Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.5, Oct. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.5.827

가상키보드 비밀번호 유출 분석*

양 희 동,[1†] 이 만 희[2‡]
[1]KAIST 사이버보안연구센터 (연구원), [2]한남대학교 (교수)

Analysis of the Password Leaking in Virtual Keyboard*

Hee-dong Yang,[1†] Man-hee Lee[2‡]
[1]KAIST Cyber Security Research Center (Researcher),
[2]Hannam University (Professor)

요 약

온라인상에서 안전하게 금융서비스를 이용하기 위해서는 사용자를 인증하는 기술이 요구된다. 키보드를 사용한 비밀번호 입력 방식이 가장 일반적이나, 키보드 입력이 쉽게 유출될 수 있음이 알려짐에 따라 많은 인터넷 뱅킹 서비스 및 간편 결제 서비스에서는 가상키보드를 사용하고 있다. 하지만 안전할 것이라는 기대와 달리, 가상키보드 역시 키보드 입력이 유출될 위험성이 존재했다. 본 논문에서는 가상키보드의 비밀번호 유출 가능성을 분석하고, PC 환경에서 마우스 이벤트 후킹과 화면캡처를 활용한 비밀번호 유출 방안을 제시했다. 또한, 국내 유명 인터넷 뱅킹 웹사이트 및 간편결제 서비스에서 비밀번호 유출 공격 가능성을 직접 검사하였으며, 그 결과 PC 운영체제에서 수행되는 가상키보드를 통한 비밀번호 입력방식이 안전하지 않음을 검증하였다.

ABSTRACT

In order to use online financial services, user authentication technology is necessary. Password check through keyboard typing is the most common technique. However, since it became known that key stokes on the keyboard can be intercepted easily, many Internet banking services and easy payment services have adopted the virtual keyboard. However, contrary to the expectation that the virtual keyboard will be safe, there is a risk that key strokes on the virtual keyboard can be leaked. In this paper, we analyzed the possibility of password leaking on the virtual keyboard and presented a password leaking method using mouse event hooking and screen capture in PC operating system. In addition, we inspected the possibility of password leak attacks on several famous Korea Internet banking websites and simple payment services, and as a result, we verified that the password input method through the virtual keyboard in the PC operating system is not secure.

Keywords: Virtual Keyboard, Internet Banking, Simple Payment Service, Password Leak

I. 서 론

코로나19 이후 비대면 사회로 확산되면서 온라인에서 중요한 개인정보를 다루는 일이 증가하였다. 특히 보안이 강조되는 비대면 금융서비스가 증가하였는데 한국은행 통계자료에 따르면 2021년도 국내에서 인터넷 뱅킹(모바일 포함)을 통해 이체 및 대출 서비스를 이용한 건수는 1,732만 건으로 전년도대비 18% 증가하였고, 간편 결제 서비스와 간편 송금 서비스 실적 건수도 전년도대비 각각 36.3%, 33.0%

Received(07. 01. 2022), Modified(09. 02. 2022), Accepted(09. 05. 2022)
* 본 논문은 2021년도 한국정보보호학회 동계학술대회에 발표한 우수논문을 개선 및 확장한 것임.
* 본 논문은 과학기술정보통신부 글로벌사이버보안기술연구(과제고유번호: 1711151346) 사업의 지원과 한국연구재단의 지원(2021R1A4A2001810)을 받아 수행된 연구임.
† 주저자, heedong@kaist.ac.kr
‡ 교신저자, manheelee@hnu.kr(Corresponding author)

증가하였다. 이러한 비대면 금융서비스는 편리하지만, 보안사고가 발생한다면 금전적인 피해로 이어지게 된다. 그러므로 피해를 막기 위해 온라인상에서 서비스 이용자를 정확하게 인증하는 기술이 필요하다[1,2].

일반적으로 온라인상에서 사용자 인증을 위해 키보드로 비밀번호를 입력하는 인증방식을 주로 사용한다. 하지만 키보드를 활용한 비밀번호 인증방식은 키보드 인터럽트 하이재킹, 키보드 드라이버 해킹, DLL 인젝션 해킹 등 다양한 취약점이 존재한다. 이에 따라 새롭게 등장한 사설 인증서와 간편 결제 서비스에서는 키보드 대신 가상키보드를 통해 비밀번호를 입력받거나 생체인증 방식을 주로 사용한다. 이러한 인증방식은 키보드 보안 프로그램을 따로 설치하지 않아도 되며 가상키보드에 PIN Number를 입력하거나 모바일에 저장된 생체정보(지문, 페이스ID, 홍채 등)와 대조하여 본인을 인증하므로 편리하고 빠르다는 장점이 있어 이용자가 계속 증가하고 있다[2,3].

다양한 인증방식 중 생체정보를 이용한 인증방식이 가장 안전하지만 이를 지원하지 않는 기기에서는 사용할 수 없으므로 PC 환경에서는 가상키보드를 이용한 비밀번호 인증방식을 많이 사용한다. 해당 방식은 가상키보드를 사용하여 사용자로부터 비밀번호와 같은 민감한 데이터를 마우스로 입력받기 때문에 가상키보드 이미지와 입력하고 있는 위치정보는 반드시 보호되어야 한다. 이에 따라 해당 인증방식을 사용하고 있는 모바일 앱에서는 화면 캡처를 감지하여 가상키보드 이미지를 보호하기 위한 기술이 이미 적용하고 있다. 하지만 다양한 작업을 수행하는 PC 웹브라우저나 모바일 웹브라우저에서는 해당 기술을 적용하기 어려워 화면캡처와 마우스로거 등을 통해 입력 중인 비밀번호가 유출될 가능성이 여전히 존재한다. 특히 국내에서 개발한 개방형 OS인 구름 OS와 Mac OS처럼 키보드 보안 프로그램을 설치할 수 없는 PC 환경에서는 가상키보드를 사용해야만 정상적인 서비스를 이용할 수 있으므로 가상키보드의 보안성은 반드시 확보되어야 한다.

따라서 본 논문에서는 가상키보드를 사용하여 비밀번호 입력하는 과정에서의 비밀번호 유출 가능성을 중점으로 다루며 구성은 다음과 같다. 2장에서는 비밀번호 입력단계에서 비밀번호 값을 유출하는 데 사용할 수 있는 후킹 기술을 소개하고 비밀번호 유출을 막기 위한 기존 방어기술을 소개한다. 3장에서는 키보드와 마우스 후킹 기술과 원격 제어 프로그램을 악용한 비밀번호 유출 공격 방안을 제시하고, 4장에서 실제 국내 인터넷 뱅킹 웹사이트 및 간편 결제가 이루어진 웹사이트를 대상으로 비밀번호 유출 공격을 수행하여 공격의 효과성을 보여준다. 마지막으로 5장을 통해 실제 비밀번호 유출 가능성과 해결 방안을 제안한다.

II. 관련 연구

2.1 운영체제별 키보드, 마우스 후킹 기술

온라인상에서 사용자 인증을 위해 일반적으로 비밀번호 기반 인증 방법을 사용한다. PC 환경의 사용자는 키보드로부터 비밀번호를 입력하거나 가상키보드 이미지를 마우스로 클릭하여 비밀번호를 입력하므로 비밀번호를 보호하기 위해서는 사용자가 입력하는 키보드 데이터와 클릭하는 마우스 위치 데이터를 보호해야 한다. 하지만 각 운영체제가 키보드와 마우스를 비롯한 입력장치 데이터를 응용프로그램으로 전달하기 위한 API를 악용하여 입력을 가로채는 후킹 기술은 이미 알려져 있다. 이러한 악성 도구를 키로거라 부르며 마우스 및 키보드 데이터를 유출하는 데 사용되는 운영체제별 후킹 방법은 다음과 같다.

먼저 Windows 운영체제에서는 OS와 주고받는 메시지를 후킹 할 수 있는 API를 제공한다. Win32 API 중 *GetCursorPos* 함수를 사용하면 마우스의 X, Y 좌푯값을 실시간으로 후킹 할 수 있고, *SetWindowsHookEx* 함수를 사용한다면 DLL 인젝션을 통해 키보드의 입력 및 마우스 위치, 이벤트를 후킹 할 수 있게 된다[4].

리눅스 계열 운영체제의 경우 키보드의 입력을 후킹하기 위해서 기본적으로 /dev/input에서 입력장치를 찾아 데이터를 읽어와야 하므로 루트 권한이 필요하다. 하지만 구름 OS, Ubuntu Desktop과 같은 데스크톱 OS에서는 GUI 환경을 위해 X window system을 사용하기 때문에 Xlib의 함수를 활용한다면 키보드 입력값, 마우스 좌표 및 이벤트를 모두 후킹 할 수 있다[5].

Mac OS는 Win32 API와 유사한 Quart Event Services의 API를 통해 로우레벨의 하드웨어 이벤트 후킹 할 수 있고, *CGEventRef* 형태로 키보드 입력값, 마우스 좌표 등을 받아올 수 있다. 이처럼 각 운영체제에서 제공하고 있는 API를 사용

하여 키보드값을 읽어오면 사용자가 입력하는 비밀번호를 그대로 가져올 수 있고, 마우스 이벤트를 추출하여 좌표값을 가져온다면 클릭한 위치를 알 수 있으므로 사용자가 입력한 값을 유출하는 데 사용할 수 있다[6].

2.2 비밀번호 유출 방지 기술 현황

2.2.1 키보드 보안 기술

키로거와 같이 키보드로부터 입력받은 데이터를 탈취하려는 시도를 막기 위한 키보드 보안 프로그램이 존재한다. 국내 은행 웹사이트에서 사용 중인 키보드 보안 프로그램은 상용 키로거를 차단하고, 사용자 PC에서 실행되면서 실시간으로 탈취가 가능한 구간의 입력값들을 암호화하고 SSL 인증서를 사용하여 내부통신 구간을 보호하여 키보드 데이터를 보호한다. 해당 프로그램을 동작하고 있을 때 키로거 스크립트를 동작한다면 Fig.1.과 같이 입력값을 얻을 수 없게 된다. 하지만 키보드 보안 프로그램은 현재 금융 웹사이트에서만 적용되고 있으며 간편 결제 시스템을 가지고 있는 쇼핑몰 웹사이트에서는 적용되지 않고 있다. 또한, 리눅스 계열 운영체제와 Mac OS에서는 사용할 수 없다는 한계점이 있어 해당 운영체제에서는 다른 인증방식을 사용해야만 한다.

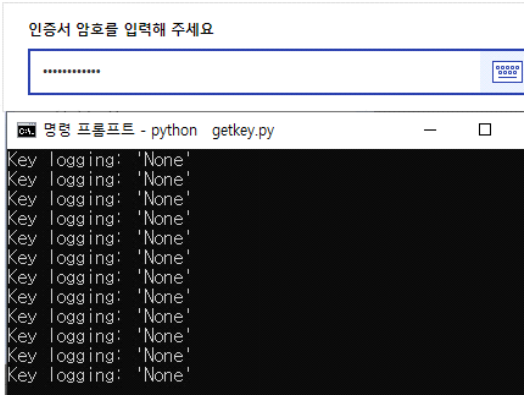

Fig. 1. Keylogger when keyboard security program running

2.2.2 화면 보호 기술

가상키보드를 활용한 비밀번호 인증방식에서는 사용자 인증을 위해 마우스로 가상 키패드를 클릭하여

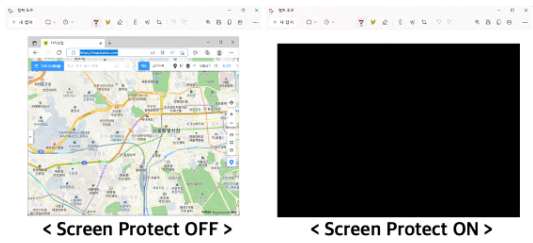

Fig. 2. Using screen protect API

비밀번호를 입력하는 방법을 사용하기 때문에 클릭한 위치정보가 해커에 의해 유출되더라도 가상키보드의 이미지만 유출되지 않는다면 비밀번호를 알 수 없다. 따라서 가상키보드를 활용한 비밀번호 인증방식을 사용하는 모바일 운영체제(안드로이드, iOS)에서는 화면 캡처 및 녹화가 감지되었을 때 앱을 강제로 종료시키거나 특정 Activity에서 캡처를 막는 코드를 삽입하여 화면 캡처를 막는 방법을 사용한다. PC 환경인 Windows 운영체제에서도 Win32 API 중 *SetWindowDisplayAffinity* 함수를 사용하여 RGB의 색깔을 덧입히는 방식으로 구현하면 Fig.2.와 같이 화면을 보호할 수 있다[4,7].

하지만 해당 기술은 PC 운영체제 중에서는 Windows에서만 사용 가능할 뿐만 아니라 화면 미러링을 이용한 캡처, Direct X를 활용한 캡처 등 다양한 방식의 화면 캡처를 원천적으로 모두 막기는 어려우며, PC나 모바일 웹브라우저에 해당 기술을 적용할 경우 다른 작업을 수행하는 데 방해가 될 수 있어 사실상 적용하기 어렵다.

2.2.3 훔쳐보기 공격 보호 기술

가상키보드를 사용한 사용자 인증방식은 화면캡처와 같이 가상키보드 이미지 유출뿐만 아니라 어깨너머공격(Shoulder Surfing Attack)이라 불리는 물리적인 훔쳐보기 공격에도 취약하다. 따라서 기존 연구들[8-11]에서는 이러한 취약점을 해결하기 위해 가상키보드에서의 어깨너머공격을 분석하고, 가상키보드의 키 배열 조합을 분석하여 훔쳐보기 방지 기술을 제안하였다. 실제로 대다수의 인터넷 뱅킹 서비스 및 간편결제 서비스에 사용되는 가상키보드에는 Fig.3.과 같이 키패드의 배열을 무작위로 섞어 마우스 좌표 위치가 유출되더라도 어떠한 값을 입력했는지 숨기는 기술과 Fig.4.과 같이 가짜 마우스 좌표

Fig. 3. Virtual keyboard with random array

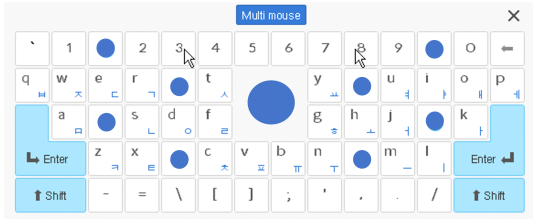

Fig. 4. Virtual keyboard with multi mouse

를 모니터에 보이게 만들어 실제 마우스 좌표를 숨기는 멀티마우스 기술이 적용되고 있다. 해당 기술들을 적용한 가상키보드에서는 비밀번호를 입력할 때 시각적으로 어떠한 키를 입력했는지 훔쳐보기는 어렵지만, 앞서 소개한 마우스 이벤트 클릭 후킹 기술을 활용한다면 입력한 좌표를 정확히 알 수 있으므로 비밀번호 유출 공격에 대한 완벽한 해결책이 될 수는 없다.

III. 가상키보드 비밀번호 유출 공격 방안

비밀번호 유출을 막기 위한 연구의 대부분은 키로거, 피싱 공격, MitM(Man-in-the-Middle)공격, MitB(Man-in-the-Browser)공격을 차단하는 데에 집중한다[12]. 하지만 키보드, 마우스 데이터 후킹 및 원격 제어 시스템을 악용한다면 가상키보드로 비밀번호를 입력하는 과정 전체를 유출할 수 있다. 3장에서는 마우스 이벤트 후킹과 원격 제어 시스템을 통해 가상키보드 비밀번호를 유출하기 위한 공격 방법을 소개하고, 비밀번호 유출 가능성을 검증한다.

3.1 마우스 이벤트 후킹을 사용한 비밀번호 유출

먼저, 가상키보드에 입력하는 비밀번호를 유출하기 위해 대표적인 방법인 마우스 좌표 정보 및 클릭 이벤트 후킹을 사용하여 공격 스크립트를 만들어 가상 키패드를 사용하는 플랫폼에서 비밀번호 유출 가능성을 검증하였다. 마우스 이벤트 후킹을 사용한 비

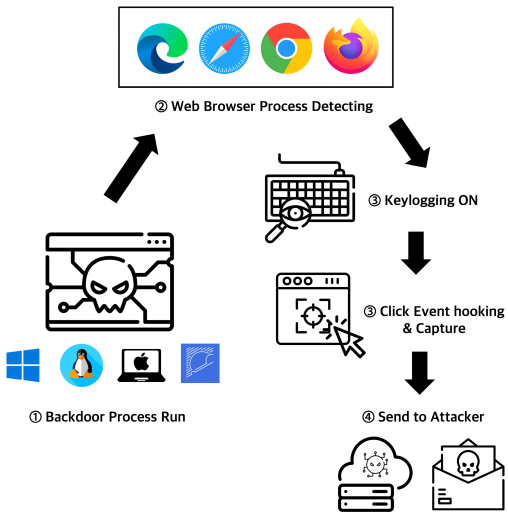

Fig. 5. Attack script flow using mouse event hooking

밀번호 유출 공격 스크립트는 Fig.5.와 같은 흐름으로 진행된다. 먼저, 각 운영체제에서 백그라운드로 실행되는 공격 프로세스는 실시간으로 실행 중인 웹 브라우저의 프로세스를 탐지한다. 만일, 웹브라우저가 실행 중이라면 마우스 클릭 이벤트를 후킹하고, 클릭 이벤트가 발생할 때 클릭한 주변 특정 픽셀 부분을 이미지로 캡처하여 저장한다. 이때 키보드의 입력값도 같이 후킹하여 클릭 이미지와 함께 일정한 주기로 공격자에게 전달하게 한다. 본 논문에서는 비밀번호를 좀 더 정확히 확인하기 위해 캡처된 이미지에서 클릭 이벤트가 발생한 좌표를 작은 점으로 추가로 표기하여 SMTP를 사용하여 공격자의 메일로 전송하도록 공격을 수행하였다. 해당 공격 스크립트를 사용하여 비밀번호 유출 공격을 수행한 결과, Fig.6.과 같이 은행 웹사이트에서 가상키보드를 사용한 비밀번호를 입력한 순서대로 유출할 수 있었다. Fig.6.의 메일 본문을 보면 희생자가 키보드로 입력한 아이디인 'abc1234'를 키로깅으로 확인할 수 있었고, Fig.6.의 메일 첨부 이미지를 통해 마우스 클릭 위치와 가상키보드를 사용한 비밀번호가 'password123!'임을 정확히 알 수 있었으며 로그인을 수행하기까지의 과정까지도 유추할 수 있었다. 해당 공격은 Windows 11, 구름 OS 3.0, Ubuntu 20.04, Mac OS 12.4에서 모두 성공적으로 수행할 수 있었다. 다만, Mac OS의 경우 사용자 권한으로는 실행 중인 프로세스 확인이 불가능했고, Mac

Fig. 6. Password leaking result

OS Catalina(10.15) 이후 버전에서 새롭게 추가된 개인 정보 보호 정책에 따라 입력 모니터링 및 화면 기록 권한을 가지고 있어야 정상적인 공격이 가능하였다.

3.2 원격 제어 시스템을 사용한 비밀번호 유출

원격 제어 시스템은 네트워크를 통해 PC를 원격으로 제어할 수 있는 도구로 악의적으로 사용될 위험성이 존재하지만, 일반적으로 원거리에서 본인의 PC에 접속하거나 서비스센터 직원이 소비자의 PC를 수리하거나 제어할 때 사용한다. 하지만 이를 악용하면 가상키보드로 입력하는 비밀번호를 유출할 수 있다. 따라서 상용 원격 제어 프로그램을 사용하여 가상키보드를 사용하는 플랫폼에서의 비밀번호 유출 가능성을 검증하였다.

원격 제어 시스템에서 비밀번호를 유출하는 방법은 원격 제어 시스템을 통해 공격자가 피해자 PC

Table 1. Commercial Remote Control Program

Remote Program	Show Pointer	Alert	Internet Banking
Team Viewer	O	O	X
VNC Viewer	O	O	X
Google Remote desktop	X	O	O
Anydesk	O	O	O

화면을 모니터링하거나 녹화를 하는 방법으로 물리적인 공격 방법인 어깨너머공격과 같이 수행한다. 이때 가상키보드에서 비밀번호를 입력하는 과정을 모두 훔쳐보기 위해서는 피해자의 마우스 포인터를 실시간으로 모니터링 할 수 있어야 성공적으로 비밀번호를 유출시킬 수 있다. 따라서 기본적으로 다중접속이 불가능한 원격 제어 프로그램인 Microsoft Remote Desktop Protocol을 제외한 대표적인 4가지 원격 제어 프로그램으로 비밀번호 유출 가능성을 확인하였다. 확인 결과, Table 1.과 같이 Google Remote desktop을 제외한 3가지 상용 원격 제어 프로그램에서 모두 사용자의 마우스 포인터 모니터링이 가능하여 비밀번호를 유출할 수 있었다. 하지만 4가지 프로그램 모두 원격 접속 중에는 원격지 PC에서 알림 문구나 트레이 아이콘으로 알려주고 있었으며 국내 인터넷 뱅킹 보안 프로그램 중 하나인 'Ahnlab safe transaction'에서는 원격 포트나 프로세스를 감지하여 팀뷰어와 VNC 뷰어를 차단하고 있다. 또한, 피해자의 원격 접속 프로그램 계정을 알 수 없거나 접속 포트를 알지 못한다면 접속하기 어려우므로 사실상 공격자가 몰래 비밀번호를 유출하기는 어렵다.

IV. 가상키보드 비밀번호 유출 방안 효과성 검증

본 논문에서는 이미지 인증방식을 사용한 실제 웹사이트에서의 비밀번호 유출 방안의 효용성을 증명하기 위해 3장에서 소개한 방법을 사용하여 비밀번호 유출 실험을 직접 수행하였다. Windows 11(MS Eage & Google Chrome), Mac OS 12.4(Safari), 구름OS 3.0(구름 브라우저), Ubuntu 20.04(Firefox)에서 각각 실험하였으며 웹페이지에서 제공하는 보안 프로그램을 모두 설치한 뒤 비밀번호 유출 공격을 수행하였다.

4.1 인터넷 뱅킹 웹사이트 비밀번호 유출 실험

Table 2.는 국내 은행 중 규모가 큰 5개의 은행 웹사이트에서 앞서 소개한 3가지 공격 방법으로 가상키보드로 입력하는 비밀번호를 유출 실험을 수행한 결과이다. 현재 인터넷 뱅킹을 사용하기 위해 키보드를 사용하여 비밀번호를 입력할 때는 반드시 키보드 보안 프로그램을 설치해야 하며 설치할 수 없는 환경에서는 가상키보드로만 입력해야 한다. 따라서 5개 은행에 대해서 Windows 11, Mac OS 12.4, 구름OS 3.0, Ubuntu 20.04 모두 키보드로 입력하는 비밀번호는 유출할 수 없었다.

또한, 인터넷 뱅킹에서 사용되는 가상키보드에서는 가상 키 배열을 섞거나 멀티마우스를 통해 마우스 위치를 훔쳐보기를 방지 기술이 적용되어 있다. 하지만 Windows 및 리눅스 기반 운영체제에서는 3장에서 소개한 공격 방법과 같이 마우스 이벤트에 대한 후킹과 화면 캡처를 동시에 수행 가능하므로 훔쳐보기 방지 기술과 상관없이 가상키보드에 입력하는 비밀번호를 모든 은행 웹사이트에서 성공적으로 유출할 수 있었다. 다만 최신 Mac OS(12.4)에서는 개인정보 보호 정책에 따라 공격 프로세스가 입력 모니터링 및 화면 기록 정책 권한을 부여해야만 성공적으로 비밀번호를 유출할 수 있다. 원격 제어 시스템 활용한 비밀번호를 사용한 비밀번호 유출 공격의 경우 'Ahnlab safe transaction'(Windows Ver.)보안 프로그램을 사용하는 은행 웹사이트에서만 차단되어 공격을 수행할 수 없었고, 리눅스 및 Mac OS에서는 차단하지 않아 비밀번호 유출이 가능하였다.

Table 2. Password leaking result of domestic internet banking service

Victim OS	Attack method	Bank				
		K	S	N	W	H
Windows 11	Keylogging	X	X	X	X	X
	Mouse Event hooking	O	O	O	O	O
	Remote Program	X	X	X	O	O
Linux (Gooroom, Ubuntu)	Keylogging	X	X	X	X	X
	Mouse hooking	O	O	O	O	O
	Remote Program	O	O	O	O	O
Mac OS 12.4	Keylogging	X	X	X	X	X
	Mouse hooking	△	△	△	△	△
	Remote Program	△	△	△	△	△

4.2 간편 결제 웹사이트 결제 비밀번호 유출 실험

인터넷 뱅킹 웹사이트와 달리 간편 결제는 다양한 쇼핑몰 및 간편 결제 서비스를 지원하는 모든 웹사이트에서 사용할 수 있다. 또한 키보드 보안 프로그램과 같은 보안 프로그램 설치가 의무화되어 있지 않아 비밀번호 유출 공격에 상대적으로 더 취약하다. Table 3.은 이전실험과 동일한 방법으로 잘 알려진 8개의 국내 간편결제 서비스로 결제를 진행할 때 사용되는 결제 비밀번호 유출 실험을 수행한 결과이다. 인터넷 뱅킹과는 달리 대부분 간편 결제 서비스는 사전에 등록한 6자리 숫자 형태의 비밀번호를 가상키보드로 입력하는 방식으로 키보드 보안 프로그램을 사용하지 않는다. 따라서 Mac OS를 제외한 다른 운영체제에서는 입력 모니터링 권한을 제한하거나 원격 제어 프로그램을 차단하지 않아 키보드로 입력하는 웹사이트의 비밀번호도 추가로 유출할 수 있었다.

간편결제 서비스에서도 가상키보드의 키 배열을 섞는 훔쳐보기 방지 기술이 적용되었으나 이전실험과 동일하게 마우스 이벤트에 대한 후킹 및 화면 캡처를 동시에 수행한다면 성공적으로 비밀번호를 유출할 수 있었다. 하지만 삼성페이와 카카오페이(Fig.7.)와 같이 모바일 앱 인증을 통해 결제할 수 있도록 만든다면 비밀번호 유출 공격을 수행할 수 없다.

Fig. 7. Simple Payment service using smart phone application

Table 3. Password leaking result of Simple Payment service

Victim OS	Attack method	Simple Payment Service							
		A pay	B pay	C pay	D pay	E pay	F pay	G pay	H pay
Windows 11	Keylogging	O	O	O	O	O	O	O	O
	Mouse Event hooking	X	X	O	O	O	O	O	O
	Remote Program	X	X	O	O	O	O	O	O
Linux (Gooroom, Ubuntu)	Keylogging	O	O	O	O	O	O	O	O
	Mouse Event hooking	X	X	O	O	O	O	O	O
	Remote Program	X	X	O	O	O	O	O	O
Mac OS	Keylogging	X	X	X	X	X	X	X	X
	Mouse Event hooking	X	X	△	△	△	△	△	△
	Remote Program	X	X	△	△	△	△	△	△

V. 가상키보드 비밀번호 유출 분석 및 제안

기존 연구들[8-12]에서는 가상키보드를 사용한 인증방식에서 비밀번호 유출을 막기 위해 훔쳐보기 방지 기술과 가상키보드로 입력받은 비밀번호를 안전하게 전송하기 위한 보안 기술에 집중하고 있다. 하지만 본 논문에서는 이러한 보안 기술이 적용된 가상키보드에서 마우스 이벤트 후킹과 화면캡처를 사용하여 비밀번호를 충분히 유출할 수 있음을 실험을 통해 증명하였다. 최신 Mac OS에서는 제약이 있었지만, 대부분의 PC 환경에서 가상키보드로 입력하는 비밀번호를 어렵지 않게 유출할 수 있었다. 즉, 가상키보드를 통한 비밀번호 입력방식은 기존의 키로거 공격보다 안전한 방법으로 널리 사용되고 있으나 비밀번호 유출이 가능하다는 것을 의미한다. 비록 해당 공격방식은 키보드에 입력되는 문자열을 유출하는 기존 키로거와 달리 캡처되는 이미지를 유출하므로 더 큰 오버헤드가 발생하지만, 2장에서 소개한 것과 같이 마우스 이벤트 후킹은 키보드 데이터 후킹과 유사한 API를 사용하기 때문에 기존에 알려진 키로깅 악성코드와 유사하게 수행할 수 있다.

최근 스팸메일을 통해 유포되고 있는 스네이크 키로거(Snake Keylogger) 악성코드는 PDF와 같은 문서형 악성코드 형태로 웹브라우저 및 다양한 프로그램들에서 피해자의 계정 정보 탈취한 후 SMTP를 통해 공격자에게 전달하여 정보를 유출한다. 만일, 키로깅 대신 마우스 로깅을 통한 캡처 이미지를 전달하는 닷넷 악성코드를 포함하여 유포한다면 가상키보드로 입력되는 비밀번호 정보 역시 실제로 유출될 수 있다. 추가로 다이어(Dyre) 악성코드와 같이 DLL 인젝션을 통해 특정 인터넷 주소에 접속했을 때만 해당 공격을 수행하도록 만든다면 더욱더 정밀한 공격도 가능할 것으로 보인다[13,14].

본 논문에서 소개한 비밀번호 유출 공격은 화면캡처를 방지하는 기술을 적용하면 막을 수 있으나 PC 환경의 인터넷 브라우저에서는 이를 완벽하게 막기 어렵다는 한계점이 존재한다. 따라서 인터넷 뱅킹 서비스 및 간편 결제 서비스를 제공자는 가상키보드를 통해 입력받은 비밀번호의 유출을 막기 위해 중요한 정보를 입력받을 때 키보드 보안 프로그램에서 키보드 데이터뿐만 아니라 마우스 데이터도 같이 암호화하고 마우스 로깅 API를 탐지하는 기술이 적용되어야 한다. 더불어 기존 키보드 보안 프로그램과 같이 암호화를 수행할 수 없는 환경이라면 번거롭더라도 가상키보드 비밀번호 입력 시 모바일을 활용한 2차 사용자 인증을 추가로 수행하거나 생체인식 기

반 인증기술인 FIDO(Fast IDentity Online) 인증을 활용하여 취약점을 보완하는 것이 필요하다[15-17].

VI. 결 론

대부분의 인터넷 뱅킹 서비스 및 간편 결제 서비스 제공자는 키보드나 가상키보드로 입력받은 비밀번호를 안전하게 메모리에 저장하고 전송하기 위한 보안 기술에 집중한다. 하지만 키로깅과 같이 웹브라우저를 통해 비밀번호가 서버로 전송되기 전 비밀번호 입력과정에서도 비밀번호 유출이 가능하므로 본 논문에서는 마우스 이벤트 후킹과 화면 캡처를 통해 가상키보드로 입력하는 비밀번호 유출 공격을 제시하고, 비밀번호 유출 가능성을 검증하였다.

국내에서 민감한 정보를 다루는 인터넷 뱅킹 및 간편 결제 서비스를 지원하는 웹사이트를 대상으로 실험한 결과, 키보드에 비해 안전하다고 알려진 가상키보드로 입력된 비밀번호를 대부분의 PC 환경에서 성공적으로 유출할 수 있었다. 가상키보드 입력과정을 보호하기 위한 멀티마우스 기술이나 무작위로 키 배열을 섞는 기술이 적용되고 있으나 운영체제에서 화면캡처를 제한하지 않다면 비밀번호 유출 공격은 막을 수 없다. 따라서 민감한 데이터를 다루는 서비스 제공자는 키보드 데이터뿐만 아니라 마우스 데이터를 보호하기 위해 암호화 및 마우스 로깅을 탐지하는 기술을 적용해야 하고, 추가로 FIDO 표준의 생체인식 인증방식을 적용한 모바일 앱을 활용하여 사용자 인증 방식을 보완할 필요가 있다. 향후 연구로 최근 발표된 Apple의 'Passkeys'와 같이 모든 PC 환경에서 기존 비밀번호 인증방식의 취약점을 해결하고 편리함과 안전성을 모두 갖춘 사용자 인증을 수행할 수 있는 연구를 수행하여 안전하게 금융서비스를 사용할 수 있기를 기대해본다.

References

[1] The Bank of Korea, "Use of Korea Bank Internet Banking Service during 2021," Mar. 2022.

[2] The Bank of Korea, "Use of Electronic Payment Service during 2021," Mar. 2022.

[3] Kang-Bin Yim and Kwang-Jin Bae, "Analysis of an Intrinsic Vulnerability on Keyboard Security", Journal of the Korea Institute of Information Security & Cryptology 18(3), pp. 89-95, Jun. 2008

[4] Microsoft, "Window App Development - winuser.h header", https://docs.microsoft.com/en-us/windows/win32, 2022.

[5] Gettys James, Robert W. Scheifler and Ron Newman, "Xlib: C language X interface (X version 11, release 4)" Vol. 29, Silicon Press, 1990.

[6] Apple, "API Collection - Quartz Event Services", https://developer.apple.com/documentation/coregraphics/quartz_event_services, 2022.

[7] Jong-Hyeok Lee, "Implementation of anti-screen capture modules for privacy protection", Journal of the Korea Institute of Information and Communication Engineering 18(1), pp. 91 - 96, Jan. 2014.

[8] Manu Kumar, Tal Garfinkel, Dan Boneh and Terry Winograd. "Reducing shoulder-surfing by using gaze-based password entry.", SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security, pp. 13-19. ACM, July. 2007.

[9] Bobur Shakirov, Hye-jin Kim, Kyung-Hee and Dae-Hun Nyang, "Analysis on Vulnerability of Password Entry Using Virtual Onscreen Keyboard", Journal of the Korea Institute of Information Security & Cryptology 26(4), pp. 857 - 869, Aug. 2016.

[10] Tea-Nam Cho and Sook-Hee Choi, "Vulnerabilities and Countermeasures of Dynamic Virtual Keyboard in Android Banking Apps", KIPS Transactions on Computer and Communication Systems 8(1), pp. 9 - 16, Jan. 2019.

[11] Sung-Hwan Kim, Min-Su Park and Seung-Joo Kim, "Shoulder Surfing Attack Modeling and Security Analysis on Commercial Keypad Schemes", Journal of the Korea Institute of Information Security & Cryptology 24(6), pp. 1159 - 1174, Dec. 2014.
[12] Sung-Hoon Lee, Seung-Hyn Kim, Eui-Yeob Jeong, Dae-Seon Choi and Seung-Hun Jin, "An Attack of Defeating Keyboard Encryption Module using Javascript Manipulation in Korean Internet Banking", Journal of the Korea Institute of Information Security & Cryptology 25(4), pp. 941 - 950, Aug. 2015.
[13] AhnLab, "Snake Keylogger Being Distributed via Spam E-mails", https://asec.ahnlab.com/en/22074, April, 2021.
[14] AhnLab, "[Vol.66] 'Dyre', a malware that steals financial information", ASEC Report, https://www.ahnlab.com/kr/site/securityinfo/asec/asecView.do?groupCode=VNI001&seq=23903, July. 2015.
[15] Fido Alliance, "How FIDO Works", https://fidoalliance.org/how-fido-works
[16] Sang-Nae Cho, Dae-Seon Choi, Seung-Hun Jin and Hyung-Hyo Lee, "Passwordless Authentication Technology-FIDO", Electronics and telecommunications trends 29(4), pp. 101-109, Aug. 2014.
[17] Seong-Min Yoo, Seok-Jin Choi, Jun-Hoo Park and Jae-Cheol Ryou, "POSCAL : A Protocol of Service Access Control by Authentication Level", Journal of the Korea Institute of Information Security & Cryptology 28(6), pp. 1509-1522, Dec. 2018.

〈저자소개〉

양 희 동 (Hee-dong Yang) 정회원
2019년 2월: 한남대학교 컴퓨터통신무인기술학과 학사
2021년 2월: 한남대학교 컴퓨터공학과 석사
2022년 3월~현재: 한국과학기술원 사이버보안연구센터 연구원
〈관심분야〉 바이너리 분석, 사이버보안, 시스템보안, AI 보안

이 만 희 (Man-hee Lee) 종신회원
1995년 2월 경북대학교 컴퓨터공학과 공학사
1997년 2월 경북대학교 공학석사
2008년 8월 Texas A&M 대학교 컴퓨터공학과 공학박사
1997년~2003년 한국과학기술정보연구원 연구원
2008년~2009년 Cisco Systems, San Jose
2010년~2012년 국가보안기술연구소 선임연구원
2012년~현재 한남대학교 교수
〈관심분야〉 네트워크/시스템/스마트폰/공급망 보안, 고성능 시스템, 컴퓨터교육