은닉된 모듈식 하드웨어 키로거 탐지 방안

박 재 곤*, 강 성 문**, 고 승 철***

요 약

최근 하드웨어 키로거는 키보드 내부에 설치할 수 있는 작은 크기와 Wi-Fi 기능을 내장하고 있는 다양한 모듈식 키로거 제품들이 유통되고 있다. 이러한 키로거는 제3자에 의해서 악의적인 목적으로 사용될 경우 탐지가 어려워 정부와 군, 기업과 개인의 중요정보와 민감정보가 유출될 가능성이 높지만, 소프트웨어 키로거와 달리 대응 보안 솔루션과 탐지 방법에 대한 연구가 미흡한 실정이다. 따라서 본 논문에서는 하드웨어 키로거에 의한 보안 취약점과 기존 연구된 탐지 방법들을 살펴보고 키보드의 소비전력, 적외선 온도, X-RAY, 무게, 전자파 등의 비파괴 측정 방법을 통해 모듈식 하드웨어 키로거의 탐지 가능성을 향상 시킬 수 있는 방법을 실험 결과와 함께 제안한다.

Concealed Modular Hardware Keylogger Detection Methods

Jae-kon Park*, Sung-moon Kang**, Sung-cheol Goh***

ABSTRACT

Hardware Keyloggers are available in a variety of modular keylogger products with small size and Wi-Fi communication capabilities that can be concealed inside the keyboard. Such keyloggers are more likely to leak important information and sensitive information from government, military, business and individuals because they are difficult to detect if they are used by a third party for malicious purposes. However, unlike software keyloggers, research on security solutions and detection methods are relatively small in number. This paper, we investigate security vulnerability caused by hardware keylogger and existing detection methods, and improve the detection possibility of modular hardware keylogger through non-destructive measurement methods, such as power consumption of keyboard, infrared temperature, and X-ray. Furthenmore, We propose a method that can be done with experimental results.

Key words : Hardware Keylogger Detection, Hardware Keylogger, HKL

접수일(2018년 10월 1일), 수정일(1차: 2018년 10월 23일),
게재확정일(2018년 10월 30일)

* 국방보안연구소, 수원대학교/컴퓨터학과
** 국방보안연구소
*** 수원대학교/정보보호학과

1. 서 론

하드웨어 키로거(Hardware Keylogger, 이하 HKL)는 키보드와 컴퓨터 본체사이에 설치된 하드웨어 회로에 의해 모든 Keystroke 수집하는 장치이다. 자체적으로 내부 메모리를 가지고 있고 미리 정의 된 일련의 문자키를 입력하여 숨겨진 메모리에 액세스해 기록된 키로그들을 확인할 수 있다. 일반적으로 PS2 또는 USB 방식 키보드 내부나 외부 케이블에 설치된다[1][2].

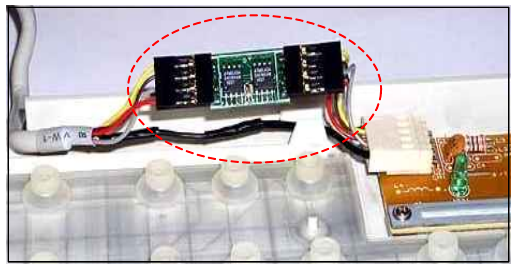
최근 인터넷을 통해 유통되는 HKL의 종류를 보면 <표 1>과 같이 수집된 키로그를 Wi-Fi를 통해 지정된 사용자에게 무선으로 송신하거나 키보드 케이스를 열고 내부에 모듈형태로 삽입할 수 있는 제품도 판매되고 있다[3][4][5].

<표 1> 상용 HKL 제품

형 태	제 원
	【Gender Type】[3] o 방식 : PS/2, USB o 용량 : 2GB o 전원 : 4.5V-5.5V DC o 전력 : 65mA(0.33W) o 가격 : $59.99~$69.99
	【Wi-Fi Gender Type】[4] o 방식 : PS/2, USB o 용량 : 4GB o 전원 : 4.5V-5.5V DC o 전력 : 220mA(1.1W) o 가격 : $139.99~$144.99
	【Module Type】[5] o 방식 : PS/2, USB o 용량 : 16MB~2GB o 전원 : 4.5V-5.5V DC o 전력 : 65mA(0.33W) o 가격 : $36.99~$56.99

이러한 모듈식 HKL은 악의적인 목적으로 사용자 몰래 키보드 내부에 설치될 경우에는 육안으로도 식별이 어려워 정부와 군, 기업과 개인의 각종 기밀정보나 민감정보가 제3자에게 유출될 가능성이 매우 높다.

실제로 2012년 미국 로스앤젤레스(LA) 지역의 고등학교 학생 3명이 교사들이 사용하는 컴퓨터에 HKL를 설치한 후 아이디와 패스워드를 빼내, 성적을 조작하고 컴퓨터에 저장된 시험 문제까지 유출해 같은 학교 학생들에게도 판매한 사실이 드러난바 있는데[6], HKL을 판매하고 구매하는 행위 자체가 불법이 아니기 때문에 누구나 쉽게 구할 수 있고, 인터넷을 통해 HKL의 설계도면, 소스코드, 제작 방법 등이 공개되어 있어 원하는 형태나 기능을 포함해 자체제작도 가능하다[7].



(그림 1) 모듈식 HKL 설치 사진[5]

이와 같이, HKL은 (그림 1)과 같이 키보드와 컴퓨터 사이의 물리적인 위치에 설치되어 입력되는 모든 키로그를 저장할 수 있고, 전문지식이 없는 사람도 쉽게 구해 설치와 사용이 가능지만, 은닉된 HKL을 발견하는 것은 쉽지 않아 보안상 매우 취약하다.

이를 해결하기 위한 유일한 방법은 키로거를 찾아내 제거하는 방법이지만 현재, 소프트웨어 키로거와 달리 HKL에 대한 대응 보안 솔루션과 탐지 방법에 대한 연구가 미흡해 유용하고 효율적인 다양한 탐지기법에 대한 새로운 연구가 필요하다.

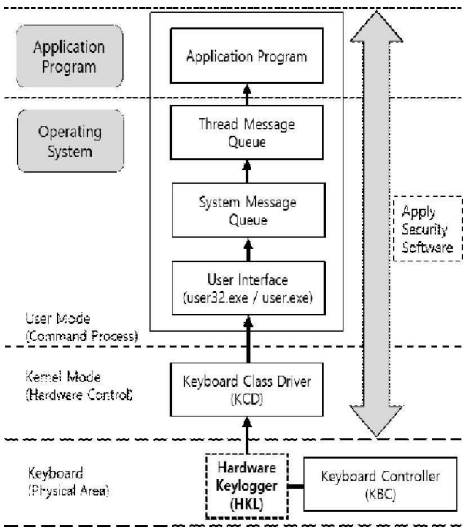
따라서, 본 논문에서는 HKL의 보안취약요인과 기존 국내외 탐지방법 연구사례를 살펴보고 추가적으로 HKL의 전기 및 물리적 특성을 이용하여 키보드의 소비전력, 적외선온도, X-RAY, 무게, 전자파 등을 측정해 모듈식 HKL을 효율적으로 탐지할 수 있는 다양한 방안을 제시 한다. 또한 제시한 방안들에 대한 실제 실험결과를 포함해 효과를 증명 하였다.

2. 관련 연구

2.1 HKL에 의한 보안 취약점

HKL은 대부분의 다른 컴퓨터 디바이스와는 달리 별도의 추가 드라이버나 프로그램 설치 없이도 동작이 가능하기 때문에 컴퓨터의 운영체제 없이 키보드에 전원이 공급되기만 하면 키로그 수집을 시작한다. 즉, Operating system booting 이전에도 입력되는 모든 키로그를 수집할 수 있는데, 컴퓨터 사용을 위한 첫 번째 접근통제 수단인 Power on Password나 CMOS BIOS Password까지도 제한 없이 모든 영역의 키로그 기록이 가능하기 때문에 유출될 경우 시스템의 Supervisor 권한 탈취는 물론 키보드로 입력한 모든 키스트로크의 수집이 가능하다.

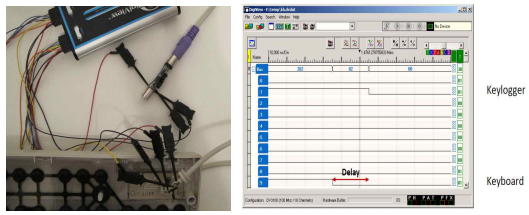
또한 HKL은 (그림 2)와 같이 키보드 컨트롤러(KBC)를 포함하고 있는 물리적 영역의 키보드 내부에 위치하고 있어 소프트웨어 보안 솔루션들의 적용을 받지 않고 사용이 가능하다[8][9]. 따라서 HKL를 탐지하거나 키스트로크 암호화 기술을 적용하는데 제한이 되기 때문에 별도의 탐지 및 보안대책이 필요하다.



(그림 2) 키스트로커 입력 과정과 HKL 설치 위치

2.2 기존 HKL 탐지 방법 조사

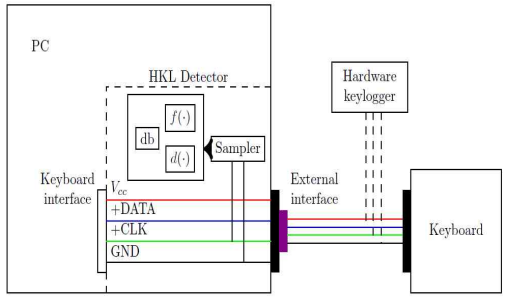
2010년 HACK.LU에서 Fabian Mihailowitsch은 (그림 3)처럼 HKL이 설치된 키보드와 설치되지 않은 키보드의 Clock Signal을 Logic Analyzer 장치로 수집해 Clock의 Delay를 비교하는 것으로 HKL을 탐지하는 방안을 발표했다[10]. 하지만 Clock Signal의 Delay만으로 HKL 특정하기 어려운 한계가 있고 키보드 케이스를 열거나 Probe에 케이블을 연결해야 하는 불편함이 있다.



Clock Signal 수집 Delay 비교 화면

(그림 3) Clock Signal HKL 탐지

2014년 미국 유타주립대 Saptarshi Mallick은 자신의 논문 'Physical-Layer Detection Methodology'에서 HKL이 부착된 시스템의 필연적인 전기적 특성을 이용한 탐지 방안을 제시하였다. 이 방안은 Kirchhoff's law을 적용한 전류와 전압의 관계를 이용해 HKL이 시스템의 전압을 떨어트린다는 이론을 기반으로 (그림 4)와 같이 HKL Detector Architecture를 제안했지만 전기적인 특성만으로 HKL을 특정하기 어렵고, 키보드의 Clock을 수집해야하는 장치를 개발해야하는 한계가 있다[11].



(그림 4) HKL Detector Architecture

3. HKL 탐지 방법 제안

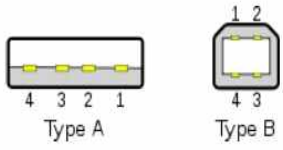
본 장에서는 2장에서 조사한 Clock signal과 Kirchhoff's law를 이용한 탐지 방법 보다 빠르고 효율적으로 HKL을 탐지하기 위해 키보드의 소비전력, 표면온도, X-Ray, 무게, 전자파를 이용한 방법을 제안한다.

3.1 키보드 소비전력 측정

모든 HKL는 (그림 1)과 같이 전자부품과 회로로 구성되어 있다. 따라서 직류회로나 교류회로에 전압을 가하게 되면 부하(load)에서 전기가 소비된다. 이때 전기 에너지는 전력(electric power)이라고 하고, 전력(P)은 전기기기에 사용되는 단위시간당 에너지로 전압(V)과 전류(I)의 곱으로 P=VI로 표현되고 단위는 와트(W)이다[12].

즉, 전력을 사용하는 기본 회로에 반도체나 저항 등을 포함하고 있는 HKL 회로 K가 추가되면, 전류의 양이 증가하므로 P=V×(I+K)에 따라 전력량도 함께 상승하게 된다. 이를 통해 키보드가 최대 소비전력을 상회하거나 초과한 측정값이 나올 경우 키보드가 불량이 아니라면 기본 기능 외에 또 다른 동작을 하는 회로가 추가 되어 있을 가능성이 높다고 가정할 수 있다.

따라서, HKL이 설치되지 않은 키보드 전력과 키로거가 설치된 키보드의 전력차를 비교함으로써 키보드 케이스를 개봉하지 않고 HKL 삽입여부를 의심해 볼 수 있다.

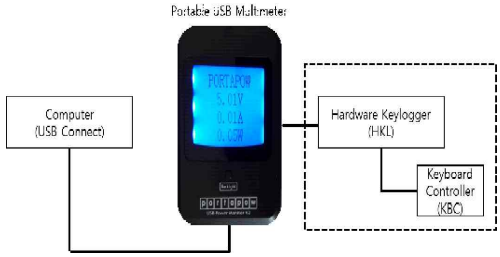


USB 1.x/2.0 standard A/B

Pin	Name	Color	Description
1	VCC	Red	+5 V
2	D-	White	Data -
3	D+	Green	Data +
4	GND	Black	Ground

(그림 5) 표준 USB 케이블 구조

전력측정 방법은 (그림 5)와 같이 USB 키보드 컨넥터의 전력을 공급하는 1번과 4번 라인을 계측기 Probe를 통해 측정하거나, (그림 6)처럼 USB 키보드의 경우에는 Portable USB Multimeter를 이용해 오실로스코프나 멀티 테스터기 같은 비교적 고가의 전문 전력계측기를 대신해 빠르고 편리하게 측정이 가능하다.



(그림 6) USB 키보드 소비전력측정 방법

그러나 전력량 차이만으로 은닉된 장치가 반드시 HKL이라고 단정할 수 없기 때문에 이를 응용해 키보드 제조사의 모델별로 제공하고 있는 소비전력 제원과 각종 HKL의 소비전력을 Database로 만들어 자동 비교할 수 있는 프로그램을 구현함으로써 HKL의 탐지 가능성을 높이는데 응용이 가능하겠다.

3.2 키보드 표면온도 열화상 측정

일반적으로 전자부품이 소비하는 전력량과 온도는 정비례 관계에 있기 때문에 HKL이 설치된 키보드에 전원이 공급되면 동일한 키보드의 제품이라고 해도 특정부분의 표면온도에 차이가 발생하게 된다.

이러한 특성을 이용해 미세한 온도의 차이까지 컬러로 구분해 디스플레이해 주는 적외선 열화상카메라로 키보드를 촬영하면 특정 회로가 삽입되었거나 불량인 키보드의 경우 해당 부분의 표면에 비정상적으로 높은 온도가 표시되는 것을 확인할 수 있으며, 이 경우 HKL의 삽입 가능성을 의심해 볼 수 있다. 이 방법은 휴대형 열화상카메라를 이용해 한 번에 다수의 키보드를 실시간 검사할 수 있는 장점이 있다.

3.3 키보드 X-RAY 검사

대부분 플라스틱 재질로 만들어진 키보드의 경우 X선 투과가 가능해 HKL 탐지에 활용이 가능하다.

이 방법은 X-RAY 검색 시스템을 보유하고 상시 운용하는 곳에서 적용할 수 있다. 검색요원이 키보드 내부의 고유 전자회로와 HKL을 육안으로만 식별하기 어려울 수 있지만, 형태와 밀도를 자동 검출하는 기능을 이용하면 탐지 가능성을 높일 수 있다. 또한 반출입 물품에 대한 보안 규정을 강화해 모바일 통신기기, 저장매체 같은 제품처럼 직원과 유지보수 인력의 일반 키보드에 대해서도 반입반출 시 검색을 강화해야 하겠다.

3.4 키보드 무게 정밀 측정

HKL 제품이 대부분 소형화되어 있지만 무게는 반드시 존재한다. 따라서 측정대상이 되는 키보드의 제원상 무게나 물리적인 무결성이 검증된 키보드의 무게를 기준으로 하고 동일 모델 키보드의 무게를 디지털 저울로 정밀 측정해 오차범위를 초과하는 경우 HKL 삽입여부를 의심해 보아야 한다.

3.5 키보드 전자파 측정

전자전기 제품 주위에는 전기장과 자기장의 흐름에서 발생하는 전자기 에너지인 전자파가 반드시 발생한다. 따라서 전자파의 세기의 차이는 있지만 키보드와 HKL 모두 전원이 공급되면 전자파를 발산하게 되는데, 전자파의 세기는 발생원점과의 거리가 가까울수록 강해지기 때문에 전자파 측정기로 키보드 전자파를 측정해 비정상적으로 높은 전자파가 측정되면 HKL의 삽입 여부를 의심해 볼 필요가 있다.

4. 실험 결과

앞서 제안한 HKL 탐지 방안의 효과를 분석하기 위해 동일한 USB 방식 키보드 2대 중 한 대에 KeeLog社의 USB 모듈형 HKL인 'KeyGrabber USB Module 8GB' 삽입하고 키보드의 소비전력, 표면온도, X-RAY, 무게, 전자파를 측정한 실험결과이다.

4.1 키보드 소비전력 측정 결과

Portable USB Multimeter를 이용해 USB 키보드의 소비전력을 측정한 결과이다. (그림 7)과 같이 평상시 HKL이 삽입되지 않은 키보드는 0W, HKL이 삽입된 키보드는 0.15W로 측정되었다.

A: HKL 미삽입 키보드 B: HKL 삽입 키보드

(그림 7) USB 키보드 소비전력측정 결과

4.2 키보드 표면온도 열화상 측정 결과

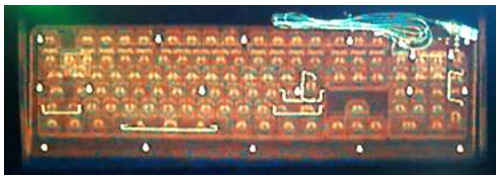
열화상카메라를 이용해 HKL이 설치된 키보드에 전원을 공급하고 5분이 경과된 시점에 측정한 결과이다. (그림 8)과 같이 HKL이 설치된 부분에 집중적으로 밝게 표시되고 최고온도는 22.4℃로 측정되었다. HKL 설치 부분과 이격된 부분의 최저온도는 17.3℃로 최대 약 5.1℃의 차이를 보였다.

(그림 8) 키보드 표면온도 열화상 측정 결과

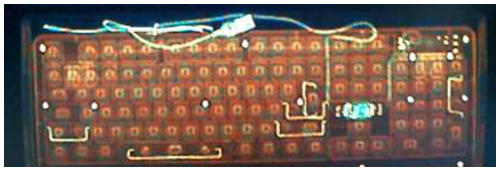
4.3 키보드 X-RAY 검사 결과

X-RAY 보안검색대에 키보드를 통과 시켜 촬영한 결과이다. (그림 9)와 같이 HKL 삽입 키보드 사진에서 키보드 컨트롤러와 연결된 모듈형 H

KL의 형상이 방향키 부분의 빈공간에서 보이는 것을 볼 수 있다.



A: HKL 미삽입 키보드



B: HKL 삽입 키보드

(그림 9) 키보드 X-RAY 검사 결과

4.4 키보드 무게 정밀 측정 결과

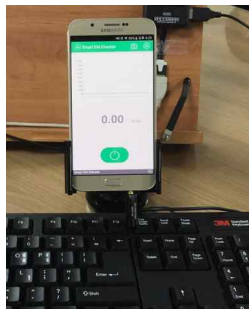
디지털 저울을 이용해 키보드의 무게를 측정한 결과이다. (그림 10)과 같이 HKL이 삽입된 키보드의 무게가 HKL이 없는 키보드보다 17.62g 더 무거운 것을 확인할 수 있다.

A: HKL 미삽입 키보드 B: HKL 삽입 키보드

(그림 10) 키보드 무게 측정 결과

4.5 키보드 전자파 측정 결과

스마트폰에 전자파 측정 센서를 연결하고 키보드의 전자파를 측정한 결과이다. (그림 11)과 같이 HKL이 설치된 부분에서 전자파 수치가 올라가는 것을 볼 수 있다.



A: HKL 미삽입 키보드 B: HKL 삽입 키보드

(그림 11) 키보드 전자파 측정

5. 결 론

앞서 살펴본 내용과 같이 HKL은 소프트웨어 기반의 보안 솔루션을 통해 탐지와 대응이 어려운 물리적 영역에서 동작한다. 때문에 현재 원치 않는 HKL의 설치여부를 컴퓨터 사용자가 알 수 있는 방법은 육안으로 확인할 수밖에 없다. 하지만, 키보드 속에 은닉할 수 있는 모듈 타입의 HKL은 육안으로도 확인이 어렵기 때문에 불법적으로 정보를 수집하고 이용하는데 악용될 경우 보안상 취약할 수밖에 없다.

본 논문에서 HKL 탐지 방법인 키보드의 소비전력, 적외선온도, X-RAY, 무게, 전자파 측정 등의 탐지 방법이 은닉된 HKL을 100% 특정하지는 못하겠지만 제시한 방법들을 상호 보완한다면 탐지 성공 확률을 반드시 높일 수 있을 것이다. 또한 기존 연구된 Clock Signal, 전류와 전압 등 전기적 특성들을 이용한 방법과 논문에서 제시한 방안들을 융합해 보다 편리하고 높은 확률로 HKL을 탐지할 수 있는 연구가 향후 필요하겠다. 끝으로 이 논문의 결과가 정부와 군, 기업의 보안담당자와 개인 사용자의 보안 인식제고와 유사연구에 활용되기를 기대한다.

참고문헌

[1] 최인영, '키로거에 의한 정보유출 실시간 탐지 및 키로거 탐지 솔루션 설계 및 구현', p.9, 영산대학교, 2015

[2] Wikipedia, 'Hardware keylogger', https://en.wikipedia.

org/wiki/Hardware_keylogger (accessed August 5, 2018).
[3] KeeLog, 'User's Guide KeyGrabber TimeKeeper', https://www.keelog.com/files/KeyGrabberTimeKeeperUsersGuide.pd f(accessed August 5, 2018).
[4] KeeLog, 'User's Guide, KeyGrabber Wi-Fi Premium', https://www.keelog.com/files/KeyGrabberWiFiPremiumUsersGuide.pdf (accessed August 5, 2018).
[5] KeeLog, 'User's Guide, KeyGrabber Module', https://www.keelog.com/files/KeyGrabberModuleUsersGuide.pdf, (accessed August 5, 2018)
[6] khoon@yna.co.kr, "미 한인 고교생, 학교 컴퓨터 해킹해 성적 조작", 연합뉴스, 2012.1.29.
[7] KeeLog, 'Wireless Keylogger - Do It Yourself', http://www.keelog.com/wireless_keylogger.html (accessed May 5, 2018)
[8] 강신범, 정현철, "인터넷 뱅킹 해킹 유형과 대응기술", 한국정보보호학회, 정보보호학회지, 제15권, 제4호, pp. 28-37, 2005
[9] 금융ISA, '키보드 해킹기법 및 대응기술 분석', p.5, Korea Financial Information Sharing& Analysis Center, 2005.11.
[10] Fabian Mihailowitsch, "Detecting Hardware Keyloggers", HACK.LU 2010, October 28, 2010
[11] Saptarshi Mallick, "Physical Layer Detection of Hardware Keyloggers", Utah State University, 2014
[12] 두산백과, http://terms.naver.com/entry.nhn?docId=1261879&cid=40942&categoryId=32240 (accessed May 13, 2018)

〔저 자 소 개〕

박 재 곤 (Jae-kon Park)
2007년 8월 서울사이버대학교
컴퓨터공학과 학사
2009년 8월 아주대학교
정보통신공학과 석사
2016년 3월~현재 수원대학교
컴퓨터학과 박사과정
2015년 1월~현재 국방보안연구소
email : topsafe@naver.com

강 성 문 (Sung-moon Kang)
1985년 2월 한남대학교
전자계산학과 학사
1990년 8월 성균관대학교
컴퓨터감사학과 석사
2008년 8월 고려대학교
정보보호대학원 박사
2018년 5월~현재 국방보안연구소
email : smkang111@korea.com

고 승 철 (Sung-cheol Goh)
1981년 2월 연세대학교 수학과 학사
1983년 2월 연세대학교 수학과 석사
1992년 8월 포항공과대학교
수학과 박사
2011년 9월~현재 수원대학교
정보보호학과 교수
email : goh5703@hanmail.net