8

개인정보보호를 고려한 HCI 기술에 대한 고찰

세종대학교 ▌신수연 · 권태경

1. 서 론

HCI는 Human-Computer Interaction의 약칭으로 인간과 컴퓨터가 쉽고 편하게 상호작용할 수 있도록 작동시스템을 디자인, 평가 완성 하는 과정과 이 과정을 둘러싼 중요 현상들에 관해 연구하는 학문으로 인간과 컴퓨터의 상호작용은 사용자 인터페이스를 통해 이루어진다. 최근 컴퓨터 보급의 증가로 사용자의 편의성을 요구하는 일반대중은 인간에게 친숙한 HCI 기술의 출현을 바라고 있으며, HCI의 목적은 컴퓨터가 인간의 요구를 만족시키고 사용하기 편리하도록 만들어 인간과 컴퓨터의 상호작용을 향상시키는 것이다. HCI 기술의 목적을 달성하기 위해, 현재의 많은 그래픽 기반의 사용자 인터페이스가 HCI적 접근을 통해 음성 사용자 인터페이스와 지능형 시각 사용자 인터페이스 중심으로 발전하고 있다.

HCI는 심리학, 전산학, 디자인은 물론 경영학, 인류학 인간 공학 등 매우 다양한 분야에서 연구가 이루어지고 있다. 하지만, 주로 유용성 및 사용성 등 인간 중심의 컴퓨터를 실현하기 위한 HCI 기술에 초점을 두어 사용자 인터페이스를 통한 개인정보 노출에 대한 문제가 야기되고 있다. 최근 프라이버시 침해 문제가 심각해짐에 따라 유럽과 미국을 포함한 많은 국가에서는 개인정보보호법 및 정책을 제정하였고 HCI 기술에도 적용이 되고 있다. 개인정보보호를 고려한 HCI 기술에 대한 많은 연구가 이루어지고 있으며 특히, 개인정보보호를 고려할 때, 우선적으로 사용자 인증을 위한 키 입력 인터페이스에 대한 연구가 중요하므로 개인정보보호를 위한 키 입력 인터페이스에 대한 연구가 활발히 진행 중에 있다. 예를 들어, 사용자 인증을 위해 많이 사용하는 ATM 기기의 키패드를 이용한 키(PIN 번호) 입력 인터페이스와 키보드 혹은 마우스를 통한 패스워드 입력 인터페이스도 HCI적 접근을 통해 사용자가 편리하게 사용할 수 있는 인터페이스로 발전되어왔지만 사용자의 유용성과 사용성에 반해 프라이버시 침해에 관한 문제들이 대두되고 있다. 사용자가 키보드, 키패드, 마우스 혹은 터치스크린 등 컴퓨터 입력 장치를 통해 비밀 정보를 입력할 때, 직접 관찰하여 비밀 정보를 획득하는 shoulder surfing 공격이 대표적인 예이며, 최근 국내에서는 ATM 기기 상단에 몰래 카메라를 설치하여 사용자의 카드 비밀번호를 알아내는 금융사기 범죄도 발생하였다.

본 논문에서는 개인정보보호를 고려한 다양한 HCI 기술 중에서 우선적으로 키 입력 인터페이스에 대한 연구가 중요하므로, shoulder surfing 공격과 같이 프라이버시 침해 공격에 강인한 프라이버시 보호 키 입력 기술들에 대해 살펴본다. 먼저 프라이버시 침해 공격인 shoulder surfing 공격에 대해 알아보고, 사용자 인증을 위한 키 입력 기술에 대해 알아본다. 또한 개인정보보호 고려한 키 입력 기술인 그래픽 패스워드 인증, 텍스트 패스워드와 그래픽 패스워드를 동시에 사용하는 하이브리드 인증, 응시기반 인증의 동향과 대표적인 기법에 대해서 살펴본다. 마지막으로 인지 인증 프로토콜에 대한 소개와 공격에 대해 알아본다.

2. Shoulder surfing 공격

Shoulder surfing 공격은 사용자의 로그인 과정을 직접 관찰하는 방법을 사용하여 패스워드 인증 방식을 공격하는 기술로 패스워드를 암호화하는 등의 사용자를 안전하게 인증하기 위한 프로토콜과 기법들을 모두 무력화시킬 수 있다.

Shoulder surfing 공격의 가장 잘 알려진 방법은 단어 그대로 누군가가 패스워드를 입력하는 것을 어깨너머로 관찰하여 다른 사람의 패스워드를 획득하는 것이다. 이 공격은 쇼핑몰, 커피샵, 공항 등 붐비는 공공장소의 무선 핫스팟 주변에서 그 위험이 더 크며 그림 1과 같이 ATM에서 PIN을 입력하는 경우에도

† 본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력 핵심기술개발사업의 일환으로 수행하였음[2008-F-036-01, 익명성 기반의 u-지식 정보보호 기술 개발].

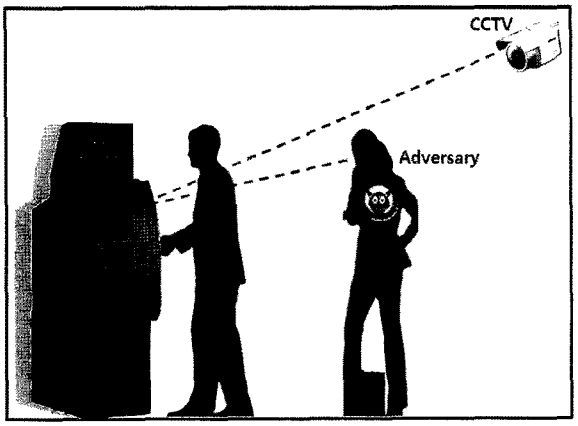


그림 1 Shoulder surfing 공격의 예

마찬가지로 위험하다. 이를 방어하기위해서는 사용자가 몸으로 입력 스크린을 막는 방법이 있지만, 더 강력한 shoulder surfing 공격자는 쌍안경, 비디오 카메라, 비디오 모바일 폰, 전자기 센서, spyware, Trojan software 등 기술을 사용하기도 하며, 이러한 기술 기반 공격은 사용자가 인지하지 못하는 가운데 원격으로도 사용자의 패스워드 혹은 PIN 등 중요한 정보를 획득하는 것이 가능하므로 방어하는 것이 매우 어렵다.

3. 개인정보보호를 고려한 키 입력 인터페이스 기술

현재 키 입력 인터페이스의 대부분은 사용자 인증을 위해 사용되고 있으며, 이러한 키 입력 기술 기반의 인증 방법은 크게 지식 기반 인증, 물리적 토큰 기반 인증, 생체인식 기반 인증, 세 가지로 분류된다[19]. 첫 번째는 지식 기반 인증 방법으로 텍스트 기반 패스워드 기법과 그래픽 기반 패스워드 기법 등을 포함한다. 가장 일반적이고 널리 사용되는 지식 기반 인증 방법은 텍스트 기반 패스워드 기법으로 사용자가 로그인 시, 로그인 ID와 패스워드를 입력하는 방식을 사용한다. 하지만 사용자는 기억하기 쉬운 간단하고 짧은 패스워드를 선택하는 경향이 있으며, 이는 brute forth 검색 공격과 dictionary 공격 등과 같은 다양한 공격에 굉장히 취약하다. 이러한 공격에 방어하기 위해서는 사용자가 길고 랜덤한 텍스트 기반 패스워드를 선택하여 사용해야 하지만, 이러한 패스워드는 사용자가 기억하기 어려우므로 사용자는 사용하기를 꺼린다. 이로 인해, 텍스트 기반 패스워드는 shoulder surfing 공격에 굉장히 취약하다. 이를 보완하기 위해 물리적 토큰 기반 인증과 생체인식 기반 인증 방법이 제안되었다. 두 번째 방법인 물리적 토큰 기반 인증 방법은 키 카드, 은행 카드, 스마트카드 등을 물리적 토큰으로 사용하며 많은 토큰 기반 인증 시스템은 안전성을 강화하기 위해 지식 기반 기술과 함께 사용하는 경우가 많다. 하지만, 물리적 토큰을 사용하는 경우에는 텍스트 기반 패스워드 기법에 비해 shoulder surfing 공격에는 강인하지만, 사용자가 들고 다녀야 하는 불편함이 있으며 잃어버리거나 도난당할 가능성이 크다. 마지막 방법은 생체인식 기반 인증 방법으로 지문이나 홍채와 같은 사용자의 유일한 생물학적 특징을 사용하므로 복제가 어려우며 shoulder surfing 공격에 완벽하게 강인하다고 할 수 있다. 하지만, 취소 및 사용자가 가진 생물학적인 특징을 변경하는 것이 불가능하므로 한 번 노출되면 사용이 불가능하다는 단점을 가진다. 위에서 언급한 인증 방법들의 단점을 보완하면서 개인정보보호를 위해 shoulder surfing 공격에 강인한 키 입력 인터페이스를 이용한 새로운 인증 기술이 활발히 연구되고 있으며, 해당 기술의 동향과 대표적인 기법을 살펴본다.

- 그래픽 패스워드 인증: 인증을 위해 텍스트 대신 그래픽을 패스워드로 사용하는 기법
- 하이브리드 인증: 인증을 위해 텍스트 패스워드와 그래픽 패스워드를 동시에 사용하는 기법
- 응시기반 인증: 인증을 위해 사용자가 눈을 이용하여 패스워드의 일부를 선택하는 기법
- 인지기반 인증: 일련의 질문에 대한 대답의 올바름을 판단하여 인증하는 기법

4. 그래픽 패스워드 인증

그래픽 패스워드 기법은 사용자가 시스템에서 제공하는 그래픽 혹은 이미지를 사용자가 클릭하여 패스워드를 생성하는 기법으로 Blonder에 의해 1996년에 제안되었다[1]. 사람이 텍스트 보다 그림을 더 기억하기 쉬운 점을 이용하여 텍스트 기반 패스워드 기법을 대체하기 위해 제안되었다. 그림이 일반적으로 텍스트 보다 기억 혹은 인지가 더 쉬우며 만약 가능한 그림의 수가 충분히 크다면 그래픽 패스워드 기법의 가능한 패스워드 공간은 텍스트 기법의 패스워드 공간을 초과하므로 dictionary 공격에 더 강인하다. 이와 같은 그래픽 패스워드 기법의 장점들로 연구가 활발히 이루어지고 있으며, 워크스테이션이나 웹 로그인 애플리케이션, ATM 기기, 모바일 장치 등에서 사용되고 있다.

4.1 그래픽 패스워드 기법의 동향

1999년 Jermyn et al.은 "Draw-A-Secret (DAS)"라 불리는 그래픽 패스워드 기법을 제안하였는데 이 기

법은 사용자가 유일한 패스워드를 2D 그리드 상에 그리도록 하였다[12]. 사용자가 그리기를 끝내면 시스템은 그림으로 채워진 그리드의 좌표를 저장하고 인증 단계에서 사용자는 해당 그림을 다시 그린다. 만약 그리는 과정에서 올바른 순서로 동일 그리드를 터치하는 경우 사용자는 인증 받을 수 있다. 해당 기법의 패스워드 공간은 텍스트 기반 패스워드의 최대 공간보다 더 크며, Thorpe and van Oorschot은 DAS의 기억 가능한 패스워드 공간을 분석하고 DAS 기법의 복잡도 속성으로 패스워드 길이와 stroke-count의 영향을 연구하였다[20,21]. 이 외에도 DAS에 대한 더 많은 연구가 이루어졌다[3,18].

"Passface"는 Passfaces Corporation(과거 Real User Corporation)에서 개발한 그래픽 패스워드 기술로 사람은 다른 그림보다 사람 얼굴을 더 쉽게 기억한다는 점을 이용하여 개발되었다[29]. 사용자는 얼굴 데이터베이스에서 패스워드로 사용할 네 개의 얼굴 이미지를 선택하고 인증 단계에서 사용자는 사용자가 선택한 하나의 얼굴 이미지와 미끼로 사용될 여덟 개의 얼굴 이미지로 구성된 아홉 개의 얼굴들의 그리드를 보고 알고 있는 얼굴을 클릭한다. 이러한 과정을 여러 번 반복하고 사용자가 올바르게 모든 얼굴을 식별하면 사용자는 인증에 성공한다. Brostoff et al.은 Passface를 텍스트 기반 패스워드와 비교하여 로그인 실패율이 더 낮음을 보였다[2].

2003년에 Man et al.은 shoulder surfing 공격에 강인한 알고리즘을 제안하였다[17]. 이 알고리즘에서 사용자는 pass-objects로 다수의 그림을 선택하고 각 pass-object는 여러 개의 변형을 가진다. 각 변형은 유일한 코드를 가지며 인증 단계에서 사용자는 여러 개의 장면으로 도전을 받는다. 각 장면은 여러 개의 pass-objects와 많은 수의 미끼 objects를 포함하고 사용자는 현재 장면에서의 pass-object의 변형과 일치하는 유일한 코드를 입력한다. Hong et al.은 후에 이러한 접근 방법을 확장시켜 사용자가 자신의 코드를 pass-object 변형에 할당하는 방법을 사용하였다[8]. 하지만, 두 가지 방법 모두 숨겨진 카메라로부터 패스워드가 노출되는 것을 막을 수는 있지만 사용자가 너무 많은 텍스트 문자열을 기억해야 하는 단점을 가진다.

Jansen et al.은 모바일 장치를 위한 그래픽 패스워드를 2003년에 제안하였다[9-11]. 등록 단계 동안 사용자는 섬네일(thumbnail) 사진들로 구성된 테마를 선택하고 일련의 이미지들을 패스워드로 등록하고, 인증 단계에서 사용자는 등록한 이미지를 순서대로 입력해야한다. 이 기법의 섬네일 이미지의 수가 30개로 제한을 가지므로 패스워드 공간이 매우 작은 단점을 가진다. 또한, 각 섬네일 이미지에는 숫자 값이 할당되고 사용자의 일련의 이미지 선택은 숫자 패스워드를 생성하므로 이미지 열의 길이가 일반적으로 텍스트 패스워드의 길이보다 짧은 문제도 가지고 있다.

Blonder가 제안한 그래픽 패스워드 기법은 사용자가 이미지의 여러 위치를 클릭하여 패스워드를 생성하게 하고 인증 동안 사용자가 패스워드로 선택한 위치의 대략적인 영역을 클릭하도록 하였다[1]. 2005년 Wiedenbeck et al.이 제안한 "PassPoint" 시스템은 사전 정의된 한도를 제거하고 보조 이미지를 사용가능 하도록 하여 Blonder가 제안한 그래픽 패스워드 기법의 아이디어를 확장시킨 시스템이다[24]. 즉, 사용자는 패스워드를 생성하기 위해 이미지의 어떤 위치든 클릭할 수 있으며 각 선택된 픽셀 주변의 허용오차(tolerance)가 계산된다. 인증을 위해 사용자는 선택된 픽셀의 허용오차 이내에서 클릭할 수 있다. 또한 Wiedenbeck et al.은 2006년에 CHC(Convex Hull Click)이라는 그래픽 패스워드 기법을 제안하였다[25]. CHC 기법에서 사용자는 패스 아이콘으로 여러 개의 아이콘을 선택하고 인증 시, 화면에 보이는 굉장히 많은 랜덤하게 배치된 아이콘들 중에서 최소의 패스 아이콘들을 찾아 패스 아이콘들의 볼록한 꼭짓점(convex hull) 이내를 클릭한다. 이러한 과정을 차례로 여러 번 수행하고 만약 사용자가 모두 올바르게 클릭하는 경우 인증된다.

Weinshall은 인지(cognitive) 기반 인증 기법을 제안하였다[23]. 해당 기법에서 사용자는 패스워드로 그림들을 선택하고 이를 기억해야만 한다. 로그인 단계에서 사용자는 머릿속으로 패스워드 그림들이 포함된 경로를 따라 가야하며 다지선다 질문에 대답을 해야한다. 이러한 도전-응답 과정을 여러 번 수행하여 인증이 이루어진다. 사용자만이 경로를 따라가는 것이 가능하므로 인간 혹은 소프트웨어 관찰자가 올바른 패스워드를 결정하는 것은 불가능하다는 주장을 하였지만, 2007년에 Golle과 Wagner는 Weinshall의 인기 기반 인증 기법은 공격자가 성공적인 로그인 과정을 조금만 관찰하면, SAT(Boolean satisfiability problem) solver로 몇 초 내로 사용자의 비밀 키를 알아내는 것이 가능하다는 것을 밝혔다[4].

4.2 그래픽 패스워드 기법의 예: CHC

CHC(Convex Hull Click) 기법은 shoulder surfing 공격에 강인하면서도 인증을 위해 게임과 같은 그래픽 방법을 사용하는 기법으로 2006년 Wiedenbeck et al.

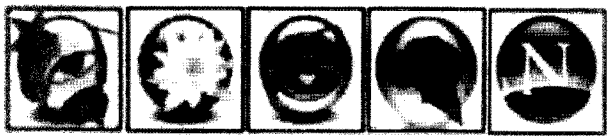


그림 2 패스-아이콘으로 선택된 아이콘의 예[25]

에 의해 제안되었다. CHC 기법은 사용자가 패스워드 이미지를 직접 클릭할 필요가 없으므로 안전하지 않은 장소에서도 사용자가 자신의 그래픽 패스워드로 안전하게 인증 받는 것이 가능하다.

해당 시스템은 몇 백 개의 아이콘들로 구성된 매우 큰 포트폴리오를 사용하며 아이콘들은 텍스트 없이 이미지만을 사용하여 보여 진다. 사용자는 패스워드를 생성하기 위해 포트폴리오에서 자신의 패스-아이콘(pass-icons)으로 그림 2와 같이 몇 개의 아이콘들을 선택하고 사용자는 선택한 패스-아이콘들을 기억해야만 한다.

로그인 단계가 시작되면 화면에는 그림 2와 같이 포트폴리오에서 랜덤하게 선택된 수많은 아이콘들이 화면에 배치된다. 이 아이콘들은 3개 이상의 사용자 패스-아이콘들과 많은 다른 아이콘들로 구성된다. 사용자는 해당 화면의 아이콘들 중에서 자신의 패스-아이콘들은 찾아 머릿속으로 각 패스-아이콘을 꼭짓점(convex hull)으로 그림 3의 색이 칠해진 부분처럼 잇는다. 실제로 칠해진 부분은 사용자의 머릿속에서 그리는 그림으로 사용자는 해당 부분의 어떤 곳이든 클릭해도 된다. 최종 인증을 위해 이 과정을 몇 번 반복하게 된다.

CHC 기법의 유용성 테스트를 통해 shoulder surfing 공격을 방어하면서 인증을 하기위해서는 더 많은 시간 비용이 들지만, 초보자도 정확하게 자신의 그래픽 패스워드 입력이 가능하며 시간이 지날수록 자신의 그래픽 패스워드를 더 잘 기억함을 보였다.

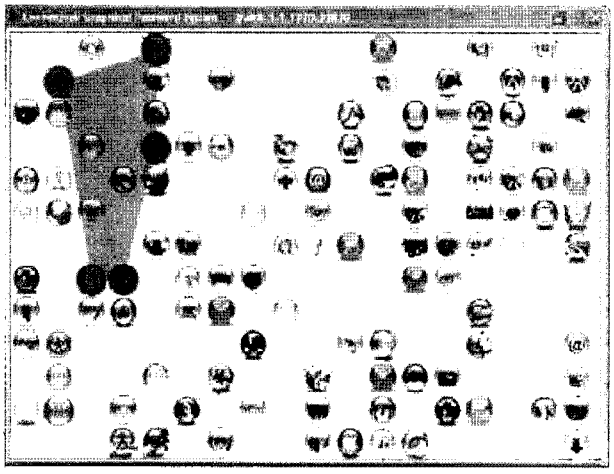


그림 3 다섯 개의 패스-아이콘으로 이루어진 convex hull을 포함한 그래픽 패스워드 인터페이스의 예[25]

5. 하이브리드 인증

하이브리드 인증 방식은 텍스트 기반 패스워드 기법과 그래픽 패스워드 기법을 혼용하여 shoulder surfing 공격에 취약한 텍스트 기반 패스워드 기법의 문제점과 단순한 방식의 그래픽 패스워드 기법이 직접관찰로 어느 정도 추측이 가능하고 shoulder surfing 공격에 강인하기 위해서 여러 번의 시도가 필요하다는 단점을 보완하기 위해 제안되었다.

5.1 하이브리드 기법의 동향

2007년 Zhao와 Li는 대부분의 그래픽 패스워드 기법의 시스템 요구 사항과 통신비용이 텍스트 기반 패스워드에 비해 현저히 크다는 점과 여전히 shoulder surfing 공격에 취약하다는 점을 지적하고 텍스트 기반 패스워드와 그래픽 패스워드를 통합한 S3PAS (Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication System)을 제안하였다[26]. S3PAS는 로그인 단계에서 사용자는 로그인 이미지에서 자신의 텍스트 패스워드를 찾아 보이지 않는 삼각형 지역 내를 클릭하는 방식이다.

2009년 Zheng et al.은 또 다른 하이브리드 인증 방식인 stroke 기반 텍스트 패스워드 인증 기법을 제안하였다[27]. 이 기법의 기본적인 아이디어는 그리드의 stroke의 연결을 패스워드로 사용하고 인증 시 이 stroke 연결에 있는 문자를 클릭한다. 기존 컴퓨터 시스템 외에도 모바일 장치에서도 사용 가능하다는 장점을 가지지만, 일반 사용자에게 상대적으로 친숙하지 않아 사용자가 단순하고 약한 strokes를 패스워드로 가질 수 있다는 결점을 가진다. 또한 다른 그래픽 패스워드 기법에 비해 로그인 단계에서 더 많은 시간을 요구한다는 단점 또한 가진다.

5.2 하이브리드 기법의 예: S3PAS

S3PAS(Scalable Shoulder-surfing Resistant Textual-Graphical Password Authentication System)은 그래픽 방식과 텍스트 방식을 혼합하여 사용하는 하이브리드 기법으로 2007년 Zhao와 Li에 의해 제안되었다[26]. S3PAS는 기존 텍스트 기반 패스워드 기법과 그래픽 패스워드 기법의 다리 역할을 하며 완벽하게 shoulder surfing 공격과 brute forth 공격에 안전하다. 또한 기존에 사용하던 사용자 패스워드 프로필을 변경할 필요 없이 동시에 사용가능하며, 기존 패스워드 기법을 쉽게 대체하는 것도 가능하다.

S3PAS 기법은 서로 다른 환경과 보안 요구사항에 따라 단일-세트 기법, 역할 기반 기법, 강화된 그래픽 기법 등 몇 가지의 변형된 기법을 포함하며 기본 S3PAS 기법인 단일-세트 기법의 인증 과정은 다음과 같다.

사용가능한 패스워드 아이콘 세트 T는 기존 텍스트 기반 패스워드 시스템과 같이 출력가능한 모든 문자들의 집합이다. 사용자가 이전에 선택하고 기억하고 있는 패스워드를 "오리지널 패스워드(original password)"라 부르고 이들은 문자열 k로 나타낸다. 문자열 k의 문자들을 "오리지널 패스-문자(original pass-characters)"라고 부른다. 로그인 단계에서 시스템은 그림 4와 같이 세트 T를 랜덤하게 로그인 이미지에 보여준다.

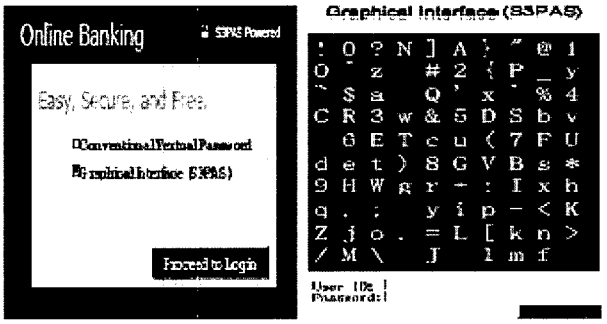
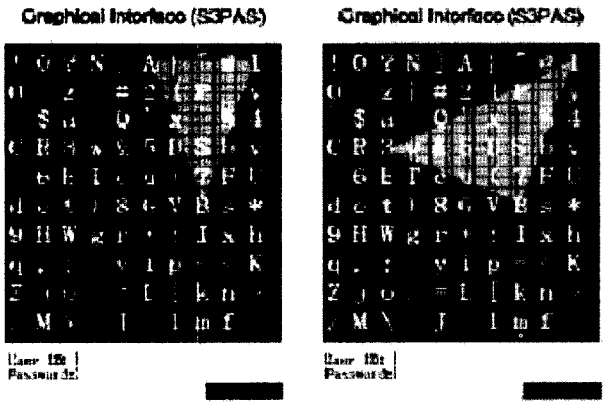
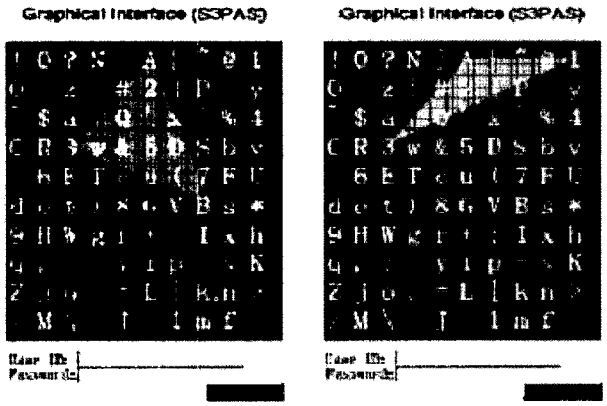


그림 4 S3PAS의 로그인 인터페이스[26]



(a) 패스-삼각형 A1B (b) 패스-삼각형 1B3



(c) 패스-삼각형 B3A (d) 패스-삼각형 3A1

그림 5 S3PAS의 로그인 과정[26]

로그인을 위해 사용자는 로그인 이미지에 보이는 자신의 오리지널 패스-문자들을 모두 찾아야만 하며 "패스-삼각형(pass-triangles)"이라 불리는 보이지 않는 삼각형의 내부를 클릭한다. 패스-삼각형은 특정 클릭 규칙을 따라 세 개의 오리지널 패스-문자들로 생성된다. 대체 방법으로 사용자는 마우스로 클릭하는 대신 패스-삼각형 내부 혹은 경계로부터 텍스트 문자를 입력 혹은 타이핑 할 수 있다. 이 때 선택된 문자들을 "세션 패스-문자(session pass-characters)"라 부른다. 즉, 마지막 입력들은 몇 개의 세션 패스-클릭이거나 혹은 몇 개의 세션 패스-문자일 것이고 이러한 세션 패스-클릭 혹은 세션 패스-문자는 사용자의 세션 패스워드가 된다.

위에서 언급한 것과 같이 S3PAS에서 사용자는 오리지널 패스워드와 세션 패스워드, 총 두 개의 패스워드를 가지며, 사용자는 계정 생성 시에는 오리지널 패스워드를 선택하고 모든 로그인 과정에서 사용자는 서로 다른 세션 패스워드를 입력한다. 따라서 사용자의 오리지널 패스워드가 노출되는 것을 막을 수 있다.

로그인 과정의 예는 다음과 같다. 먼저, 어떤 사용자의 오리지널 패스워드 k가 A1B3라고 가정한다. 이 사용자는 인증을 위해 순서대로 정확하게 네 번 클릭을 해야 한다. 사용자의 패스워드의 조합을 순서대로 표현하면 A1B, 1B3, B3A, 3A1이 된다. 그림 5(a)에서 보여 지는 것과 같이 사용자는 로그인 이미지에서 A1B의 각 문자를 찾고 세 개의 문자로 생성되는 패스-삼각형의 안을 클릭하거나 삼각형 내의 세션 패스-문자(예를 들어, P)를 입력한다. 이러한 과정을 그림 5(b)-(d)와 같이 패스워드의 나머지 조합에 대해서도 수행한다. 사용자가 보이지 않는 패스-삼각형의 안을 네 번 올바르게 클릭하거나 삼각형 안의 세션 패스-문자(예를 들어, PD52)를 네 번 모두 올바르게 입력하면 사용자의 인증이 완료된다.

6. 응시 기반 인증

응시 기반 인증 방식은 기존 인증 방법에서 공격자가 패스워드 혹은 PIN을 결정을 위해 관찰 시, 입력의 모호함을 주기 위해서는 부가적인 단계가 필요하다는 단점을 보완하기 위해 제안되었다.

6.1 응시기반 기법의 동향

2004년 Maeder et al.은 응시 기반 사용자 인증 기법을 제안하였으며, 해당 기법에서 사용자는 로그인을 위해 이전에 정한 이미지의 관심 포인트를 사전 정의된 순서로 오래 응시한다.

Hoanca et al.은 그리드에서 얼굴 선택 시, 응시 기법을 사용하여 Passface를 확장하였다[6,7]. 하지만, 두 개의 응시 기반 인증 기법 모두 기존 패스워드의 사용이 불가능하다는 단점을 가진다.

이 외에도 응시 기반 타이핑에 관한 많은 연구가 이루어졌으며[5,14-16], 이 중에서 일부는 상업 시스템으로 사용되고 있다[28,30].

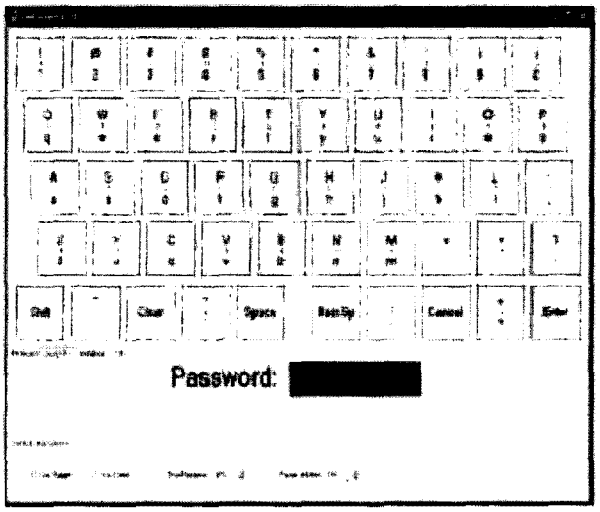
Thorpe et al.은 인간의 뇌파를 이용한 인증 시스템인 "Pass-thoughts"을 제안하면서 응시 기반 방법은 사용자가 눈을 이용하여 패스워드의 일부를 선택하도록 하여 텍스트 기반 혹은 그래픽 패스워드 기법이 제공하는 동일 강도의 관찰 불가능한 패스워드를 가능케 한다고 응시 기반 패스워드 입력에 대한 개념을 소개하였다[22].

2007년 Kumar et al.은 위에서 Thorpe et al.이 언급한 응시 기반 패스워드 입력에 대한 개념을 기반으로 "EyePassword"를 제안하였다[13]. Eyepassword는 shoulder surfing 공격을 완화하기 위해 제안된 시스템으로 해당 시스템에서 사용자는 패스워드 혹은 PIN과 같은 중요한 정보를 스크린의 키보드를 눈으로 응시하여 선택 가능하다. 또한 사용자를 통한 조사로 부가적인 입력 시간이 필요하지만 기존 키보드 입력과 동일한 정확성을 가짐을 보였다.

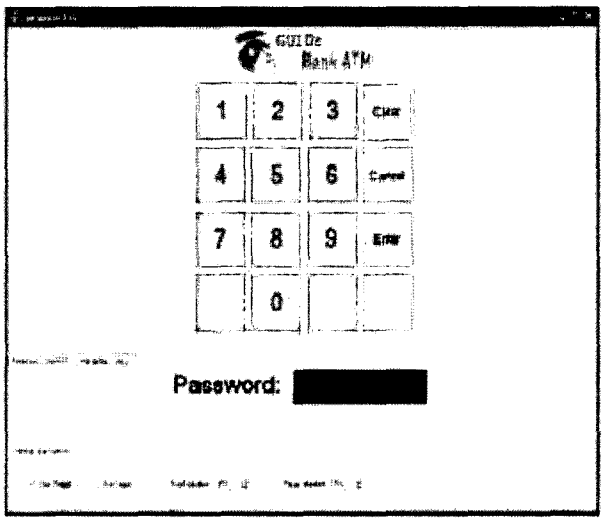
6.2 응시기반 패스워드 기법의 예: EyePassword

EyePassword 시스템은 2007년에 Kumar et al.에 의해 제안되었으며[13], shoulder surfing 공격과 음향(acoustic) 공격을 완화시키면서도 기존 패스워드 사용이 가능한 패스워드 입력 방식을 포함한다. EyePassword는 장애인 사용자를 위해 개발된 기술인 응시 기반 타이핑 기술을 활용하며 컴퓨터 비전 기술을 이용하여 응시 추적(tracking)을 가능케 한다. 즉, 사용자가 스크린 어느 곳을 응시하는지 계산하기 위해 컴퓨터 비전 기술을 이용하여 사용자의 눈동자의 방위를 추적한다. 응시 기반 패스워드 입력은 의도하지 않은 관찰자가 패스워드에 대한 정보 수집을 어렵게 만들면서도 사용자를 위해서는 단순함을 유지하고 사용이 용이하게 한다.

시스템의 동작과정은 키를 타이핑하거나 스크린을 제외하는 것이 아니라 키패드 및 스크린을 응시한다는 점 이외에는 기존의 일반 패스워드 입력과 동일하다. 따라서 그림 6의 스크린 상의 키패드 뿐 만 아니라 기존의 그래픽 패스워드 기법에서 사용하는 그래픽을 포함한 키패드 또한 사용 가능하다.



(a) QWERTY 형식 레이아웃



(b) 키패드 레이아웃

그림 6 응시 기반 패스워드 입력을 위한 스크린 상의 키보드 레이아웃[13]

문자 선택을 기동시키는 방법으로는 머무르는 방법(dwell-based method)과 멀티-모달 방법(multi-modal method)이 있는데 EyePassword는 머무르는 방법에 초점을 두었다. 머무르는 방법은 사용자가 선택하고자 하는 문자를 향한 응시를 고정하고 있은 후, 스페이스 바와 같은 전용 트리거 키를 눌러 특정 문자의 선택을 인식한다. 게다가 눈 추적(eye tracking)의 정확성을 높이기 위해 각 키의 가운데에 빨간색 포커스 포인트를 두었다.

실제로 응시 기반 방식을 사용할 때는 실제 해당 문자가 제대로 선택되었는지에 대한 피드백(feedback)이 필요하다. 특히, 응시 기반 타이핑 기술에서는 사용자에게 올바르게 타이핑이 되었음에 대한 피드백을 반드시 해 주어야하지만, 응시 기반 패스워드는 눈에 보이는 피드백을 하는 경우 해당 피드백으로부터 정

보가 노출될 위험이 있으므로 소리를 이용하거나 스크린의 화면을 반짝거리게 하는 방식을 사용할 수 있으며 패스워드 필드의 부분도 입력된 문자를 그대로 표시하는 것이 아니라 별표(*)와 같이 해당 문자를 알 수 없도록 해야만 한다.

Kumar et al.은 Tobii 1750 눈 추적기[30]를 사용하여 EyePassword를 구현하였으며, 사용자 실험을 통해 입력을 위해 부가적인 시간이 필요하지만 기존 키보드 입력 방식과 유사한 정확성을 가지고 다수의 사용자들이 선호한다는 결과를 얻었다.

7. 인지기반 인증 기법과 공격

인지 기반 인증 기법은 Weinshall이 제안한 기법으로 컴퓨터가 사용자에게 일련의 질문을 하고 사용자가 이에 대해 올바른 대답을 하는 경우 인증이 이루어진다[23]. 사용자에게 주어지는 질문은 사용자와 컴퓨터 사이에서 공유하는 비밀에 기반하며, 해당 비밀은 많은 수의 그림 집합에서 사용자가 선택한 그림들로 구성된다.

Golle과 Wagner는 인지 기반 인증 기법을 SAT solver를 통해 몇 번의 성공 로그인을 관찰하여 사용자의 비밀 인증 키를 몇 초 안에 발견할 수 있는 공격을 성공시켰다[4]. 공격의 핵심은 모든 사용자의 인증 질의에 대한 응답을 공격자가 관찰하는 것으로 사용자의 비밀 키 비트들 사이에서의 boolean 관계를 알 수 있다는 것이다. 충분한 관계들과 SAT solver를 이용하면 사용자의 키를 빠르게 알아내는 것이 가능하다.

7.1 인지 인증 프로토콜

Weinshall이 제안한 인지 인증 프로토콜[23]은 공통 그림의 집합 B를 사용하고, N은 B 집합의 그림의 수를 의미한다. 사용자는 비밀 인증 키로 B의 부분집합 F를 선택하고 F의 크기는 $M < N$이다. 해당 프로토콜은 다른 기법들과 달리 별도의 훈련 단계를 가지며, 사용자는 훈련 단계에서 전체 그림 집합인 B에서 자신의 패스워드로 사용될 비밀 인증 키 부분집합 F를 구별하는 훈련을 받게 된다. 인증 프로토콜은 여러 번의 질의와 응답 라운드로 구성되며 라운드의 수는 요구되는 보안 수준에 따라 결정된다. 각 라운드에서 사용자는 부분집합 F에 대해 P개의 가능한 응답 중에서 하나를 선택하여 응답하며, 모든 질의에 맞는 응답을 한 경우에만 인증이 이루어진다. 각 라운드에서 응답하는 방법은 패널의 맨 왼쪽 위의 그림부터 시작하여 각 셀의 그림이 F에 속한 그림인지를 판단하여 F에 속한 그림 즉, 비밀 인증 키인 경우에는 아래 셀로 이동하고 그렇지 않은 경우에는 오른쪽 셀로 이동한다. 이러한 과정으로 계속 경로를 만들며 진행해 가다가 오른쪽 끝에 도착하거나 아래쪽 끝에 도착하면 끝 쪽에 있는 정수 값을 P개의 가능한 응답 중에서 선택하여 클릭한다. 인지 인증 프로토콜은 high complexity 버전과 low complexity 버전을 가지지만, 본 논문에서는 high complexity 버전과 그에 대한 공격만 언급한다.

High complexity 버전에서 각 라운드마다 사용자에게 B에서 랜덤하게 선택된 $n < N$개의 그림을 R열과

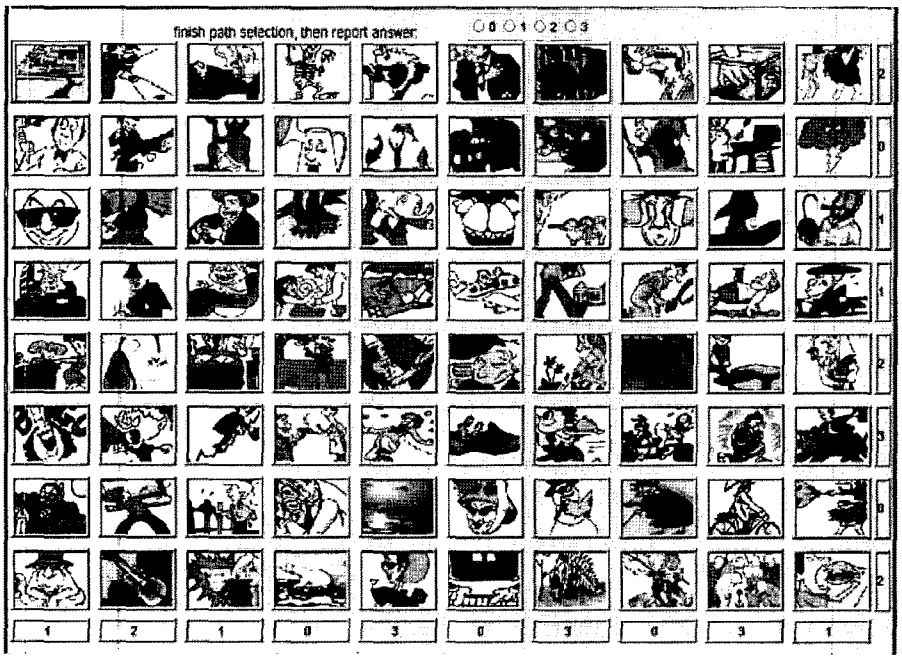


그림 7 인지 인증 프로토콜의 high complexity 패널[23]

C행의 사각형 패널에 랜덤한 순서로 보여준다. 또한 각 행의 오른쪽 끝과 각 열의 아래쪽 끝에는 $[0;P-1]$ 범위의 정수가 할당된다.

그림 7은 high complexity 버전 질의 패널의 예로 $n=N=80$, $M=30$, $P=4$, $R=8$, $C=10$인 경우로 오른쪽 끝과 아래쪽 끝 부분에는 $[0;3]$ 범위의 수가 랜덤하게 배치되며, 사용자는 경로의 최종 값으로 선택된 $[0;3]$ 범위의 정수를 패널 위쪽 라디오 버튼으로 클릭하여 해당 라운드의 질의에 응답한다.

7.2 인지기반 인증 기법에 대한 공격

Golle과 Wagner가 인지 인증 기법의 high complexity 버전을 공격한 방법[4]을 소개한다. 먼저, B 집합의 N개의 그림들에 할당된 boolean 변수인 $A_1,\ldots,A_N$을 정의한다. 만약 i번째 그림이 F에 속하는 그림이라면 $A_i=1$이고, 그렇지 않으면 $A_i=0$이다. A_i의 부정을 $\overline{A_i}$로 표기한다. 사용자의 키를 알아내는 것은 $A_1,\ldots,A_N$ 값을 결정하는 것과 동일하다.

인증 프로토콜의 각 라운드에서 사용자의 키 즉, 변수 $A_1,\ldots,A_N$에 대한 정보를 얻을 수 있다. 이를 위해 각 라운드의 부가적인 boolean 변수를 정의할 필요가 있다. v_r은 r 열 끝에 할당된 정수를 나타내며, w_c는 c 행 끝에 할당된 정수를 나타낸다. $1\le r\le R$과 $1\le c\le C$에 대해, k번째 라운드의 패널의 (r,c) 셀에 할당된 boolean 변수를 $B^k_{(r,c)}$로 나타낸다. 만약 k번째 라운드에서 사용자가 결정하는 경로가 (r,c) 셀을 통과하면 $B^k_{(r,c)}=1$이고, 그렇지 않으면, $B^k_{(r,c)}=0$이다. $1\le r\le R$에 대해, 만약 경로가 패널의 r 열의 오른쪽으로 나가게 되면 $B^k_{(r,C+1)}=1$이고, 그렇지 않으면, $B^k_{(r,C+1)}=0$이다. $1\le c\le C$에 대해, 만약 경로가 패널의 c 행의 아래쪽으로 나가게 되면 $B^k_{(R+1,c)}=1$이고, 그렇지 않으면, $B^k_{(R+1,c)}=0$이다.

질의에 대한 사용자 응답이 주어지면, $A_1,\ldots,A_N$과 $B^k_{(r,c)}$ 사이의 boolean 식을 얻어낼 수 있다. 가장 먼저 알 수 있는 것은 각 라운드에서 사용자의 경로는 패널의 왼쪽 맨 위의 코너에서 시작한다는 점이므로, 이를 이용하여 boolean 식 $B^k_{(1,1)}=1\ \forall k$을 얻을 수 있다. 사용자는 현재 셀의 그림이 비밀 부분집합 F에 속한 그림이라면 아래로 이동하므로, 이를 다음의 boolean 식으로 표현할 수 있으며, 식에서 $f(k,r,c)$는 라운드 k에서의 (r,c) 셀에 포함된 그림의 인덱스를 의미한다.

$$(A_{f(k,r,c)}\wedge B^k_{(r,c)})\Rightarrow B^k_{(r+1,c)}$$
$$\forall k,\forall r\in\{1,\ldots,R\}\text{ and }\forall c\in\{1,\ldots,C\}$$

또한 사용자는 해당 셀의 그림이 B-F에 속한 그림이라면(즉, 사용자의 비밀 키가 아닌 그림이라면) 오른쪽으로 이동하므로, 이를 다음의 boolean 식으로 표현 할 수 있다.

$$(\overline{A}_{f(k,r,c)}\wedge B^k_{(r,c)})\Rightarrow B^k_{(r,c+1)}$$
$$\forall k,\forall r\in\{1,\ldots,R\}\text{ and }\forall c\in\{1,\ldots,C\}$$

k번째 라운드에서 사용자의 응답을 $p^k\in\{0,\ldots,P-1\}$로 나타낼 때, 만약 $v_r\neq p^k$이면 경로는 열 (r)에서 끝나지 않으며, 만약 $w_c\neq p^k$이면, 경로는 행 (c)에서 끝나지 않는다. 이를 boolean 식으로 표현하면 다음과 같다.

$$\overline{B^k}_{(r,C+1)}\ \forall r\ such\ that\ v_r\neq p^k$$
$$\overline{B^k}_{(R+1,c)}\ \forall c\ such\ that\ w_c\neq p^k$$

마지막으로 경로는 r 열에서 끝나서 $v_r=p^k$가 되거나, c 행에서 끝나서 $w_c=p^k$가 되어야만 하며, 이를 boolean 식으로 표현하면 다음과 같다.

$$\Big(\bigvee_{r|v_r=p^k}B^k_{(r,C+1)}\Big)\vee\Big(\bigvee_{c|w_r=p^k}B^k_{(R+1,c)}\Big)$$

위의 모든 boolean 식은 논리합 정규형(disjunctive normal form)의 boolean 식으로 변형하여 SAT solver의 입력으로 사용한다. 충분한 식이 주어졌을 때, SAT solver는 변수 $A_1,\ldots,A_N$의 유일한 값을 빠르게 출력할 수 있으며, 해당 출력 값으로 사용자의 비밀 키를 알아낼 수 있다.

결론적으로 인지 인증 프로토콜의 모든 규칙들을 boolean 식으로 표현하여 boolean 식들과 SAT solver를 이용하여 사용자의 비밀키를 알아내는 공격을 시도하였다. 이 공격을 통해 인지 인증 프로토콜을 단 몇 초 내로 공격하였으며, 다음의 표는 다양한 프로토콜 파라미터 설정에 대한 high complexity 인증에 대한 공격 비용을 보여준다.

표 1 High complexity 인증에 대한 공격 비용[4]

Authentication protocol para.				Attack complexity	
N	M	P	Pannel size	#Rounds	Time (sec)
80	30	4	8 by 10	60	102
80	30	4	8 by 10	100	7
12	45	4	8 by 10	500	45
12	45	2	8 by 10	1000	≈960

8. 결 론

본 논문에서는 프라이버시 보호를 위한 HCI 기술 중 누군가가 PIN 번호나 패스워드와 같이 중요한 정보를 입력할 때, 어깨너머로 관찰하여 해당 정보를 획득하는 shoulder surfing 공격에 강인한 키 입력 기술에 대해 살펴보았다. Shoulder surfing 공격에 강인한 기술로는 그래픽 패스워드 인증 기술, 텍스트 기반 패스워드와 그래픽 패스워드를 동시에 사용하는 하이브리드 기술과 응시 기반 기술이 있으며, 해당 기술들의 동향과 대표적인 기법에 대해 살펴보았다. 해당 기술들은 shoulder surfing 공격에 강인하여 프라이버시를 보호하는 것이 가능하지만, 현재 사용하고 있는 기술에 비해 부가적인 입력 과정과 시간이 필요하며 친숙해지기 위해서는 훈련 기간이 필요하다. 또한 여전히 공격에 취약한 기법도 존재한다. 따라서 프라이버시 보호를 제공하면서 동시에 기존의 기술이 가지는 단순함과 편리성을 제공할 수 있는 키 입력 기술에 대한 연구가 필요하다.

참고문헌

[1] G. E. Blonder, "Graphical passwords", United States Patent 5559961, 1996.

[2] S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords: A field trial investigation", In Proceedings of HCI 2000, Springer, pp. 405-424, 2000.

[3] J. Goldberg, J. Hagman and V. Sazawal, "Doodling Our Way to Better Authentication", In Proceedings of Human Factors in Computing Systems (CHI), 2002.

[4] P. Golle and D. Wagner, "Cryptoanalysis of a Cognitive Authentication Scheme (Extended Abstract)", In Proceedings of the 2007 IEEE Symposium on Security and Privacy, pp. 66-70, 2007.

[5] J. P. Hansen, K. Torning, A. S. Johansen, K. Itoh and H. Aoki, "Gaze Typing Compared with Input by Head and Hand", In Proceedings of Eye Tracking Research & Applications (ETRA) Symposium, ACM, pp. 131-138, 2004.

[6] B. Hoanca and K. Mock, "Screen Oriented Technique for Reducing the Incidence of Shoulder Surfing", In Proceedings of International Conference on Security and Management (SAM), 2005.

[7] B. Hoanca and K. Mock, "Secure Graphical Password System for High Traffic Public Areas", In Proceedings of Eye Tracking Research and Applications (ETRA) Symposium, ACM, pp. 35, 2006.

[8] 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, 2002.

[9] W. Jansen, "Authenticating Users on Handheld Devices", In Proceedings of Canadian Information Technology Security Symposium, 2003.

[10] W. Jansen, S. Gavrila and V. Korolev, "A Visual Login Technique for Mobile Devices", In National Institute of Standards and Technology Interagency Report (NISTIR) 7030, 2003.

[11] W. Jansen, "Authenticating Mobile Device User Through Image Selection", In Data Security, 2004.

[12] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter and A. D. Rubin, "The Design and Analysis of Graphical Passwords", In Proceedings of the 8th USENIX Security Symposium, 1999.

[13] M. Kumar, T. Garfinkel, D. Boneh and T. Winograd, "Reducing Shoulder-surfing by Using Gaze-based Password Entry", In Proceedings of Symposium on Usable Privacy and Security (SOUPS), ACM, pp. 13-19, July 2007.

[14] P. Majaranta and K. J. Räihä, "Twenty Years of Eye Typing: Systems and Design Issues", In Proceedings of Eye Tracting Research & Application (ETRA) Symposium, ACM, pp. 15-22, 2002.

[15] P. Majaranta, I. S. MacKenzie, A. Aula and K. J. Räihä, "Auditory and Visual Feedback During Eye Typing", In Proceedings of CHI, ACM, pp. 766-767, 2003. http://www.yorku.ca/mack/chi03d.html

[16] P. Majaranta, A. Aula and K. J. Räihä, "Effects of Feedback on Eye Typing with a Short Dwell Time", In Proceedings of Eye Tracting Research & Application (ETRA) Symposium, ACM, pp. 139-146, 2004.

[17] S. Man, D. Hong and M. Mathews, "A shoulder-surfing resistant graphical password scheme", In Proceedings of International Conference on Security and Management (SAM), 2003.

[18] D. Nail and J. Thorpe, "Analyzing User Choice in Graphical Passwords", Technical Report, School of Information Technology and Engineering, University of Ottawa, May 2004.

[19] X. Suo, Y. Zhu and G. S. Owen, "Graphical passwords: A survey", In Proceedings of the 21st An-

nual Computer Security Applications Conference (ASCSAC'05), 2005.

[20] J. Thorpe and P. C. v. Oorschot, "Graphical dictionaries and the memorable space of graphical passwords", In Proceedings of the 13th USENIX security Symposium, 2004.

[21] J. Thorpe and P. C. v. Oorschot, "Towards secure design choices for implementing graphical passwords", In Proceedings of the 20th Annual Computer Security Applications Conference, IEEE, 2004.

[22] J. Thorpe, P. C. van Oorschot and A. Somayaji, "Pass-thoughts: authenticationg with our minds", In Proceedings of New Security Paradigms Workshop, ACM, pp. 45-56, 2005.

[23] D. Weinshall, "Cognitive Authentication Schemes Safe Against Spyware (Short Paper)", In Proceedings of IEEE Symposium on Security and Privacy, pp. 295-300, May 2006.

[24] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy and N. Memon, "PassPoints: design and longitudinal evaluation of a graphical password system", In International Journal of Human-Computer Studies, 63, pp. 102-127, 2005.

[25] S. Wiedenbeck, J. Waters, L. Sobrado and J. C. Birget, "Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme", In Proceedings of AVI, ACM, pp. 177-184, 2006.

[26] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme", In Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07), IEEE, pp. 467-472, 2007.

[27] Z. Zheng, X. Liu, L. Yin and Z. Liu, "A Stroke-based Textual Password Authentication Scheme", In Proceedings of the 1st International Workshop on Education Technology and Computer Science, IEEE, pp. 90-95, 2009.

[28] The EyeGaze Communication System, 2009 by LC Technologies, Inc., http://www.eyegaze.com.

[29] PassFaces: patented technology that uses the brain's natural power to recognize familiar faces, PassFaces corporation, http://www.passfaces.com.

[30] MyTobii Communication System, 2008 Tobii Technology AB, http://www.tobii.com.

신 수 연

2004 세종대 컴퓨터공학과 학사
2006 세종대 컴퓨터공학과 석사
2009 세종대 컴퓨터공학과 박사과정 재학 중
관심분야 : 프라이버시 보호기술, 익명성 기술, 센서 네트워크 등
E-mail : shinsy80@sju.ac.kr

권 태 경

1992 연세대 컴퓨터과학과 학사
1995 연세대 컴퓨터과학과 석사
1999 연세대 컴퓨터과학과 박사
1999~2000 U.C. Berkeley Post-Doc.
2001~현재 세종대 컴퓨터공학부 컴퓨터소프트웨어과 부교수, 정보보호학회 이사 및 편집위원
관심분야 : 정보보호, 응용암호, 네트워크 프로토콜, 프라이버시 보호, HCI 등
E-mail: tkwon@sejong.ac.kr