DOI : 10.5392/JKCA.2011.11.4.033

훔쳐보기 방지를 위한 한글 패스워드 시스템

Hangul Password System for Preventing Shoulder-Surfing

김종우*, 김성환**, 박선영**, 조환규**
부산대학교 U-Port정보기술산학공동사업단*, 부산대학교 컴퓨터공학과**

Jong-Woo Kim(jwkim@pusan.ac.kr)*, Sung-Hwan Kim(sunghwan@pusan.ac.kr)**,
Sun-Young Park(parksy@pusan.ac.kr)**, Hwan-Gue Cho(hgcho@pusan.ac.kr)**

요약

전통적인 텍스트 기반 패스워드들은 가장 일반적인 인증 방법으로 사용되고 있음에도 불구하고, 추측, 사전공격, 키 로거, 훔쳐보기와 같은 심각한 문제점을 가지고 있다. 이러한 문제점을 개선하기 위한 대안으로 그래피컬 패스워드에 대한 연구 및 개발이 이루어져 왔다. 하지만 그래피컬 패스워드는 전통적인 텍스트 기반 패스워드에 비해 오히려 훔쳐보기 공격에 더 취약하다는 문제점을 가지고 있다. 본 논문에서는 훔쳐보기 방지를 위한 한글 기반의 새로운 패스워드 입력 방법을 제안한다. 제안 방법은 패스워드로 한글을 사용하고, 사용자가 패스워드를 직접 입력하는 대신 회전하는 그리드 상에 패스워드를 위치시키도록 한다. 제안 방법은 로그인 화면에서 사용자의 패스워드를 유인 문자와 함께 보여줌으로써 공격자가 패스워드를 훔쳐보는 것을 어렵게 만든다. 본 논문에서는 제안 방법에 대한 무작위 공격, 사전공격 및 훔쳐보기 공격에 대한 안전성을 분석하였으며, 분석 결과는 이들 공격에 대해 안전하다는 것을 보여준다.

■ 중심어 : | 인증 | 패스워드 | 훔쳐보기 | 그리드 기반 패스워드 | 한글 |

Abstract

Although conventional text-based passwords are used as the most common authentication method, they have significant drawbacks such as guess attacks, dictionary attacks, key loggers, and shoulder-surfing. To address the vulnerabilities of traditional text-based passwords, graphical password schemes have been developed as possible alternative solutions, but they have a potential drawback that they are more vulnerable to shoulder-surfing than conventional text-based passwords. In this paper, we present a new Hangul password input method to prevent shoulder-surfing attacks. Our approach uses Hangul as a password, and it requires the users to locate their password in the given wheeling password grid instead of entering the password. Our approach makes it difficult for attackers to observe a user's password since the system shows the users' passwords with decoy characters as the noise on the screen. Also, we provide security analysis for random attacks, dictionary attacks, and shoulder-surfing attacks, and it shows that our password system is robust against these attacks.

■ keyword : | Authentication | Password | Shoulder-surfing | Grid-based Password | Hangul |

* 이 논문은 부산대학교 자유과제 학술연구비(2년)에 의하여 연구되었음.

접수번호 : #101109-002
접수일자 : 2010년 11월 09일
심사완료일 : 2011년 01월 19일
교신저자 : 조환규, e-mail : hgcho@pusan.ac.kr

I. 서 론

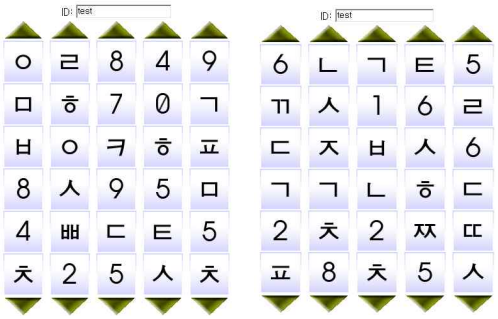
인터넷 사용의 보편화와 함께 사용자 인증은 다양한 인터넷 서비스를 사용하기 위한 필수적인 요소기술이 되고 있다. 사용자 인증은 일반적으로 글자와 숫자의 조합으로 사용자 이름과 패스워드를 키보드를 통해 입력하는 문자 기반 패스워드가 가장 많이 사용되고 있다. 하지만 이와 같은 전통적인 텍스트 기반 패스워드 인증 방법은 추측, 사전공격, 키 로거, 사회공학, 스피이웨어, 훔쳐보기(Shoulder-Surfing) 등의 공격에 취약하다는 보안상의 심각한 문제점을 가지고 있다[1].

이러한 문자 기반 패스워드의 취약점을 보완하기 위해 Draw-A-Secret[2], GrIDsure[3], PassFaces[4]와 같은 다양한 그래피컬 패스워드(Graphical Password)들이 연구되어 왔다[5-8]. 하지만 그래피컬 패스워드는 일반적인 텍스트 기반의 패스워드보다 오히려 훔쳐보기 공격에 더 취약하다는 문제점을 가지고 있다 [1]. 훔쳐보기 공격은 패스워드에 대한 대표적인 공격방법 중 하나로서, 공격자는 로그인 과정을 직접 관찰하거나 사용자의 인증 과정을 녹화하는 방식을 통하여 패스워드에 대한 정보를 얻을 수 있다[9][10].

훔쳐보기 공격을 방지하기 위한 일반적인 방법은 관찰자가 사용자의 입력을 정확히 알기 힘들도록 방해요소를 첨가하는 것이다[11-14]. 예를 들어, Hoanca[11]는 Passfaces를 시선 추적을 이용하여 선택할 수 있도록 확장하였으며, Tan[14]은 여러 단계의 간접적인 선택을 통하여 관찰자가 패스워드를 알기 어렵게 만드는 스크린 키보드를 제안하였다. 하지만 이러한 방법들은 사용자 인증을 위해 추가적인 고가의 장비나 복잡한 연산이 요구된다. 또한 이러한 방법들은 물리적으로 작은 입력장치와 화면크기, 제한된 계산 자원 및 전력 소모 문제와 같은 여러 가지 제약을 가지고 있는 스마트폰과 같은 모바일 디바이스에서 사용하기에 적합하지 않다.

이에 본 논문에서는 사용하기 간단하고 훔쳐보기 공격에 강한 새로운 패스워드 입력 방법을 제안한다. 제안 방법은 사용자 인증을 위해 사용자에게 자신의 패스워드를 직접 입력하도록 하는 대신 [그림 1]과 같이 주어진 $M \times N$ 격자의 각 열을 회전시켜 한글 패스워드 문자를 그리드 상에 위치시키도록 한다. 즉, 제안 방법은 추가적인 장비나 복잡한 연산 없이도 훔쳐보기 공격을 방지할 수 있으며, 모바일 환경에서도 누구나 쉽게 사용할 수 있는 직관적인 사용자 인터페이스를 제공한다.

본 논문의 구성은 다음과 같다. 2장에서는 제안하는 패스워드 입력 방법에 대해 기술하고, 3장에서 제안 패스워드 입력 방법의 안전성을 분석한다. 4장에서는 결론을 기술한다.



(a) 인증에 성공한 경우 (b) 인증에 실패한 경우

그림 1. 제안 패스워드 시스템의 입력화면. 입력된 패스워드는 “ㅂㅅㄷㅎㄱ"로 ”부산대학교“라는 단어를 통해 쉽게 기억할 수 있다.

II. 그리드 기반 한글 패스워드 입력 방법

본 장에서는 제안하는 그리드 기반 한글 패스워드 입력 방법의 원리와 안전성에 영향을 주는 요소에 대해 소개한다. 제안하는 패스워드 입력 방법은 그림 1과 같이 패스워드를 생성하기 위해 한글 초성과 숫자 및 특수문자를 사용하고, 사용자에게 자신의 패스워드를 직접 입력하도록 하는 대신 주어진 $M \times N$ 격자의 각 열을 회전시켜 패스워드 문자를 그리드 상에 위치시키도록 함으로써 사용자를 인증을 한다. 사용자는 자신의 패스워드를 직접 입력하는 대신 주어진 M X N 그리드 상에 위치시킴으로써 인증을 거친다. 사용자는 각 열을 스크롤함으로써 다른 문자를 선택하는 입력을 할 수 있다. 제안 방법은 사용자의 패스워드 문자와 함께 다른

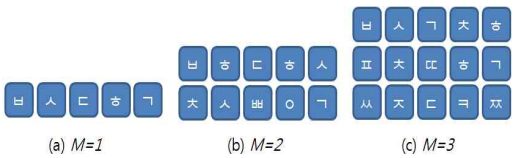
유인문자들(decoy characters)을 방해요소로 사용함으로써 공격자가 사용자의 패스워드를 쉽게 알 수 없도록 한다.

제안 방법에서 $M \times N$ 그리드를 가지는 제안 패스워드 모델을 $FG(\Sigma, M, N)$라고 하면, Σ, M, N은 다음과 같이 정의된다.

- Σ는 패스워드를 구성하는 모든 문자의 집합이다. Σ 내의 문자 개수는 $|\Sigma|$로 표기한다.
- M은 그리드를 구성하는 행의 개수이며, 사용자가 각 열에서 한 번에 볼 수 있는 문자의 개수와 일치한다.
- N은 그리드를 구성하는 열의 개수이며, 패스워드의 길이를 의미한다.

[그림 2]는 M의 크기에 따른 제안하는 패스워드 입력 예를 보여준다. [그림 3]에서 공격자가 사용자의 인증 과정을 지켜본다고 할 때, $M=1$인 경우 공격자는 사용자의 패스워드가 "ㅂㅅㄷㅎㄱ"라는 사실을 쉽게 알 수 있다 ([그림 2](a)). 반면 $M>1$인 경우에는 화면을 통해 추측할 수 있는 후보 패스워드가 유일하지 않다. 예를 들어, $M=2$인 경우 공격자가 인증 화면을 통해 얻을 수 있는 후보 패스워드는 "ㅂㅎㄷㅎㅅ", "ㅊㅎㄷㅎㅅ", "ㅂㅅㄷㅎㅅ", "ㅊㅅㄷㅎㅅ" 등 32개이다 ([그림 2](b)). M이 큰 값을 가질수록 인증화면을 통해 공격자가 정확한 패스워드를 추측할 확률이 작아진다. 예를 들어 $M=3$이라면 공격자는 사용자의 인증과정을 지켜본다고 하더라도 단지 사용자의 패스워드가 $3^5=243$개의 후보 패스워드 중 하나라는 사실밖에 알 수 없다 ([그림 2](c)).

한편 최초의 훔쳐보기 공격 이후에 추가적인 노출이 있는 경우에는 후보 패스워드의 개수가 줄어든다. [그림 3]은 "ㅂㅅㄷㅎㄱ"("부산대학교"의 초성)을 패스워드로 사용하는 사용자의 인증과정이 공격자에게 두 번 노출된 결과를 보여준다. $pw(G_t)$를 사용자가 올바른 패스워드를 입력한 후의 격자 화면 G_t로부터 추측할 수 있는 후보 패스워드의 집합이라고 할 때, [그림 3]의 두 입력 화면 G_a, G_b에 대하여 $pw(G_a)$와 $pw(G_b)$는 각각 243개의 후보 패스워드를 가지고 있지만 공격자가 두 화면을 통하여 추측할 수 있는 후보 패스워드는 두 집합의 교집합, 즉 $pw(G_a) \cap pw(G_b)$={"ㅂㅅㄷㅎㄱ", "ㅂㅅㄷㅊㄱ"}이다. 그림 4는 $M=6$일 때의 예이다. [그림 4](a)와 [그림 4](b)의 입력화면에서 후보 패스워드의 교집합은 [그림 4](b)에 나타나는 것과 같이 $2 \times 1 \times 3 \times 3 \times 1 = 18$개다. [그림 4](c)와 같은 입력화면이 추가로 노출 되었을 때는 후보 패스워드는 2개로 줄어든다. 즉, $pw(G_a) \cap pw(G_b) \cap pw(G_c)$ = {"ㅂㅅㄷㅎㄱ", "ㅂㅅㄷㅌㄱ"}이다.



(a) M=1 (b) M=2 (c) M=3

그림 2. 그리드 기반 패스워드 시스템의 예. M이 클수록 후보 패스워드 개수가 많아지므로 공격자는 사용자의 패스워드를 쉽게 추축하지 못한다.

(a) k=1 (b) k=2

그림 3. M=3인 환경에서 공격자에 의해 획득된 2개의 로그인 화면. 추가적인 훔쳐보기에 의하여 후보 패스워드가 줄어든다는 사실을 알 수 있다. 후보 패스워드의 교집합이 (b)에 다른 색으로 표시되어 있다.

(a) k=1 (b) k=2 (b) k=3

그림 4. M=6인 환경에서 공격자에 의해 획득된 3번의 로그인 화면. 후보 패스워드의 교집합이 (b)에 다른 색으로 표시되어 있다.

III. 제안 방법의 안전성 분석

2장에서는 본 논문에서 제안하는 그리드 기반 한글 패스워드 입력 방법과 안전성에 영향을 주는 요소들을 간단한 예를 통해 설명하였다. 본장에서는 제안 모델에 대한 무작위 공격 및 훔쳐보기 공격의 안전성을 분석하기 위한 모델을 제시하고, 제안모델의 안전성을 분석한다.

1. 무작위 공격에 대한 안전성 분석

본 절에서는 제안 패스워드 모델 $FG(\Sigma,M,N)$ 상에서 권한 없는 제삼자의 무작위 입력에 의하여 인증이 통과될 확률 *RAR(Random Attack Resistance)*과 사용자의 성공적인 인증과정을 K번 지켜본 공격자가 사용자의 패스워드를 정확히 알아낼 확률 *SRR (Shoulder-surfing Resistance in Random attack)*을 사용하여 제안 패스워드 모델의 안전성을 분석한다.

정리 1. 제안 패스워드 모델 $FG(\Sigma,M,N)$ 상에서 RAR은 다음 수식 (1)과 같다.

$$RAR(\Sigma,M,N)=\left(\frac{M}{|\Sigma|}\right)^N \quad (1)$$

증명. i번째 열에서 i번째 패스워드 문자가 그리드화면상에 위치할 확률은 $|\Sigma|$개의 문자 중에서 선택되는 M개에 포함되면 되므로 $M/|\Sigma|$이다. 각 열에서의 선택은 독립적이므로 공격이 성공할 확률, 즉 모든 패스워드 문자가 그리드 상에 위치할 확률은 $(M/|\Sigma|)^N$이다.

정리 2. 주어진 시스템 $FG(\Sigma,M,N)$에서 $C(K)$을 K번의 서로 다른 인증과정이 노출된 상태에서의 후보 패스워드의 평균 개수라고 하면, SRR은 다음 수식 (2)과 같다.

$$SRR(\Sigma,M,N,K)=\frac{1}{C(K)} \quad (2)$$

이 때,

$$C(K)=\left(1+\left(\frac{M-1}{|\Sigma|-1}\right)^{K-1}(M-1)\right)^N \quad (3)$$

증명. 공격자가 K번의 서로 다른 인증과정으로부터 얻은 후보 패스워드의 수를 $C(K)$라고 하면, 공격자가 인증에 성공할 확률은 $1/C(K)$임이 자명하다. 한 사용자의 서로 다른 인증 과정이 K번 노출되었을 때 각각의 입력 화면에는 패스워드 문자가 각 열에 배치되어 있다. 즉 입력화면의 각 열에는 하나의 패스워드 문자가 반드시 있고 $M-1$개의 나머지 문자가 $|\Sigma|-1$개의 문자 중에서 동일한 확률을 가지고 무작위로 선택된다. 따라서 최초의 입력 화면에 나타난 패스워드에 해당하지 않는 하나의 문자가 나머지 $K-1$번의 인증 화면에도 계속 나올 확률은 $((M-1)/(|\Sigma|-1))^{K-1}$이고, 이러한 문자들이 각 열에 $M-1$개씩 있으므로 K번의 모든 인증화면에 나타나는 패스워드가 아닌 문자의 평균 개수는 $((M-1)/(|\Sigma|-1))^{K-1}(M-1)$이다. 따라서 각 열에 대하여 평균적으로 $1+((M-1)/(|\Sigma|-1))^{K-1}(M-1)$개의 문자가 K번의 인증화면에 모두 나타나며, 총 N개의 열이 있으므로 평균 후보 패스워드의 개수 $C(K)=(1+((M-1)/(|\Sigma|-1))^{K-1}(M-1))^N$이다.

이때, 실제 공격자가 한 사용자의 인증화면을 훔쳐보는 것은 매우 어려운 일이므로 공격자에 의해 사용자의 인증화면이 K번 노출될 확률을 0.1^K라 가정하면, 실제로 공격자가 훔쳐보기 공격에 성공할 확률 *PSRR (Practical Shoulder-surfing Resistance in Random attack)*은 다음 수식 (4)과 같다.

$$PSRR(\Sigma,M,N,K)=SRR(\Sigma,M,N,K)\times 0.1^K \quad (4)$$

[그림 5]와 [그림 6]은 정리 1과 정리 2에 따라 무작위 공격에서의 RAR과 PSRR을 분석한 결과이다. 제안 패스워드 입력 방법은 한글 초성과 숫자 및 특수문자를 사용하지만, 본 논문에서는 분석의 편의성을 위해 한글 초성으로만 이루어진 패스워드를 대상으로 분석한다. 따라서 제안 방법의 실제 안전성은 본 논문에서의 분석 결과보다 높다.

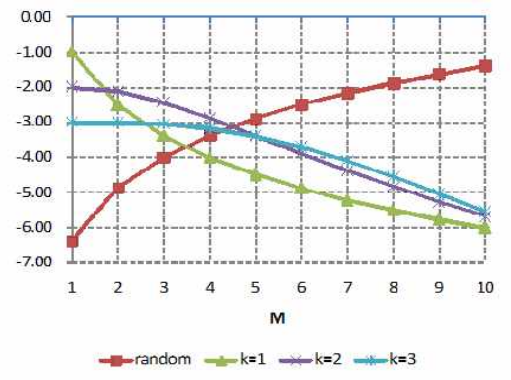


그림 5. $|\Sigma|=19$, N=5일 때, M의 변화에 따른 무작위 공격과 훔쳐보기 공격의 성공 확률.
y축은 $\log_{10}RAR(\Sigma, M, 5)$와 $\log_{10}PSRR(\Sigma, M, 5, K)$를 나타낸다.

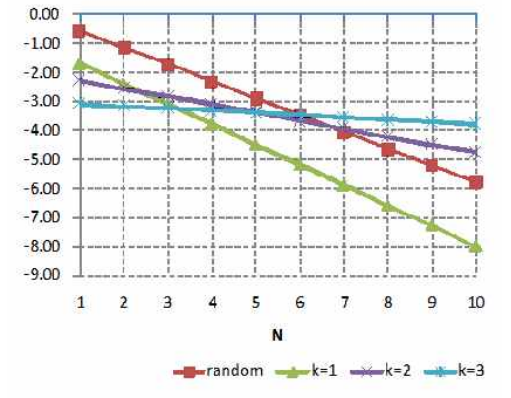


그림 6. $|\Sigma|=19$, M=5일 때, N의 변화에 따른 무작위 공격과 훔쳐보기 공격의 성공 확률.
y축은 $\log_{10}RAR(\Sigma, 5, N)$와 $\log_{10}PSRR(\Sigma, 5, N, K)$를 나타낸다.

제안 방법에서 한글 초성만을 패스워드로 사용한다고 하면, 패스워드를 구성하는 모든 문자의 집합 Σ = {ㄱ, ㄲ, ㄴ, ㄷ, ㄸ, ㄹ ㅁ, ㅂ, ㅃ, ㅅ, ㅆ, ㅇ, ㅈ, ㅉ, ㅊ, ㅋ, ㅌ, ㅍ, ㅎ}으로 $|\Sigma|=19$이다. N=5일 때 M의 증가에 따른 RAR과 $PSRR$의 변화는 [그림 5]와 같다. 그래프에서 M이 증가할수록 훔쳐보기 공격을 통한 패스워드 추측은 어려워지는 반면, 무작위 공격이 용이해진다는 것을 알 수 있다. M이 커지면 무작위 공격 시 패스워드 문자가 그리드 화면상에 나타날 확률이 높아지고, 이는 RAR의 증가를 초래한다. 반면 후보 패스워드 문자의 개수가 많아져 $PSRR$값은 감소한다. [그림 5]의 예에서는 3×5 그리드나 4×5 그리드를 사용하면 RAR과 $PSRR$ 모두 1/1000정도 되므로 무작위 공격에 비교적 안전하다고 볼 수 있다.

[그림 6]은 M=5일 때, N의 증가에 따른 RAR과 $PSRR$의 변화를 나타낸 그래프이다. 그래프에서 N이 증가함에 따라 RAR, $PSRR$ 모두 감소하여 안전성이 높아짐을 볼 수 있다. 하지만 N이 증가하면 사용자는 더 긴 패스워드를 기억해야 하고 인증 시간도 길어진다. [그림 6]의 예에서는 5×8 그리드를 사용할 경우 비교적 안전하다고 볼 수 있다.

2. 사전 공격에 대한 안전성 분석

제안 시스템은 3.1절에서 분석한 결과와 같이 무작위 공격에 비교적 안전하다고 볼 수 있으나, 한글 초성을 패스워드로 사용할 경우 사전 공격에 노출될 위험이 크다. [그림 6][그림 7][그림 8]은 한글 명사 사전을 분석한 결과이다. 여기서, 단일단어는 해당 음절수를 가지는 명사의 집합이며, 복합단어는 두개의 명사의 조합을 허용하는 경우를 의미한다.

[그림 7]은 음절수에 따른 단일명사와 복합명사의 단어 수를 비교한 것으로, 한글 명사는 2음절 3음절 명사가 가장 많은 것을 볼 수 있다. 하지만 2-3음절 명사로는 충분한 패스워드 스페이스를 확보하기 어렵기 때문에 복합단어를 허용하는 것이 바람직하다. 제안 패스워드 시스템에서 사전 공격을 위해 실제로 사용되는 한글 초성 조합의 분포는 [그림 8]과 같다. 한글 명사 사전에 실제로 나타나는 한글 초성의 조합은 4음절 단어가 가장 많지만, 두 단어의 조합을 허용할 경우 5음절 이상에서도 사용 가능한 초성 조합의 개수가 계속 증가함을 볼 수 있다. [그림 9]는 전체 한글 초성 조합에 대한 실제 사용 가능한 한글 초성 조합의 비율을 나타내며, 단일단어를 사용할 경우 3음절 이상에서 그 효율이 급격히 떨어지는 반면, 복합단어를 허용할 경우 효율이 비교적 천천히 감소함을 볼 수 있다. [표 1]은 한글 명사 사전을 분석한 구체적인 결과이다.

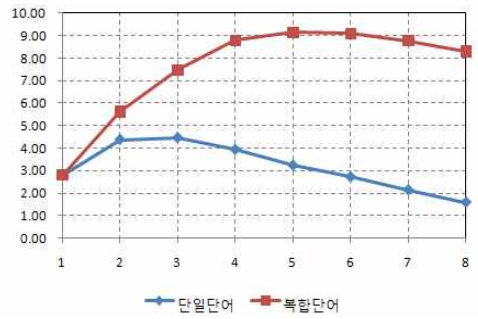


그림 7. 음절수에 따른 한글 명사 단어 수 비교.

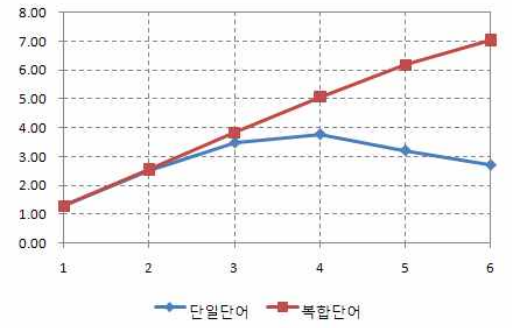


그림 8. 음절수에 따른 한글 명사에서 나타나는 초성 조합의 수.

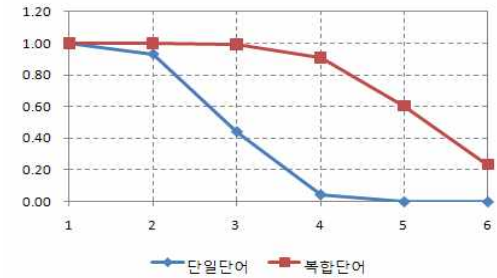


그림 9. 음절수에 따른 전체 가능한 한글 초성 조합에 대한 실제 한글 명사에서 나타나는 초성조합의 수의 비율.

표 1. 음절수에 따른 한글 명사의 초성 조합의 개수 비교

음절수	가능한 초성조합수	단일단어	복합단어
1	19	19	19
2	361	336	361
3	6859	3034	6804
4	1303	5919	118514
5	2476099	1627	1496527
6	47045881	510	10944756

본 논문에서는 한글 명사 사전으로 추출한 유효한 초성 조합들을 사용한 사전공격 확률 *DAR (Dictionary Attack Resistance)*과 사전공격에서의 훔쳐보기 공격 성공 확률 *SRD (Shoulder-surfing Resistance in Dictionary attack)*을 통해 제안 방법의 사전 공격에 대한 안전성을 분석한다. 사전 공격에서 a*(N)*를 *N*음절을 가지는 명사의 이론적 패스워드 공간이라고 하면, a(N)는 [표 1]의 전체 가능 초성 조합 수 와 같다. *r(N)*을 *N*음절을 가지는 명사의 전체 한글 초성 조합에 대한 실제 사용 가능한 한글 초성 조합의 비율이라 하면, 본 논문에서는 [표 1]의 가능한 초성 조합 수(a(N))에 대한 단일단어 및 복합단어의 유효한 조합 수의 비율이 *r(N)*에 해당한다.

정리 3. 제안 패스워드 모델 $FG(\Sigma, M, N)$ 상에서 DAR은 다음 수식 (5)과 같다.

$$DAR(\Sigma, M, N) = \frac{M^N \times r(N)}{|a(N)|} \quad (5)$$

증명. $M \times N$ 그리드 상에 존재할 수 있는 유효한 패스워드의 수는 평균적으로 $M^N \times r(N)$ 개 이므로, 사전 공격이 성공할 확률은 $(M^N \times r(N))/|a(N)|$이다.

정리 4. 제안 패스워드 모델 $FG(\Sigma, M, N)$에서 $C(K)$을 K번의 서로 다른 인증과정이 노출된 상태에서의 후보 패스워드의 평균 개수라고 하면, SRD은 다음 수식 (6)과 같다.

$$SRD(\Sigma, M, N, K) = \frac{1}{C(K)} \quad (6)$$

이 때,

$$C(K) = 1 + \left(\frac{(M^N - 1) \times r(N)}{|a(N)| - 1} \right)^{K-1} \times (M^N - 1) \times r(N) \quad (7)$$

증명. 공격자가 K번의 서로 다른 인증과정으로부터 얻은 후보 패스워드의 수를 $C(K)$라고 하면, 공격자가 인증에 성공할 확률은 $1/C(K)$임이 자명하다. 한 사용자의 서로 다른 인증 과정이 K번 노출되었을 때 각각의 입력 화면에는 반드시 하나의 패스워드가 존재해야 한다. 이를 제외한 $M^N - 1$개의 가능한 초성의 조합 중

N에 따른 일정한 확률 r(N)의 비율로 유효한 패스워드 후보가 평균적으로 존재한다. 따라서 첫 번째 인증화면에서 사용자의 패스워드를 제외한 유효한 패스워드 후보의 수는 $(M^N-1)\times r(N)$이고, 최초 입력화면에 나타난 패스워드가 이후의 K-1번의 인증화면에도 계속 나올 확률은 $(((M^N-1)\times r(N))/|a(N)|-1)^{K-1}$이므로, K번의 인증화면에 모두 나타나는 후보 패스워드의 평균 개수는 수식 (7)과 같다.

이때, 공격자에 의해 사용자의 인증화면이 K번 노출될 확률을 0.1^K라 가정하면, 실제로 공격자가 훔쳐보기 공격에 성공할 확률 *PSRD(Practical SRD)*은 다음 수식 (8)과 같다.

$$PSRD(\Sigma,M,N,K) = SRD(\Sigma,M,N,K)\times 0.1^K \quad (8)$$

[그림 10]과 [그림 11]은 단일단어를 사용할 경우 M과 N의 증가에 따른 *DAR*과 *PSRD*의 변화를 나타낸 그래프이다. [그림 9]에서 *DAR*과 *PSRD*값이 모두 좋은 값을 가지는 M=6의 경우에도 *DAR*과 *PSRD*이 1/100정도로 사전공격에 안전하지 않은 것을 볼 수 있으며, [그림 10]에서도 역시 DAR과 PSRD(K=1인 경우) 1/1,000보다 커서 사전공격에 안전하지 않은 것을 볼 수 있다. 반면, [그림 12]와 [그림 13]에서 보는 바와 같이 복합단어를 허용할 경우 단일단어만을 사용할 경우에 비해 안전성이 크게 개선되었으며, *DAR*과 *PSRD(K=1인 경우)*가 1/1,000 이하인 안전한 패스워드를 구성할 수 있다.

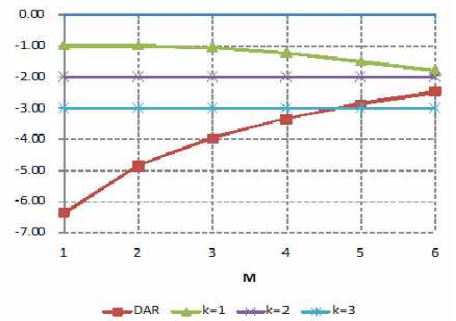


그림 10. N=5일 때, M의 변화에 따른 단일단어에 대한 사전 공격과 훔쳐보기 공격의 성공 확률.
y축은 $\log_{10}DAR(\Sigma, M, 5)$와
$\log_{10}PSRD(\Sigma, M, 5, K)$를 나타낸다.

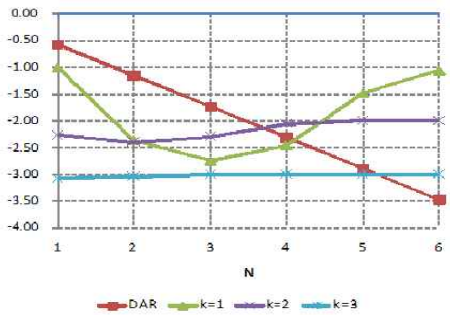


그림 11. M=5일 때, N의 변화에 따른 단일단어에 대한 사전 공격과 훔쳐보기 공격의 성공 확률.
y축은 $\log_{10}DAR(\Sigma, 5, N)$와
$\log_{10}PSRD(\Sigma, 5, N, K)$를 나타낸다.

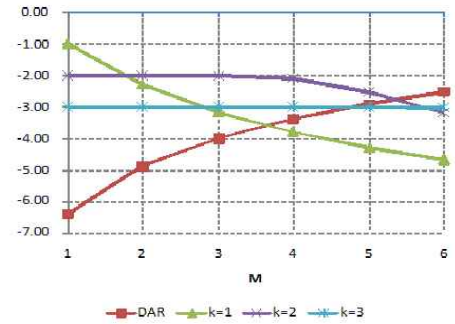


그림 12. N=5일 때, M의 변화에 따른 복합단어에 대한 사전 공격과 훔쳐보기 공격의 성공 확률.
y축은 $\log_{10}DAR(\Sigma, M, 5)$와
$\log_{10}PSRD(\Sigma, M, 5, K)$를 나타낸다.

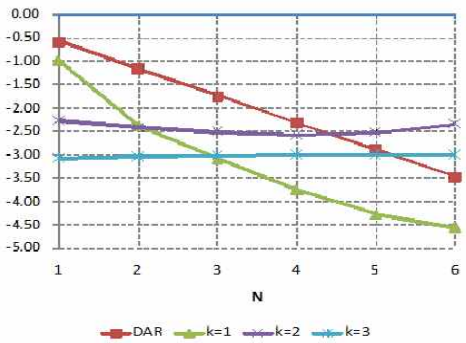


그림 13. M=5일 때, N의 변화에 따른 복합단어에 대한 사전 공격과 훔쳐보기 공격의 성공 확률.
y축은 $\log_{10}DAR(\Sigma, 5, N)$와
$\log_{10}PSRD(\Sigma, 5, N, K)$를 나타낸다.

IV. 결 론

본 논문에서는 모바일 기기에서 사용하기에 편리하면서 훔쳐보기 공격에 보다 견고한 새로운 한글 패스워드 시스템을 제안하였다. 제안방법은 패스워드를 생성하기 위해 한글 초성을 사용하며, 패스워드를 직접 입력하는 대신 주어진 그리드 상에 패스워드를 위치시킴으로써 사용자를 인증한다.

- 제안방법은 무작위 공격에 비교적 견고하다. 예를 들어, 3 X 5, 4 X 5 및 5 X 6과 같은 크기의 그리드를 사용할 경우 *RAR*과 P*SRR*이 약 1/1,000 정도가 된다.
- 제안방법은 사전 공격에서 단일단어만을 패스워드로 사용할 경우 안전성을 보장하기 어렵지만, 두 명사의 복합단어를 허용할 경우, *DAR*과 *PSRD*가 1/1,000 이하인 안전한 패스워드를 구성할 수 있다.
- 9명의 사용자에 대해 실험한 결과, 5 X 5 그리드에서 제안 방법은 평균 23.2초 정도의 인증시간이 소요되어 기존의 문자 패스워드 입력 방법에 비해 다소 많은 시간을 요구한다. 하지만, 모바일 기기 및 인터넷 뱅킹과 같이 훔쳐보기 공격 방지가 중요한 경우에 사용하기에 적합하다.

제안방법은 사용자가 패스워드로 단일 단어를 사용할 경우 사전공격에 의해 노출될 가능성이 있었다. 따라서 향후 본 논문에서 분석한 한글 단어의 초성 조합 빈도를 고려하여 한글 초성 배치를 최적화함으로써 사전공격에 대한 견고성을 향상시키기 위한 연구가 필요하다.

참 고 문 헌

[1] A. H. Lashkari, O. B. Zakaria, S. Farmand, and R. Saleh, "Shoulder surfing attack in graphical password authentication," International Journal of Computer Science and Information Security, Vol.6, No.2, pp.145-154, 2009.

[2] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," Proc. of the 8th USENIX Security Symposium, 1999.

[3] http://www.gridsure.com/

[4] http://www.passfaces.com/

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

[6] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," Proc. of ESORICS 2007, pp.359-374, 2007.

[7] H. Tao and C. Adams, "Pass-go: A proposal to improve the usability of graphical passwords," International Journal of Network Security, Vol.7, No.2, pp.273-292, 2008.

[8] D. Weinshall, "Cognitive authentication schemes safe against spyware," Proc. of IEEE Symposium on Security and Privacy, pp.295-300, 2006.

[9] Y. Berger, A. Wool, and A. Yeredor, "Dictionary attacks using keyboard acoustic emanations," Proc. of the 13th ACM Conf. on Computer and Communications Security, pp.245-254, 2006.

[10] M. G. Kuhn, "Electromagnetic evaesdropping risks of flat-panel displays," Proc. of the 4th Workshop on Privacy Enhancing Technologies, pp.23-25, 2004.

[11] B. Hoanca and K. Mock, "Screen oriented technique for reducing the incidence of shoulder surfing," Proc. of the Int. Conf. on Security and Management 2005, pp.334-340, 2005.

[12] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password

scheme," Proc. of AVI 2006, pp.177-184, 2006.
[13] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing shoulder-surfing by using gaze-based password entry," Proc. of the Symposium On Usable Privacy and Security, pp.13-19, 2007.
[14] D. S. Tan, P. Keyani, and M. Czerwinski, "Spy-resistant keyboard: More secure password entry on public touch screen displays," Proc. of 17th Australia Conf. on Computer-Human Interaction, pp.1-10, 2005.

저 자 소 개

김 종 우(Jong-Woo Kim) 정회원

- 1998년 : 부경대학교 전자계산학과(이학사)
- 2003년 : 부경대학교 전자계산학과(이학석사)
- 2006년 : 부경대학교 정보보호학과(공학박사)
- 2007년 ~ 2009년 : 대구대학교 정보통신공학부 초빙교수
- 2009년 10월 ~ 2011년 1월 : 부산대학교 U-Port정보기술산학공동사업단 박사후연구원

<관심분야> : HCI, 사용자 인증, 정보검색

김 성 환(Sung-Hwan Kim) 준회원

- 2011년 : 부산대학교 정보컴퓨터공학부(공학사)
- 2011년 ~ 현재 : 부산대학교 컴퓨터공학과 석사과정

<관심분야> : 한글언어처리, 정보검색, HCI

박 선 영(Sun-Young Park) 준회원

- 2010년 : 부산대학교 정보컴퓨터공학부(공학사)
- 2010년 ~ 현재 : 부산대학교 컴퓨터공학과 석사과정

<관심분야> : 한글언어처리, 정보검색, HCI

조 환 규(Hwan-Gue Cho) 정회원

- 1984년 : 서울대학교 계산통계학과(이학사)
- 1986년 : KAIST 대학원 전산학과(공학석사)
- 1990년 : KAIST 대학원 전산학과(공학박사)
- 1990년 3월 ~ 현재 : 부산대학교 컴퓨터공학과 교수

<관심분야> : 알고리즘, 응용 그래프 이론, 생물정보학