情報保護學會論文誌
第 21 卷 第 3 號, 2011. 6

PS/2 키보드에서의 RESEND 명령을 이용한 패스워드 유출 취약점 분석

이 경 룰†, 임 강 빈‡
순천향대학교 정보보호학과

Analysis on a New Intrinsic Vulnerability to Keyboard Security

Kyung-roul Lee†, Kang-bin Yim‡
Dept. of Information Security Engineering, Soonchunhyang University

요 약

본 논문은 현재 컴퓨팅 플랫폼 상의 기본 입력장치인 PS/2 기반 키보드에서, 키보드 내부에 정의된 명령코드 중 RESEND 명령을 이용한 키보드 스캔코드의 수집 가능성을 제시하였다. 또한 제시한 방식을 활용한 키보드 감시 소프트웨어를 실제로 구현한 후 상용 보안 소프트웨어 환경에서 실험하여 사용자 인증 시에 패스워드가 유출될 수 있음을 확인함으로써 제시한 취약점의 위험성을 검증하였다. 이는 현재 플랫폼 상에 존재하는 하드웨어 취약점 중의 하나로써 설계 당시 하드웨어적인 보안 대책을 마련하지 않았기 때문에 발생하는 문제점이라 할 수 있어 해당 취약점을 해결하기 위해서 근본적으로 하드웨어적인 보안 대책이 필요할 것으로 사료된다.

ABSTRACT

This paper introduces a possibility for attackers to acquire the keyboard scan codes through using the RESEND command provided by the keyboard hardware itself, based on the PS/2 interface that is a dominant interface for input devices. Accordingly, a keyboard sniffing program using the introduced vulnerability is implemented to prove the severeness of the vulnerability, which shows that user passwords can be easily exposed. As one of the intrinsic vulnerabilities found on the existing platforms, for which there were little considerations on the security problems when they were designed, it is required to consider a hardware approach to countermeasure the introduced vulnerability.

Keywords: keyboard sniff, password authentication, hardware vulnerability, RESEND command

I. 서 론

온라인 금융거래 서비스와 전자상거래가 실생활에 널리 보급되면서 인터넷을 통한 재화의 이동이 증가하고 있다. 온라인으로 금융 결제 서비스를 이용할 경우 결제 당사자의 인증을 위해 기본적으로 아이디와 패스워드를 사용하며, 이들은 공히 키보드를 통하여 수집되는 문자열을 기반으로 구성된다. 인터넷을 통한 금융 거래 서비스에서는 높은 수준의 보안이 요구되므로 이를 위하여 사용자의 키보드로부터 입력되는 문자열을 안전하게 보호하기 위한 기술이 반드시 필요하다.

현재 이를 해결하기 위한 방안으로 많은 키보드 보안 프로그램이 널리 보급되어 있으나[1], USB 기반 키보드는 물론이고[2] PS/2 키보드와 관련된 하드웨어 또는 그 취약점에 직접 접근하는 악의적 소프트웨어에 의해 키보드 정보가 쉽게 유출될 수 있음이 제기되었다[3][4][5]. 이를 해결하기 위해 키보드 입력 정보에 잡음을 섞어 패스워드를 보호하는 기술이 개발

접수일(2010년 9월 4일) 재재확정일(2010년 12월 27일)
† 주저자, carpedm@sch.ac.kr
‡ 교신저자, yim@sch.ac.kr

되었으나[7][8] C/D 비트 취약점이 발견[6]되면서, 이들 기술이 무력화되었으며 해당 취약점에 대응하기 위하여 몇 가지 해결방안이 제시되었다. 이 중 대표적인 방안으로 키보드컨트롤러 내부 메모리를 활용한 방법이 있다[9]. 해당 대응방안은 잡음을 섞는 방법의 일종으로 C/D 비트 취약점을 효과적으로 해결하였다. 그러나 본 연구에서 제시하는 RESEND 명령 취약점을 활용하면 잡음을 섞는 방법을 이용하는 모든 대응방안이 무력화됨을 확인하였다.

본 논문의 구성은 다음과 같다. 제2장에서는 키보드 보안의 기존 기술들에 대해 분석하였으며, 제3장에서는 RESEND 명령 취약점을 이용한 스캔코드 감시 방안을 제시한다. 제4장에서는 실제 스캔코드 감시 결과를 보이며, 제5장에서는 현재 키보드 보안의 한계를 서술하고, 해결방안을 제시하는 것으로 결론을 내린다.

II. 키보드 보안의 기존 기술 분석

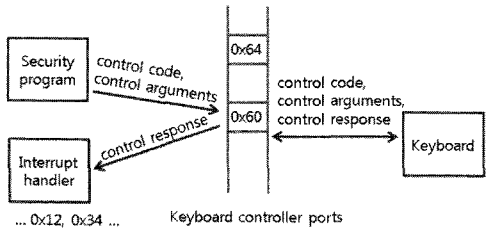
현재 사용자가 키보드를 이용하여 입력하는 정보를 보호하기 위해 키보드 보안 프로그램들이 대거 등장하였으나, 이를 무력화하여 스캔코드를 탈취하기 위한 공격 기술도 나날이 진화하고 있다. 유저모드 취약점을 이용한 방법에서부터 커널모드 취약점을 이용한 다양한 방법이 등장하였으며, 그 결과로 방어자와 공격자가 경쟁 상태에 이르게 되었다[10]. 하지만 이미 많은 연구에 의해 대부분의 공격기술을 무력화하기 위한 방안들이 제시되었으며, 최근 키보드컨트롤러 내의 제어코드를 활용하는 방안이 시도되어 보다 우수한 안전성을 확보하였다. 이 방안의 대표적인 것으로 0xD2 제어코드를 활용하여 무작위 시간에 무작위 스캔코드를 생성하여 공격자를 교란하는 방법이 있다. 하지만 이 방법에 의해 추가된 교란 스캔코드는 키보드컨트롤러가 가지는 C/D 비트 하드웨어 취약점으로 인해 쉽게 구분 가능하여 스캔코드가 노출되는 취약점을 가진다[6]. 키보드컨트롤러 내의 C/D 비트는 입력버퍼를 통해 전달되는 다양한 정보의 종류를 키보드컨트롤러가 구분할 수 있도록 하기 위하여 입력된 정보가 어느 포트를 통해 전달되는지를 알려준다. 따라서 0xD2 제어코드를 이용하여 스캔코드를 교란하는 동작은 C/D 비트의 변화를 유발하므로 이를 추적하면 교란 스캔코드를 제거할 수 있어 실제 키보드로부터 입력된 스캔코드가 노출되는 위험성을 가진다.

따라서 보다 높은 보안성을 지원하기 위하여 새로운 연구가 진행되었다. 상기 문제점은 C/D 비트가 폴링에지를 발생하기 때문에 나타나는 문제이므로 C/D 비트의 폴링에지를 발생시키지 않고 스캔코드를 교란시킬 수 있는 방법을 찾는다면 새로운 방안을 마련할 수 있다. 즉, 보안 프로그램 입장에서 C/D 비트의 폴링에지를 발생시키지 않으면서 교란코드와 실제코드를 구별할 수 있다면 새로운 감시 방지 대책을 마련할 수 있는 것이다. 제어코드 중에는 인자를 가지지 않으면서 응답을 만들어내는 코드들이 존재하는데 이를 활용하면 C/D 비트의 폴링에지를 발생시키지 않으면서 교란코드를 생성할 수 있다. 0xD2 제어코드를 이용하여 교란 스캔코드를 생성한 직후에 인자를 가지지 않는 제어코드를 수행하는 루틴을 임계영역으로 묶어 수행할 수 있다. 이러한 제어코드를 활용하는 방안은 감시 프로그램을 효과적으로 회피하기는 쉽지 않지만 복수의 제어코드를 연속적으로 활용한다면 C/D 비트의 폴링에지를 감추는 일이 가능해진다. 하지만 활용 가능한 제어코드가 제한적이기 때문에 교란코드와 실제코드를 분류할 수 있는 최소한의 정보를 제공할 수 있고, 운영체제가 제공하는 타임퀀텀에 대해 비교적 많은 시간을 수행하므로 시스템에 따라 과부하를 초래하는 경우가 발생한다.

이를 보완하기 위해 새로운 대응방안이 제시되었다. 키보드컨트롤러에는 현재 활용되지는 않으나 읽거나 쓰는 것이 가능한 내부메모리가 존재하는데[11], 내부 메모리를 읽을 경우에는 C/D 비트가 폴링에지를 발생하지 않기 때문에 임의의 메모리에 교란 스캔코드를 써 넣은 후 무작위로 내부메모리에 접근하여 이를 읽어낸다면 부하가 적으면서도 폴링에지를 발생시키지 않는 방안을 만들 수 있다. 내부메모리는 0x60~0x7f까지의 영역만 존재하기 때문에 이를 추적하면 노출될 가능성이 있어 별도의 처리기를 통해 내부메모리 값을 비주기적으로 변경하여 보다 안전성을 높일 수 있다.

III. 키보드 프로토콜에서의 RESEND 명령을 이용한 공격

현재 다수의 데스크탑 및 모든 노트북 PC 플랫폼이 사용하는 PS/2 기반의 키보드는 정확하게 AT 키보드라 불린다. AT 키보드는 과거 XT 키보드와는 달리 IBM의 PS/2 시스템에서 사용되는 키보드의 많은 특성을 계승하고 있다. 특히, 플랫폼과의 하드웨어 인터페이스 및 전송 프로토콜이 동일하다고 할 수 있으며, 양방향 전송 특성을 가지고 있어 키보드 스캔코드의



〔그림 1〕 AT 키보드 프로토콜

전송[13]뿐만 아니라 플랫폼으로부터의 요구 및 인자를 수신하고 응답하는 등의 역할을 수행할 수 있다. 기본적인 AT 키보드 프로토콜을 〔그림 1〕에 보인다.

AT 키보드는 〔표 1〕과 같이 플랫폼과의 상호작용을 위하여 프로토콜 내에 다양한 기능을 수행할 수 있는 명령코드를 정의하고 있는데, PC 플랫폼의 경우 AT 키보드로의 명령코드, 명령인자 및 명령응답의 전달을 위하여 입/출력 포트 0x60 번지를 활용하고 있다[14][15][16][17].

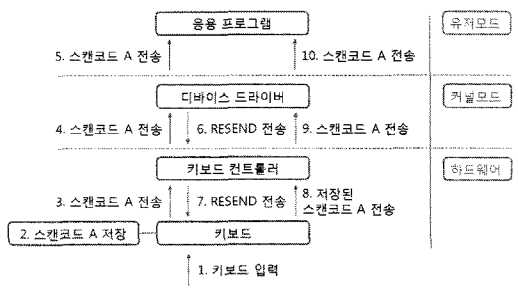
AT 키보드는 다양한 스캔코드 세트를 준비하여 이를 선택적으로 활용할 수 있도록 하거나 키보드의 키가 한계시간 이상 눌러졌을 경우 반복 스캔코드를 생성하는 시점 및 주기를 설정하는 등의 기능을 제공하며, 이를 위하여 키보드컨트롤러의 명령코드를 활용하고 있다. 특히, AT 키보드 명령코드 중에 RESEND (0xFE) 명령코드는 키보드에서 생성된 마지막 정보를 키보드컨트롤러로 재전송하는 역할을 하는데, 이는 원래 키보드의 간단한 동작 테스트나 키보드와 키보드 컨트롤러 사이의 통신 과정에서 오류가 발생하였을 경우를 대비한 것으로 키보드로부터 전송되는 스캔코드가 호스트에 정의되어 있지 않거나 전송 시 오류에 의하여 잘못된 스캔코드 및 정보를 수신하였을 경우 재전송을 요구함으로써 오류에 의한 손상된 정보를 복구하는 데 사용된다.

〔표 1〕 키보드컨트롤러의 주요 명령코드

명령 코드(HEX)	종류	인자 유무	응답 유무
0xF5	Disable	X	X
0xEE	Echo	X	0xEE
0xF4	Enable	X	0xFA(ACK)
0xF7~ 0xFD	Set Key Type Make	X	0xFA(ACK)
0xEF~ 0xF2	Read ID	X	0xAB, 0x83
0xFF	Reset	X	0xFA(ACK)
0xF6	Set Default	X	X
0xF3	Set Typematic Rate/Delay	O	
0xFA	Set All Keys Typemetic/Make/Break	X	0xFA (ACK)
0xAA	AT Completion Code	X	
0xF0	Set Scan Code	O	0xFA (ACK)
0xFE	Resend	X	마지막 전송 값 (스캔코드 등)

상기의 RESEND 명령코드는 매우 유용한 코드로 생각되지만 현재의 PC 플랫폼에서 실행되는 소프트웨어에서는 거의 사용되지 않으며 오히려 키보드 감시 소프트웨어에 의하여 악용되면 매우 치명적인 도구가 될 수 있다. 즉, 제2장에서 서술한 키보드 입력정보를 보호하기 위하여 마련된 공격자를 교란시키기 위한 모든 방안은 RESEND 명령코드를 이용하면 그 효과를 상실한다. 이는 호스트에 의하여 생성된 교란 스캔코드와는 무관하게 키보드로부터 최종 입력된 스캔코드가 RESEND 명령에 의해 재전송되므로 공격자가 실제 입력한 스캔코드만을 분류할 수 있기 때문이다.

공격자가 RESEND 명령을 이용하여 스캔코드를 탈취하는 과정에 대해 자세히 서술하면 다음과 같다. 악의적인 프로그램은 스캔코드가 전송되었음을 알려주는 Output Buffer Full(OBF)을 주기적으로 감시하여 OBF가 설정됨과 동시에 스캔코드를 취득하고, 키보드에 RESEND 명령코드(0xFE)를 전송하여 사용자가 입력한 실제 스캔코드의 재전송을 요구한다. 이후 OBF의 발생으로 수집한 스캔코드와 RESEND 명령을 이용하여 재전송된 스캔코드를 비교함으로써 방어자가 임의로 생성한 스캔코드를 걸러내고 키보드에서 생성된 실제 키보드의 스캔코드를 취득할 수 있다. 〔그림 2〕는 RESEND 명령을 이용할 경우



〔그림 2〕 RESEND 명령에 따른 동작과정

의 동작과정에 대해 나타내었다.

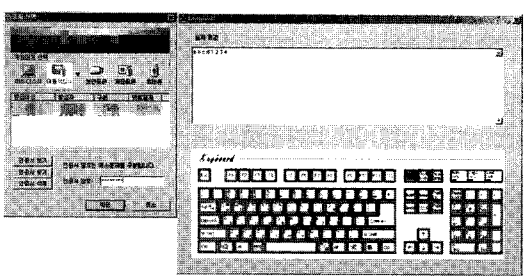
키보드에서 입력되는 문자열에는 동일한 문자가 연속으로 위치하는 경우가 있다. 이러한 문자열에서는 재전송을 요구할 경우 새로운 문자인지 기존의 문자인지 구분할 수가 없다. 그러므로 정확한 스캔코드 수집을 위하여 키보드에 저장되어 있는 마지막 스캔코드를 활용한 후 제거할 필요가 있다. 따라서 감시 프로그램은 〔표 1〕에 나타난 제어코드를 이용하여 저장된 스캔코드를 갱신함으로써 연속으로 입력하는 스캔코드에 대해서도 분류가 가능하도록 하였다.

IV. 실험결과

본 논문에서는 제3장에 기술한 바와 같이 키보드 프로토콜 상의 RESEND 명령을 이용한 실제의 감시 프로그램을 구성하고 그 결과를 분석하였다. 상기의 취약점을 이용하여 구현된 감시 프로그램은 현재 서비스 중인 모든 키보드 보안 프로그램을 무력화시킬 수 있으며, 사용자가 입력하는 모든 키보드 정보를 감시하고, 수집할 수 있다. 구현된 감시 프로그램의 결과는 〔그림 3〕, 〔표 2〕와 같다. 프로그램의 세부사항은 그 특성상 본 논문에서 생략하기로 한다. 실험은 Intel Core2 Quad 2.33GHz CPU와 4GB 메모리를 가진 PC 환경에서 수행되었으며, 스캔코드 수집을 위한 디바이스 드라이버와 이를 출력하기 위한 응용 프로그램으로 구성되었다.

V. 결 론

본 논문은 기존의 PS/2 기반의 키보드 공격 및 보안 기술들에 대해 소개하고, 키보드 프로토콜 내에 정의된 RESEND 명령코드를 이용한 취약점과 공격 가능성에 대해 분석하였다. 분석된 내용을 토대로 사용자가 입력한 패스워드를 탈취할 수 있는 악의적인 감



〔그림 3〕 감시 프로그램 실행 결과

〔표 2〕 감시 구간에서의 스캔코드 노출 결과

감시 구간	방어 방법	스캔코드 노출결과
윈도우 메시지 후킹	유저모드 프로그램에서의 윈도우 메시지를 보안 소프트웨어가 후킹	O
필터 드라이버 삽입	키보드 드라이버에 필터 드라이버를 삽입하여 스캔코드 선점	O
인터럽트 객체 대체	키보드를 누를 때 발생하는 인터럽트를 처리하는 객체를 대체하여 스캔코드 선점	O
인터럽트 벡터 테이블 대체	키보드를 누를 때 발생하는 인터럽트를 처리하는 벡터 테이블을 대체하여 스캔코드 선점	O
임의의 스캔코드 발생 (0xD2)	키보드를 누르는 것과 관계없이 임의의 스캔코드를 발생시킴으로써 공격자에게 사용자가 입력한 스캔코드를 숨김	O
임의의 스캔코드 발생 (내부 메모리)	키보드를 누르는 것과 관계없이 임의의 스캔코드를 발생시킴으로써 공격자에게 사용자가 입력한 스캔코드를 숨기며 C/D 비트의 폴링에지를 발생시키지 않음	O

시 프로그램의 예를 구성하였으며, 이를 실제로 구현하여 대개의 사이트에서 실험함으로써 공격 가능성을 확인하였다. 본 논문의 실험결과, 키보드 입력정보를 보호하기 위하여 현재 사용 중인 키보드 보안 프로그램 및 해당 보안 기술들이 본 논문에서 제시한 취약점을 전혀 방어하지 못하는 것으로 나타났다. 상기의 취약점은 모든 키보드 입력정보를 감시하고 수집하기에 충분한 심각성을 가지고 있으며 이를 해결하지 못할 경우 모든 인증 응용에서 사용자가 입력하는 패스워드를 안전하게 전달할 수 없다.

상기의 취약점은 현재 PC 플랫폼과 키보드 하드웨어 상에 존재하는 것으로서 근본적으로 하드웨어 자체가 보안 기능을 지원하지 않는 한 현재의 구조에서 소프트웨어적으로 대응하기에는 다소 무리가 있는 것으로 판단된다. 물론, 키보드 하드웨어 자체만이 아니라 운영체제가 제공하는 접근 권한이나 트랩, 디버깅 등을 이용하여 존재하는 모든 프로세스에 대한 추적이 가능하다. 하지만 현재의 상용 운영체제가 커널/유저의 2등급 특권수준을 제공하고 있기 때문에 결국 보안 소프트웨어와 감시 프로그램의 선점문제를 야기한다. 이는 시스템의 안전성을 추구해야 하는 보안 소프트웨

어의 특성 상 공격 프로그램이 우월한 위치에 있기 때문에 소프트웨어적으로 보안 채널을 구성한다는 것은 어려운 문제이므로 이를 해결하기 위하여 커널 드라이버 인증기능의 강화와 더불어 하드웨어를 이용하는 방안도 연구되어야 할 것으로 사료된다.

참고문헌

[1] 최성욱, 김기태, "안전하고 신뢰성 있는 전자상거래를 위한 키보드 입력 보안시스템의 설계 및 구현," 한국정보처리학회 논문지, 13-C(1), pp. 55-62, 2006년 2월.

[2] Kangbin Yim, "A fix to the HCI specification to evade ID and password exposure by USB sniff," Proceedings of the APIC-IST 2008, pp. 191-194, Dec. 2008.

[3] Linda D. Paulsoin, "Key snooping technology causes controversy," IEEE Computer, pp. 27, Mar. 2002.

[4] Kyungroul Lee, Kwangjin Bae, and Kangbin Yim, "Hardware approach to solving password exposure problem through keyboard sniff," Proceedings of the ACADEMIC SCIENCE RESEARCH (WASET), pp. 23-25, Oct. 2009.

[5] 임강빈, "키보드 보안," 2008년도 한국정보보호학회 유비쿼터스 정보보호워크샵, pp.13-25, 2008년 5월.

[6] 배광진, 임강빈, "키보드 보안의 근본적인 취약점 분석," 한국정보보호학회 논문지, 18(3), pp. 89-95, 2008년 6월.

[7] Kangbin Yim, "A new noise mingling approach to protect the authentication password," IEEE CICIS 2010 Conference, pp. 839-842, Feb. 2010.

[8] 태커스(주), "가상 데이터 전송을 이용한 키보드 해킹 방지 장치 및 방법," 대한민국특허청, 등록번호:10-0735727, 2007년 6월.

[9] 정태영, 임강빈, "키보드컨트롤러의 하드웨어 취약점에 대한 대응 방안," 한국정보보호학회 논문지, 18(4), pp. 187-194, 2008년 8월.

[10] Daniel G. Treat, "Keyboard encryption outlining ways to pad yourself with protection," IEEE Prtential, pp. 40-42, Aug. 2002.

[11] "PS/2 model 50 and 60 technical reference," IBM Corporation, Chap.4, pp. 7-18, Apr. 1987.

[12] 배광진, 이경률, 임강빈, "디버그 트랩 기반 접근 감시 기술의 취약성 분석," 2009년도 한국정보보호학회 하계학술대회, 19(1), pp. 64-68, 2009년 6월.

[13] "Enhanced super I/O controller with keyboard/mouse wake-up," Standard Microsystems Corporation, pp. 119-130, Mar. 2000.

[14] Tom Shanley, "ISA system architecture," Mindshare Press, pp. 407-414, 1993.

[15] Michael Tischer, "PC intern: system programming," Abacus, pp. 292, 1995.

[16] Frank V.Gilluwe, "The undocumented PC," Addison Wesley, pp. 261, 1994.

[17] Sanchez, IBM PC/AT technical reference, IBM Corporation, 1985.

〈著者紹介〉

이 경 룰 (Kyungroul Lee) 학생회원
2008년 8월: 순천향대학교 정보보호학과 공학사
2010년 8월: 순천향대학교 정보보호학과 공학석사
2010년 9월~현재: 순천향대학교 정보보호학과 박사과정
2011년 5월~현재: (미)퍼듀대학교 정보보호교육연구센터 연구원
〈관심분야〉 vulnerability analysis, obfuscation, system security, insider threats

임 강 빈 (Kangbin Yim) 종신회원
1992년 2월: 아주대학교 전자공학과 공학사
1994년 2월: 아주대학교 전자공학과 공학석사
2001년 2월: 아주대학교 전자공학과 공학박사
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〉 insider threats, security assurance, vulnerability analysis, malware analysis, virtualized obfuscation, secure hardware architecture, homeland security