Journal of Korea Multimedia Society Vol. 14, No. 1, January 2011(pp. 15-23)

서브클래싱 기반의 키보드보안 기법

황성진†, 박경환††

요 약

본 연구에서는 하드웨어적 지원없이 액티브엑스를 지원하지 않는 웹브라우저에서도 적용가능한 서브클래싱 기반의 키보드보안기법을 제안하고 이를 구현한 방법을 보인다. 최근 파이어폭스, 사파리, 크롬 등 액티브엑스를 지원하지 않는 웹브라우저의 사용자가 증가하고 모바일폰 사용자의 확산에 따라 액티브엑스를 사용하지 않고 소프트웨어적으로 키보드보안을 지원할 필요성이 점차 증대되고 있다. 따라서 본 논문에서는 플러그인을 사용한 서브클래싱 기반의 사용자 모드 키보드 보안기법을 개발하였다. 이 방법은 하드웨어적 지원이 필요하지 않고, 액티브엑스를 지원하지 않는 웹브라우저에서도 사용할 수 있으며, 커널모드 보안 프로그램과 상호연동성을 갖는 장점이 있다.

A Keyboard Security Method Based on a Subclassing

Sung-Jin Hwang†, Kyung-Hwan Park††

ABSTRACT

In this paper, we propose a keyboard security method that is based on a subclassing. This method doesn't need an additional hardware and can be applied to Web browsers that do not support ActiveX controls. As the users of Web browsers such as Firefox, Safari, Chrome etc. are increased, it is more required to have the keyboard security methods that are based on software and don't use ActiveX controls. Thus we developed the user mode keyboard security method that is based on a subclassing with plugins. Our method doesn't need an additional hardware module and is interoperable with general kernel mode security programs.

Key words: Keyboard Security(키보드보안), Subclassing(서브클래싱), Firefox(파이어폭스), Keylogger (키로거), ActiveX(액티브엑스)

1. 서 론

인터넷을 기반으로 한 금융거래가 증가됨에 따라 보안의 중요성이 증대되고 있으며 이의 일환으로 키보드 입력정보에 대한 안정성과 신뢰성의 확보가 중요한 문제로 대두되고 있다.

키보드보안은 웹페이지 상에서 키보드를 통해 입력되는 개인의 아이디, 비밀번호 등 중요 정보가 키보드 입력정보를 가로채는 키로거(keylogger)라는 해킹 툴에 의해 불법적으로 유출되는 것을 방지하는 것을 말한다[1].

키보드 보안은 크게 하드웨어 및 소프트웨어 방법으로 달성될 수 있다. 국내에서는 거의 모든 금융거래에 키보드 보안을 적용하고 있으며, 인터넷뱅킹의 보안프로그램들이 대부분 마이크로소프트 인터넷 익스플로러에 기반하고 있기 때문에 액티브엑스

※ 교신저자(Corresponding Author) : 박경환, 주소 : 부산광역시 사하구 하단2동 840 컴퓨터공학과(604-714), 전화 : 051)200-7779, FAX : 051)200-7783, E-mail : khpark@dau.ac.kr
접수일 : 2010년 8월 9일, 수정일 : 2010년 9월 18일
완료일 : 2010년 10월 11일

† 준회원, 동아대학교 컴퓨터공학과 박사과정
(E-mail : jupiterrace@naver.com)
†† 종신회원, 동아대학교 컴퓨터공학과 교수
※ 이 논문은 동아대학교 학술연구비 지원에 의하여 연구되었음.

(ActiveX) 기반으로 구현되고 있는 실정이다[2]. 따라서 현재 인터넷뱅킹에 적용되고 있는 키보드보안, 방화벽, 공인인증서, 백신 등의 보안프로그램은 거의 대부분 액티브엑스 기반이다. 액티브엑스는 인터넷 익스플로러에서만 지원하는 형식이며 모질라 파이어폭스(Mozilla Firefox), 사파리(Safari), 구글 크롬(Google Chrome), 오페라(Opera) 등 다른 웹브라우저에서는 액티브엑스를 지원하지 않는다. 그러므로 다른 웹브라우저에서 키보드보안을 적용하기 위해서는 인터넷 익스플로러의 키보드보안과는 다른 방법이 필요하다. 해외의 은행들은 아직 온라인 계좌이체 부분에 있어서 자유도가 극히 낮다. 인터넷 뱅킹의 용도가 잔액 확인과 사전에 확인되고 알려진 계좌에 대한 제한적인 이체 외에는 사용빈도가 높은 편은 아니나 키로거 탐지를 위한 다양한 방법이 개발되고 있으며, 키보드 보안을 위해 하드웨어적 방법을 많이 사용하고 있다[3-5].

전 세계적으로 파이어폭스, 사파리, 크롬 등의 웹브라우저 사용자가 증가 추세에 있으며 스마트폰의 사용자가 증가함에 따라 액티브엑스를 지원하지 않는 웹브라우저 또는 마이크로브라우저에서도 하드웨어적 지원없이 소프트웨어적으로 효과적인 키보드 보안을 지원할 수 있는 기법이 요구되고 있다.

따라서 본 논문에서는 키보드 보안과 관련한 기존의 다양한 연구 결과를 살펴보고, 기존의 액티브엑스 기반의 키보드 보안을 소개한 후 액티브엑스를 지원하지 않는 웹브라우저에 적용할 수 있는 서브클래싱(subclassing)에 기반한 키보드보안 기법을 제시하고, 국내외적으로 가장 보편화된 윈도우 운영체제 환경과 모질라 파이어폭스에서 이를 개발한 방법을 소개한다. 마지막으로 기존의 방법과 본 연구에서 개발한 방법을 비교・검토한다.

2. 관련 연구 및 키보드보안 방법

키보드 보안은 보안 키보드 예를 들면 KeyGhost 키보드 등과 같은 하드웨어적 방법과 그림 1과 같이 키보드 입력정보의 흐름에 따른 여러 취약점을 소프트웨어적으로 해킹으로부터 보호하도록 하는 방법이 있다.

사용자가 입력한 키보드 입력정보는 키보드 하드웨어에서 시작하여 컴퓨터시스템 내 커널 모드(kernel mode)를 거쳐 사용자 모드(user mode)에 이르러 최종적으로 응용프로그램에 전달된다.

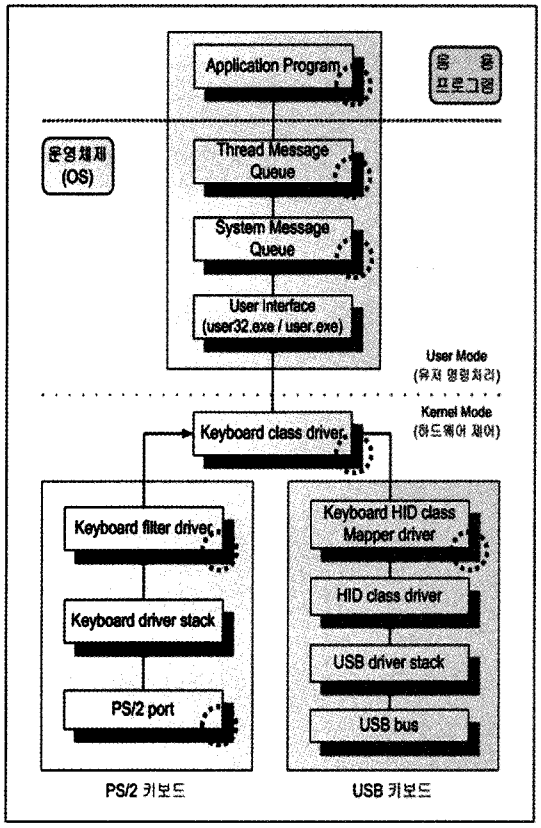

그림 1. 키보드 입력정보 흐름에 따른 취약점

컴퓨터시스템에서 키보드 장치로는 PS/2, USB의 2가지 타입을 주로 사용하고 있다. PS/2 키보드 장치와 USB 키보드 장치는 하위 커널 레벨에서만 상호 동작하는 방식이 다르며, 논리적인 키보드 드라이버(kdbclass.sys) 이후 사용자 레벨에서는 서로 동일한 처리 절차를 따른다.

이러한 키보드 입력정보 흐름은 다음 그림 1에서와 같이 키로거를 통해 키보드 입력정보를 가로챌 수 있는 취약점이 존재한다[6].

또한 키보드 입력정보의 흐름에 따른 운영 환경에서는 표 1과 같은 키보드 취약점이 있다.

2.1 커널모드 보안

커널모드의 해킹은 크게 키보드 입출력 포트 스캔, 키보드 컨트롤러의 하드웨어 취약점 이용, 키보드 인터럽트 하이재킹과 키보드 드라이버 해킹으로

표 1. 운영체제 환경에서 키보드 취약점

모드	해킹 기법	키보드타입
커널 모드	키보드 입출력 포트 스캔	PS/2
	키보드컨트롤러의 하드웨어 취약점	PS/2
	키보드 인터럽트 하이재킹	PS/2
	키보드 드라이버 해킹	PS/2, USB
사용자 모드	DLL Injection 해킹	PS/2, USB
	액티브엑스 키프레스 이벤트 핸들러	PS/2, USB
	인터넷 익스플로러 외의 다른 웹브라우저 미지원	PS/2, USB

나누어 볼 수 있다.

키보드 입출력 포트는 PS/2 키보드에서 입력되는 키보드 입력정보가 최초 저장되는 곳이며, 중앙처리장치로 키보드 스캔코드를 전송한 다음에도 키보드 입력정보는 이 포트에 그대로 남아 있다. 즉 이곳의 데이터를 지속적으로 감시하면 어떠한 정보가 키보드로 눌러지는지 확인 가능하다. 키보드 입출력 포트 스캔을 이용한 이러한 보안 취약점을 막기 위한 방법으로 지속적으로 키보드 포트의 값을 지우는 방법[7], 키보드 컨트롤러의 0xD2 제어코드를 활용한 방법, 디버그 레지스터를 이용하여 포트에 인가되지 않는 프로그램의 접근을 막는 방법 등이 있다[8,9].

다음으로 키보드 컨트롤러의 하드웨어 취약점을 이용하는 방법이 있다. 키보드 입출력 포트 스캔을 막기 위한 방법 중에 키보드 컨트롤러의 0xD2 제어코드를 활용하여 무작위 코드 및 무작위 시간으로 스캔코드를 교란하는 방법이다. 이것을 막기 위한 방법으로 Operation3 형태의 제어코드를 선택적으로 추가하는 방법이 있다[10].

또한 키보드 입력 취약점을 이용하는 해킹기법으로 키보드 인터럽트 하이재킹이 있다. 키보드 입출력 포트에 키보드 입력정보가 기록되면서 키보드 인터럽트가 발생하면, 중앙처리장치는 인터럽트 벡터 테이블에 저장된 키보드 인터럽트 처리함수의 주소를 파악하여, 해당 주소의 인터럽트 처리함수를 수행한다. 만약 인터럽트 벡터 테이블에 저장된 키보드 인터럽트 처리함수의 주소를 정보침입자가 정의한 인터럽트 처리함수 주소로 변경하게 되면, 중앙처리장치는 시스템상의 키보드 인터럽트 처리함수가 아닌 해킹 프로그램을 수행하게 되어 키보드 입력정보가 유출될 수 있다. 이러한 취약점을 막기 위해 도입된 방법으로는 지속적인 인터럽트 처리함수 주소 감시 방법, JUMP 코드 삽입 방법[11] 등이 개발되어 있다.

마지막으로 키보드 드라이버, 필터 드라이버 해킹 기법이 있다. 해킹용 키보드 드라이버를 개발해 키보드 입력값 처리를 담당하는 기존 키보드 드라이버를 대체하거나[6], 키보드 필터 드라이버(filter driver)가 제3의 개발자에게 제공한 키보드 입력정보에 관한 통신 내용을 읽고 제어할 수 있는 기능을 통하여 관련 키보드 제작자들에게 키보드 하드웨어 장치에 대한 추가적인 기능을 삽입할 수 있는 환경을 제공함과 동시에 키보드 입력정보를 유출시킬 수 있는 도구로 악용될 수도 있다. 이를 막기 위한 방법으로 보안 키보드 필터 드라이버가 가장 뒤에 오도록 유지하여 항상 먼저 키보드 입력정보를 가져가는 방법이 있다.

2.2 사용자 모드 보안

윈도우 메시지 형태의 키보드 입력정보가 처리되는 과정에서 응용프로그램의 원래 호출되는 함수의 시작번지를 해킹코드가 위치한 주소로 바꿔 메시지 후킹기술을 사용함으로써 공격자가 만든 해킹 함수가 대신 호출되게 함으로써 DLL Injection 해킹으로 키보드 입력정보를 유출할 수 있다[4]. DLL Injection 해킹을 막는 방법은 보안을 위한 DLL을 최우선적으로 Injection하여 차순위 또는 나머지 Injection을 무력화시키는 방법을 사용한다[12].

또한 응용 프로그램 수준의 보안 노력으로 액티브엑스 키 프레스(keypress) 이벤트 핸들러 해킹 기법이 있다. 이 방법에서는 인터넷 익스플로러로 키보드 입력정보가 전달되면, 인터넷 익스플로러는 고유의 윈도우 프로시저를 수행하고 이벤트를 발생시킨다. 이 후 액티브엑스를 통해 등록된 DHTML의 키 프레스 이벤트 핸들러가 존재하면 해당 핸들러를 수행시킨 후 사용자 단말기의 화면에 문자를 출력시킨다. DHTML 이벤트 중 키보드관련 이벤트는 onkeydown, onkeyup, onkeypress가 있다. 키보드보안에서는 onkeypress 이벤트에 키보드보안 키 프레스 이벤트 핸들러를 설치하여 더미 정보를 수신한다.

공격자가 자신의 키 프레스 이벤트 핸들러를 등록하여 문자출력단계 이전에 키보드 입력정보를 유출할 수도 있다. 키보드보안에서는 보안 키 프레스 이벤트 핸들러를 등록하고, 다른 키 프레스 이벤트 핸

들러가 등록되지 않도록 막는 방법을 사용한다[13].

2.3 전통적 키보드보안 방법

키보드보안은 키보드입력이 일어난 시점에서 키보드 입력정보를 처리하여, 기존 운영체제의 기본적인 키보드 입력정보 전달과정을 거치지 않고 별도의 채널을 통해 응용프로그램으로 전달한다. 이렇게 함으로써 기본적인 키보드 입력정보 전달과정에서 키로거를 무력화시킬 수 있다.

키보드보안은 커널모드의 보안 취약 구간 이전에 키보드 입력정보를 가져와 암호화하여, 사용자모드 키보드보안 프로그램으로 전달한다. 그리고 사용자모드 키보드보안 프로그램에서 복호화 후 응용프로그램으로 출력함으로써 보안 취약 구간을 거치지 않기 때문에 키보드 입력 정보를 보호할 수 있다.

소프트웨어적인 키보드보안은 크게 커널모드 키보드보안 프로그램과 사용자모드 키보드보안 프로그램으로 이루어져 있다. 커널모드 키보드보안 프로그램은 사용자의 키보드 입력정보를 가져와 암호화 후 사용자모드 키보드보안 프로그램으로 전달하는 기능을 한다. 사용자모드 키보드보안 프로그램은 암호화된 키보드 입력정보를 가져와 복호화하고 화면에 출력되도록 응용프로그램에 전달하는 기능을 한다. 다음 그림 2는 인터넷뱅킹에 적용되는 액티브엑스 기반 키보드보안의 흐름을 보여주고 있다[13,14].

따라서 인터넷뱅킹에 적용되는 키보드보안의 흐름은 그림 2에 기반하여 다음과 같이 단계별로 구분하여 살펴볼 수 있다.

단계 1 : 액티브엑스는 암호화된 키보드 입력정보를 가져온다.

단계 2 : 액티브엑스는 암호화된 키보드 입력정보를 복호화한다.

단계 3 : 액티브엑스는 복호화된 키보드 입력정보와 대응되는 더미정보를 생성하여 시스템 메시지 큐로 전달한다.

단계 4 : 키보드보안 키 프레스 이벤트 핸들러에 더미정보가 들어오면, 액티브엑스로부터 복호화된 키보드 입력정보를 가지고 온다.

단계 5 : 더미정보와 복호화된 키보드 입력정보를 교체하면 응용프로그램으로 출력된다.

위와 같이 기존의 키보드보안 방식에서는 사용자모드 키보드보안 프로그램이 액티브엑스 이기 때문에 인터넷 익스플로러 외의 다른 웹브라우저에서는 동작할 수 없다. 그러므로 다른 웹브라우저를 지원하기 위해서는 액티브엑스가 수행하는 기능을 대신할 수 있는 기법이 필요하다.

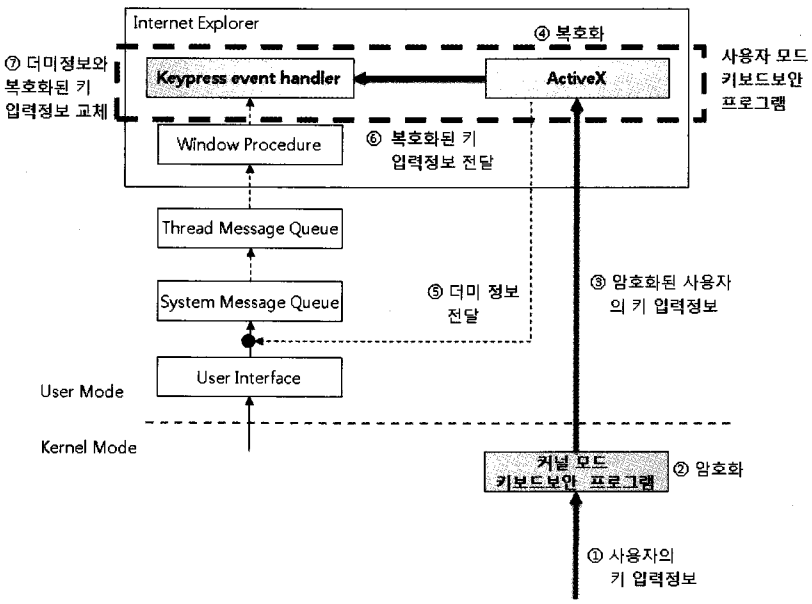

그림 2. 인터넷 뱅킹에 적용되는 키보드보안의 흐름

3. 서브클래싱 기반의 키보드 보안

서브클래싱이란 윈도우 프로시저(Windows procedure)를 후킹하는 것으로, 어플리케이션 내 윈도우상에서 후킹이란 용어 대신에 그 기능에 주안점을 두어 서브클래싱을 사용한다.

키보드 관련 메시지 처리 단계에서 응용프로그램 고유의 윈도우 프로시저가 정보침입자가 만든 가상의 처리 함수로 교체될 때, 즉 서브클래싱을 이용한 공격에서 공격자의 처리 함수가 키보드 입력정보를 가져가 유출시킬 수 있다.

본 논문에서 제시하는 서브클래싱 기반의 키보드 보안 방법은 인터넷 익스플로러 외의 액티브엑스를 지원하지 않는 다른 웹브라우저에서도 키보드 보안 문제를 해결할 수 있다.

특히 사용자 모드에서 어떻게 키보드보안을 적용할 것인가를 다루기 때문에 커널모드 키보드보안 프로그램이 어떠한 형태이든지 상관이 없으므로, 제안하는 키보드보안 방법은 사용자모드 키보드보안을 지원한다.

사용자모드 키보드보안 프로그램은 응용프로그램 내에 존재하게 된다. 특히 윈도우 운영체제환경에서 웹브라우저는 하나의 윈도우이므로 윈도우 메시지를 처리하는 윈도우 프로시저가 존재한다. 그러므로 서브클래싱을 통하여 키보드 입력 정보를 가로챌 수 있다.

따라서 키보드 보안을 위해 그림 3과 같이 플러그인(plugin)에서 윈도우 프로시저를 서브클래싱하여 키보드보안 서브클래스를 설치하는 방식을 사용한다.

그림 3에서와 같이 서브클래싱 기반의 키보드보안 방법을 단계별로 기술하면 다음과 같다.

단계 1 : 커널모드 키보드보안 프로그램이 사용자 키보드 입력정보를 가져온다.

단계 2 : 커널모드 키보드보안 프로그램이 가져온 키보드 입력정보를 암호화한다.

단계 3 : 키보드보안 플러그인은 암호화된 키보드 입력정보를 가져온다.

단계 4 : 키보드보안 플러그인은 암호화된 키보드 입력정보를 복호화한다.

단계 5 : 키보드보안 플러그인은 복호화된 키보드 입력정보와 대응되는 더미정보를 생성 하여 시스템 메시지 큐로 전달한다.

단계 6 : 키보드보안 서브클래스에 더미 정보가 들어오면, 키보드보안 플러그인으로부터 복호화된 키보드 입력정보를 가지고 온다.

단계 7 : 더미정보와 복호화된 키보드 입력정보를 교체한다.

단계 8 : 기존의 윈도우 프로시저로 복호화된 키

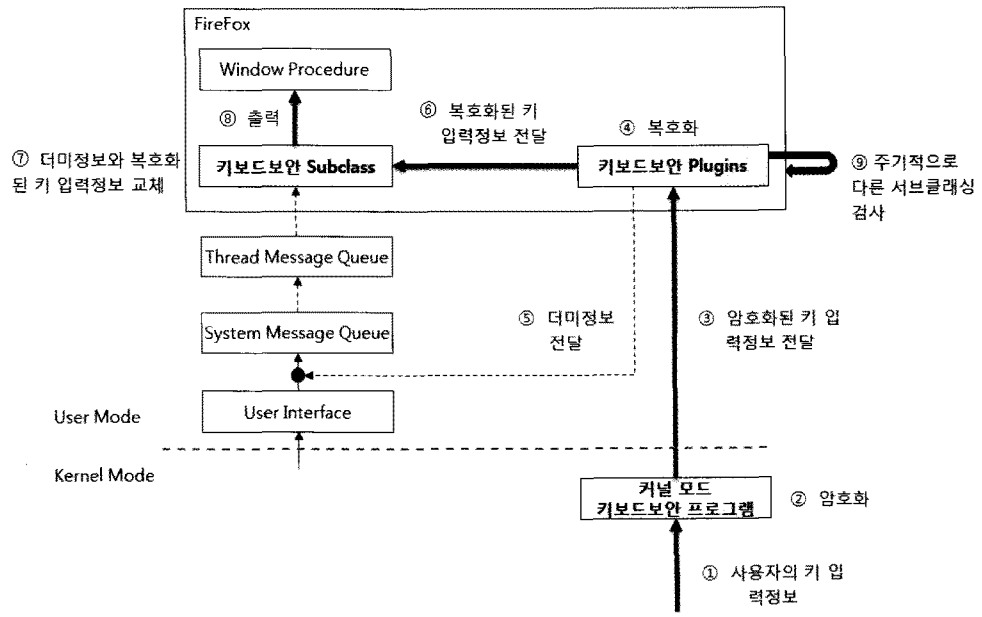

그림 3. 서브클래싱 기반의 키보드보안 방법

보드 입력정보를 전달하여 출력한다.

단계 9 : 주기적으로 다른 서브클래싱이 이뤄졌는지 검사한다.

따라서 기존의 액티브엑스에 기반한 키보드 보안 기능을 웹브라우저 플러그인에서 윈도우 프로시저를 서브클래싱하여 키보드보안 서브클래스를 설치하는 방식으로 대치함으로써 액티브엑스를 지원하지 않는 웹브라우저에서도 이 기능을 수행할 수 있다.

4. 서버클래싱 기반 보안기법의 구현

본 장에서는 서브클래싱 기반의 키보드 보안을 구현한 플러그인과 서브클래스의 구현 방법을 보인다. 구현환경으로는 액티브엑스를 지원하지 않는 웹브라우저 중 가장 많이 사용되는 파이어폭스와 개발언어로 C/C++를 사용하였다.

4.1 키보드보안 플러그인

서브클래싱에 기반한 키보드 보안을 구현하기 위해 그림 3의 키보드보안 플러그인은 파이어폭스의 Gecko 플러그인으로 구현하였다. Gecko 플러그인은 C/C++ SDK를 제공하므로, Win32 API를 사용할 수 있다. 또한 프로젝트 설정과 MFC 헤더를 포함하면 MFC를 사용할 수 있다.

Gecko 플러그인은 다음 3개의 함수가 Export되어야 파이어폭스에 설치된다.

① NPError OSCALL NP_Initialize(NPNetscape Funcs* aNPNFuncs)
② NPError OSCALL NP_GetEntryPoints (NPPluginFuncs* aNPPFuncs)
③ NPError OSCALL NP_Shutdown()

키보드보안 플러그인은 키보드보안이 적용된 웹페이지에 접속시 설치되고, 설치 후 초기화 함수 NP_Initialize()를 호출한다. 다음 그림 4는 NP_Initialize()의 프로시저를 보여준다.

NP_Initialize()에서 볼 수 있듯이 키보드보안 플러그인에서는 다음과 같은 기능을 한다.

① 커널모드 키보드보안 프로그램 설치
② Win32 API를 이용한 드라이버 설치
③ 커널모드 키보드보안 프로그램 설치와 지속적인 통신
④ 다른 서브클래싱 감시

```
static LRESULT CALLBACK Subclass(HWND, UINT,
      WPARAM, LPARAM);
static WNDPROC lpOldProc = NULL;
static WNDPROC lpMyProc = NULL;
NPWindow* pNPWindow;
DWORD WINAPI ThreadFunc(LPVOID lParam);

NPError OSCALL NP_Initialize(NPNetscapeFuncs*
        aNPNFuncs)
{
 // [커널모드 키보드 보안 프로그램 설치]
 // Win32 API를 이용한 Driver 설치

 // [서브클래싱]
 if(pNPWindow == NULL)
   return FALSE;
 mhWnd = (HWND)pNPWindow->window;
 if(mhWnd == NULL)
   return FALSE;
 lpOldProc = SubclassWindow(mhWnd, (WNDPROC)
             Subclass);
 SetWindowLong(mhWnd, GWL_USERDATA, (LONG)this);

 // [키보드 보안 Subclass 주소 저장]
 lpMyProc = (WNDPROC)GetWindowLongPtr(mhWnd,
            GWLP_WNDPROC);
 // [커널모드 키보드보안 프로그램과 지속적인 통신]
 // [다른 서브클래싱 감시]
 CreateThread(NULL,0,(LPTHREAD_START_ROUTINE)
             ThreadFunc,this,0,&this);
}
```

그림 4. NP_Initialize() 프로시저

4.2 키보드보안 서브클래스

키보드보안 서브클래스는 키보드보안 플러그인에서 생성되고 파이어폭스에 서브클래싱된다. 키보드보안 서브클래스 기능은 다음과 같다.

① 키보드보안 시작/종류
② 더미정보 수신
③ 더미정보를 복호화된 키보드 입력정보로 교체
④ 기존의 윈도우 프로시저로 복호화된 키보드 입력정보 전달

다음 그림 5는 위에서 설명한 키보드보안 서브클래스 기능을 가진 프로시저를 보여준다.

다음은 위에서 제시된 서브클래싱 기반 파이어폭스 키보드보안 방법으로 키보드보안을 구현하여 키보드보안이 정상적으로 수행되는 것을 실험을 통하여 보여주는 화면들이다.

```
static LRESULT CALLBACK Subclass(HWND hWnd,
   UINT msg, WPARAM wParam, LPARAM lParam)
{
 switch (msg) {
 case WM_SETFOCUS:
      // 키보드 보안 시작
      break;
 case WM_KILLFOCUS:
      // 키보드 보안 종료
      break;
 case WM_KEYDOWN:
      switch(wParam) {
        // wParam이 더미 문자일 경우:
        // 복호화된 키 입력정보로 복호화
      }
      break;
 default:
      break;
 }
 // wParam = 복호화된 키 입력정보;
 return CallWindowProc(lpOldProc2, hWnd, msg,
        wParam, lParam)
}
```

그림 5. 키보드보안 서브클래스 프로시저

다음 그림 6은 키보드보안 플러그인이 설치되고, WM_SETFOCUS일 때 키보드보안이 시작되는 것을 보여주는 화면이다. 키보드보안이 시작할 때는 하단에 트레이 아이콘이 표시되고, 종료되면 트레이 아이콘이 사라지도록 구현하였다.

다음 그림 7은 키보드보안 플러그인 설치시 키로거의 해킹을 막는 것을 보여주고, 파이어폭스 페이지

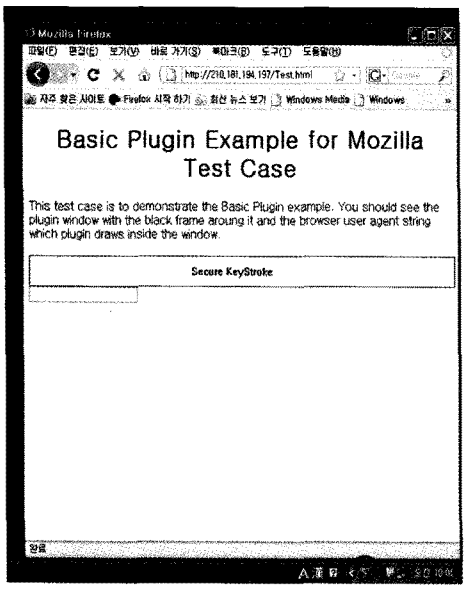

그림 6. 키보드보안 시작

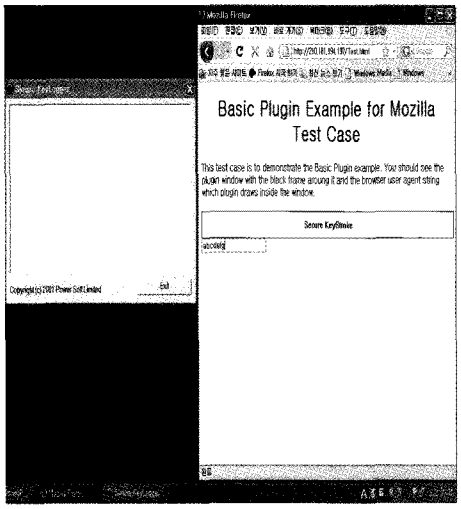

그림 7. 키보드보안 플러그인 설치시 키로거의 해킹 방지

에 입력한 키보드 입력정보가 정상적으로 출력되는 것을 보여준다.

따라서 액티브엑스를 지원하지 않는 파이어폭스 웹브라우저에서 플러그인을 사용한 서브클래싱 기반의 사용자 모드 키보드 보안이 키로거의 해킹으로부터 보호됨을 확인할 수 있었다.

5. 구현결과의 평가 및 비교

플러그인을 사용한 서브클래싱 기반의 사용자 모드 키보드 보안기법이 액티브엑스의 지원없이 키보드 보안을 할 수 있음을 보았다. 본 연구에서 제안하고 구현한 서브클래싱 기반의 키보드 보안 기법과 기존의 키보드 보안 방법을 여러 측면에서 비교 검토하면 다음 표 2와 같다.

본 연구에서 개발한 서브클래싱에 기반한 기법은 표 2에서 보는 바와 같이 하드웨어적 방법에 비해 추가적인 하드웨어 모듈이 필요 없으므로 경제적이다. 또한 기존의 액티브엑스에 기반한 방법은 인터넷 익스플로러에서만 적용될 수 있으나 본 기법은 액티브엑스를 지원하지 않는 파이어폭스 웹브라우저에서도 적용이 가능하며 키보드 I/O 포트스캔, 인터럽트 벡터 교환 등과 같은 커널모드 보안프로그램과 연동을 하게 할 수 있다. 그러나 제안한 기법은 아직까지 모든 웹브라우저를 지원하지 않는 제약은 있으나 최근 활용도가 높아지고 있는 모바일 기반의 스마트폰용 마이크로브라우저에서도 확대하여 적용할

표 2. 키보드 보안 기법의 비교 (○: 지원, ×: 미지원)

기능성 \ 보안기법		하드웨어 방법	스크린 키보드 방법	키보드 보안 드라이버의 인코딩 방법	액티브엑스에 기반한 방법	본 연구의 서브클래싱에 기반한 기법
하드웨어 추가지원		○	○	×	×	×
인터넷 익스플로러 외의 웹 브라우저 지원		○	×	○	×	○
커널 모드 보안프로그램과 상호 연동성	키보드 I/O 포트 스캔	×	×	×	○	○
	인터럽트벡터테이블 주소 교환	×	○	×	○	○
	다양한 키보드 드라이버 지원	○	×	○	○	×
기법의 스마트폰 지원 확장 가능성		○	○	×	×	○

수 있는 장점이 있다.

6. 결 론

본 논문에서는 플러그인을 사용한 서브클래싱 기반의 사용자 모드 키보드 보안 기법을 제안하고 이를 액티브엑스를 지원하지 않는 파이어폭스 웹브라우저에서 구현한 방법을 보였다.

기존의 소프트웨어적인 키보드 보안 방법에서 액티브엑스는 별도의 채널을 통해 가져온 암호화된 키보드 입력정보를 복호화하여 인터넷 익스플로러로 전달하는 역할을 하였지만, 액티브엑스를 지원하지 않는 웹브라우저에서는 이러한 방법을 사용할 수 없다. 따라서 본 연구에서는 이러한 문제점을 해결하기 위해 기존의 액티브엑스와 키 이벤트 핸들러에서 처리되는 기능을 플러그인을 사용한 서브클래싱 기반의 방법으로 키보드 보안 기능을 처리하도록 하였다. 따라서 이 방법의 특징은 다음과 같다.

첫째, 제안한 기법은 소프트웨어적으로 사용자 모드에서 액티브엑스를 지원하지 않는 웹브라우저에서 키보드 보안을 지원할 수 있다.

둘째, 하드웨어적 추가 모듈이 필요하지 않으므로 기존의 보안 키보드에 비해 경제적이다. 셋째, 전통적 커널모드 보안 프로그램과 상호 연동성을 유지할 수 있다.

마지막으로, 모바일 기반의 스마트폰용 마이크로브라우저에서도 액티브엑스를 사용하지 않기 때문에 본 기법을 확장하여 적용할 수 있다.

앞으로는 본 연구에서 제시한 플러그인을 사용한 서브클래싱 기반의 키보드보안 기법을 다양한 브라우저 및 마이크로브라우저에 적용하여 그 활용성을 증대시키고 이 기법과 관련한 전자거래 전반의 새로운 보안 취약점이 발견되면 이를 개선하는 일이다. 또한 Gecko 플러그인을 사용하지 않는 서브클래싱 기반의 키보드 보안 방법을 개발하는 일이다.

참 고 문 헌

[1] Muzammi M. Baig and W. Mahmood, "A Robust Technique of Anti Key-Logging using Key-Logging Mechanism," 2007 Inaugural IEEE International Conference on Digital Ecosystems and Technologies, pp. 314-318, 2007.

[2] 전상훈, "인터넷 뱅킹 해킹의 이면," ZDNet Korea, http://www.zdnet.co.kr/ArticleView.asp?artice_id=20090525192302, 2009.

[3] Jun Fu et al., "Detecting Software Keyloggers with Dendritic Cell Algorithm," International Conference on Communications and Mobile Computing, Vol.1, pp. 111-115, 2010.

[4] Y. Al-Hammadi and U. Aickelin, "Detecting Bots Based on Keylogging Activities," Proceedings of the Third International Conference on Availability, Reliability and Security, pp. 896-902, 2008.

[5] Ze-Guang Jin, Heau-Jo Kang, and Yoon-Ho Kim, "The Research of Keyboard Security for u-Trading," The 2007 International Conference on Intelligent Pervasive Computing, pp.

165-169, 2007.
[6] 금융ISAC, "키보드 해킹기법 및 대응기술 분석," 금융 ISAC, pp. 8-10, 2005.
[7] 테커스㈜, "액티브엑스 기반의 키보드 해킹 방지 방법 및 장치," 대한민국특허청, 등록번호: 10-0378586, 2003.
[8] 배광진, 임강빈, "키보드보안의 근본적인 취약점 분석," 한국정보보호학회 논문집 제18권 제3호, pp. 89-95, 2008.
[9] 태커스㈜, "가상 데이터 전송을 이용한 키보드 해킹 방지 장치 및 방법," 대한민국특허청, 등록번호: 10-075727, 2007.
[10] 정태영, 임강빈, "키보드컨트롤러의 하드웨어 취약점에 대한 대응 방안," 한국정보보호학회 논문집 제18권 제4호, pp. 187-194, 2008.
[11] 소프트캠프㈜, "인터럽트 처리함수 교체에 의한 키보드 입력정보의 무단유출을 차단하는 방법," 대한민국특허청, 등록번호: 10-0549646, 2006.
[12] 소프트캠프㈜, "키보드 입력정보 보안시스템 및 그 방법," 대한민국특허청, 공개번호: 10-2007-0074897, 2007.
[13] 소프트캠프㈜, "키보드 입력정보 보안방법," 대한민국특허청, 등록번호: 10-0549647, 2006.
[14] 최성욱, 김기태, "안전하고 신뢰성있는 전자상거래를 위한 키보드 입력 보안 시스템의 설계 및 구현," 한국정보처리학회논문지C 제13권, 제1호, pp. 55-62, 2006.

황 성 진

2001년 동아대학교 컴퓨터공학과 학사
2003년 동아대학교 컴퓨터공학과 공학석사
2003년~현재 동아대학교 컴퓨터공학과 박사과정

2004년~2010년 소프트캠프 근무
2010년~현재 삼성SDS 근무
관심분야 : 정보보호, 멀티미디어시스템, 모바일 컴퓨팅

박 경 환

1981년 경북대학교 컴퓨터공학전공 학사
1983년 서울대학교 컴퓨터공학과 공학석사
1990년 서울대학교 컴퓨터공학과 공학박사

1998년 University of California, Irvine 객원교수
1987년~현재 동아대학교 컴퓨터공학과 교수
관심분야 : 멀티미디어시스템, 모바일 컴퓨팅, 원격교육