한국항행학회 논문지 제15권 제3호 2011년 6월

개인 영상 및 음성 정보의 임의수집에 대한 대응방안

A Countermeasure to the Stealth Sniff of the Private Media Information

이경률*, 임강빈*

Kyung-Roul Lee*, Kang-Bin Yim*

요 약

본 논문은 개인용 컴퓨터에서 발생할 수 있는 프라이버시 영상 및 음성 정보 수집의 기술적 문제를 지적하고 이에 대응하기 위한 방안을 제시한다. 개인용 컴퓨터와 노트북의 사용이 보편화되면서 주변 기기들의 보급 또한 늘어나고 있으며 특히 카메라와 마이크의 경우 개인 프라이버시에 대한 침해가 일어날 수 있어 각별한 주의가 필요하다. 현재 카메라의 경우 사용 여부를 표시하기 위해 점멸등이 장착되어 있으나 그렇지 않은 경우가 대부분이며, 마이크의 경우에는 사용 여부를 표시하기 위한 수단이 전혀 준비되어 있지 않다. 이러한 허점은 장치 사용에는 아무런 문제가 되지 않으나, 사용자가 인지하지 못하는 시점에 악의적인 공격자에 의해 장치가 동작하여 영상이나 음성 같은 정보가 노출되어 개인 프라이버시의 침해를 일으킬 수 있다. 따라서 본 논문은 이를 대응하기 위하여 개인용 컴퓨터에 연결된 카메라와 마이크에 대한 접근을 시도하는 경우 이를 감지하여 사용자에게 통보하기 위한 방안을 제시하고 실제의 도청감시 소프트웨어 및 대응 소프트웨어를 구현하여 실험하였다. 제안한 방안을 실제 환경에 적용하면 프라이버시 노출문제를 효과적으로 해결할 수 있을 것으로 사료된다.

Abstract

This paper introduces technical aspects of the privacy exposure problem of the video and the audio information on the personal computer and proposes a countermeasure to them. According to the increased number of peripherals for computers, especially including the cameras and the mikes, it is required to be careful on the privacy exposure. Currently, some incorporated or standalone cameras have a pilot lamp to indicate their usage. However, many other cameras and all mikes have not equipped with the pilot lamp or other dedicated indicator. Even though this problem doesn't obstruct their assigned functionalities, it should make the devices susceptible to be exposed with the information they are gathering without any notice to the owners. As a countermeasure to the problem, this paper proposes a reasonable solution that alarms the access trials to the devices and implements programs for the practical sniffing and its counterpart.

Key words : USB Camera, MIC, Privacy Threats

I. 서 론

개인용 컴퓨터의 보편화와 네트워크의 발전으로

* 순천향대학교 정보보호학과(Department of Information Security Engineering, Soonchunhyang University)
· 제1저자 (First Author) : 이경률 · 교신저자 (Corresponding Author) : 임강빈
· 투고일자 : 2011년 4월 27일
· 심사(수정)일자 : 2011년 4월 28일 (수정일자 : 2011년 6월 22일)
· 게재일자 : 2011년 6월 30일

인해 인터넷을 이용하는 사용자가 증가하였고, 사용자의 편의를 위한 주변 기기들도 다양하게 개발되고 있다. 하지만 급격한 발전으로 인해 보안은 고려되지 못하였고, 그에 따른 문제들이 일어나고 있다. 최근 인터넷 상에서의 프라이버시 침해 문제가 이슈가 되고 있으며, 이러한 문제들은 주변 기기들과 맞물려 현실화되고 있다[1]-[12]. 특히, 카메라와 마이크의 경우 인터넷을 통한 화상회의, 화상채팅, 화상통화 등의 서비스 이용이 보편화됨에 따라 보급률과 사용률이 증가하고 있어 그에 따른 보안 경각심이 요구된다.

카메라와 마이크를 통하여 생성된 영상과 음성 데이터는 많은 프라이버시 정보들을 포함하고 있기 때문에 영상의 유출이나 도청을 통하여 심각한 프라이버시 침해가 발생할 수 있어 보다 각별한 관심과 안전한 보안대책이 필요하다. 하지만 일부 카메라의 경우를 제외하고 일반적으로 카메라와 마이크가 작동중일 경우 해당 사용자에게 장치의 작동 여부를 인지시킬 수 있는 방안이 마련되어 있지 않다. 이는 컴퓨터 사용자가 인지하지 못하는 사이에 자신의 영상과 음성이 외부로 유출될 수 있음을 의미한다[13]. 보편적으로 사용되고 있는 카메라 및 마이크는 노트북에 장착되어 생산되는 내장형 카메라와 마이크, 외부에서 USB 형태로 연결되는 외장 카메라 및 마이크, 플러그인 형태로 컴퓨터와 연결되는 마이크 등의 형태를 이루고 있다. 본 논문에서는 상기와 같은 카메라와 마이크를 대상으로 장치가 동작 중일 경우 이를 감지하여 사용자가 인지할 수 있는 방안에 대해 제시하고자 한다.

본 논문의 구성은 다음과 같다. 제2장에서는 프라이버시 정보 및 침해 현황에 대해서 서술하고, 제3장에서 카메라 및 마이크의 동작 감지 과정을 기술하며, 제4장에서 구현된 감지 소프트웨어를 통한 감지 결과를 나타내고, 제5장에서 결론을 맺는다.

Ⅱ. 프라이버시 정보 및 침해현황

프라이버시 정보란 “생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)”를 말한다[13][14].

PC용 카메라의 등장으로 카메라가 일반화됨에 따라 영상과 음성, 텍스트를 이용한 통신이 증가하고 있으며, 화상통신이 일반화되고 보편화되면서 이와 비례하게 증가한 것이 개인의 사생활 침해와 보호에 대한 관심이다[15]. 특히 개인정보보호기본법에서는 영상을 통하여 개인정보를 수집, 처리하는 경우 정보주체가 이를 알 수 있도록 엄격하게 규정하고 있다[13][16]. 영상과 음성 정보 내에는 개인의 중요한 프라이버시 정보들뿐만 아니라 개인을 포함한 외부의 공동 공간에 대한 프라이버시 정보들이 포함될 수 있기 때문에 각별한 보안이 필요하다. 이러한 카메라에 의한 프라이버시 침해 사건의 일례로 democracynow.org의 2010년 2월 25일 기사를 통해 알려진 미국의 고등학교에서 발생한 사건을 들 수 있다. 교육 당국이 학생들에게 교육용으로 나눠준 노트북에 부착되어 있던 웹캠이 감시카메라 역할을 하고 있던 것으로 밝혀지면서 문제가 된 것인데, 이 사건은 학교 당국이 불법으로 학생을 감시했다는 문제점과 함께 학생뿐만 아니라 학생의 가정과 가족이 감시대상이 될 수 있었다는 문제점을 포함하기 때문에 미국에서 상당히 충격적인 사건으로 보도되었다.

일례에서도 볼 수 있듯이 사용자의 카메라와 마이크에 대한 보안 의식이 부재하고, 대개의 제품에서 카메라와 마이크의 작동 여부 표시를 하지 않는 등 생산하는 시점부터 보안에 대하여 소홀함을 알 수 있다. 즉, 현재 임의의 공격자는 영상 및 음성 정보의 수집 사실을 고의로 사용자가 인지할 수 없도록 함으로써 사용자의 프라이버시를 침해할 수 있으며, 개인 컴퓨터의 경우 정보들의 획득이 더 쉬울 것으로 보인다. 개인 컴퓨터의 경우 개인 공간에서 정보를 생성하는 상황이 많아 프라이버시 정보의 비중이 높기 때문에 그 피해는 더 심각할 것으로 사료된다.

Ⅲ. 프라이버시 정보 및 침해현황

개인용 컴퓨터와 노트북에서 사용되는 카메라와 마이크는 각각의 장치로 컴퓨터에 인식되어 작동하기 때문에 윈도우 내의 드라이버를 이용하여 데이터가 이동하게 된다. 따라서 드라이버를 통하여 이동하는 데이터를 감시하여 카메라와 마이크의 작동 여부를 감지할 수 있다. 본 논문에서 구현한 카메라 및 마이크의 감지 소프트웨어는 기본적으로 커널모드의 디바이스 드라이버, 디바이스 드라이버와 통신하는 유저모드의 알림 소프트웨어의 구조를 가지고 있으며, 드라이버에서 장치 사용 시도를 감지할 경우 유저모드의 알림 소프트웨어와 통신하여 사용자가 인식할 수 있도록 알려주고 있다.

디바이스 드라이버에서 카메라와 마이크의 작동 여부를 감지해 내기 위한 방법으로는 필터 드라이버를 삽입하는 방식, 드라이버의 majorFunction을 후킹하는 방식, 드라이버 내의 특정 함수를 인라인 후킹하는 방식 등이 가능하다. 본 논문에서는 카메라를 감지하는 방법으로 majorFunction을 후킹하는 방식을 사용하였으며 마이크를 감지하는 방법으로 인라인 후킹 방식을 사용하였다. MajorFunction 후킹이란 드라이버의 majorFunction에 등록되는 dispatch routine을 후킹하여 자신의 함수가 먼저 호출되도록 하는 방식으로, 이 후킹 드라이버를 통해 카메라의 작동 여부를 감시하게 된다. 그림 1은 디바이스 스택상에서의 후킹 드라이버의 위치를 보인다.

커널 드라이버 내에서 특정 장치의 사용 여부를 확인하는 방법은 많이 있을 수 있으나 USB 카메라와 내장 카메라 모두 USB 데이터로 전송하기 때문에 본 논문에서는 카메라 장치로부터 전송되는 데이터의 크기를 확인함으로써 사용 여부를 판단하였다.

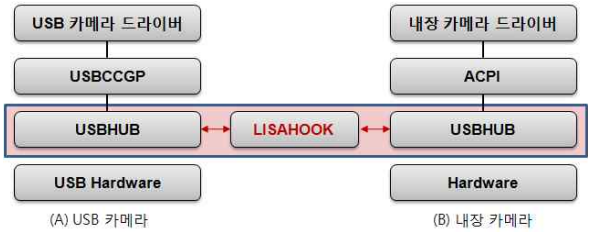


그림 1. 카메라의 디바이스 스택구조 및 후킹 드라이버의 위치
Fig. 1. Location of the hooking driver within the driver stack for the camera device

전송크기에 대한 정보는 실제의 영상 정보와 함께 IRP(I/O Request Packet)를 통하여 전달된다. IRP는 클라이언트의 요구를 통해 생성되어 전달되며 이 IRP는 디바이스 스택 상에서 가장 하위의 드라이버까지 순서대로 전달된 후 다시 상위의 드라이버로 전달된다.

본 논문은 커널 드라이버들이 다른 드라이버와의 통신을 위해 사용하는 internal dispatch routine(IRP_MJ_INTERNAL_DEVICE_CONTROL)을 후킹하였다. 후킹 드라이버를 통하여 USB HUB 드라이버로 전달되는 USB 데이터를 얻기 위해 IOCTL 코드 값이 IOCTL_INTERNAL_USB_SUBMIT_URB인 IRP에 대해서만 처리하여 필터링하였으며, 카메라와 마이크 데이터는 USB 전송의 경우 ISOCRONOUS 전송을 하기 때문에 후킹된 함수로 넘겨진 IRP 내의 정보를 이용하여 구한 URB 구조체에서 _URB_HEADER 구조체의 Function 필드를 검사하여

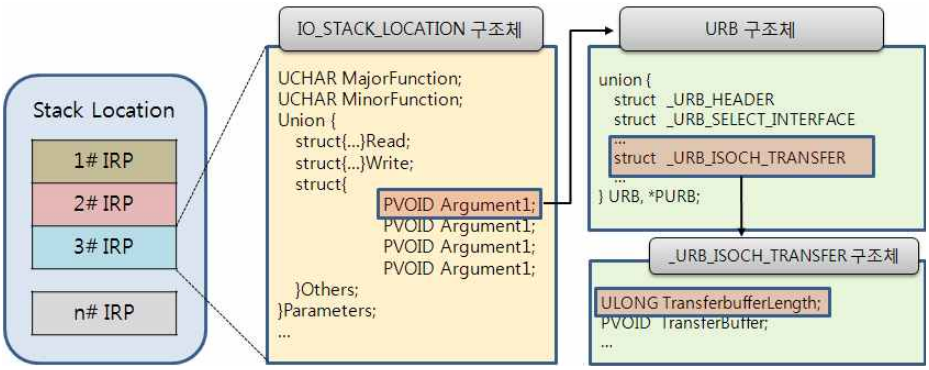


그림 2. USB 데이터 전송 IRP 내 데이터 크기 필드(TransferbufferLength) 위치
Fig. 2. Location of the data length field(TransferbufferLength) in an IRP of the USB bulk transfer

#	Time	Debug Print
2419	61.86135864	len : 6
2420	61.87137985	len : 6
2421	61.88280106	len : 6
2422	61.89185715	len : 6
2423	61.90145493	len : 6
2424	61.91151047	len : 6
2425	61.92111206	len : 6
2426	61.93091965	len : 6
2427	61.94125748	len : 6
2428	61.95020676	len : 6
2429	62.21474838	len : 6
2430	62.21486282	len : 4
2431	62.28806686	len : 6
2432	62.28815460	len : 4

(A) 기본상태

#	Time	Debug Print
6117	134.40069580	len : 96832
6118	134.40864563	len : 112640
6119	134.41679382	len : 109056
6120	134.42466736	len : 111616
6121	134.43263245	len : 96832
6122	134.44068909	len : 112640
6123	134.44865417	len : 109056
6124	134.45668030	len : 111616
6125	134.46472168	len : 96832
6126	134.46667480	len : 21
6127	134.47430420	len : 112640
6128	134.48103333	len : 109056
6129	134.48869324	len : 111616
6130	134.49681091	len : 103488

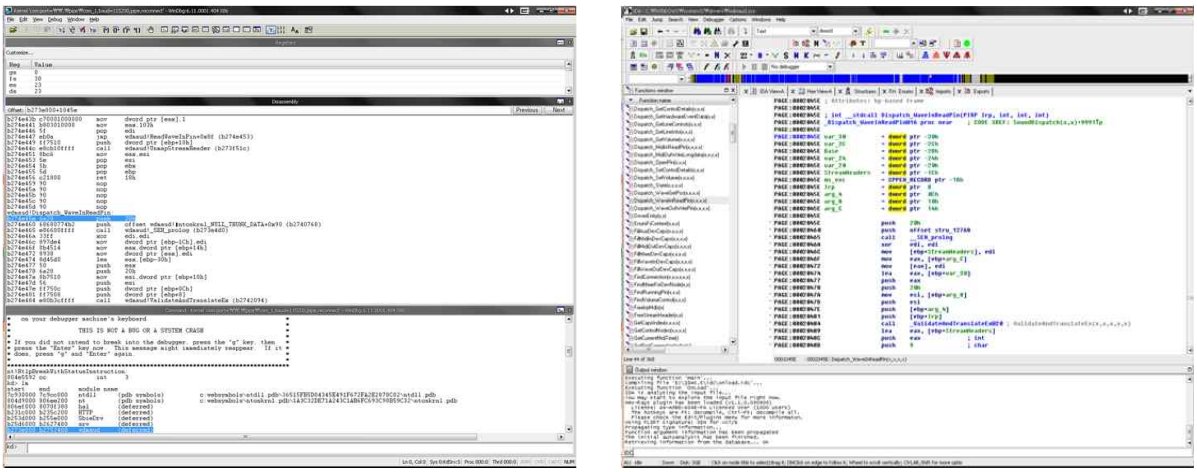
(B) USB 카메라 실행 후

#	Time	Debug Print
5942	32.19141388	len : 31
5943	32.19163513	len : 512
5944	32.20054245	len : 393216
5945	32.21649933	len : 393216
5946	32.23274994	len : 393216
5947	32.24874115	len : 393216
5948	32.26474762	len : 393216
5949	32.28077698	len : 393216
5950	32.29179764	len : 6
5951	32.29671860	len : 393216
5952	32.30800247	len : 6
5953	32.31291199	len : 393216
5954	32.31323242	len : 31
5955	32.31340790	len : 512

(C) 내장 카메라 실행 후

그림 3. 데이터 크기 추출 결과

Fig. 3. Extraction of the data length



(A) WinDbg (B) IDApro

그림 4. WinDbg와 IDA를 이용한 Dispatch_WaveInReadPin() 함수 확인

Fig. 4. Dispatch_WaveInReadPin() function exposed by debuggers

URB_FUNCTION_ISOCH_TRANSFER 값을 가지는지 확인한다. 이후 URB 구조체 내의 _URB_ISOCH_TRANSFER 구조체를 통해 USB 데이터의 크기를 구하며 이를 그림 2에 나타내었다.

결과적으로 TransferbufferLength 필드를 통하여 USB 데이터의 크기를 구할 수 있으며, USB 카메라와 내장 카메라의 작동 과정에서 얻어지는 필드의 값을 확인하면 특정 범위를 가지는 데이터의 크기를 구할 수 있다. 전송되는 데이터의 크기를 추출한 결과에 대해 그림 3에 나타내었다. 따라서 본 논문에서는 그림 3에서의 결과를 분석하여 카메라가 동작 중일 경우의 최소값과 최대값의 평균을 산출하였으며, 그 결과 카메라의 경우 60000 ~ 400000 범위이며, 이를 활용하여 필터링한 결과 USB 카메라 및 내장 카메라의 동작 여부를 감지할 수 있었다.

USB 마이크의 경우도 마찬가지로 특정 범위의 값을 얻을 수 있었으나, 노트북에 포함된 내장 마이크와 플러그인 형태의 마이크의 경우 디바이스 스택의 차이로 인하여 USB HUB 드라이버의 majorFunction 후킹 방식으로는 감지할 수 없었다. 따라서 마이크 장치의 감지를 위해서 인라인 후킹 방식을 사용하였다. 인라인 후킹이란 마이크 및 오디오와 관련된 드라이버인 wdmaud 드라이버를 코드 패치하여 wdmaud 드라이버 내에서 호출되는 함수 대신 구현된 드라이버 내의 함수가 호출되도록 하는 방식이다. 이러한 작업을 수행하기 위해 먼저 wdmaud 드라이버 내에서 마이크를 사용하는 소프트웨어가 동작할 경우 호출되는 함수를 조사하여야 하며, WinDbg를 통해 Dispatch_WaveInReadPin() 함수가 연속적으로 호출되는 것을 확인하였다. 그림 4는 WinDbg와 IDA

를 이용하여 Dispatch_WaveInReadPin() 함수를 확인한 결과이다. 코드패치 동작과정을 그림 5에 나타내었으며 구현된 드라이버의 동작과정은 다음과 같다.

Step 1. Dispatch_WaveInReadPin() 함수를 통해 wdmaud 드라이버가 로딩된 메모리 내의 BaseAddress를 확인한다.

Step 2. CheckFunction() 함수에서 wdmaud 드라이버 내의 Dispatch_WaveInReadPin() 함수의 주소 값을 확인한다.

Step 3. Hook() 함수에서 Dispatch_WaveInReadPin() 함수의 처음 5바이트 값을 메모리에 복사한 후 FAR JMP 코드로 패치한다.

Step 4. HookHandler() 함수에서 마이크 플래그를 설정하고 패치하였던 원래의 5바이트 인라인 어셈코드를 실행시키고 패치된 바로 다음주소 즉, 6번째 바이트로 점프한다.

Step 5. 이후 Dispatch_WaveInReadPin() 함수가 호출될 때마다 HookHandler() 함수가 호출되어 장치의 작동여부를 감시한다.

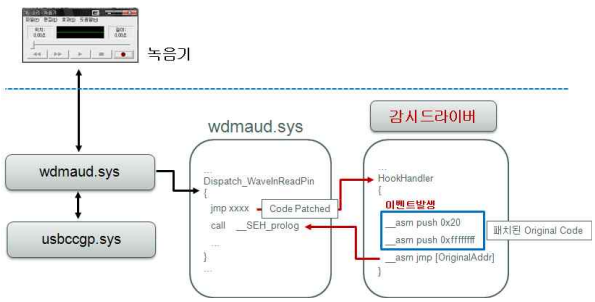


그림 5. 코드패치 동작과정
Fig. 5. Process of the code patch

상기와 같이 인라인 후킹 방법으로 커널모드에서 특정 드라이버를 감시함으로써 장치가 작동 중일 경우 계속적인 이벤트를 발생시켜 유저모드의 감시 소프트웨어는 이벤트를 감지하게 되며, 결과적으로 사용자가 장치의 작동 여부를 확인할 수 있는 정보가 된다. 그림 6은 구현된 커널모드의 디바이스 드라이버와 감시 소프트웨어가 이벤트를 통하여 통신하는 방법을 보인다.

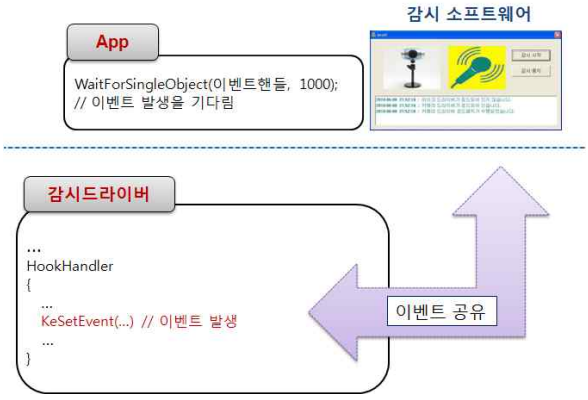


그림 6. 드라이버와 감시 소프트웨어의 통신방법
Fig. 6. Communication between the driver and the secure monitoring software

Ⅳ. 실험결과

본 논문에서 테스트를 위해 사용된 프로그램으로는 윈도우 기본 프로그램인 녹음기, 상용 메신저의 화상채팅, 테스트용으로 제작된 영상 및 음성 출력용 데모 프로그램, 카메라 제조회사에서 제공되는 전용 프로그램을 사용하였다. 개발 환경은 Microsoft Windows XP SP3이며, Microsoft Visual Studio 2005, Windows Driver Kit을 사용하여 구현하였다. 표 1은 각 테스트 프로그램에 대한 카메라와 마이크의 작동여부 감지 결과를 보인다.

표 1. 작동여부 감지 결과
Table 1. Results of the activity detection

소프트웨어 종류 / 카메라 종류	녹음기	화상 채팅	데모 프로그램	전용 프로그램
USB 외장형 마이크	○	○	○	○
내장 마이크	○	○	○	○
플러그인 마이크	○	○	○	○
USB 외장형 카메라	N/A	○	○	○
내장 카메라	N/A	○	○	○

구현된 드라이버와 응용 소프트웨어를 테스트한 결과 카메라와 마이크에 대해서 작동 여부 감지가 가능하였다. 그림 7로부터 그림 12까지는 카메라 및 마이크의 작동 감지 상태 화면을 나타내었다. 카메라와 마이크가 동작 중일 경우에는 빨간 바탕으로 표시되어 사용자에게 사용 중임을 알려줌으로써 외부에 의해 임의로 영상이나 음성 정보가 수집되는 것을 방지할 수 있다.

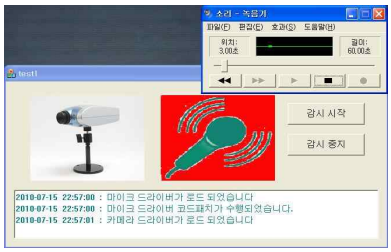


그림 7. 녹음기 실행 후
Fig. 7. Test result on Recorder

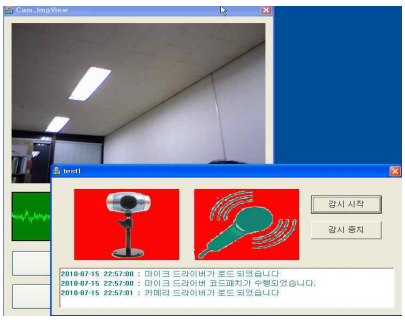


그림 8. 데모 프로그램 실행 후(카메라, 마이크)
Fig. 8. Test result on the demo program

그림 9. 상용 메신저 화상채팅 전
Fig. 9. Test result of video chatting on a commercial messenger program

그림 10. 상용 메신저 화상채팅 후
Fig. 10. Test result of video chatting on commercial messenger program

그림 11. 카메라 제조사 전용 프로그램 실행 후
Fig. 11. Test result of capturing on a private program supported camera manufacturer

그림 12. 카메라 제조사 전용 프로그램 녹화 후
Fig. 12. Test result of recording on a private program supported camera manufacturer

Ⅴ. 결론 및 향후과제

본 논문은 개인용 컴퓨터에서 사용되고 있는 카메라와 마이크가 사용자에게 장치의 작동여부를 알리지 못하고 있는 실정에 대해 문제점을 지적하였고, 이와 같은 문제점으로 인하여 프라이버시가 쉽게 노출될 수 있으므로 그 대응방안에 대해 제안하였다. 제안한 결과를 실제 구현을 통해 검증하였으며, 장치가 사용 중일 경우 사용자에게 감지한 결과를 알림으로써 프라이버시 노출을 방지할 수 있었다.

그러나 공격자가 특정 하드웨어에 직접 접근하는 등 본 논문에서 접근하고 있는 커널모드의 디바이스 드라이버보다 더 낮은 레벨에서 접근한다면 영상과 음성 정보의 수집이 가능할 것으로 보이며, 이를 해결하기 위해서는 그보다 더 낮은 레벨에서의 대응방안이 필요할 것으로 사료된다.

일례로 각 장치마다 알림 소리 또는 표시등이 하드웨어적으로 장착되어 소프트웨어적으로는 분리제어가 불가능하도록 함으로써 사용자가 언제라도 장치의 작동 여부를 인지할 수 있도록 한다거나 장치의 정보수집 과정에 추가의 알고리즘을 도입하여 잡음을 섞고 빼는 등의 처리를 하는 기능을 기본으로 가지는 하드웨어적 대응방안에 대한 향후 연구가 진행되어야 할 것으로 사료된다.

일부의 사양이 상호 다르긴 하나 현재 일반 PC 대응 카메라 및 노트북 컴퓨터에 장착된 카메라의 경우 USB 인터페이스를 통하여 연결되는 UVC (USB Video Class) 사양을 따르고 있으며 이 사양에는 카메라 동작 여부 확인을 위한 표시등의 소프트웨어 제어 기능이 포함되지 않으므로 카메라로의 접근이 발견되는 경우 하드웨어 수준에서 표시등을 점등하도록 구성하는 것이 이미 가능하다. 그럼에도 불구하고 대개의 노트북 컴퓨터들이 단가 절약을 위하여 표시등을 장착하지 않고 있어 이에 대한 정책적 지원이 필요할 것으로 사료된다.

특히, 마이크의 경우 기반 하드웨어는 PCI 기반 사운드카드나 USB AUDIO 기반 사운드카드로 구분이 되나 이들은 현재까지 공히 사용자 접근에 대한 알림 기능을 가지고 있지 못한 상태여서 공무 수행이나 기밀 업무에 활용되는 컴퓨터마저도 공공연한 도청에 대한 우려가 매우 크다. 따라서 사운드카드의 경우에도 마이크 입력에 대한 사용자 접근이 발견되면 소프트웨어와 무관하게 표시등을 자동 점등하는 등의 대책이 필요하다.

참 고 문 헌

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

[2] 정태영, 임강빈, "키보드컨트롤러의 하드웨어 취약점에 대한 대응방안," 정보보호학회논문지, 18(4), pp. 187-194, 2008년 8월.

[3] 정태영, 임강빈, "키보드해킹에 대비한 새로운 영상기반 패스워드," *정보보호학회학회지*, 18(3), pp. 41-47, 2008년 6월.

[4] 이경률, 배광진, 임강빈, "USB 데이터 보안 취약성 분석," *정보보호학회하계학술대회논문집*, 19(1), pp. 59-63, 2009년 10월.

[5] 이경률, 임강빈, "PS/2 키보드에서의 RESEND 명령을 이용한 패스워드 유출 취약점 분석," *정보보호학회논문지*, 21(3), pp. 3-8, 2011년 6월.

[6] 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.

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

[8] Kyungroul Lee, Kwangjin Bae, and Kangbin Yim, "Hardware Approach to Solving Password Exposure Proboem through Keyboard Sniff," *ACADEMIC SCIENCE RESEARCH, WASET*, pp. 23-25, Oct. 2009.

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

[10] 정태영, 이경률, 배광진, 임강빈, "스니핑 방지를 위한 키보드 프로토콜," *정보보호학회하계학술대회논문집*, 18(1), pp. 375-379, 2008년 6월.

[11] 최영태, 이경률, 육형준, 김완수, 임강빈, "USB 키보드 후킹을 통한 데이터 탈취 가능성 진단," *정보보호학회충청지부학술대회논문집,* pp. 25-30, 2010년 10월.
[12] Kyungroul Lee, Wansoo Kim, Kwangjin Bae, and Kangbin Yim, "A Solution to Protecting USB Keyboard Data," *Proceedings of BWCCA 2010,* pp. 108-111, Nov. 2010.
[13] 김완수, 이경률, 배광진, 임강빈, "영상 및 음성정보의 임의 수집을 통한 프라이버시 침해," *정보보호학회충청지부학술대회논문집,* pp. 109-115, 2009년 10월.
[14] 박훤일, "개인정보에 대한 시장의 역할과 국제동향," *정보통신산업협회 정보화사회,* 2001년 7/8월.
[15] 배건태, 곽수영, 배혜란, "화상 통신에서의 사생활 보호를 위한 실시간 전경 분리 및 배경 대체," *통신학회논문지,* 34(5), pp. 505-513, 2009년 5월.
[16] 박성수, "유비쿼터스와 치안서비스," *정보화정책,* 12(4), pp. 42-56, 2005년.

이 경 률 (李庚栗)

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 (任綱彬)

1992년 2월: 아주대학교 전자공학과 (공학사)
1994년 2월: 아주대학교 전자공학과 (공학석사)
2001년 2월: 아주대학교 전자공학과 (공학박사)
1999년 3월~2000년 2월: (미)아리조나 주립대학교 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, security assurance, secure hardware architecture, malware analysis, virtualized obfuscation, homeland security