을 제공하기 위한 연구가 다양하게 진행 중이다[1-5]. 그러나 현재 진행되고 있는 그래픽 기반의 패스워드는 사용자들에게 충분한 안전성과 편의성을 제공해 주지 못하고 특히 모바일 기기에서는 사용하기 부적합하다는 문제점이 있다.

본 논문에서는 기존의 패스워드 입력 방법의 약점을 보완하고 사용자에게 어느 정도 편의성을 보장해주는 세 가지의 새로운 패스워드 입력 방법을 제안한다. 첫 번째 입력 방법은 음성 등 별도의 안전한 채널을 이용하여 패스워드를 입력하는 방법이고 두 번째 방법은 패스워드 중복을 이용하여 인증하는 방법이다. 마지막 방법은 이 두 가지 방법을 복합하여 인증하는 방법이다. 제안한 방법들은 모바일 장치의 작은 화면 표시 공간에도 사용가능하다는 장점이 있고, 또한 텍스트 패스워드를 이용하는 기존의 인증 방법과 호환이 가능하며 기존 방법들에 비해 안전하고 편리하다. 본 논문에서는 제안한 방법과 이전 방법의 안전성과 편의성을 비교하였으며, 그 결과 기존의 방법보다 제안 방법이 SSA에 강하고 안전성과 편의성 모두를 고려하였을 때 사용자들이 제안 방법을 더 선호함을 보였다.

본 논문의 구성은 다음과 같다. 2장에서는 SSA를 고려한 기존의 다양한 패스워드 입력 방법에 대해서 기술한다. 3장에서는 본 논문에서 제안하는 SSA에 강한 새로운 패스워드 입력방법에 대해 설명한다. 4장에서는 제안한 새로운 입력방법의 안전성 분석을 하고 5장에서는 사용자 평가 결과를 제시한다. 마지막으로 6장에서는 결론을 맺고 향후 연구 방향에 대해 논의하도록 한다.

II. SSA에 강한 그래피컬 패스워드

대부분의 기존 연구들은 SSA를 방지하기 위해 그래픽적인 요소를 이용하고 있다. 이렇게 사진이나 그림 등 그래픽적인 요소를 기반으로 한 패스워드를 그래피컬 패스워드라고 한다. 이런 그래피컬 패스워드는 사람들이 글이나 숫자보다 사진이나 그림 같은 이미지를 더 쉽게 기억한다는 기본 아이디어에 기반하고 있으며, 일반적인 텍스트 기반의 패스워드에 비해 스파이웨어(Spyware)나 키 로거(Key Logger)와 같은 공격에 강하다는 추가적인 장점이 있다[6]. 본 장에서는 SSA에 강한 기존 방법들 중 대표적인 세 가지 방법에 대해 언급하겠다.

2.1 CONVEX HULL CLICK SCHEME[1]

기존의 패스워드로 사용되는 글이나 숫자 대신 pass-icon이라는 icon을 패스워드로 이용하여 인증

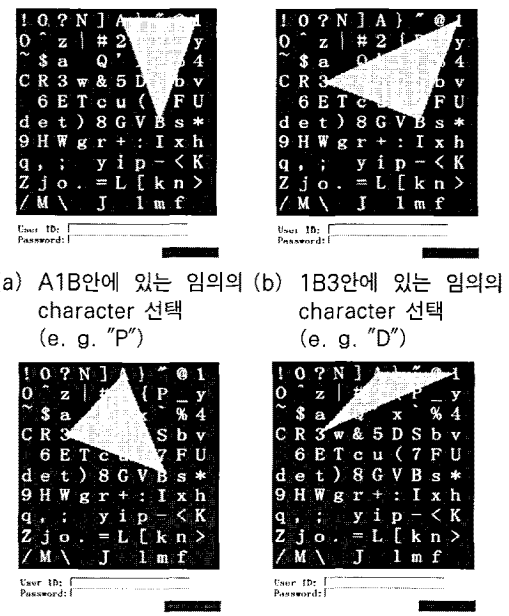
[그림 2] Pass-icon[1]

[그림 3] CONVEX HULL CLICK SCHEME을 이용한 인증 방법[1]

하는 방법이다. 사용자는 등록 단계에서 자신의 패스워드로 이용될 [그림 1]과 같은 pass-icon들을 선택한다. 인증 단계에서는 [그림 2]와 같이 사용자가 사전에 등록한 pass-icon으로 생성되는 가상의 다각형 영역에 속하는 icon을 클릭하여 사용자를 인증하게 된다. 이 방법은 세션 간 교차 공격(Intersection Attack)으로 인하여 SSA를 하게 되는 경우 사용자의 패스워드를 유추 할 수 있다. 또한 기존의 텍스트 기반의 패스워드와 호환이 되지 않아 실생활에 사용하기에는 많은 추가적인 비용이 들고, 인증 화면에서 pass-icon을 찾아 가상의 다각형을 구성하는 과정이 쉽지 않으므로 사용 편의성이 떨어진다. 더욱이 모바일 장치와 같은 작은 디스플레이를 가진 장치에 사용하기에는 다소 무리가 있다는 단점이 있다.

2.2. S3PAS[2]

S3PAS(A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme) 방법은 CONVEX HULL CLICK SCHEME과 비슷하지만 기존에 사용되었던 문자와 숫자 기반의 패스워드를 그대로 이용 할 수 있다는 장점이 있다. 이 방법의 등록 과정은 기존에 사용되었던 문자와 숫자 기반의 패스워드 방법과 동일하며, 인증 단계에서는 각 패스워드 글자들로 생성된 가상의 삼각형 영역에 속하는 임의의 문자를 마우스나 키보드로 입력하여 사용자 인증을 수행한다. 예를 들어 비밀번호가 A1B3이라고 하면 [그림 3]과 같이 삼각형 'A1B', '1B3', 'B3A', '3A1'에 대해서 수행하여 인증 가능 하다. 이 방법은 CONVEX HULL SCHEME과 마찬가지로 모바일 환경에서 사용하기에 다소 무리가 있고 교차 공격(Intersection Attack)으로 쉽게 패스워드를 유추 할 수 있다. 또한 삼각형이 만들어지는 크기에 의하여 무작위로 입력할 경우 인증될 확률이 다른 기법들에 비해 높다는 단점이 있다.

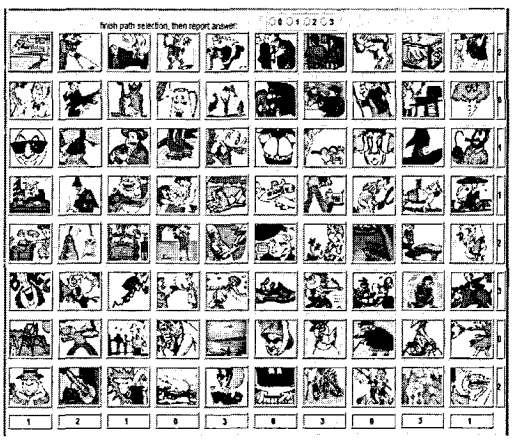


(a) A1B안에 있는 임의의 character 선택 (e. g. "P")
(b) 1B3안에 있는 임의의 character 선택 (e. g. "D")
(c) B3A안에 있는 임의의 character 선택 (e. g. "5")
(d) 3A1안에 있는 임의의 character 선택 (e. g. "2")

[그림 3] S3PAS를 이용한 인증 방법[2]

2.3 길 찾기 방법[3]

사용자는 등록 단계에 자신의 패스워드로 사용할 임의의 그림들을 고른다. 인증 단계에서는 [그림 4]와 같이 주어진 이미지의 가장 왼쪽 윗부분 에서부터 시작하여 화면의 오른쪽 또는 아래쪽으로 이동하는데, 현재 위치의 이미지가 사용자가 선택했던 패스워드에 해당하는 이미지라면 아래쪽으로 이동하고 아니라면 오른쪽으로 이동한다. 이를 반복하여 오른쪽 끝이나 아래쪽 끝에 도착한 경우 해당되는 숫자를 입력하여 사용자를 인증하는 방법이다. 이 방법도 앞서 설명한 방법들과 마찬가지로 기존의 텍스트 기반의 패스워드와 호환이 되지 않아 실생활에 사용하기에는 많은 추가적인 비용이 들고 인증을 위한 시간이 오래 걸린다



[그림 4] 길 찾기 방법을 이용한 인증[3]

는 단점이 있다. 또한 모바일 장치와 같은 작은 디스플레이 장치를 가진 장치에 사용하기에는 다소 무리가 있으며, 안전성 측면에서도 이미 [4]와 같은 공격이 알려진 바 있다.

III. 제안하는 방법

2장에서 나열된 SSA 방지 방법들은 공통적으로 사용자가 계산 또는 조작해야 할 정보가 많고 인증에 요구되는 시간이 길어 사용 편의성이 현저히 떨어진다는 단점이 있다. 또한 본 논문에서 고려하고 있는 대상인 모바일 장치의 경우 디스플레이 영역이 매우 제한적이므로, 인증을 위해 다양한 이미지를 한 화면에 표시해야 하는 2장의 방식들은 사용이 거의 불가능하다. 이에 본 장에서는 이러한 문제점들을 해결하는 동시에 기존의 텍스트 또는 숫자 기반 패스워드와 호환 가능한 새로운 세 가지 패스워드 입력 방법을 제안한다.

설명의 편의상 이 장에서는 패스워드의 개별 문자가 알파벳 26글자 및 숫자 10개의 36개 중 하나인 경우의 예를 보이고 있으나, 제안하는 방법들은 특수기호 등을 포함한 더 많은 문자를 포함하는 경우에도 같은 방식으로 적용될 수 있다.

3.1 안전한 별도 채널을 이용한 패스워드 인증 방법 (Secure Channel Scheme)

패스워드 기반의 인증 방법에서는 일반적으로 사용자와 기기 간에 패스워드 정보가 미리 공유되어 있고 사용자가 이를 올바로 입력할 수 있는지를 테스트함으로써 인증이 이루어진다. 한편 매 인증 세션마다 기기가 사용자에게 랜덤한 챌린지를 주고 사용자가 이 챌린지와 패스워드를 결합하여 적절한 응답을 하도록 하면 같은 패스워드에 대해서도 매번 사용자 응답이 달라지므로 replay attack에 대한 안전성을 향상시킬 수 있다. 그러나 공격자가 SSA를 통해 챌린지와 사용자 응답을 모두 관찰한다면 패스워드에 대한 정보가 누출될 수 있다는 문제점이 있다. 본 논문에서 제안하는 첫 번째 방법은, 공격자가 접근할 수 없는 안전한 별도의 채널을 통하여 챌린지가 전달된다면 공격자는 단순히 사용자 응답만을 관찰함으로써 패스워드에 관한 의미 있는 정보를 얻을 수 없다는 관찰에 기반하고 있다. 본 논문에서는 이러한 안전한 채널로써, 쉽게 구현 가능한 음성 채널을 이용하였다.

먼저 패스워드 등록 방법은 기존의 글과 숫자 기반의 패스워드 등록 방법과 동일하다. [그림 5]는 인증을 하기 위한 화면을 나타내고 있다. 먼저 사용자 패스워드를 나타내는 영어 알파벳과 숫자들이 화면에 나타나고 각 문자 아래에는 pass-object들이 있다. 여기서 pass-object란 사용자가 임시로 선택하기 위한 객체를 의미한다. 본 논문에서는 아홉 개의 서로 다른 도형에 네 가지 색을 조합하여 36개의 pass-object를 이용한다. 조작하기 위한 인터페이스로는 'up', 'left', 'right', 'down', 'start/enter', '←', '다시듣기' 버튼이 있다. 사용자는 'up', 'left', 'right', 'down' 버튼을 이용하여 pass-object를 이동 할 수 있고 'start/enter' 버튼을 통해 값을 입력한다. 만약 사용자가 잘못된 값을 입력한 경우에는 '←' 버튼을 이용하여 수정이 가능하다. '다시듣기' 버튼은 음성 채널을 통해서 들어오는 값을 다시 들을 수 있다. 패스워드를 입력하는 단계는 다음과 같다.

단계 1. 사용자는 인증을 시작 할 시 인증 서버로부터 세션 키로 사용될 임의의 pass-object에 대한 정보를 별도의 채널을 이용하여 얻는다. 별도의 채널로 음성 채널을 이용할 경우 공격자가 이 정보를 얻을 수 없도록 이어폰 등을 이용하여야 한다.

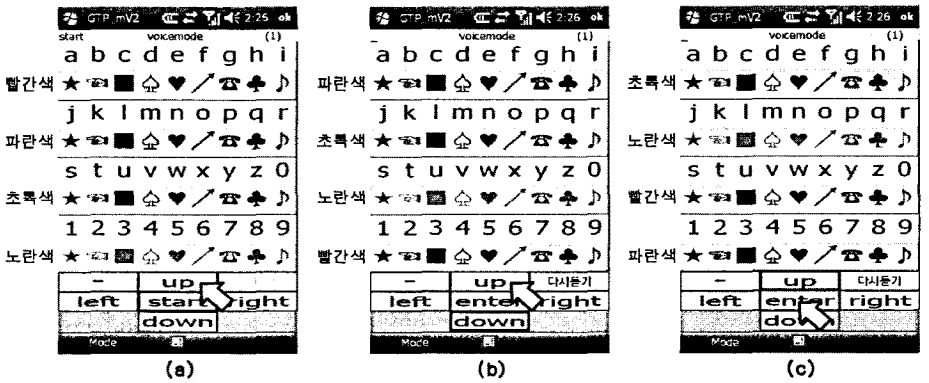
단계 2. 사용자는 'up', 'left', 'right', 'down' 버튼들을 통하여 자신의 패스워드의 첫 번째 문자 밑에 별도의 채널을 통해 얻은 세션 키를 위치하도록 한 후 'start/enter' 버튼을 누른다.

단계 3. 동일한 방법으로 사용자는 별도의 채널을 통해서 새로운 세션 키에 대한 정보를 얻은 후 자신의 다음 패스워드 문자 밑으로 채널을 통해 얻은 세션 키를 이동 한 후 'start/enter' 버튼을 누른다.

단계 4. 사용자의 남은 패스워드 길이만큼 단계 3을 반복한다.

단계 5. 인증 서버로부터 받은 세션 키들이 모두 사용자의 패스워드의 각 문자 밑에 올바르게 위치한 경우 인증에 성공하고 그렇지 않은 경우 인증에 실패한다.

예를 들어 사용자의 비밀번호의 첫 번째 자리가 'u'이고 사용자가 들은 세션 키로 사용될 pass-object가 '빨간색 ■'라 하면 인증 과정은 [그림 5]와 같다. 사용자는 인증 서버로부터 자신의 세션 키가 '빨간색 ■'라는 것을 안전한 음성 채널을 통하여 들은 후 자신의 패스워드 'u' 밑에 세션 키가 위치하도록 'up' 버튼

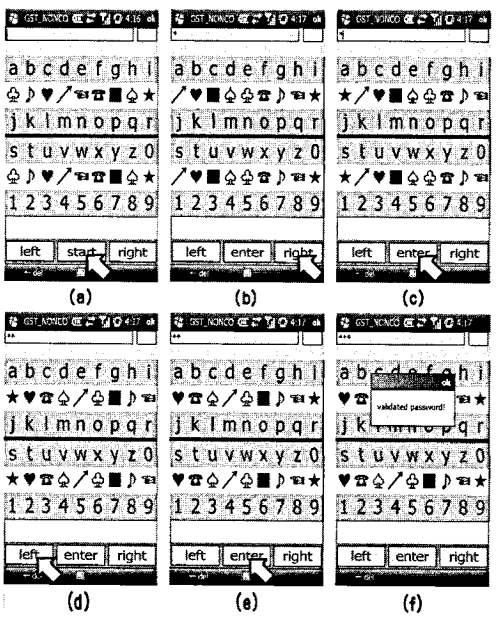


〔그림 5〕 안전한 별도의 채널을 이용한 패스워드 인증 방법 (세션 키가 빨간색 '■' 패스워드가 'u'인 경우)

을 두 번 누른다. 이렇게 하여 'u'를 안전하게 입력할 수 있으며, 패스워드 글자 수 만큼 같은 과정을 반복하여 패스워드 문자열을 안전하게 입력할 수 있다.

3.2 패스워드 중복을 허용하는 인증 방법 (Simple Redundancy Scheme)

본 절에서는 전 절에서 소개한 안전한 별도의 채널을 이용한 패스워드 인증 방법보다 인증 시간을 단축시키고 별도의 채널을 사용하지 않는 방법을 제안한다. 이 방법의 패스워드 등록 방법 역시 기존의 방법과 동일하나, 인증 과정에서는 'left', 'right' 버튼만 사용하여 전 절의 방법보다는 간편하게 pass-object들을 이동시킬 수 있다. 또한 'start/enter' 버튼을 통해 값을 입력할 수 있으며, '← del'버튼을 이용하여 입력한 값을 수정할 수 있다. 패스워드를 입력하는 단계는 다음과 같다.



〔그림 6〕 패스워드 중복을 허용하는 인증방법 (사용자의 패스워드가 'ucs' 인 경우)

단계 1. 사용자는 자신의 패스워드 첫 번째 글자와 같은 열에 위치한 pass-object를 세션 키로 기억 한 뒤 'start' 버튼을 누른다.

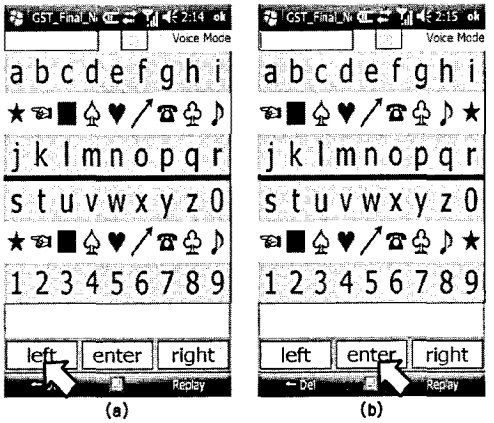
단계 2. 단계 1에서 기억하였던 pass-object가 자신의 패스워드의 두 번째 문자와 같은 열에 위치할 수 있도록 좌우로 이동시킨 후 확인 버튼을 누른다.

단계 3. 사용자가 값을 입력한 후에는 pass-object들의 위치가 임의로 바뀌게 된다. 동일한 방법으로 자신의 전 단계에서 사용하였던 pass-object를 자신의 다음 패스워드 문자와 같은 열에 위치할 수 있도록 이동한 후 'enter' 버튼을 누른다.

단계 4. 사용자의 남은 패스워드 길이만큼 단계 3을 반복한다.

단계 5. 사용자의 패스워드의 모든 문자들과 같은 열에 동일한 pass-object가 존재 하였다면 인증에 성공하고 그렇지 않은 경우 인증에 실패한다.

〔그림 6〕은 사용자의 패스워드가 'ucs'일 때 상기의 방법을 이용하여 인증하는 간단한 예를 보여주고 있다. 〔그림 6〕의 (a)에서 사용자는 자신의 첫 번째 패스워드 글자 'u'의 밑에 있는 '♥'를 사용자의 세션 키로 기억한 뒤 'start' 버튼을 눌러 인증을 시작한다. pass-object 배열이 랜덤하게 섞어져 나오게 되고 사용자는 자신의 세션 키를 찾고 자신의 패스워드의 두 번째 문자인 'c' 밑에 세션 키 '♥'가 위치하도록



〔그림 7〕 복합 인증 방법 (세션 키가 '♤,' 패스워드가 'u'인 경우)

'right' 버튼을 이용하여 세션 키를 이동시킨 후 'enter' 버튼을 통해 입력한다. 자신의 패스워드의 마지막 자리인 's'에 대해서도 'left' 버튼을 이용하여 세션 키를 이동 시킨 후 'enter'를 입력하면 인증이 완료된다.

3.3 복합 인증 방법(Combined Scheme)

이 방법은 전 절에 소개한 패스워드 중복을 허용하는 인증 방법의 안전성을 향상시키기 위하여 사용자가 처음에 세션 키를 설정하는 대신 3.1절에 소개한 방법처럼 매 인증 단계 마다 안전한 채널을 통하여 세션 키에 대한 정보를 받아서 인증을 하는 방법이다. 〔그림 7〕은 이 방법의 간단한 예제 화면이다. (a)에서 사용자는 서버로부터 음성 채널을 통해 세션 키가 '♤'라는 사실을 전달받고 'left' 버튼을 눌러서 자신의 패스워드 'u' 밑에 '♤'가 위치하도록 한 후 'enter' 버튼을 눌러서 인증을 한다.

IV. 안전성 분석

본 장에서는 위에 제시하였던 각각의 방법들에 대해서 안전성을 분석한다. 분석에 앞서서 기존에 널리 사용되는 텍스트 및 숫자 기반의 일반적인 패스워드 입력 방법을 REG, 3.1절에서 제안하였던 별도의 채널을 이용한 패스워드 인증 방법을 SCS, 3.2절에서 제안하였던 패스워드 중복을 허용하는 인증 방법을 SRS, 그리고 3.3절에 제안하였던 복합 인증 방법을 CS라고 하겠다. 〔표 1〕은 본 절에서 소개하는 방법들

〔표 1〕 파라미터 정의

파라미터	의 미
C	패스워드에 사용 될 수 있는 모든 문자들의 수
T	Text field의 알파벳과 숫자들의 총 개수
K	한 개의 pass-object와 매칭 되는 알파벳 또는 숫자들의 최대 개수 ($K \geq 2$)
J	pass-object의 개수
L	패스워드의 길이 (패스워드를 구성하는 글자 또는 숫자의 개수)

의 안전성을 분석하기 위한 파라미터의 정의들이다.

C는 패스워드에 사용 될 수 있는 모든 문자들, 즉 키보드로 입력 가능한 모든 문자의 개수이며, 일반적으로 $C=94$ 이다. T는 화면에 표시되는 text field의 알파벳과 숫자들의 총 개수를 나타낸다. 예를 들어 〔그림 5〕 및 〔그림 6〕의 경우에는 T는 36이다. K는 한 개의 pass-object와 매칭 되는 알파벳 또는 숫자들의 개수로 〔그림 5〕의 K는 1이고 〔그림 6, 7〕의 경우는 4이다. J는 서로 구분되는 pass-object의 개수로 $J= T/K$인 관계가 성립하며, 〔그림 5〕는 J가 36, 〔그림 6, 7〕의 경우에는 9이다. T가 J의 배수가 아닌 경우에는 각 pass-object마다 매칭되는 알파벳 또는 숫자의 개수가 다를 수 있으므로, 이때는 K를 각 pass-object마다 매칭되는 알파벳 또는 숫자의 개수 중 최대값으로 정의한다. L은 패스워드의 길이로, 보통 많이 사용되는 여덟 글자 패스워드의 경우 $L=8$이 된다.

4.1 Random guessing attack

Random guessing attack (RGA)이란, 공격자가 추측을 통하여 임의로 비밀번호를 입력하는 공격이다. 편의상 사용자의 패스워드 선택이 랜덤하다고 가정할 때 유효한 패스워드 공간의 크기가 클수록 안전성이 높을 것이므로 사용자 또는 공격자가 입력 가능한 조합의 수를 RGA에 대한 안전성으로 정의하기로 한다.

REG의 경우 알파벳, 숫자, 특수 기호 및 공백 등 모든 문자들이 패스워드가 될 수 있기 때문에 RGA에 대한 안전성은 C^L이 된다. SCS의 경우는 화면에 나타날 수 있는 패스워드 문자 및 pass-object의 개수가 각각 T개이므로 RGA에 대한 안전성은 T^L이 된다. 한편 CS의 경우 한 단계에서 선택 가능한 입력의 수가 J개이므로 RGA에 대한 안전성은 J^L이 된다.

〔표 2〕 J, T를 다양화하였을 때 RGA에 대한 안전성(각 수치의 역수는 RGA의 성공 확률임)

			$L=8$			
		J	REG	SCS	SRS	CS
T	36	9	94^8	36^8	9^7	9^8
		18		36^8	18^7	18^8
	94	24	94^8	94^8	24^7	24^8
		47		94^8	47^7	47^8

〔표 3〕 J, T를 다양화하였을 때 RA에 대한 안전성 (각 수치의 역수는 RA의 성공 확률임)

			$L=8$			
		J	REG	SCS	SRS	CS
T	36	9	1	36^8	9^7	9^8
		18		36^8	18^7	18^8
	94	24	1	94^8	24^7	24^8
		47		94^8	47^7	47^8

SRS의 경우도 CS와 거의 같지만 SRS의 첫 단계는 사용자로부터 입력을 받는 데 사용되는 것이 아니라 사용자의 세션 키를 설정하는데 사용되기 때문에 SRS의 RGA에 대한 안전성은 J^{L-1}이 된다.

〔표 2〕는 패스워드 글자 수 L을 8로 고정하고 J와 C를 다양화 하였을 때 각 방법들의 RGA에 대한 안전성의 변화를 보여준다. 일반적으로 알파벳, 숫자, 특수 기호, 공백 등 패스워드에 사용되는 모든 가능한 글자는 94개이므로 $C=94$이다. 한편, T가 C와 같게 된다면 REG와 SCS는 같은 안전성 값을 가지게 되나, 모바일 환경의 제한적인 디스플레이로 인해 T를 C보다 작게 잡을 경우, 예를 들어 앞의 예제와 같이 $T=36$으로 잡을 경우, RGA에 대한 안전성이 다소 떨어지게 된다. 일반적으로 random guessing attack에 대해서 각 방법들 간 안전성의 관계는 다음 수식과 같이 된다는 것을 알 수 있다.

$$\mathrm{REG} \geq \mathrm{SCS} > \mathrm{CS} > \mathrm{SRS} \quad (1)$$

즉, SRS가 RGA에 대한 안전성이 가장 떨어지나, $T=36$, $J=9$, $L=8$와 같은 보수적인 파라미터의 경우에도 이 값이 $9^7 \approx 4.8\times10^6$으로 어느 정도의 안전성을 보장할 수 있음을 확인 할 수 있다.

4.2 Replay attack

Replay attack (RA)이란, 인증 시 사용되는 정보를 도용하여 재사용하는 공격을 말한다. 일반적인 패스워드 및 개인식별번호 기반의 인증 방법(REG 방법) 같은 경우 사용자가 누르는 손모양이나 누르는 위치를 그대로 따라하는 경우 인증에 100% 성공하게 된다. 하지만 우리가 제안하는 세 가지 방법에서는 같은 패스워드에 대해서도 매번 사용자에게 요청되는 응답이 바뀌기 때문에 단순히 사용자의 응답을 공격자가 반복한다고 해서 인증에 성공할 확률은 매우 낮다. 예를 들어 SCS 및 CS 방법은 인증 기기에서 음성 채널로 요청하는 세션 키에 대한 정보가 매번 다르며, SRS 방법에서도 매 인증 세션마다 pass-object 배열이 임의로 바뀌기 때문에 사용자의 세션 키 역시 매번 달라지게 된다. 결국 제안하는 세 가지 방법에서 RA는 RGA와 같은 성공률을 가지는 반면 REG 방법에 대한 RA의 성공률은 100%이므로, RA에 대한 각 방법들의 안전성의 관계는 다음 수식과 같다.

$$\mathrm{SCS} > \mathrm{CS} > \mathrm{SRS} > \mathrm{REG} \quad (2)$$

〔표 3〕은 L이 8이고 J와 T를 다양화 하였을 때 각 방법의 RA에 대한 안전성의 변화를 보여준다. 〔표 3〕에 의하면 패스워드 길이가 8이라고 할 때 적어도 SCS는 REG 방법보다 36^8배, SRS는 9^7배, CS는 9^8배 정도 더 안전하다고 볼 수 있다.

4.3 Shoulder surfing attack

SSA에 대한 안전성을 분석하기 위해, SSA 수행 후 공격자가 설정할 수 있는 패스워드 후보 집합의 크기를 P라고 정의하자. 예를 들어 기존의 REG 방법에서 공격자는 인증 과정을 관찰한 후 사용자의 패스워드를 정확히 얻을 수 있기 때문에 P는 1이 된다. SCS와 CS에서는 공격자가 사용자의 모든 입력 과정을 관찰하고 완벽하게 기억 또는 저장한다고 하여도 P는 RGA로 시도해야 하는 값과 같다는 것을 쉽게 알 수 있는데, 이는 공격자가 별도의 채널에서 오는 세션 키(챌린지) 정보를 얻지 못하는 한 이들 방식이 일종의 one-time pad와 같은 역할을 하기 때문이다. 한편 SRS 방법에서는 인증 과정의 각 단계에서 정확히 어떤 값이 입력되는지는 공격자가 알 수 없으나 패스워드 각 글자들이 계속 같은 pass-object에 대응된다는 사실을 알고 있으므로 J개의 pass-object와 연결된 각 글자 집합들을 단계별로 연결하면

패스워드 후보 집합 크기를 $P = J \times K^L$로 좁힐 수 있다. 이들 분석을 종합하면 SSA에 대한 안전성 P에 대해 다음 관계식을 얻을 수 있다.[1)]

$$SCS > CS > SRS > REG \quad (3)$$

하지만 위의 분석은 모든 인증 과정이 녹화 장치 등으로 기록이 되거나 공격자가 모든 과정을 완벽하게 기억하는 상황을 가정한 분석이다. 만약 모든 기록이 이루어지지 않고 단순히 사람의 기억에 의존하여 SSA를 한다면 일반적으로 사람의 기억력에는 한계가 있기 때문에 다른 각도로 안전성을 고려해야 한다. 이에 안전성을 각 방법에서 공격자가 기억해야 할 객체(문자, 숫자, 기호, 이미지 등)의 수로 재정의 하자. 예를 들어 SRS의 경우 공격자는 각 단계에서 사용자가 'enter' 버튼을 누르는 순간의 pass-object 배치를 모두 기억해야 하므로 단계별로 패스워드 글자들의 배치가 무작위로 바뀌지 않도록 설정할 경우에도 기억해야 할 정보의 양은 $J \times L$이 된다. 이것은 위에서 기록에 기반을 둔 SSA의 $P = J$에 비해 현저히 큰 숫자이다.

〔표 4〕는 안전성을 각 방법의 기억해야 할 객체의 수라고 정의할 때, J, T의 변화에 따른 REG와 SRS의 안전성 변화를 보여준다. 〔표 4〕에 의하면 SRS방법은 REG방법에 비하여 적게는 9배, 많게는 42배 정도 SSA에 대해 안전하다고 볼 수 있다. Vogel과 Machizawa의 최근 연구 결과[7]에 의하면 사람의 영상 단기 기억력은 세 개에서 네 개 객체로 제한되어 있으므로, 공격자가 특별한 기억력의 소유자이거나 별도의 기록 장비를 가지고 있지 않는 한 SRS는 SSA에 안전하다고 할 수 있다.

마지막으로, 같은 사용자에 대해 SSA이 여러 번 반복될 경우의 안전성을 고려해 보자. 먼저 SCS와 CS에 대해서는 SSA를 아무리 반복하여도 공격자가 추가로 얻을 수 있는 정보가 없으므로 여러 차례의

〔표 4〕 J, T를 다양화하였을 때 SSA에 대한 안전성

			$L=8$	
		J	REG	SRS
T	36	9	8	72
		18		144
	94	24	8	192
		47		376

SSA에 대해서도 안전함을 쉽게 알 수 있다. 한편 SRS의 경우는 SSA를 통하여 사용자가 입력한 모든 값과 화면의 값을 공격자가 모두 기록한다고 가정한다면 SSA를 2회 반복함으로써 높은 확률로 패스워드를 얻어낼 수 있다. 즉, 공격자는 2회의 SSA로부터 두 개의 패스워드 후보 집합을 구하고 이들 두 집합의 교집합을 구하는 교차 공격(intersection attack)을 수행하면 된다. 물론 실제 패스워드가 아닌 다른 문자열이 이 두 개의 후보 집합에 모두 우연히 속하게 되어 패스워드를 하나로 정확히 복원해낼 수 없는 경우도 있을 수 있으나 다음의 분석에 의하면 이 확률은 매우 작음을 알 수 있다. 먼저 L자리 SRS의 유효한 패스워드 수는 T^L개인데, 1회의 SSA으로부터 공격자는 패스워드 후보집합 크기를 $P \approx J \times K^L$으로 줄일 수 있으므로, 조합 가능한 모든 L자리 패스워드 문자열 중 임의의 문자열이 SSA에 의한 패스워드 후보 집합에 속할 확률은

$$P/T^L \approx 1/J^{L-1} \quad (4)$$

이다. 따라서 SSA를 2회 반복했을 때 임의의 L자리 문자열이 두 후보 문자열이 두 후보 두 후보 집합에 모두 속할 확률은 대략 $1/J^{2L-2}$이며, 결국 교집합 내의 원소 수의 기댓값은 대략

$$T^L/J^{2L-2} \approx K^L/J^{L-2} \quad (5)$$

이다. 4.1 및 4.2절에서 보인 바와 같이 RGA나 RA에 대한 안전성을 보장하기 위해서는 J가 충분한 크기를 가져야 하므로 보통 $J \gg K$로 잡게 되는데, 이렇게 되면 (5)의 기댓값은 1보다 훨씬 작다. 즉, 확률적으로 임의의 L자리 문자열이 두 개의 후보 집합에 모두 속하는 경우는 거의 없으며, 두 개의 후보 집합에 모두 속하는 문자열은 실제 패스워드가 유일하다. 따라서 공격자가 사용자의 인증 과정 전체를 모두 기

1) 만약 〔그림 6〕에서처럼 매 단계별로 패스워드 글자들의 배치를 무작위화하지 않는다면 각 열을 구성하는 문자들의 조합은 항상 고정이 되므로 하나의 글자처럼 취급할 수 있는데, 예를 들어 첫 번째 열에 위치한 문자들의 집합 {a, j, s, 1}은 논리적으로 하나의 문자로 해석될 수 있다. 이 경우 실질적으로 $K=1$이 되어 $P=J$가 된다. 즉 공격자가 SRS 방법에 대한 SSA를 1회 수행한 후 다시 SRS 방법으로 인증을 시도할 경우 $1/J$확률로 성공할 수 있게 된다. 따라서 SSA에 대한 안전성 측면에서는 패스워드 글자들의 배치를 매 단계마다 무작위화하는 것이 바람직하다.

록 또는 기억할 수 있는 환경에서는 SRS는 2회 이상의 SSA에 대해서는 안전성을 보장하지 못한다.

V. 사용자 평가

본 논문에서는 우리가 제안한 세 가지 방법(SCS, SRS, CS)과 기존에 사용되는 텍스트 기반의 패스워드 입력 방법(REG 방법)의 편의성 및 선호도를 비교하는 실험을 하였다.

5.1 평가 방법

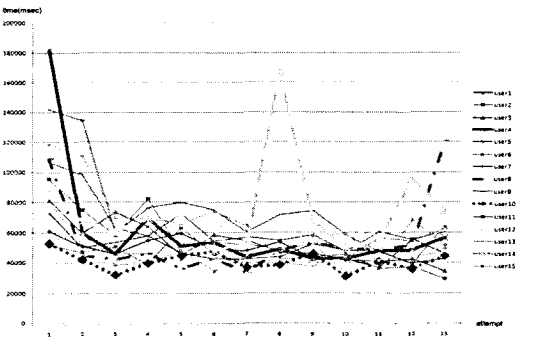
우리는 총 15명의 대학생들을 대상으로 기존의 텍스트 기반의 패스워드와 우리가 제안한 방법들에 대하여 모의실험 및 설문 조사를 하였다. 모의실험은 삼성 SCH-M490(옴니아)을 이용하여 실험을 하였다. 실험 기기의 OS는 Windows Mobile 6.1을 이용하였고 CPU는 PXA312 624MHz이다. 디스플레이 크기가 3.3인치인 실험기기의 해상도는 400×800이다. 실험을 하기 위한 SCS의 파라미터 값은 $T=36$, $K=1$, $J=36$, $L=8$을 이용하였고 CS와 SRS의 파라미터는 $T=36$, $K=4$, $J=9$, $L=8$이다. 실험 절차는 다음과 같다.

① 사용자에게 먼저 각 입력 방법들에 대해서 설명을 한다.
② 기존의 방법을 가상 키보드, 필기인식을 이용하여 각각 5번 반복 한다.
③ SCS, SRS, CS 순서대로 각각의 방법에 대해 13번씩 패스워드를 입력해 본다. 이 중 3회는 적응 단계, 10회는 실제 테스트 단계이다.
④ 각 입력 방법에 대한 설문에 응답한다.

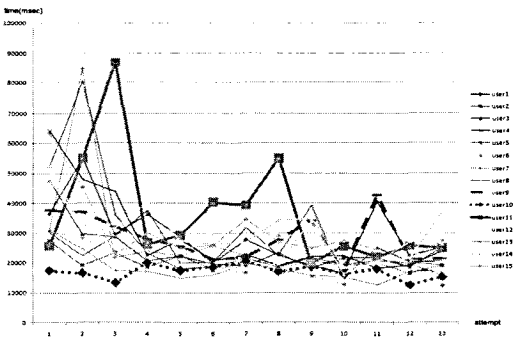
5.2 결과 분석

5.2.1 실험 결과 분석

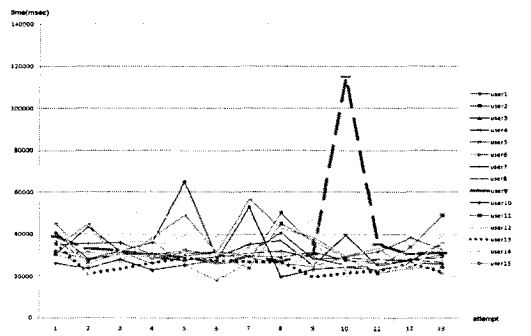
기존의 방법들과 사용 편의성을 비교하기 위해 우리는 사용자들의 인증시간을 분석하였다. [그림 8-10]은 우리가 제안한 방법을 이용하여 인증하였을 때 사용자들의 인증시간을 분석한 그래프이다. [그림 8, 9]에서 보면 대부분 사용자들의 로그인 시간이 처음 세 번의 시도에 급격히 감소하는 것을 볼 수 있다. SCS의 경우는 처음 세 번 시도의 인증시간 평균이 뒤의 10회 시도 이후 인증시간 평균보다 약 18초 정도



[그림 8] SCS의 각 사용자들의 인증시간 분석 그래프



[그림 9] SRS의 각 사용자들의 인증시간 분석 그래프



[그림 10] CS의 각 사용자들의 인증시간 분석 그래프

더 느리고 SRS의 경우에는 약 15초 정도 차이가 나는 것을 볼 수 있었다. 이는 사용자가 약 세 번 정도 새로운 인증 방법을 연습하게 되면 그 방법에 어느 정도 익숙해짐을 의미한다. 또한 일부 사용자들은 10회 이상 시도를 할 때 인증 시간이 증가하게 되는 현상을 볼 수 있는데 이는 사용자들의 집중력 저하로 인한 결과로 추정된다.

흥미로운 점은 [그림 10]을 보면 [그림 8]과 [그림 9]에서 보이던 시간이 지나감에 따라 인증시간이 감소

〔표 5〕 각 인증 방법별 인증률 및 인증시간 비교

	REG-가상키보드	REG-필기인식	SCS	SRS	CS
전체 인증률	95%	93.33%	73.43 %	91.79 %	89.74 %
연습 후 인증률	-	-	72.66 %	91.33 %	91.33 %
전체 인증시간 (sec)	8.532	15.983	56.856	26.193	31.410
연습 후 인증시간	-	-	82.655	22.896	30.986
연습 후 특별한 경우를 제외한 시간 평균	8.294	15.521	50.754	21.904	29.387

하는 현상을 볼 수가 없다는 것인데 이는 먼저 SCS와 SRS의 실험 후에 CS 실험을 수행하였기 때문에 CS 방식에 바로 적응하게 된 현상으로 파악된다. 한편 〔그림 10〕의 user9의 열 번째 시도와 같이 사용자들의 집중력 저하 또는 주위의 영향으로 시간이 심하게 증가되는 현상도 볼 수 있었다. 이에 우리는 정확한 소요 시간을 알아보기 위하여 전체 인증 시간, 처음 세 번의 연습을 제외한 10회의 인증 시간, 이들 중 상위 10%, 하위 10%를 제외한 시간의 평균을 구하고 비교 하였으며, 각각에 대해 인증 성공률도 측정하였다. 단, 키보드 및 필기입력은 이미 많은 사용자들이 익숙한 방법이므로 연습 단계를 따로 고려하지 않았다.

〔표 5〕를 보면 SCS 같은 경우는 인증률이 72.66%로 상당히 저조 하지만 SRS, CRS는 90%가 넘는 기존의 방법과 비슷한 인증률을 보여주었다. 또한 가상 키보드를 이용한 REG는 약 8.5초, 필기인식을 이용하였을 때 약 16초 정도의 인증 시간이 소요되었다. SCS는 필기 인식보다 약 3.3배, 키보드를 이용한 방법보다 약 6.17배 시간이 더 소요 되었지만 SRS는 키보드 인증 방법보다는 2.68배, 필기입력 방법 보다는 1.4배 정도 밖에 느리지 않았다. CS는 키보드를 이용한 방법보다 3.3배, 필기인식 방법보다 1.93배로 SRS보다는 인증 시간이 오래 걸렸지만 SCS와 비교 하였을 경우는 상대적으로 적은 시간이 소요됨을 알 수 있었다.

분석 결과를 종합해 보면 SRS와 CS는 기존 방법보다 약간 느리기는 하지만 실제로 충분히 사용 가능한 인증률과 인증 시간을 보여 주었으며, SCS는 가장 높은 안전성을 보장하는 반면 인증률과 인증 속도가 다소 떨어진다는 점이 확인되었다. 제안 방법들의 편의성 및 안전성에 관한 평가는 다음 절의 사용자 평가에서도 확인할 수 있다.

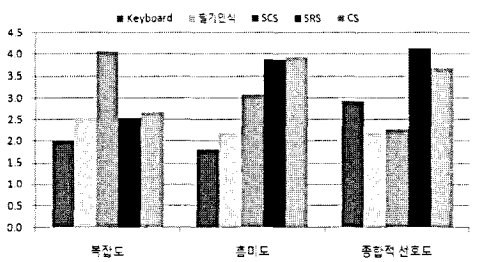
5.2.2 설문조사 결과 분석

우리는 먼저 사용자들에게 현재 로그인 방법의 안전성에 대한 인식과 더 안전한 로그인 방법을 사용하기 위한 추가적인 노력에 대해 질문하였다. 그리고 기존의 방법들(가상 키보드를 이용한 REG, 필기 인식을 이용한 REG)과 우리가 제안한 방법들을 직접 사용하도록 한 뒤 각 방법들의 복잡도, 흥미도, 안전성과 편의성을 고려한 종합적 선호도를 묻는 질문을 하였다. 〔표 6〕을 보면 약 80%의 사람들이 현재 사용되고 있는 인증 방법이 SSA에 대해 안전하지 않다고 대답하였다. 또한 80%이상의 사람들이 좀 더 안전하게 인증하기 위해 추가적인 노력을 하겠다고 대답하였다. 〔그림 11〕은 각 방법들의 복잡도, 흥미도, 종합적 선호도에 관한 설문 결과를 나타내는 그래프로, 사용자들에게 각 항목에 1에서 5의 점수를 부여하도록 한 것이다. 그 결과 복잡도는 SCS가 가장 높아 사용자들이 사용하기에 어려워한다는 사실을 알 수 있었으나

〔표 6〕 다음 질문에 대한 설문 조사 결과

질문 1 : 현재 사용되는 인증 입력방법(키보드, 필기인식)이 엿보기 공격 등에 대해 안전하다고 생각 하십니까?
질문 2 : 좀 더 안전한 인증 방법을 사용하기 위해 추가적인 노력을 하실 의향이 있습니까?

	절대 아니다	아닌 편이다	보통	그런 편이다	매우 그렇다
질문 1	26.67	53.33	6.67	0.00	13.33
질문 2	0.00	13.33	0.00	53.33	33.33



〔그림 11〕 각 방법별 복잡도, 흥미도, 종합적 선호도에 대한 설문 조사 결과

SRS와 CS는 기존 입력 방법과 비슷한 복잡도를 보여서 충분히 이용 가능함을 확인할 수 있었다. 사용자들은 기존의 방법들에 비해 우리가 제안한 방법들을 상당히 흥미롭게 생각하고 있었으며, 또한 안전성과 편의성 모두를 고려하였을 때 사용자들은 기존의 방법보다도 SRS와 CS를 더 선호함을 확인할 수 있었다.

VI. 결 론

본 논문에서는 모바일 환경에서 일반적으로 이용되고 있는 텍스트 기반의 패스워드 방법보다 좀 더 안전하게 패스워드를 입력할 수 있는 엿보기 공격에 강한 패스워드 입력 방법을 제안하였다. 본 논문에서 제안한 방법은 random guessing attack에 대한 안전도는 기존의 방법보다 다소 떨어지나, replay attack 및 엿보기 공격에 대해서는 기존의 방법보다 현저히 높은 안전성을 보인다. 사용자 평가 결과, 제안한 세 가지 방법 중 SCS는 다소 낮은 인증률과 긴 인증시간으로 인해 사용자의 선호도가 낮았지만, SRS와 CS는 기존의 방법들과 비슷한 인증률을 보이고 인증 시간도 현실적이어서 안전성과 편의성을 종합적으로 고려한 사용자들의 선호도가 매우 높았다.

한편 본 논문의 실험은 15명의 대학생을 대상으로 제한적으로 이루어졌으나, 이후에는 연령대 별, 성별로 더 많은 사용자에 대해 평가를 확대 실시하여 전 연령층의 편의성을 확인해야할 것으로 보인다. 또한 사용자에게 충분한 편의성을 제공하면서도 인증 과정을 모두 기록이 가능하였을 때의 SSA를 효율적으로 막을 수 있는 패스워드 입력 방법을 추가적으로 연구해야할 것이다. 아울러 패스워드가 특수기호 등 더 많은 문자들의 집합에서 선택될 수 있는 상황을 고려하면, 모바일 단말기의 작은 디스플레이에서 더 많은 정보를 효과적으로 보여줄 수 있는 인터페이스에 대한 연구도 진행되어야 할 것이다. 마지막으로, SCS와 CS 방법의 경우 소리를 들을 수 있는 사용자만을 대상으로 하므로 기존의 REG 방법에 비해 사용자층이 다소 좁아진다는 문제점이 있으므로, 청각장애우들도 사용 가능한 입력 방법을 개발하는 것도 바람직한 연구 방향 중 하나가 될 수 있을 것이다.

참고문헌

[1] S. Wiedenbeck, J. Waters, L. Sobrado, and J. Birget, "Design and evaluation of a shoulder- surfing resistant graphical password scheme," Proceedings of the Advanced Visual Interfaces, pp. 177-184, May 2006.

[2] H. Zhao and X. Li, "S3PAS: a scalable shoulder-surfing resistant textual-graphical password authentication scheme," Proceedings of the 21st IEEE International Conference on Advanced Information Networking and Applications Workshops, vol. 2, pp. 467-472, May 2007.

[3] D. Weinshall, "Cognitive authentication schemes safe against spyware," Proceedings of the 2006 IEEE Symposium on Security and Privacy, pp. 1-16, May 2006.

[4] P. Golle and D. Wagner, "Cryptanalysis of a cognitive authentication schme," Proceedings of the 2007 IEEE Symposium on Security and Privacy, pp. 66-70, May 2007.

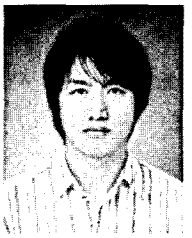
[5] H. Jameel, R.A. Shaikh, H. Lee, and S. Lee, "Human identification through image evaluation using secret predicates," Proceedings of the Cryptographer's Track at RSA Conference, LNCS 4377, pp. 67-84, 2007.

[6] X. Suo, Y. Zhu, and G.S. Owen, "Graphical passwords: a survey," Proceedings of the 21st Annual Computer Security Applications Conference, pp. 463-472, Dec. 2005.

[7] E.K. Vogel and M.G. Machizawa, "Neural activity predicts individual differences in visual working memory capacity," Nature 428, pp. 748-751, Apr. 2004.

〈著者紹介〉

김 창 순 (Chang Soon Kim) 학생회원
2008년 2월: 인하대학교 컴퓨터정보공학부 졸업
2010년 2월: 인하대학교 정보공학과 석사
2010년 3월~현재: 우전앤한단 연구원
〈관심분야〉 정보보호, 모바일 보안, 알고리즘



윤 선 범 (Sun-Bum Youn) 일반회원
2009년 2월: 인하대학교 컴퓨터정보공학부 졸업
2009년 8월~현재: 한국과학기술연구원 위촉 연구원
〈관심분야〉 HCI, AI

이 문 규 (Mun-Kyu Lee) 정회원
1996년 2월: 서울대학교 컴퓨터공학과 (학사)
1998년 2월: 서울대학교 컴퓨터공학과 (공학석사)
2003년 8월: 서울대학교 전기컴퓨터공학부 (공학박사)
2003년 8월~2005년 2월: 한국전자통신연구원 선임연구원
2005년 3월~현재: 인하대학교 컴퓨터정보공학부 조교수
〈관심분야〉 암호알고리즘, 부채널분석, 모바일 보안 등