보안 USB 키보드의 데이터 탈취 가능성 진단

Vulnerability Assessment on the Secured USB Keyboard

이 경 률* 임 강 빈**
Kyungroul Lee Kangbin Yim

요 약

보안 시스템에서 사용자 인증은 필수적이며 가장 중요한 절차 중의 하나이다. 대개의 사용자 인증은 키보드를 통한 문자 기반의 패스워드를 이용하여 이루어지므로 키보드 정보의 보호는 무엇보다 중요하다(7)(8). 이러한 이유로 키보드 보호를 위한 소프트웨어들이 주요 사이트에 적용되어 있다. 본 논문은 현재 보편적으로 사용되고 있는 USB 키보드의 취약점을 소개하고 이를 이용하는 예제 코드를 구현하여 키보드 보안 소프트웨어가 실행되고 있는 상황에서의 키보드 데이터의 탈취 가능성을 진단한다. 또한 결과의 비교를 통하여 해당 취약점에 대응하기 위한 보안 대책을 제안한다.

ABSTRACT

The user authentication on the security applications is one of the most important process. Because character based password is commonly used for user authentication, it is most important to protect the keyboard. Due to the reason, several software solutions for keyboard security have been applied to critical sites. This paper introduces vulnerabilities to the commonly used USB keyboard, implements a sample code using the vulnerabilities and evaluates the possibility for the keyboard data to be stolen in the guarded environment. Through the comparison of the result, a countermeasure to the vulnerabilities is proposed.

☞ keyword : USB keyboard, vulnerability assessment, secure keyboard software, keyboard sniffing, password authentication

1. 서 론

인터넷과 개인 컴퓨터의 보급이 맞물린 시점의 586컴퓨터 시대에서 현재의 쿼드코어 컴퓨터까지 컴퓨터는 급격한 발전을 거듭해왔다. 그에 따라 더 나은 성능을 위한 다양한 장치들이 개발되었으며 장치들에 대한 인터페이스 역시 발전되어 왔다. 그중에서도 우리가 가장 많이 알고 있고, 쉽게 접할 수 있는 것이 USB(Universal Serial Bus)이다.

USB는 직렬 포트의 일종으로, 키보드, 카메라, 마우스 등과 같은 주변기기와 컴퓨터 간의 연결을 지원해준다. 이 인터페이스는 플러그 앤 플레이와 핫플러깅의 편리성과 최대 127개까지의 주변장치를 연결할 수 있는 확장성을 가지고 있으며 480Mbps(USB 2.0 기준)의 빠른 속도를 지원하기 때문에 다양한 기기에 적용되고 있으며[1] 현재 일상생활에서도 흔히 볼 수 있듯이, 컴퓨터뿐만 아니라 휴대용 장치까지 확장되어 사용되고 있다.

하지만 이처럼 폭넓게 사용되고 있는 USB 장치들의 취약점들이 속속들이 드러나고 있고[2,3,9,10,14,16,19,25], 대중화되어 있는 만큼 그에 따른 피해 규모가 심각할 수 밖에 없다. 더욱이 USB 인터페이스를 이용하는 대표적인 장치인 키보드, 마우스, USB 저장장치 뿐만 아니라, USB 인터페이스를 이용하는 대부분의 장치가 개인정보와 밀접한 관련이 있는 정보들을 다루고 있기 때문에 작게는 정보유출에서 크게는 금전적 손해까지 끼칠 수 있다. 현재 인터넷 뱅킹, 인터넷

* 준 회 원 : 순천향대학교 정보보호학과 박사과정
carpedm@sch.ac.kr
** 종신회원 : 순천향대학교 정보보호학과 부교수
yim@sch.ac.kr(교신저자)
[2011/04/28 투고 - 2011/05/11 심사 - 2011/08/05 심사완료]

결재 등 인터넷을 통한 금전거래가 빈번하게 이뤄지고 있는 시점에서, 그에 대한 보안 문제가 언급되어 많은 보안회사에서 연구 중에 있지만 피해사례가 속출하고 있다. 앞서 말한 USB 장치들 중 가장 많이 사용되고 개인정보가 쉽게 노출될 수 있는 장치는 키보드라 할 수 있다. 키보드는 PS/2 인터페이스와 USB 인터페이스를 사용하고 있는데, 현재 USB 인터페이스로 대부분 교체되고 있다. 하지만 PS/2 인터페이스에서의 취약점뿐만 아니라[4-6,12,13,15] USB 인터페이스 키보드에 대한 취약점이 발견되고 있고, 더욱이 USB 인터페이스는 메모리를 사용하는 구조상의 취약점 때문에 PS/2 방식보다 보안상의 안전성이 뒤떨어진다고 보고되기도 했다[3,7,11]. 이러한 상황에서 현재 USB 3.0이 개발되어 보급이 시작되었고, 앞으로 USB의 사용이 더 확대될 것으로 예상되고 있어 USB에 대한 보안문제의 해결이 시급한 실정이다.

본 논문에서는 USB 키보드의 안전성을 진단하기 위하여 두 가지 서로 다른 시각에서의 취약점을 소개하고 이를 이용하는 소프트웨어를 실제로 구현하여 실험하였다. 이를 통하여 USB 키보드를 통해 전달되는 USB 데이터의 탈취가 가능함을 확인하였다. 이러한 실험은 현재 인터넷 뱅킹에서 동작하고 있는 보안 프로그램이 실행되는 상태에서 이루어진 것으로서, 이를 통해 USB 기반 키보드의 보안 취약성을 확인하고, 해결방안을 도출하는 데에 일조할 수 있을 것으로 사료된다.

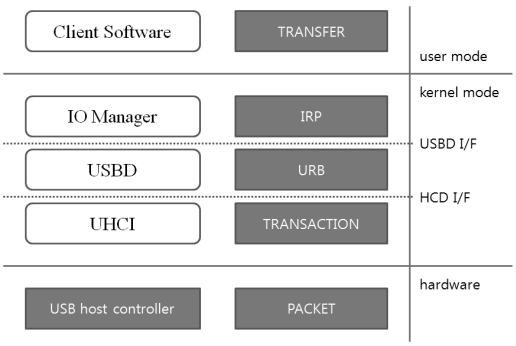
본 논문의 구성은 다음과 같다. 2장에서 USB 키보드의 데이터 전송구조를 살펴보고, 3장에서 USB 키보드의 데이터를 탈취 가능성을 보인다. 그리고 4장의 결론으로 논문을 마무리한다.

2. USB 키보드의 데이터 전송 구조

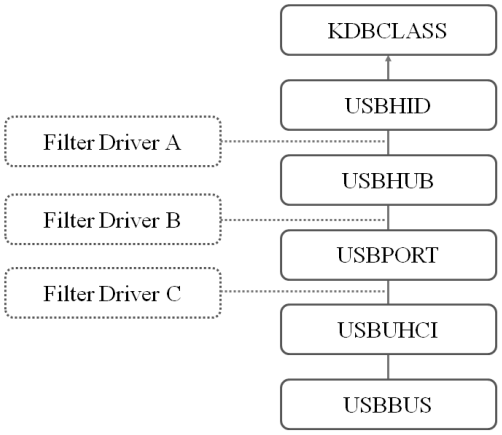
USB는 일반적으로 (그림 1)과 같은 데이터 전송 구조를 갖고 있다[1]. (그림 1)을 보면 USB 호스트 컨트롤러와 USB 시스템 소프트웨어 사이에서 인터페이스를 담당하는 HCD(Host Controller Driver)와 USB 시스템 소프트웨어와 클라이언트 소프트웨어의 인터페이스를 담당하는 USBD (USB Driver)를 확인 할 수 있다. USB는 (그림 1)과 같은 과정을 통해 패킷, 트랜잭션, IRP(I/O Request Packet), 데이터의 전송이 이뤄진다. 또한 USB는 데이터의 요구조건과 특성에 따라 여러 가지의 전송 형태를 보인다. 호스트와 장치 간의 통신을 구축하고 유지하는 데 사용하는 제어(Control) 전송 형태, 실시간 음성이나 영상을 전송하는 등시(Isochronous) 전송 형태, 프린터나 저장 장치 등 비정기적 대용량 데이터를 전송하는 벌크(Bulk) 전송 형태, 그리고 마우스나 키보드와 같이 소량의 데이터를 주기적으로 전송하는 인터럽트(Interrupt) 전송 형태를 들 수 있다. USB 키보드 데이터의 탈취는 인터럽트 전송 형태의 데이터를 감시하고, 전송되는 데이터 들 중 키보드 데이터를 필터링함으로서 가능하다.

3. USB 키보드의 데이터 탈취 가능성 진단

USB 키보드의 드라이버 구조는 (그림 2)와 같다. 그림에서 보이는 것과 같이 USBUHCI와 바로 연결되어 있는 USBPORT 드라이버에서 키보드의 데이터를 가장 먼저 취득하게 된다. 본 논문에서는 키보드 보안 소프트웨어가 실행되고 있는 상태에서 키보드 데이터의 탈취 가능성을 확인하기 위하여, 필터 드라이버를 USB 드라이버에 삽입하는 방법과 USBPORT 드라이버 상에서 인라인 코드 패치를 통한 함수 후킹 방법의 서로 다른 두 수준에서, 키보드 데이터의 수집을 시도하였다. 탈취 가능성 진단 방법은 커널 모드를 통해서 동작이 이루어지며, 이를 위하여 각각 커널 모드에서 실행되는 디바이스 드라이버를 구현하여 연동함으로써, 수집한 키보드 데이터를 출력하는 소프트웨어를 구현하였다.



(그림 1) 시스템 관점에서의 USB 데이터 전송 구조



(그림 2) USB 드라이버의 계층 구조

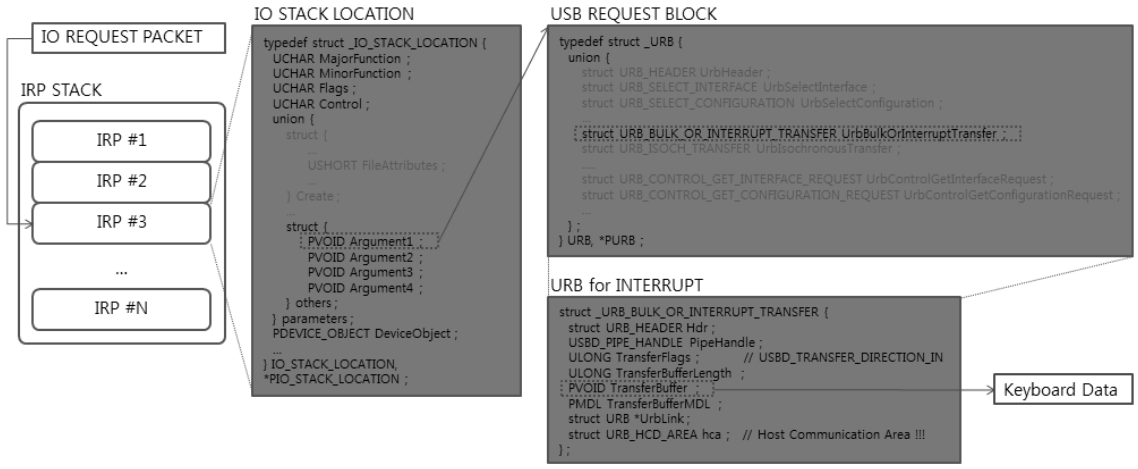
3.1 필터 드라이버로의 접근 방법

필터 드라이버를 USB 드라이버 사이에 삽입하여 보안 프로그램보다 먼저 키보드 데이터를 획득하기 위해서는 USBPORT에 Upper Filter형태로 어태치(attached)해야 한다. 필터 드라이버는 디바이스 스택의 기능 드라이버를 부연하는 목적을 가진 드라이버로서[20], 필터 드라이버를 통해 기능 드라이버(USBPORT)를 감시하여 키보드 데이터를 탈취하는 것이 가능하다. 이러한 시도에서 얻고자 하는 정보는 키보드 데이터이며, 이는 IRP에 존재하고 있으므로 IRP를 후킹함으로써 키보드 데이터를 획득할 수 있다.

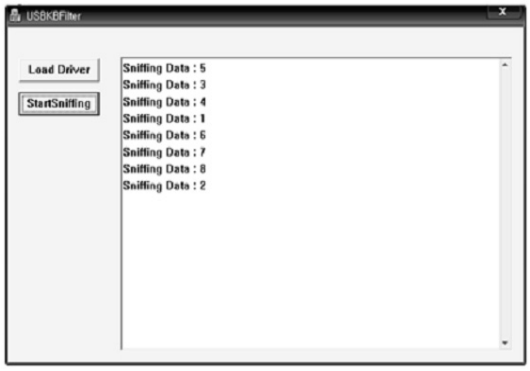
모든 커널 드라이버들은 다른 드라이버와의 통신을 통해서 디스패치 루틴을 호출할 수 있는데, 이러한 통신을 사용하기 위한 것이 바로 IRP 구조체이다. 클라이언트가 IRP를 전달하면 디바이스 스택 상에서 가장 하위의 드라이버까지 전달된 후에 다시 가장 상위의 스택으로 전달되는 형태를 갖고 있으므로, 필터 드라이버를 삽입함으로써 IRP를 후킹할 수 있다[20,23,24].

(그림 3)에서와 같이 키보드 데이터는 USB 드라이버 계층을 경유하여 전송되는 IRP를 통하여 확인할 수 있다. 즉, 해당 IRP와 연관되는 IO_STACK_LOCATION의 Parameters.Others.Argument1 포인터가 USB 데이터를 위한 URB 구조체를 가리키고 있고 키보드는 인터럽트 전송 형태를 갖고 있기 때문에 URB의 URB_BULK_OR_INTERRUPT_TRANSFER 구조체 내에서 키보드 데이터를 획득할 수 있다. 구현한 필터 드라이버의 삽입 위치 때문에 USB 컨트롤러로 직접 연결된 키보드의 데이터 탈취에는 실패하였으나, 컴포지트에 연결된 USB 키보드의 경우 데이터 탈취가 가능하였다. 컴포지트란, 무선 키보드, 무선 마우스의 형태를 동작하게 해주는 것으로, 다른 장비들을 혼합 사용할 수 있게 해준다. 무선 키보드, 무선 마우스의 사용이 점차 확대됨에 따라 USB 키보드의 데이터 탈취 뿐만 아니라 USB 컴포지트에 연결된 키보드의 데이터 탈취는 큰 문제가 될 것이다. 더욱이, 필터 드라이버의 삽입 위치에 따라 USB 키보드 또한 키보드 데이터의 탈취가 가능할 것으로 판단된다.

본 논문은 USB 컴포지트에 연결된 키보드를 이용하여 현재 상용화되어 사용 중인 6개의 키보드보안 소프트웨어를 대상으로 키보드 데이터 탈취 가능성 및 탈취행위의 탐지 여부를 진단하였다. 그 결과, (그림 4)에서와 같이 현재 인터넷 뱅킹에서 사용되고 있는 대부분의 보안 소프트웨어의 경우 키보드 데이터의 탈취를 방어하지 못하고 있었고, 1개의 보안 소프트웨어만이 키보드 데이터의 탈취를 방어하고 있었다. 더욱이 필터 드라이버의 존재여부조차도 탐지하지 못하고



(그림3) USB 데이터 전송 과정에서의 IRP 내 키보드 정보 위치



USB 키보드 스니핑 화면

업체명	드라이버 탐지경고	스니핑 여부
A사	X	가능
B사	X	가능
C사	X	불가능
D사	X	가능
E사	X	가능
F사	X	가능

보안업체별 보안프로그램 우회 스니핑 여부

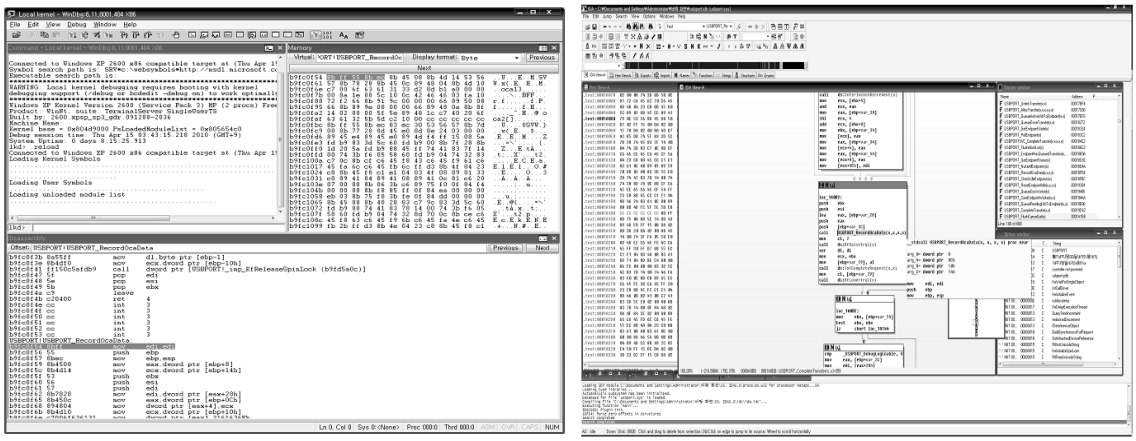
(그림 4) USB 키보드 데이터 탈취 가능성 확인

있었다.

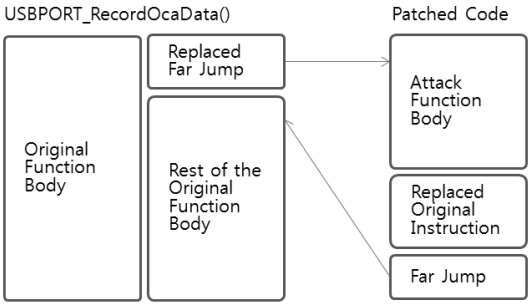
데이터의 취득이 불가능한 1개의 경우에는 보안 소프트웨어가 데이터를 취득하고 자신의 영역에 데이터를 보관한 후 IRP 내에 있는 키보드 데이터를 지워버리는 방식을 사용하기 때문인 것으로 판단된다. 그러나 결국 필터 드라이버가 현재 삽입된 위치인 USBHUB와 USBHID 사이(그림 2의 A)보다 더 아래(그림 2의 B)에 삽입되게 된다면, 보안 프로그램보다 먼저 IRP를 획득하여 키보드 데이터를 탈취당할 것이라 판단된다. 하지만 USB 드라이버의 구조에서 USBHUB 아래에 위치한 USBPORT의 경우 USBHUB처럼 드러나 있는 커널 드라이버가 아니기 때문에 포인터를 얻어오거나 하는 방법들을 사용하여 어태치하는 것이 어려울 것으로 사료된다.

3.2 인라인 코드 패치를 통한 접근 방법

3.1절에서와 같이 USBPORT에 필터 드라이버를 어태치하는 것이 불가능하더라도 USBPORT 드라이버 자체를 인라인 코드 패치하는 것이 더 심각한 공격방법이 될 수 있다[21,22]. 인라인 코드 패치란 USBPORT드라이버 내의 함수를 후킹하여 USBPORT 내에서 호출되는 함수대신 공격



(그림 5) WinDbg, IDA를 이용한 USBPORT_RecordOcaData() 함수 확인



(그림 6) 인라인 코드 패치 방식

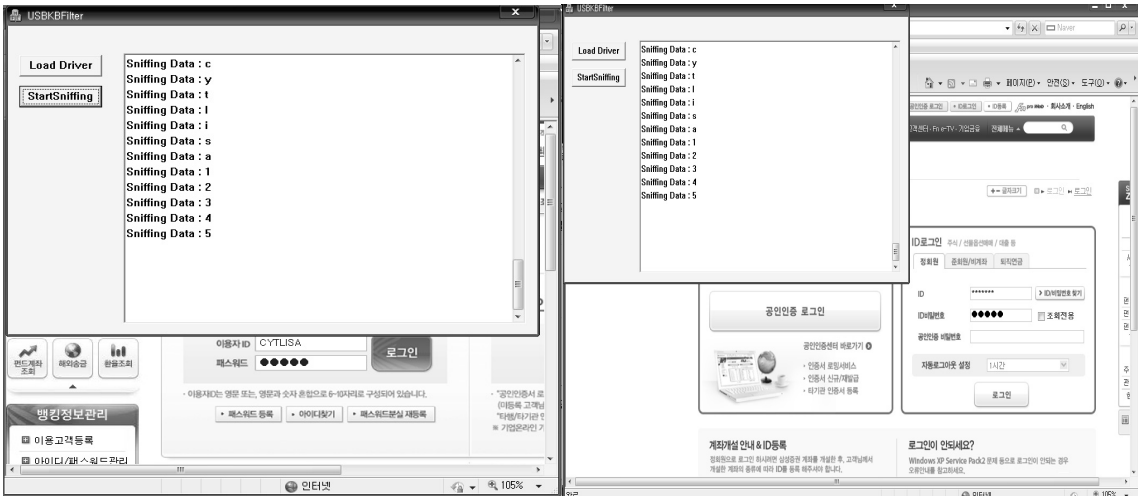
자가 만들어 놓은 함수를 호출하도록 하는 방법을 의미한다. 공격자가 이러한 공격방법을 수행하기 위해서는 먼저 USBPORT 드라이버 내에서 키보드 데이터를 다루고 있는 함수를 찾아야 한다. (그림 5)와 같이 WinDbg와 IDA 등의 도구를 이용하여 키보드 데이터를 다루는 함수가 USBPORT_ USBPORT_RecordOcaData() 임을 쉽게 확인할 수 있다.

공격자는 가장 먼저 키보드 데이터를 얻기 위해서 USBPORT_RecordOcaData() 함수가 키보드 데이터들을 수집하기 이전에 자신의 공격 함수를 호출하도록 할 것이다. 또한, 공격 함수를 수행한 후 다시 정상적인 실행을 위해 USBPORT_ Record OcaData() 함수가 패치되기 전과 같은 루틴을 수행해야 한다. 이러한 인라인 코드 패치 방식을 (그림 6)에서 나타내었다[9].

(표 1) 인터넷 사이트에서의 키보드 데이터 탈취 가능성 여부

보안 업체명	사이트명	탐지경고	스니핑 가능여부
B 사	ㄱ 은행	X	가능
D 사	ㄴ 은행	X	가능
B 사	ㄷ 은행	X	가능
D 사	ㄹ 은행	X	가능
B 사	ㅁ 은행	X	가능
D 사	ㅂ 은행	X	가능
C 사	ㅅ 은행	X	가능
B 사	ㅈ 은행	X	가능
A 사	ㅊ 은행	X	가능
E 사	ㅋ 증권	X	가능
F 사	ㅌ 사이트	X	가능

본 논문에서는 상기 방식의 한 예를 구현하여 실험하였다. 실험을 통해 USB 키보드의 키보드 데이터를 수집할 수 있었으며, 실제의 보안 소프트웨어들을 대상으로 탈취 가능성을 확인한 결과 (그림 7) 및 (표 1)과 같은 결과를 얻을 수 있었다. 모든 경우에 대하여 키보드 데이터의 탈취가 가능하였으며, 이는 USB 키보드, 더 나아가 USB 데이터의 보안문제가 얼마나 심각한지를 보



(그림 7) 금융권 사이트에서의 키보드 데이터 탈취 가능성 확인 결과

여주고 있다. (표 1)과 같은 결과를 얻을 수 있었다. 모든 경우에 대하여 키보드 데이터의 탈취가 가능하였으며, 이는 USB 키보드, 더 나아가 USB 데이터의 보안문제가 얼마나 심각한지를 보여주고 있다.

4. 결 론

본 논문에서는 USB 인터페이스의 안전성을 확인해 보기 위해 USB 장치 중 하나인 USB 키보드를 대상으로 USB 데이터의 탈취 가능성을 확인하였다. 확인결과 USB 키보드의 데이터를 탈취할 수 있었으며, 보안 프로그램 역시 우회할 수 있었다. 기본적으로 USB 키보드 데이터의 탈취가 가능하다는 것 자체도 큰 문제이지만, 보안 프로그램이 동작하는 중에도 탈취가 가능하다는 것은 악의적인 해커들에 의해 크나큰 금전적 피해를 가져올 수 있기 때문에 그 심각성이 매우 크다. 더욱이, 키보드뿐만 아니라 USB 인터페이스를 사용하는 모든 장치들에 대해서도 위와 같은 공격방법의 적용이 가능할 것으로 예상된다. 비록, 위에서 제시한 공격방법의 경우 해당 코드를 원래의 코드와 비교하여 탐지하는 방법으로 어느 정도 해결할 수 있을 것으로 보이지만, 이러한 것들은 임시적인 방편에 불과하다. 소프트웨어상의 대응은 새로운 공격방법들에 의해 새로운 취약점이 드러날 가능성이 항상 존재하며, USB 인터페이스는 이러한 문제들보다 더 큰 문제를 가지고 있다. USB는 하드웨어의 취약점에 기인하여 발생하는 문제를 갖고 있으며, 이는 상당히 큰 피해를 야기할 것으로 보여진다. 더구나 이미 USB 구조상의 취약점을 이용하여 USB 최하위 단계인 USBUHCI 아래 하드웨어에서의 데이터 스니핑 가능성에 대한 연구가 진행된 바 있으며, 이러한 방법은 USB가 메모리를 통해 통신을 한다는 구조적인 취약점을 이용한 공격방법이기에 그 구조를 바꾸기 이전에는 취약점을 완전히 없애는 것은 불가능할 것으로 사료된다. 이러한 이유로 키보드를 대체하기 위한 인증방법들이 다수 연구되고 있지만 현재까지 뚜렷한 해결책이 마련되지 못하고 있다[17,18,26]. 따라서 보다 안전한 전자거래를 위해서는 인증환경을 위한 기존 하드웨어 플랫폼의 수정이나 별도의 하드웨어 구성 등도 고려되어야 할 것으로 사료된다. 일례로, 기존 하드웨어 플랫폼의 수정 측면에서는 범용 양방향성의 주 메모리에 매핑된 USB

호스트컨트롤러의 레지스터 및 통신영역(HCCA: Host Controller Communication Area)에 대하여 쓰기만 가능한 단방향성 메모리로의 하드웨어적인 변경을 권고할 수 있으며 별도의 하드웨어 구성 측면에서는 기존의 1차원적인 메모리 구조를 탈피하여 다차원의 부가(Redundant) 메모리 및 보안 프로세싱 엔진 설계를 통한 적극적 대응 방안이 가능할 것이다.

참 고 문 헌

[1] Universal Serial Bus Specification Rev2.0, Compaq, HP, Intel, Lucent, MS, NEC, Philips, Apr. 2000

[2] 임강빈, “USB 보안 취약점 보고서”, 한국정보보호진흥원, 2008년 11월

[3] 이경률, 배광진, 임강빈, “USB 데이터 보안 취약성 분석”, 한국정보보호학회 하계학술대회 논문지, 제19권 제1호, pp.59-63, 2009년 6월

[4] Kyungroul Lee, Kwangjin Bae, Kangbin Yim, “Hardware Approach to Solving Password Exposure Problem through Keyboard Sniff”, ACADEMIC SCIENCE RESEARCH, WASET, pp.23-25, 2009. 10

[5] 정태영, 임강빈, “키보드컨트롤러의 하드웨어 취약점에 대한 대응 방안”, 한국 정보보호학회 논문지 제18권 제4호, pp187-194, 2008년 8월

[6] 배광진, 임강빈, “키보드 보안의 근본적인 취약점 분석”, 한국정보보호학회 논문지 제18권 제3호, pp.88-95, 2008년 6월

[7] 이경률, “개인정보 관리에서의 하드웨어 플랫폼 및 디바이스 인증 취약점에 관한 연구”, 순천향대학교 석사학위논문, 2010년 8월

[8] Linda Paulson, “Key Snooping Technology Causes Controversy,”IEEE Computer, pp.27, Mar. 2002

[9] John Clark, Sylvain Leblanc and Scott Knight, “Hardware Trojan Horse Device based on Unintended USB Channels,” NSS2009, IEEE Computer Society, pp.1-9, Oct. 2009

[10] Kyungroul Lee, Hyeungjun Yeuk, Youngtae Choi, Sitha Pho, Ilsun You, Kangbin Yim, “Safe Authentication Protocol for Secure USB Memories”, JoWUA(Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications), Vol.1,No.1, pp.46-55, Jun. 2010

[11] Kyungroul Lee, Wansoo Kim, Kwangjin Bae, Kangbin Yim, “A Solution to Protecting USB Keyboard Data”, Proceedings of BWCCA 2010(International Conference on Broadband and Wireless Computing, Communication and Applications), pp.108-111, Nov. 2010

[12] Kangbin Yim, “A new noise mingling approach to protect the authentication password”, Proceedings of CICIS2009, pp.191-194, Feb. 2010

[13] Kyungroul Lee, Kangbin Yim et al., “Password Sniff by. Forcing the Keyboard to Replay Scan Codes,” Proceedings of. JWIS2010, pp.9-11, Aug. 2010

[14] 이경률, 배광진, 임강빈, “USB 데이터 보안 취약성 분석”, 한국정보보호학회 하계학술대회 논문집, pp.59-63, 2009년 6월

[15] 정태영, 이경률, 배광진, 임강빈, “스니핑 방지를 위한 키보드 프로토콜”, 정보보호학회 하계학술대회논문집 제18권 제1호, pp.375-379, 2008년 06월

[16] 최영태, 이경률, 임강빈 외, “USB 키보드 후킹을 통한 데이터 탈취 가능성 진단”, 정보보호학회 충청지부학술대회 논문집, pp111-115, 2010년 10월

[17] 이경률, 임강빈 외, “터치패드 취약점을 통한 이미지 기반 패스워드의 보안 취약성 분

석", 정보보호학회 동계학술대회 논문집, pp.171-175, 2010년 12월
[18] 이경률, 임강빈 외, "코드 난독화를 위한 새로운 가상머신 모델 제안", 정보보호학회 동계학술대회 논문집, pp.176-181, 2010년 12월
[19] Kangbin Yim, "A fix to the HCI specification to evade ID and password exposure by USB sniff", KSII&CSU, Proceedings of APIC-IST 2008, pp.191-194, Dec. 2008
[20] Art Baker, Jerry Lozano, The Windows 2000 Device Driver Book, Prentice Hall, Nov. 2000
[21] Greg Hoglund, Jamie Butler, Rootkit, Addison-Wesley Professional, Jul. 2005
[22] 이경률, 임강빈 외, "분석기법 우회 악성코드 분석방법 연구", 한국인터넷진흥원 연구보고서, 2010년 11월
[23] 이경률, 임강빈 외, "터치 센서 모듈의 잡음 제거 연구", (주)포인칩스., 2010년 2월
[24] 이경률, 임강빈 외, "PALM Rejection 기능의 투과형 정전용량 터치스크린 개발", 나노티에스(주), 2011년 1월
[25] 이경률, 임강빈 외, "USB 키보드 후킹을 통한 키보드데이터 탈취 가능성 진단", 금융보안연구원 연구보고서, 2010년 5월
[26] 이경률, 임강빈 외, "프레임버퍼 수집을 통한 개인 스크린 정보 탈취 가능성 진단", 금융보안연구원 연구보고서, 2010년 5월

◐ 저 자 소 개 ◑

이 경 률

2008년 8월 순천향대학교 정보보호학과 졸업(학사)
2010년 8월 순천향대학교 대학원 정보보호학과 졸업(석사)
2010년 9월~현재 순천향대학교 대학원 정보보호학과 박사과정
2011년 5월~현재 (미)퍼듀대학교 정보보호교육연구센터 연구원
관심분야 : vulnerability analysis, virtualized obfuscation, system security, insider threats
E-mail : carpedm@sch.ac.kr

임 강 빈

1992년 2월 아주대학교 전자공학과 졸업(학사)
1994년 2월 아주대학교 대학원 전자공학과 졸업(석사)
2001년 2월 아주대학교 대학원 전자공학과 졸업(박사)
1999년 3월~2000년 2월 (미)아리조나주립대학교 연구원
2003년 3월~현재 순천향대학교 정보보호학과 교수
2005년 3월~현재 한국정보보호학회 이사
2009년 3월~현재 한국인터넷정보학회 이사
2010년 12월~현재 (미)퍼듀대학교 정보보호교육연구센터 객원교수
관심분야 : vulnerability analysis, insider threats, secure hardware architecture, homeland security
E-mail : yim@sch.ac.kr