Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.4, Aug. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.4.545

아이트래킹을 이용한 안전한 패스워드 입력 방법에 관한 연구 - 숄더 서핑 공격 대응을 중심으로*

김 슬 기,[1†] 유 상 봉,[3] 장 윤,[4] 권 태 경[2‡]
[1,2]연세대학교 정보대학원 정보보호연구실(대학원생, 교수),
[3,4]세종대학교 컴퓨터공학과(대학원생, 교수)

A Study of Secure Password Input Method Based on Eye Tracking with Resistance to Shoulder-Surfing Attacks*

Seul-gi Kim,[1†] Sang-bong Yoo,[3] Yun Jang,[4] Tae-kyoung Kwon[2‡]
[1,2]Information Security Lab, GSI, Yonsei University(Graduated student, Professor),
[3,4]Department of Computer Engineering Sejong University(Graduated student, Professor)

요 약

시선 기반 입력은 사용자가 문자를 입력하였을 때, 입력이 제대로 되었음을 확인하기 위한 피드백을 제공한다. 이미 많은 연구에서 적절한 피드백이 시선 기반 입력의 사용성을 높이는 효과가 있음을 증명하였다. 그러나 피드백을 통해 입력된 문자에 대한 정보가 노출되어 숄더 서핑 공격의 대상이 될 수 있다. 적절한 피드백을 활용하여 기존의 사용성을 유지하며 보안성을 향상시킬 필요가 있다. 본 연구에서는 숄더 서핑 공격에 대응하기 위한 새로운 시선 기반 입력 방법인 FFI(Fake Flickering Interface)를 제안한다. 또한, 실험 및 설문을 통해 기존의 피드백을 활용한 시선 기반 입력과 비교하여 FFI의 사용성과 보안성을 평가한다.

ABSTRACT

The gaze-based input provides feedback to confirm that the typing is correct when the user types the text. Many studies have already demonstrated that feedback can increase the usability of gaze-based inputs. However, because the information of the typed text is revealed through feedback, it can be a target for shoulder-surfing attacks. Appropriate feedback needs to be used to improve security without compromising the usability of the gaze-based input using the original feedback. In this paper, we propose a new gaze-based input method, FFI(Fake Flickering Interface), to resist shoulder-surfing attacks. Through experiments and questionnaires, we evaluated the usability and security of the FFI compared to the gaze-based input using the original feedback.

Keywords: Gaze-based Input, Shoulder-Surfing Attacks, Usability, Security, Feedback

Received(01. 28. 2020), Modified(06. 01. 2020), Accepted(06. 08. 2020)

* 이 논문은 2019년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2019R1A2C1088802). 또한 2019년도 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (2019-0-00136, 스마트시티 산업 생산성 혁신을 위한 AI융합 기술 개발)

† 주저자, ksg0131@yonsei.ac.kr
‡ 교신저자, taekyoung@yonsei.ac.kr(Corresponding author)

I. 서 론

시선에 관한 연구는 100년도 넘게 진행되고 있다[1][2]. 시선을 추적하기 위한 연구로부터 시작되어 추적한 시선을 이용하기 위한 연구로 발전되었다. 시선 기반 입력이란 컴퓨터와의 상호작용을 통해 사람의 시선을 이용하여 입력하는 기술이다. 시선이 마우스의 역할을 대신하여 클릭하거나 문자를 입력할 수 있는 것이다. 대부분의 시선 기반 입력은 시선 추적 시스템과 가상 키보드로 구성되어 있으며, 기존의 키보드를 이용하거나 시선 기반 입력을 위한 가상 키보드를 새로 디자인하기도 한다[3]. 시선 기반 입력은 거동이 불편한 환자들에게 의사소통 수단이 될 수 있기 때문에 더욱더 활발한 연구가 필요하다[4].

시선 기반 입력 기술이 더욱 발전하기 위해서는 효율적으로 입력하기 위한 연구가 필요하다. 미다스의 손 문제[5]처럼 사용자가 원하지 않는 불필요한 입력이 이루어지지 않도록 하는 동시에 사용자의 피로감을 최소화할 수 있어야만 한다. 특히, 시선 기반 입력 기술은 안구 마우스와 같이 거동이 불편한 환자들이 사용할 수 있어야 하므로 높은 사용성이 요구된다[6]. 이를 위해 추적한 시선을 이용하여 어떻게 입력에 활용할지에 대한 트리거 메커니즘 연구와 얼마 동안 시선을 머무르게 해야 효율적으로 입력할 수 있을지에 대한 많은 연구가 이루어져왔다. 그뿐만 아니라, 사용성을 더 높이기 위해 사용자가 제대로 입력하였다는 것을 확인할 수 있도록 하는 적절한 피드백에 관한 연구들이 계속해서 진행되고 있다.

사용성 연구를 통해 시선 기반 입력의 사용이 편리해지면서 다양한 분야에 활용되었다. 타이핑, ATM 등에 시선 기반 입력을 적용하면서 패스워드와 같은 중요 정보를 지키기 위한 보안성 연구가 주목받았다. 시선 기반 입력은 숄더 서핑 공격(Shoulder-Surfing Attacks, 어깨너머로 훔쳐보기)에 매우 취약하다[7]. 따라서 이에 대항하기 위한 보안성 연구가 필요하다. 숄더 서핑 공격에 취약한 기존의 패스워드, PIN 등을 시선 기반 입력과 결합하여 보안성을 향상시킨 연구들이 진행되었다[8][9]. 하지만 이러한 기술들은 시선 기반 입력 기술을 활용한 새로운 보안 인증 기술에만 중점을 두고 있기 때문에 활용이 제한적이다. 물론, 패스워드 입력뿐만 아니라 평상시 입력에도 활용 가능한 연구가 있었다[7]. 하지만 해당 기술은 사용자가 입력하고자 한 문자를 제대로 입력하였다는 것을 확인하기 어렵다. 피드백을 통해 입력된 문자에 대해 많은 정보를 제공한다면, 숄더 서핑 공격에 취약해지므로 제한적인 피드백을 사용하였기 때문이다.

시선 기반 입력에서 피드백의 방식에 따라 사용자가 입력하는 문자의 정보가 공격자에게 그대로 노출될 수 있다. 예를 들어 입력된 문자를 말해주는 음성 피드백의 경우, 근처에서 피드백을 엿듣는 것만으로도 쉽게 입력된 정보를 훔칠 수 있다. 혹은 입력된 문자 키를 깜빡이거나 버튼이 눌리는 효과를 주는 시각 피드백의 경우, 근처에서 피드백을 엿보는 것만으로도 쉽게 입력된 정보를 훔칠 수 있다. 이러한 이유로 피드백을 제공하지 않는다면 숄더 서핑 공격에 대한 보안성은 향상될 수 있으나 사용성이 급격히 저하된다. 시선 기반 입력은 거동이 불편한 환자들이 사용할 수 있어야 할 뿐만 아니라, 넓은 활용을 위해서는 편리하게 사용할 수 있어야만 한다. 적절한 피드백을 활용하여 기존의 사용성을 유지하며 보안성을 향상시킬 필요가 있다.

본 논문에서는 숄더 서핑 공격에 대응할 수 있는 새로운 시선 기반 입력 기술인 FFI (Fake Flickering Interface)를 제안한다. 또한, 실험 및 설문을 통해 FFI와 기존의 피드백을 활용한 시선 기반 입력 방법과 비교하여 사용성 및 보안성을 평가한다.

II. 관련 연구

2.1 시선 기반 입력 기술 사용성 연구

2003년 Majaranta 등은 시선 기반 입력에서 청각 및 시각 피드백이 미치는 영향에 관해 연구하였다[10]. 청각 피드백, 시각 피드백, 청각+시각 피드백을 이용한 시선 기반 입력으로 문자열을 입력하도록 실험하였다. 참여자 13명에게 실험한 결과, 청각 피드백을 활용하였을 때 시각 피드백에 비해 빠른 입력 속도와 낮은 오류율을 기록하였다.

2004년 Majaranta 등은 짧은 응시 시간을 가진 시선 기반 입력에서 피드백이 미치는 영향에 관해 연구하였다[11]. 이전 연구[10]보다 더 짧은 응시시간(900ms→450ms)으로 설정하여 18명의 참여자에게 실험하였다. 실험 결과 시각 피드백이 청각 피드백에 비해 빠른 입력 속도를 보였으며, 짧은 응시 시간을 가진 시선 기반 입력에서 피드백은 날카롭고 명확해야 한다는 결론을 얻을 수 있었다.

2006년 Majaranta 등은 시선 기반 입력에서 피드백과 응시 시간이 타이핑 속도와 정확성에 미치는 영향을 연구하였다[12]. 실험 결과, 짧은 청각 피드백인 "클릭" 소리를 사용하였을 때 입력 속도와 정확도 모두 향상되었다. 그리고 긴 응시 시간은 피드백을 통해 추가적인 정보를 제공할 수 있지만 짧은 응시 시간은 간단하고 명확한 피드백을 요구하였다.

2007년 Drews 등은 시선 제스처에 대해 연구하였다[13]. 시선 제스처 알고리즘을 구현하여 유저 스터디와 실험을 진행한 결과, 시선 제스처는 시선 기반 입력의 커다란 문제를 해결할 수 있었다. 시선 교정이 필요하지 않았고 정확도가 문제 되지 않아 값싼 장비를 활용할 수 있었으며 미다스의 손 문제가 드러나지 않아 사용자들의 피로감도 덜했다.

2007년 Kumar 등은 시선과 키보드 트리거를 결합한 입력 방법인 EyePoint를 제안하였다[14]. 20명의 참여자들을 대상으로 실험한 결과, EyePoint는 신체 건강한 사용자들의 일상적인 컴퓨터 작업에 사용할 수 있을 만큼 효과적이고 간단했다.

2009년 Majaranta 등은 사용자가 응시 시간을 조절할 수 있을 때 시선 기반 입력에 익숙해지면 나타나는 결과에 관해 연구하였다[15]. 11명의 참여자에게 15분 동안 가능한 한 많은 문장을 입력하도록 10회에 걸쳐 실험하였다. 실험 결과, 실험 1회 차와 10회 차를 비교하였을 때 유의하게 입력 속도가 빨라졌으며 오류율 또한 낮아졌다. 또한, 실험을 진행하면서 모든 참여자들이 응시 시간을 짧게 조절하였다.

2014년 Kangas 등은 시선 제스처와 햅틱 피드백을 결합한 연구를 수행하였다[16]. 실험 결과, 햅틱 피드백은 시선 기반 입력의 사용성을 향상시켰다. 시각 또는 음성 피드백을 사용하기 어려운 경우, 햅틱 피드백이 모바일 기기 사용에 대한 성능과 만족도를 향상시킬 수 있을 것이라 결론지을 수 있었다.

2016년 Majaranta 등은 시선 기반 입력의 햅틱 피드백을 기존의 시각 및 청각 피드백과 비교하는 연구를 수행하였다[17]. 실험 결과, 햅틱 피드백과 음성 피드백이 시각 피드백보다 입력 속도가 빠르고 오류율 또한 낮았다. 햅틱 피드백은 청각 피드백과 비슷한 결과를 보였으며, 사용자들이 가장 선호하였다.

2.2 시선 기반 입력 기술 보안성 연구

2007년 Kumar 등은 기존 패스워드 사용의 편의성을 유지하면서 숄더 서핑 공격에 대응하기 위한 시선 기반 패스워드 입력 방법인 EyePassword를 제안하였다[7]. 실험 결과, EyePassword는 기존의 키보드를 이용한 패스워드 입력보다 약 5배나 입력 속도가 느렸으나, 기존의 다른 숄더 서핑 대응 기술보다는 빠른 입력 속도를 보였다.

2007년 Luca 등은 숄더 서핑 공격에 대응하기 위한 세 가지 시선 기반 PIN 입력 방법을 평가하였다: 응시 시간을 이용한 방법, 트리거를 이용한 방법, 시선 제스처를 이용한 방법[8]. 실험 결과, 시선 제스처 방법이 다른 두 가지 방법보다 입력 속도는 느렸지만, 정확도는 더 높았다.

2009년 Luca 등은 시선 제스처를 이용한 입력 방법인 EyePassShapes를 제안하였다[18]. EyePassShapes는 PassShapes[19]와 EyePIN[8]의 두 시스템을 결합하여 결점을 제거하여 장점으로 대체시킨 것이다. 실험 결과, EyePassShapes는 기존의 PIN보다 느리지만 EyePIN보다는 빠른 입력 속도를 보였다. 또한, PIN과 PassShapes보다 보안성이 높았다.

2016년 Khamis 등은 모바일 기기에서 숄더 서핑 공격에 대응하기 위한 시선과 터치를 이용한 멀티 모달 인증인 GazeTouchPass를 제안하였다[20]. 실험 결과, 높은 사용성과 숄더 서핑 공격에 대응하기 위한 기존의 싱글 모달 인증보다 높은 보안성을 보였다.

2017년 Khamis 등은 공개된 디스플레이에서 사용할 수 있는 다중 요소 인증 GTmoPass를 제안하였다[21]. 실험 결과, 기존의 인증 방법들보다 약간 느리지만, 공개된 디스플레이에서 숄더 서핑 공격, 열 공격, 스머지 공격에 대응 가능한 것을 보였다.

2017년 Khamis 등은 시선과 터치 입력을 결합하여 모바일 기기에서 사용할 수 있는 안전한 멀티 모달 인증 GazeTouchPIN을 제안하였다[22]. 실험 결과, 다른 입력 방법들보다 입력 속도가 느리지만 숄더 서핑 공격에 훨씬 안전하였다.

2019년 Abdrabou 등은 숄더 서핑 공격에 대응하기 위한 시선, 제스처, 멀티 모달을 활용한 인증 방법의 비교 연구를 하였다[23]. 실험 결과, 시선 기반 입력 방법이 사용성과 보안성의 균형을 잘 이루고 있었으며 인증 속도가 빠르고 오류율이 낮았다.

III. FFI 설계

3.1 위협 모델

시선 기반 입력은 숄더 서핑 공격(Shoulder-Surfing Attacks)에 취약하다. 숄더 서핑 공격은 고전적이고 비기술적이지만 간단한 공격이다[24]. 숄더 서핑 공격자는 사용자의 어깨너머로 중요한 정보의 입력을 훔쳐본다. 이후 공격자는 훔친 정보를 악의적인 용도로 재사용할 수 있다.

시선 기반 입력에서의 숄더 서핑 공격은 주로 입력된 문자에 관한 피드백이 발생하는 순간 이루어진다. 피드백은 시선 기반 입력의 사용성을 높이기 위해 사용자가 문자를 입력하였을 때 문자가 제대로 입력되었음을 알려주는 것이다. 피드백 방식에 따라 입력된 문자의 정보가 공격자에게 노출될 수도 있다.

본 연구는 숄더 서핑 공격을 위협 모델로 선정하며 다음과 같은 전제에 기반을 둔다. 첫째, 공격자는 시선 기반 패스워드 입력 과정을 녹화한 뒤 영상을 보며 입력 정보를 분석할 수 없다. 둘째, 공격자는 사용자가 패스워드를 입력하는 과정의 모니터 화면과 몸의 움직임을 관찰할 수는 있지만, 사용자의 동공을 직접 볼 수는 없다. 셋째, 패스워드 입력 결과를 해킹하여 획득할 수 없다.

3.2 디자인 선택

3.2.1 키보드 레이아웃

현재 널리 사용되고 있는 키보드 레이아웃의 종류는 매우 다양하다. 심지어 관찰 공격에 대한 저항력을 높이기 위해 무작위 키보드 레이아웃을 사용할 수도 있다. 본 연구를 위한 키보드 레이아웃은 사용자가 평상시 타이핑 및 소문자, 대문자, 숫자, 특수문자로 이루어진 패스워드를 입력하기에 익숙해야 하며, 한 화면에 사용자가 인식할 수 있는 많은 문자를 나타낼 필요가 있다. 그렇기에 우리는 본 연구에서 두벌식 한영 키보드 레이아웃을 채택하였다.

3.2.2 문자 입력 방법

우리는 관련 연구를 통해 시선 기반 입력 기술에서 문자가 입력되도록 하는 트리거 메커니즘을 조사하였다. 대표적인 방법으로 사용자가 입력하고자 하는 문자 키에 특정 시간(미리 설정해둔 응시 시간) 동안 머물러 명령을 트리거 하는 방법이 있다. 다른 방법으로는 입력하고자 하는 문자 키에 시선을 머무르며 눈을 깜빡이거나 특정 버튼을 누르는 트리거 메커니즘이 있다. 이외에 시선 제스처, 시선과 제스처의 결합 및 시선과 터치의 결합과 같은 멀티 모달 방법 등이 있다.

응시 시간을 활용한 트리거 메커니즘은 별도의 장치를 필요로 하지 않는 간편한 입력이 가능하다. 또한, 멀티 모달 방법보다 오류율이 낮다[7]. 시선 제스처 방법은 미리 명령을 저장해두어야 하므로 명령이 많아질수록 커다란 저장 공간을 요구하는 문제가 발생할 수 있다[13]. 이 때문에 다양한 명령을 수행하기 어렵다. 그렇기에 우리는 본 연구에서 응시 시간을 활용한 트리거 메커니즘을 채택하였다.

3.2.3 피드백

시선 기반 입력은 사용자가 입력하고자 한 문자가 제대로 입력되었다는 피드백을 통해 사용성을 높일 수 있다. 시선 기반 입력에서 사용되는 피드백은 주로 다음과 같다. 첫 번째 방법은 입력된 키를 반짝이거나 입력된 문자를 보여주는 등의 시각적인 효과를 주는 것이다. 두 번째 방법은 기계적 신호음을 주거나 입력된 문자를 말해주는 등의 청각적인 효과를 주는 것이다[11]. 세 번째 방법은 문자가 입력되었을 때 진동을 일으켜 촉각적인 효과를 주는 것이다[17].

본 연구에서 피드백은 보안을 위해 입력된 문자에 대한 많은 정보를 제공해서는 안 된다. 별도의 장치를 필요하지 않고 간단한 피드백인 입력된 문자 키를 깜빡이는 시각 피드백을 채택하였다.

3.3 FFI 개념 및 작동

제안하는 방법은 시선 기반 입력 시 피드백을 통해 사용자가 입력한 문자에 대한 정보를 확인할 수 있도록 하여 기존 시선 기반 입력 방법의 사용성을 유지하도록 한다. 동시에 공격자는 피드백으로부터 입력된 문자에 대한 정보를 직접적으로 얻을 수 없도록 하여 기존 시선 기반 입력 방법보다 보안성을 향상시키도록 한다.

이를 위해 FFI (Fake Flickering Interface)는 입력에 대한 피드백에 중점을 두어 고안되었다.

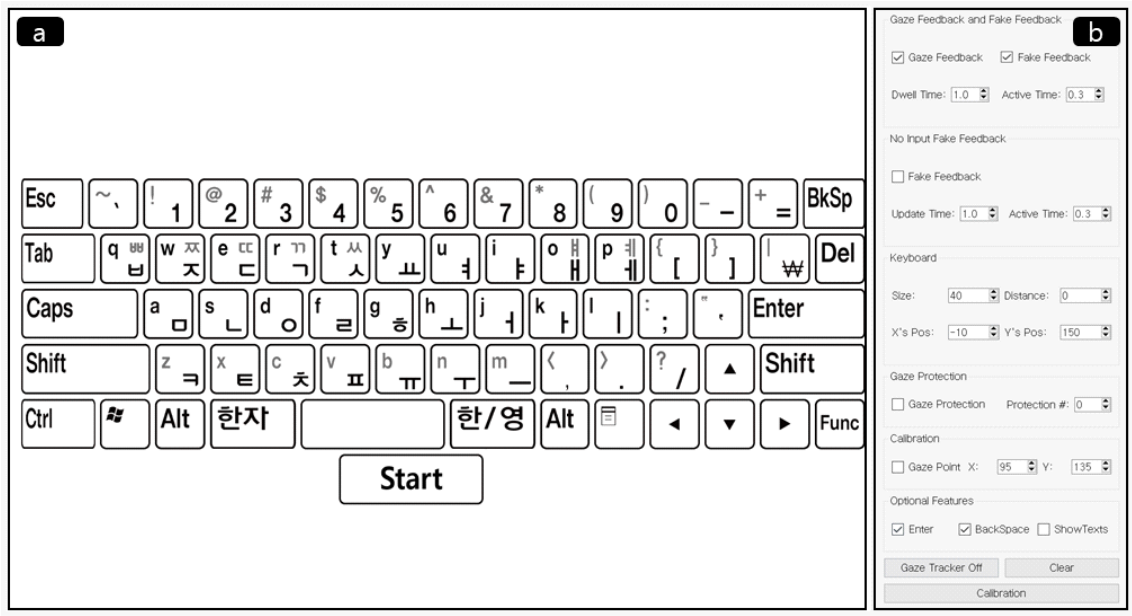

Fig. 1. Interface of FFI. (a) On-Screen Keyboard (b) Control Panel

FFI의 인터페이스는 Fig. 1.과 같다. 인터페이스의 (a) 구역은 문자를 입력할 수 있는 가상 키보드를 구현하였고, (b) 구역은 FFI의 설정값을 조절할 수 있는 제어판을 구현하였다.

기존 피드백은 사용자가 입력한 문자에 대해서만 피드백을 주지만, FFI는 사용자가 입력한 문자뿐만 아니라, 다른 랜덤한 여러 키에 동시다발적으로 피드백을 준다. 진짜 피드백 + 가짜 피드백을 주는 것이다. 사용자 입장에서는 본인이 입력한 문자에 대한 피드백을 제외한 피드백은 가짜 피드백이므로 신경 쓰지 않아도 된다. 진짜 피드백에 관한 확인을 통해 기존 시선 기반 입력 방법의 사용성을 유지할 수 있다. 단, 사용자가 입력한 키에 바로 인접한 문자 키에는 가짜 피드백이 들어오지 않는다. 이는 사용자가 본인이 입력한 키를 보다 더 쉽게 확인하기 위함이다. 만약 사용자가 입력하고자 했던 문자 키에 피드백이 들어오지 않았다면, 단순히 사용자의 실수로 다른 문자 키를 입력한 것일 뿐이다. 하지만 공격자는 진짜 피드백과 가짜 피드백을 구분할 수 없다. 그러므로 다수의 피드백으로부터 입력된 문자에 대한 직접적인 정보를 쉽게 얻을 수 없다. 이를 통해 숄더 서핑 공격에 대한 보안성을 높일 수 있다. FFI의 작동 방식은 다음과 같다.

① 사용자가 입력하고자 하는 문자 키를 응시한다.
② 입력에 대한 피드백으로 응시한 키에 대한 진짜 피드백 + 다른 랜덤한 여러 키에 대한 가짜 피드백이 주어진다.
③ 사용자는 본인이 입력한 키에 대한 진짜 피드백을 확인하며, 나머지 가짜 피드백은 무시한다.

예를 들어 사용자가 FFI를 통해 'f'를 입력할 때, 화면 상의 가상 키보드는 다음 Fig. 2.와 같이 피드백이 들어온다. 가상 키보드의 문자 키 'f'에 대한 진짜 피드백과 다른 랜덤한 여러 키에 대한 가짜 피드백이 주어진 것을 확인할 수 있다. 사용자는 가짜 피드백을 신경 쓸 필요 없이 본인이 입력한 문자 키 'f'에 대한 진짜 피드백을 확인하면 된다. 하지만 공격자는 다수의 피드백을 통해 사용자가 입력한 문자가 무엇인지 쉽게 알 수 없다.

IV. 사용성 평가

4.1 실험 준비 및 참여자

실험을 위해 아이트랙커와 노트북을 설치했다. 사용자의 시선을 탐지하기 위한 아이트랙커는 Tobii eyeX를 사용하였다. 노트북은 14인치에 해상도

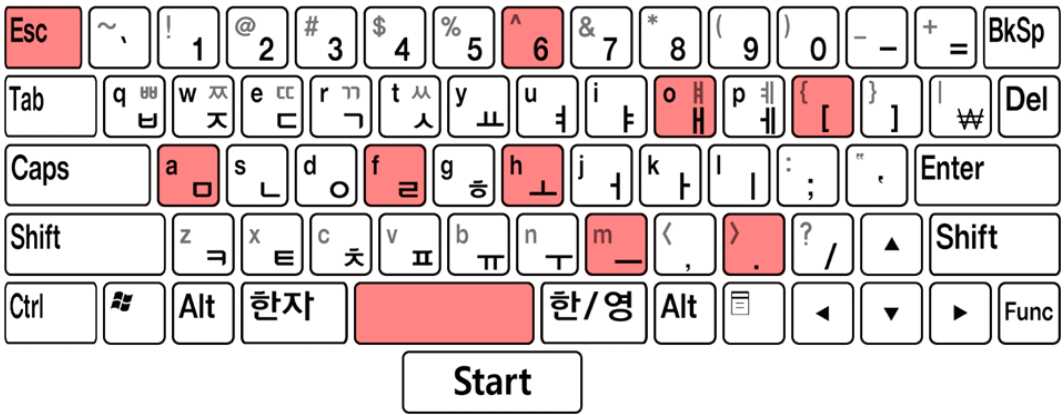

Fig. 2. Typing 'f' using FFI

1920x1080 (FHD)를 사용하였으며 모니터 아래에 아이트래커를 부착하였다. 실험 참여자들은 Fig. 3.과 같이 화면으로부터 60cm 정도 떨어진 위치에 앉게 하였다.

사용성 평가를 위한 실험의 참여자는 총 14명으로, 남성 7명, 여성 7명으로 구성되었다. 이들의 연령은 19세에서 28세 사이로 평균연령 22.93세, 표준편차 2.53이다. 이 중 안경을 쓴 참여자는 2명이었다. 보안 전공 및 직업군을 가진 참여자는 9명, 그렇지 않은 참여자는 5명이었다. 실험 참여자 모두 시선 기반 입력 기술에 대한 경험이 없었다.

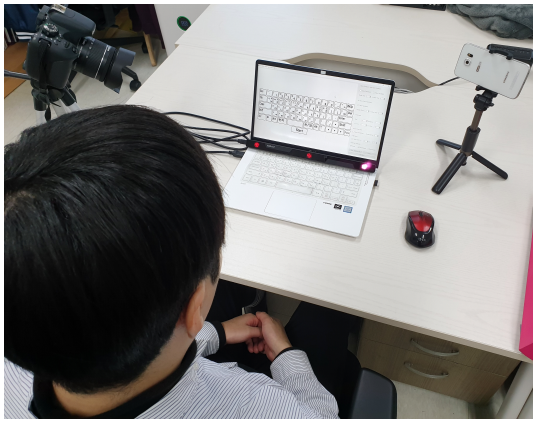

Fig. 3. Usability and Security Evaluation Environment

4.2 종속변수 및 귀무가설

사용성 평가를 위한 실험에서 각각의 입력 방법에 대해 다음 3개의 효과를 측정하였다.

- 입력 시간: 참여자가 패스워드를 입력하기 시작한 순간부터 패스워드의 입력을 끝낸 순간까지의 시간을 측정
- 오류율: 참여자가 주어진 패스워드를 완벽하게 입력하기 전까지 틀린 횟수. 만약 사용자가 하나의 문자 혹은 그 이상이 틀리게 입력하면 오류로 간주
- SUS (System Usability Scale): 사용성에 대한 주관적인 평가를 전체적으로 볼 수 있는 간단한 10개 항목[25]

귀무가설은 다음과 같다.

- $H_{0,0}$ 입력 방법과 입력 시간 사이에는 통계적으로 유의한 관계가 없다.
- $H_{0,1}$ 입력 방법과 오류율 사이에는 통계적으로 유의한 관계가 없다.
- $H_{0,2}$ 입력 방법과 SUS 점수 사이에는 통계적으로 유의한 관계가 없다.

4.3 실험 과정

본 실험은 FFI와 대표적인 기존의 두 가지 피드백을 활용한 시선 기반 입력 방법에 대해 비교하였다. 사용된 입력 방법들에 대한 설명은 다음과 같다.

- FFI: 본 논문에서 제안하는 방법으로 사용자가 입력한 문자 키와 그렇지 않은 랜덤한 여러 문자 키에 피드백을 주는 방법
- No Feedback: 사용자가 문자를 입력하여도 아

무런 피드백이 없는 방법

- 1 Feedback: 사용자가 입력한 문자 키에 대해서만 피드백을 주는 방법

또한 입력 방법들의 각 설정값을 동일하게 하였다. 해당 설정값들은 휴리스틱으로 설정하였다. 각 설정에 대한 설명과 값은 다음과 같다.

- 응시 시간: 사용자가 문자를 입력하기 위해 해당 문자 키에 시선이 고정되어야 하는 시간. 본 실험에서 1.0초로 설정하였다.
- 활성화 시간: 입력에 대한 피드백으로 문자 키가 반짝이는 불빛이 활성화되는 시간. 본 실험에서 0.3초로 설정하였다.
- 피드백 활성화 수: FFI에서 활성화되는 피드백(진짜 피드백+가짜 피드백)의 수. 본 실험에서 10개로 설정하였다.

본 실험은 피험자 내 설계를 사용하여 각각의 참여자들이 3개의 입력 방법에 대해 주어진 실험을 수행하였다. 입력 방법 간의 학습 효과를 줄이기 위해 참여자마다 실험한 입력 방법의 순서를 랜덤화하였다.

실험 시작 전 아이트랙커의 작동 방식과 더불어 진행될 실험에 대해 설명하였으며, 각각의 참여자마다 아이트랙커 사용을 위한 초점을 조정하였다. 시선 기반 입력에 적응하도록 연습용 패스워드 군을 이용하여 각각의 입력 방법에 대해 3개의 패스워드를 한 번씩 성공적으로 입력하도록 연습하였다.

연습을 끝낸 후 참여자마다 랜덤화된 순서로 세 가지 입력 방법에 대해 실험을 진행하였다. 실험에 사용된 패스워드 군은 문자 입력 노력을 고려하여 각각 10개의 패스워드로 구성하였다. 실험에 사용된 10개의 패스워드에 대한 예시는 Table 1.과 같다.

노이즈를 방지하기 위해 참여자마다 패스워드 군의 할당을 랜덤으로 하였다. 실험은 각각의 입력 방법마다 10개의 패스워드를 한 번씩 성공적으로 입력하도록 하였다. 모든 입력마다 입력 시간과 오류 횟수를 측정하였다. 모든 입력을 끝낸 후 각각의 입력 방법에 대한 SUS 설문을 요구하였다.

Table 1. Random Password List

	Type	Password
1	lower case	notebook
2	lower case	password
3	number+lower case	loveme99
4	number+lower case	1q2w3e4r
5	number+lower case +upper case	Vampire3
6	number+lower case +upper case	50Cactus
7	number+lower case+special character	@uthor36
8	number+lower case+special character	reader!1
9	number+lower case+upper case+special character	Fortres$
10	number+lower case+upper case+special character	Dr@gon11

4.4 실험 결과

4.4.1 입력 시간

평가 결과, 각각의 입력 방법에 대해 입력에 소요된 시간은 Fig. 4.와 Table 2.와 같다. 입력에 소요된 시간은 1 Feedback이 가장 짧았고, FFI가 두 번째로 짧았다. 그리고 No Feedback이 입력에 대해 가장 긴 시간이 소요되었다.

반복 측정 분산분석을 유의수준 0.05에서 검증하였다. Mauchly의 구형성 검정[26]을 충족하였다 ($x^2(2)=2.308, p=0.315$). 다중비교로 인한 제1

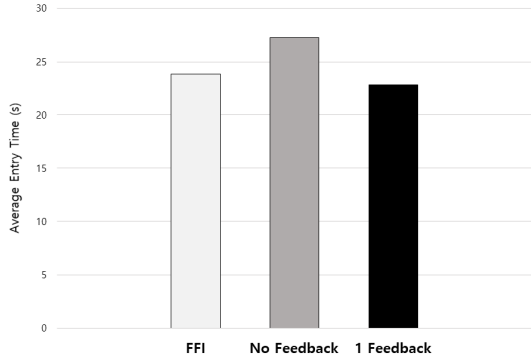

Fig. 4. Average Entry Time for Input Method

Table 2. Descriptive Statistics for Input Time

	Mean	SD
FFI	23.88	5.04
No Feedback	27.29	6.38
1 Feedback	22.82	4.20

종 오류의 보정을 위해 Bonferroni 교정[27]을 시행하였다. 입력 방법이 입력 시간에 미치는 영향이 의미 있게 나타났다($F_{2.26} = 9.99, p < 0.05$).

분석 결과, FFI (평균=23.88, 표준편차=5.04)가 No Feedback (평균=27.29, 표준편차=6.38)에 비해 유의하게 입력 시간이 짧았으며, FFI와 1 Feedback (평균=22.82, 표준편차=4.20)를 비교하였을 때 유의한 차이가 없었다. 이 결과로 인해 귀무가설 $H_{0,0}$이 기각되었으며, 입력 방법이 입력 시간에 유의한 영향을 미치는 것을 보였다.

4.4.2 오류율

평가 결과, 각각의 입력 방법에 대해 발생한 오류 횟수는 Fig. 5.와 Table 3.과 같다. 발생한 오류 횟수는 1 Feedback이 가장 적었고, FFI가 두 번째로 적었다. 그리고 No Feedback이 입력에 대해 가장 많은 오류가 발생했다.

반복 측정 분산분석을 유의수준 0.05에서 검증하였다. Mauchly의 구형성 검증을 충족하지 못해 Greenhouse-Geisser 분석[28]을 통해 제시된 p-value에 근거하여 유의성을 판단하였다. 다중비교로 인한 제1종 오류의 보정을 위해 Bonferroni 교정을 시행하였다. 입력 방법이 오류율에 미치는 영향이 의미 있게 나타났다 ($F_{1.03, 13.39} = 30.94, p < 0.05$).

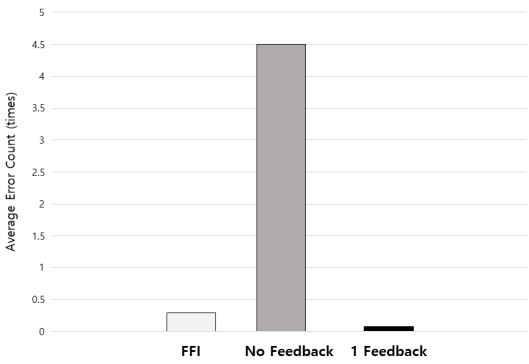

Fig. 5. Average Error Count for Input Method

Table 3. Descriptive Statistics for Error Rate

	Mean	SD
FFI	0.29	0.47
No Feedback	4.50	2.90
1 Feedback	0.07	0.27

분석 결과, FFI (평균=0.29, 표준편차=0.47)가 No Feedback (평균=4.50, 표준편차=2.90)에 비해 유의하게 오류 횟수가 적었으며, FFI와 1 Feedback (평균=0.07, 표준편차=0.27)를 비교하였을 때 유의한 차이가 없었다. 이 결과로 인해 귀무가설 $H_{0,1}$이 기각되었으며, 입력 방법이 오류율에 유의한 영향을 미치는 것을 보였다.

4.4.3 SUS 설문 평가

사용성 평가 결과, 각각의 입력 방법에 대한 SUS 점수 및 해석 결과는 Table 4.와 같다. SUS 점수는 FFI가 평균 66.07, 표준편차 13.25, No Feeback이 평균 37.68, 표준편차 13.78, 1 Feedback이 평균 72.29, 표준편차 10.67로 측정되었다. Adjective는 경험을 설명하기 위해 숫자 대신 형용사를 사용하였다. Good, OK, Poor 등과 같은 단어들이 포함되어 있다. FFI는 OK, No Feedback은 Poor, 1 Feedback은 Good에 해당한다. Acceptable은 허용 가능 또는 허용 불가의 관점으로 설명한 것이다. 대략 70 이상은 허용 가능에, 대략 50 미만은 허용 불가에 해당한다. 50-70 사이의 범위를 약간 허용 가능으로 지정하였다. FFI는 약간 허용 가능, No Feedback은 허용 불가, 1 Feedback은 허용 가능에 해당한다. Grade는 A부터 F까지 있으며, A에 가까울수록 성능이 우수하며 C는 평균을 의미한다. FFI는 C, No Feedback은 F, 1 Feedback은 C+의 Grade에 해당한다.

4.4.3의 SUS 해석에 사용된 지표는 [29]에 기반을 두고 있다. 이 결과로 인해 귀무가설 $H_{0,2}$가 기각되었으며, 입력 방법이 SUS 점수에 유의한 영향

Table 4. SUS Analysis Results for Input Method

	SUS Score	Acceptable	Adjective	Grade
FFI	66.07	Marginal	OK	C
No Feedback	37.68	Not Acceptable	Poor	F
1 Feedback	72.29	Acceptable	Good	C+

을 미치는 것을 보였다.

V. 보안성 평가

5.1 실험 준비 및 참여자

참여자는 총 12명으로, 남성 11명, 여성 1명으로 구성되었다. 이들의 연령은 24세에서 28세 사이로 평균연령 25.17세, 표준편차 0.94이다. 이 중 보안 전공 및 직업군을 가진 참여자는 6명, 그렇지 않은 참여자는 6명이었다.

5.2 종속변수 및 귀무가설

보안성 실험에서 각각의 입력 방법에 대해 레벤슈타인 거리(Levenshtein Distance)[30]를 측정하였다.

귀무가설은 다음과 같다.

$H_{1,0}$ 입력 방법과 레벤슈타인 거리 사이에는 통계적으로 유의한 관계가 없다.

5.3 실험 과정

참여자를 "희생자"와 "공격자"로 역할을 나누었다. 희생자는 시선 기반 패스워드 입력을 하는 참여자이고, 공격자는 희생자가 패스워드를 입력하는 과정을 관찰하며 숄더 서핑 공격을 하는 참여자이다. 5장에서 언급하는 참여자는 공격자를 의미한다. 본 실험은 FFI를 응시 시간, 활성화 시간, 피드백 활성화 수의 설정값을 길고 짧음, 많고 적음으로 나누어 기존의 두 가지 피드백을 활용한 시선 기반 입력 방법에 대해 비교하였다. 본 보안성 실험에서 사용한 각각의 입력 방법에 대한 설정값은 다음 Table 5.와 같이 설정하였다. 해당 설정값들은 휴리스틱으로 설정하였다. FFI의 응시 시간을 0.7초와 1.0초로, 활성화 시간을 0.3초와 1.0초로 나누었다. 또한, 피드백 활성화 수를 5개, 10개로 나누었다.

본 실험은 피험자 내 설계를 사용하여 각각의 참여자들이 10개의 입력 방법에 대해 주어진 실험을 수행하였다. 입력 방법 간의 학습 효과를 방지하기 위해 참여자마다 실험한 입력 방법의 순서는 랜덤화하였다.

Table 5. Value Used in Safety Experiments

	Dwell Time	Active Time	Active Feedback Count
FFI (1)	0.7	0.3	5
FFI (2)	0.7	0.3	10
FFI (3)	0.7	1.0	5
FFI (4)	0.7	1.0	10
FFI (5)	1.0	0.3	5
FFI (6)	1.0	0.3	10
FFI (7)	1.0	1.0	5
FFI (8)	1.0	1.0	10
No Feedback	1.0	0.3	5
1 Feedback	1.0	0.3	5

본 실험은 희생자가 시선 기반 입력을 통해 패스워드를 입력하는 과정을 공격자가 훔쳐보며 희생자가 입력한 패스워드가 무엇인지 추측하도록 하였다. 이를 위해 각각의 시선 기반 입력 방법을 통해 패스워드를 입력하는 과정을 녹화하였으며, 참여자들이 해당 영상을 보며 숄더 서핑 공격을 수행하도록 하였다. 단, 참여자는 해당 영상을 멈추거나 되감기 하는 등의 조작을 통해 입력 정보를 분석할 수는 없다. 이것은 매번 실험마다 희생자가 패스워드를 입력하는 과정을 재현하기 어려운 문제를 해결하고 참여자를 3.1에서 설정한 위협 모델로 가정하기 위함이다.

실험 시작 전 숄더 서핑 공격과 더불어 진행될 실험에 대해 설명하였다. 숄더 서핑 공격에 적응하도록 각각의 입력 방법에 대해 3개의 패스워드를 한 번씩 추측하도록 연습하였다.

연습을 끝낸 후 참여자마다 랜덤화된 순서로 10개의 입력 방법에 대해 실험을 진행하였다. 실험에 사용된 패스워드 군은 문자 입력 노력을 고려하여 각각 5개의 패스워드로 구성하였다. 또한, 학습 효과를 방지하기 위해 참여자마다 패스워드 군의 할당을 랜덤으로 하였다. 실험은 각각의 입력 방법마다 입력된 5개의 패스워드에 대해 숄더 서핑 공격을 수행하도록 하였다. 모든 공격마다 참여자들이 추측한 패스워드를 기록하여 레벤슈타인 거리를 계산하였다.

5.4 실험 결과

5.4.1 레벤슈타인 거리

반복 측정 분산분석을 유의수준 0.05에서 검증하였다. Mauchly의 구형성 검정을 충족하였다 ($x^2(44)=55.783, p=0.192$). 다중비교로 인한 제1종 오류의 보정을 위해 Bonferroni 교정을 시행하였다. 입력 방법이 레벤슈타인 거리에 미치는 영향이 의미 있게 나타났다($F_{9,99}=62.18, p<0.05$).

평가 결과, 레벤슈타인 거리는 Table 6.과 같이 측정되었다. 레벤슈타인 거리 수치는 1 Feedback이 가장 낮았고 FFI (3)이 두 번째로 낮았다. 그리고 No Feedback의 레벤슈타인 거리 수치가 가장 높았고 FFI (6)이 두 번째로 높았다. FFI (1)~(8)은 1 Feedback과 비교하였을 때 유의하게 레벤슈타인 거리 수치가 높았다. F (1), (2), (4), (6), (8)은 No Feedback과 비교하였을 때 유의한 차이가 없었다. 이 결과로 인해 귀무가설 $H_{1,0}$이 기각되었으며, 입력 방법이 레벤슈타인 거리에 유의한 영향을 미치는 것을 보였다.

Table 6. Descriptive Statistics for Levenshtein Distance

	Mean	SD
FFI (1)	5.92	1.58
FFI (2)	6.42	1.34
FFI (3)	5.10	1.25
FFI (4)	6.70	0.99
FFI (5)	5.32	1.44
FFI (6)	7.02	0.75
FFI (7)	5.15	1.44
FFI (8)	6.37	1.24
No Feedback	7.80	0.28
1 Feedback	0.53	0.95

VI. 토 론

6.1 연구 한계점

본 논문에서는 시선 기반 패스워드 입력의 보안성을 높이기 위해 FFI를 제안하였다. 그러나 본 연구에는 다음과 같은 한계점이 있다.

첫 번째, 실험에 사용된 아이트랙커의 기술적 한계이다. 눈의 크기가 작은 사람과 안경을 쓰거나 렌즈를 착용한 사람들은 시선을 탐지하기 어려웠다. 안경을 벗으면 시선 탐지가 제대로 되는 경우도 있었으나, 시력이 나쁜 사람이 안경을 쓰지 않고 화면을 보며 문자를 입력하는 것에는 어려움이 있었다. 이런 문제로 인해 실제로 많은 참여자를 모집하였으나 대다수가 실험을 진행할 수 없어 참여자 명단에서 제외되었다.

두 번째, 실험을 일반화하기에 실험 참여자의 수가 적다. 이는 첫 번째 연구 한계점과 밀접한 문제이다. 실제로 더 많은 참여자를 모집하였으나 대다수가 실험을 진행할 수 없어 참여자 명단에서 제외되었다. 추후 더욱 정교한 장비를 이용하여 사용성 평가와 보안성 평가에 대해 더 많은 실험 참여자를 동일하게 구성할 필요가 있다.

세 번째, FFI의 SUS 점수는 66.07점으로 일반적인 사용성 기준에 다소 미치지 못하는 결과가 도출되었다. 하지만 현재 아이트랙커의 기술적인 문제와 실험에 진행된 다른 두 입력 방법의 SUS 점수와 비교하면 추후 연구를 통해 개선될 여지가 있다.

네 번째, 응시 시간, 활성화 시간, 피드백 활성화 수와 같은 설정값들을 다양한 조건으로 다루지 못했다. 본 연구를 위해 진행된 사용성 및 보안성 실험의 설정값들은 기존 시선 기반 입력에 관한 연구들을 바탕으로 임의의 파일럿 테스트를 통해 휴리스틱으로 설정하였다. 이에 대해 다양한 조건을 다룰 수 있는 추가적인 연구를 진행할 필요가 있다.

6.2 향후 연구

향후 FFI의 사용성과 보안성이 균형을 이루기 위한 FFI의 최적화된 설정값에 대한 연구가 필요하다. 본 연구는 관련 연구들을 참고하여 응시 시간, 활성화 시간, 피드백 활성화 수와 같은 설정값을 휴리스틱으로 설정하였다. 때문에 향후 응시 시간, 활성화 시간, 피드백 활성화 수를 독립 변수로 하여 입력 시간과 오류율이라는 종속 변수에 미치는 영향을 연구할 필요가 있다. 이를 통해 높은 사용성을 위한 최적화된 설정값에 대한 연구가 가능하다. 또한 응시 시간, 활성화 시간, 피드백 활성화 수를 독립 변수로 하여 레벤슈타인 거리라는 종속 변수에 미치는 영향을 연구할 필요가 있다. 이를 통해 높은 보안성을 위한 최적화된 설정값에 대한 연구가 가능하다. 이와 같은 추가 연구가 이루어진다면 FFI의 성능이 더욱 향상될 것이다.

VII. 결 론

본 논문에서는 시선 기반 입력 기술에 관해 연구하였다. 시선 기반 입력 기술은 숄더 서핑 공격에 취약하다는 한계점을 가지고 있었다. 기존의 사용성을 유지하며 숄더 서핑 공격에 대응하기 위한 FFI를 제안하고 이에 대한 사용성 및 보안성 평가를 진행하였다.

FFI는 진짜 피드백과 가짜 피드백을 활용하였다. 사용자는 진짜 피드백을 통해 입력하고자 한 문자를 제대로 입력한 것을 확인할 수 있었으며, 공격자는 가짜 피드백 때문에 사용자가 입력한 문자에 대한 정보를 쉽게 얻지 못하였다. 이를 위해 시각 피드백과 응시 시간을 활용한 메커니즘을 활용하였으며, 기존의 두벌식 한영 키보드 레이아웃을 사용하여 사용자의 거부감과 피로도를 줄일 수 있었다.

사용성 평가를 위해 14명의 실험 참여자를 모집하였다. 실험 결과, FFI는 No Feedback보다 입력에 소요된 시간이 유의하게 짧았으며, 1 Feedback과 비슷한 입력 시간을 보였다. 또한, FFI는 No Feedback보다 오류 횟수가 유의하게 적으면서, 1 Feedback과 비슷한 오류 횟수를 보였다. SUS 설문 결과 FFI의 SUS 점수는 66.07점, No Feedback은 37.68점, 1 Feedback은 72.29점이었다. 즉, No Feedback보다 뛰어나면서 1 Feedback과 비슷한 사용성을 보였다.

보안성 평가를 위해 12명의 실험 참여자를 모집하였다. 본 실험은 FFI를 설정값에 따라 나누어 기존의 두 가지 피드백을 활용한 시선 기반 입력 방법에 대해 비교하였다. 실험 결과, 모든 FFI가 1 Feedback보다 공격 성공률이 낮았다. 또한, 일부 설정값을 가진 FFI가 No Feedback과 비슷한 보안성을 보였다.

본 연구에서 제안하는 FFI는 비교한 기존의 두 기술의 단점을 보완하고 장점을 결합하였다. 즉, No Feedback과 비슷한 보안성을 보이면서 1 Feedback과 비슷한 사용성을 보인다. 하지만 아직 아이트랙커의 기술적 문제 때문에 원활히 시선을 탐지할 수 있는 사용자가 제한적이었다. 이 때문에 다양한 실험 참여자 모집단을 대상으로 진행하지 못했으며, 다소 아쉬운 SUS 점수를 얻었다. 또한, 실험에 사용된 설정값들은 임의의 파일럿 테스트를 통해 휴리스틱으로 설정하였다. 향후 아이트랙커 기술의 발전뿐만 아니라 FFI의 응시 시간, 활성화 시간, 피드백 활성화 수와 같은 설정값을 어떻게 설정하였을 때 사용성과 보안성이 최적화된 균형을 이룰 수 있을지에 관한 연구가 더 필요하다.

기존의 시선 기반 입력 기술을 활용한 일부 보안 연구들은 패스워드와 보안 인증에만 활용할 수 있도록 설계되어있는 한계가 존재한다. 하지만 FFI는 평상시 타이핑을 할 때뿐만 아니라, 패스워드 혹은 민감한 정보를 입력할 때 언제든지 활용할 수 있다는 데에 의의가 있다. 활성화/비활성화 기능을 추가하여 더욱 편리하고 안전한 시선 기반 입력의 사용이 이루어질 수 있을 것이다.

특히 FFI는 키보드 보안을 중요시하고 있는 전자상거래에서 활용될 수 있다. 언제 어디서나 전자상거래가 이루어지기 때문에 이를 보호하기 위해 현재 대부분의 전자상거래는 다양한 보안 프로그램과 가상 키보드를 이용하고 있다. 대표적으로 가상 키보드의 자판 배열을 랜덤화하는 방식, 임의 각도를 회전시키는 방식, 임의 배율로 확대하는 방식이 있다. 이러한 기술들은 키로거, 메모리 해킹 등 하드웨어 레벨의 해킹 방법들에 대한 보안을 중점으로 다루고 있기 때문에 숄더 서핑 공격에 취약할 수 있다. 물론 가상 키패드에 형성되는 마우스 포인터를 다수 생성하여 가짜 정보를 통해 숄더 서핑 공격에 대응하는 기술도 있다. 하지만 이는 별도의 마우스가 없는 모바일 기기에서 사용이 어려울 수 있다. 향후 시선 기반 입력 기술이 활성화된다면 기존의 보안 기술들과 결합하여 더욱 편리하고 안전한 입력이 이루어질 것이다. 앞으로도 시선 기반 입력 기술에 관한 많은 연구가 필요하다.

References

[1] JACOB, Robert JK; KARN, Keith S. "Eye tracking in human-computer interaction and usability research: Ready to deliver the promises." In: The mind's eye. North-Holland. p. 573-605, 2003.

[2] POOLE, Alex; BALL, Linden J. "Eye tracking in HCI and usability research." In: Encyclopedia of human computer interaction. IGI Global, p. 211-219, 2006.

[3] WARD, David J.; MACKAY, David

JC. "Fast hands-free writing by gaze direction." Nature, 418(6900), p 838-838, 2002

[4] MAJARANTA, Päivi; RÄIHÄ, Kari-Jouko. "Twenty years of eye typing: systems and design issues." In: ETRA. p. 15-22, Mar, 2002

[5] JACOB, Robert JK. "Eye tracking in advanced interface design." Virtual environments and advanced interface design, 258-288, 1995.

[6] HANSEN, John Paulin, et al. "Gaze typing compared with input by head and hand." In: Proceedings of the 2004 symposium on Eye tracking research & applications. ACM, p. 131-138, Mar, 2004

[7] KUMAR, Manu, et al. "Reducing shoulder-surfing by using gaze-based password entry." In: Proceedings of the 3rd symposium on Usable privacy and security. ACM, p. 13-19, July, 2007.

[8] DE LUCA, Alexander; WEISS, Roman; DREWES, Heiko. "Evaluation of eye-gaze interaction methods for security enhanced PIN-entry." In: Proceedings of the 19th australasian conference on computer-human interaction: Entertaining user interfaces. ACM, p. 199-202, Nov, 2007.

[9] ABDRABOU, Yasmeen, et al. "eNGAGE: Resisting Shoulder Surfing Using Novel Gaze Gestures Authentication." In: Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia. ACM, p. 469-473, Nov, 2018.

[10] MAJARANTA, Päivi, et al. "Auditory and visual feedback during eye typing." In: Conference on Human Factors in Computing Systems: CHI'03 extended abstracts on Human factors in computing systems. p. 766-767, Apr, 2003.

[11] MAJARANTA, Päivi; AULA, Anne; RÄIHÄ, Kari-Jouko. "Effects of feedback on eye typing with a short dwell time." In: Proceedings of the 2004 symposium on Eye tracking research & applications. ACM, p. 139-146, Mar, 2004.

[12] MAJARANTA, Päivi, et al. "Effects of feedback and dwell time on eye typing speed and accuracy." Universal Access in the Information Society, 5(2), p. 199-208, 2006.

[13] DREWES, Heiko; SCHMIDT, Albrecht. "Interacting with the computer using gaze gestures." In: IFIP Conference on Human-Computer Interaction. Springer, Berlin, Heidelberg, p. 475-488, Sept, 2007.

[14] KUMAR, Manu, et al. "EyePoint: practical pointing and selection using gaze and keyboard." In: Proceedings of the SIGCHI conference on Human factors in computing systems. ACM, p. 421-430, Apr, 2007.

[15] MAJARANTA, Päivi; AHOLA, Ulla-Kaija; ŠPAKOV, Oleg. "Fast gaze typing with an adjustable dwell time." In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, p. 357-360, Apr, 2009.

[16] KANGAS, Jari, et al. "Gaze gestures and haptic feedback in mobile devices." In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, p. 435-438, Apr, 2014.

[17] MAJARANTA, Päivi, et al. "Haptic feedback in eye typing." 2016.

[18] DE LUCA, Alexander; DENZEL, Martin; HUSSMANN, Heinrich. "Look into my eyes!: Can you guess my password?." In: Proceedings of the 5th

Symposium on Usable Privacy and Security. ACM, p. 1-12, July, 2009.
[19] WEISS, Roman; DE LUCA, Alexander. "PassShapes: utilizing stroke based authentication to increase password memorability." In: Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges. ACM, p. 383-392, Oct, 2008.
[20] KHAMIS, Mohamed, et al. "Gazetouchpass: Multimodal authentication using gaze and touch on mobile devices." In: Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems. ACM, p. 2156-2164, May, 2016.
[21] KHAMIS, Mohamed, et al. "GTmoPass: two-factor authentication on public displays using gaze-touch passwords and personal mobile devices." In: Proceedings of the 6th ACM International Symposium on Pervasive Displays. ACM, p. 1-9, June, 2017.
[22] KHAMIS, Mohamed, et al. "GazeTouchPIN: protecting sensitive data on mobile devices using secure multimodal authentication." In: Proceedings of the 19th ACM International Conference on Multimodal Interaction. ACM. p. 446-450, Nov, 2017.
[23] ABDRABOU, Yasmeen, et al. "Just Gaze and Wave: Exploring the Use of Gaze and Gestures for Shoulder-surfing Resilient Authentication." In:Proceedings of 11th ACM Symposium on Eye Tracking Research & Application, p. 1-10, June, 2019.
[24] LONG, Johnny. "No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing." Syngress, 2011.
[25] BROOKE, John, et al. "SUS-A quick and dirty usability scale." Usability evaluation in industry, p. 189-194, 1996.
[26] MAUCHLY, John W. "Significance test for sphericity of a normal n-variate distribution." The Annals of Mathematical Statistics, 11(2). p. 204-209, 1940.
[27] ARMSTRONG, Richard A. "When to use the B onferroni correction." Ophthalmic and Physiological Optics, 34(5), p. 502-508, 2014.
[28] GREENHOUSE, Samuel W.; GEISSER, Seymour. "On methods in the analysis of profile data." Psychometrika, 24(2), p. 95-112, 1959.
[29] SAURO, Jeff. "A practical guide to the system usability scale: Background, benchmarks & best practices." Denver, CO: Measuring Usability LLC, 2011.
[30] LEVENSHTEIN, Vladimir I. "Binary codes capable of correcting deletions, insertions, and reversals." In: Soviet physics doklady, 10(8), p. 707-710, 1966.

〈저자소개〉

김 슬 기 (Seulgi Kim) 학생회원
2016년: 순천향대학교 정보보호학과 학사
2020년: 연세대학교 정보보호학과 석사
〈관심분야〉 정보보호, Usable Security, 정보보호정책

유 상 봉 (Sangbong Yoo) 학생회원
2015년: 세종대학교 컴퓨터공학과 학사
2015년~현재: 세종대학교 컴퓨터공학과 박사과정
〈관심분야〉 데이터 시각화, 시선 추적

장 윤 (Yun Jang) 정회원
2000년: 서울대학교 전기공학부 학사
2002년: 미국 Purdue University ECE 석사
2007년: 미국 Purdue University ECE 박사
2007년~2009년: Swiss National Supercomputing Center 박사 후 연구원
2009년~2011년: Swiss ETH Zurich 박사 후 연구원
2012년~현재: 세종대학교 컴퓨터공학과 부교수
〈관심분야〉 데이터 시각화, Visual Analytics, 빅데이터 분석 및 시각화, 컴퓨터 그래픽스

권 태 경 (Taekyoung Kwon) 종신회원
1992년: 연세대학교 컴퓨터과학과 학사
1995년: 연세대학교 컴퓨터과학과 석사
1999년: 연세대학교 컴퓨터과학과 박사
1999년~2000년: U.C. Berkeley EECS Post-Doc.
2001년~2013년: 세종대학교 컴퓨터공학과 교수
2007년~2008년: Univ. of Maryland, College Park 교환교수
2013년~현재: 연세대학교 정보대학원 교수
〈관심분야〉 암호 프로토콜, Usable Security, 소프트웨어/시스템 보안, 기계학습과 보안 등