한글 초성을 이용한 훔쳐보기 공격에 견고한 그래피컬 패스워드

김종우[1] 김성환[2] 김광휘[2] 조환규[2]
[1]부산대학교 U-Port정보기술산학공동사업단
[2]부산대학교 정보컴퓨터공학부
jwkim73@pusan.ac.kr, shpen@naver.com, hwi@pusan.ac.kr, hgcho@pusan.ac.kr

A Shoulder-Surfing Resistant Graphical Password Using Hangul Choseong

Jong-Woo Kim[1] Sung-Hwan Kim[2] Kwanghwi Kim[2] Hwan-Gue Cho[2]
[1]Center for U-Port IT Research and Education, Pusan National University
[2]Dept. of Computer Science and Engineering, Pusan National University

1. 서론

최근 사용이 급증하고 있는 스마트 폰을 위시한 모바일 디바이스들은 사용자의 개인적인 프라이버시와 매우 밀접한 관계가 있고, 물리적으로 작기 때문에 일시적 점유 이탈, 분실, 도난 등의 이유로 허락받지 않은 제삼자에게 노출되기 쉽기 때문에 적절한 수준의 사용자 인증은 매우 중요한 문제이다 [1]. 하지만, 이러한 모바일 디바이스는 물리적으로 작은 입력장치와 화면크기, 제한된 계산 자원 및 전력 소모 문제와 같은 여러 가지 제약을 가지고 있기 때문에 사용자 인증이 용이하지 않다.

전통적인 텍스트 기반 패스워드는 대중적으로 사용되는 방법이지만 추측, 사전 공격, 키로거, 사회공학, 훔쳐보기, 스파이웨어 등의 공격에 취약하고 이는 모바일 환경에서 더욱 심각한 문제이다 [2]. 이러한 취약점을 보완하기 위하여 그래픽 패스워드(Graphical Password)가 연구되어 왔다[3,4,5]. 하지만, 그래픽 패스워드는 일반적인 텍스트 기반의 패스워드보다 훔쳐보기(Shoulder-Surfing) 공격에 오히려 더 취약하다는 문제점을 안고 있다. 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 [2,3]. 이에 본 논문에서는 이러한 훔쳐보기 공격을 방지하기 위한 새로운 그래피컬 패스워드 시스템을 제안하고 이에 대한 안전성과 유용성을 검토한다.

2. 제안 패스워드 시스템 및 안전성 분석

제안하는 시스템은 그림1과 같이 사용자에게 자신의 패스워드를 직접 입력하도록 하는 대신 주어진 격자(grid) 상에 위치시키도록 함으로써 사용자를 인증을 한다. 사용자는 각 열을 회전시켜 다른 문자를 선택하는 입력을 할 수 있다. 제안 시스템은 사용자의 패스워드 문자와 함께 다른 가짜 문자들을 방해요소로 사용함으로써 공격자로 하여금 사용자의 패스워드를 쉽게 알 수 없도록 한다.

제안하는 패스워드 시스템에서 그리드의 행수 M은 훔쳐보기 공격에 대한 견고성에 큰 영향을 준다. 공격자가 사용자의 인증 과정을 지켜본다고 가정할 때, $M=1$인 경우 공격자는 사용자의 패스워드를 쉽게 알 수 있다. 반면 $M>1$인 경우에는 화면을 통해 추측할 수 있는 후보 패스워드가 유일하지 않으며, 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.

본 논문에서는 제안 그래피컬 패스워드의 안전성을 분석하기 위해 무작위 공격에 대한 견고성을 나타내는 척도인 *RAR(Random Attack Resistance)*와 훔쳐보기에 대한 견고성을 나타내는 척도인

*SSR(Shoulder-surfing Resistance)*를 정의하고 분석하였다. 패스워드의 길이 N이 증가하면 *RAR*과 *SSR*이 모두 감소하여 공격에 대한 견고성이 당연히 좋아진다. 하지만 패스워드 그리드의 행의 수 M이 증가하면 그림 2와 같이 SSR은 감소하지만, *RAR*이 증가하기 때문에 적당한 M의 선정이 중요하다. 예를 들어, 그림 2와 같이 $|\Sigma|=30$, $N=5$일 경우 무작위 공격과 훔쳐보기 공격의 성공률이 모두 1/1,000보다 작은 $M=6$은 좋은 선택이 될 수 있다.

그림 1 제안 그래피컬 패스워드 시스템의 입력 화면($M=6$, $N=5$). 입력된 패스워드는 "ㅈㅂㄱㅎㅎ"로 사용자는 "정보과학회"라는 단어를 통해 쉽게 기억할 수 있다.

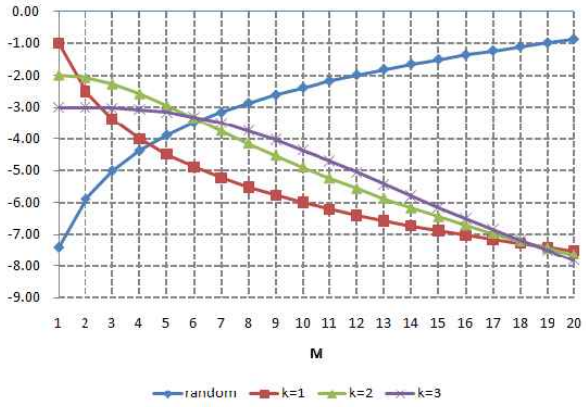

그림 2 $|\Sigma|=30$, $N=5$일 때, M의 변화에 따른 무작위 공격과 훔쳐보기 공격의 성공확률. y축은 $\log_{10}RAR(\Sigma,M,5)$, $\log_{10}PSSR(\Sigma,M,5,K)$를 나타낸다.

3. 결론

본 논문에서는 훔쳐보기 공격에 견고한 그래피컬 패스워드 입력 방법을 제안하고 훔쳐보기 공격에 대한 안전성을 분석하기 위한 모델을 제시하였다. 제안 방법은 패스워드를 직접 입력하지 않고 인증 화면상에 방해 요소 역할을 하는 문자들을 배열함으로써 공격자가 한두 번의 훔쳐보기 공격을 하더라도 사용자의 패스워드를 정확히 알아내는 것이 용이하지 않도록 하였다. 안전성 분석을 위해 RAR과 SSR을 정의하고 그리드의 행(M)과 열(N)과의 관계를 분석하였다. 예를 들어, $|\Sigma|=30$, $M=6$, $N=5$일 때 제안 시스템에서의 RAR값과 $K=1,2$일 때의 $PSSR$이 모두 1/1000 미만을 나타내므로 효율적이라 할 수 있다. 별도의 복잡한 연산 없이 패스워드 문자가 화면에 나타날 때까지 스크롤만 하면 되므로 사용자 인터페이스가 쉽고 간단하다. 인증 소요 시간은 일반적인 텍스트 패스워드보다는 다소 길었으나 보안적인 측면을 고려하면 허용 가능한 범위를 벗어나지 않는다.

4. 참고문헌

[1] W. Jansen. Authenticating mobile device users through image selection. In Data Security, 2004.

[2] 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, 6(2):145-154, 2009.

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

[4] Gridsure website. http://www.gridsure.com, Last accessed August 2010.

[5] Science behind passfaces. http://www.passfaces.com/enterprise/resources/white_papers.htm, accessed August 2010.