Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.4, Aug. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.4.871

안드로이드 스마트폰을 이용한 2.4 GHz 무선 키보드 원격제어 공격 시스템 구축*

이 수 진,[1†] 박 애 선,[1] 심 보 연,[1] 김 상 수,[2] 오 승 섭,[2] 한 동 국[1‡]
[1]국민대학교, [2]LIG넥스원

Building of Remote Control Attack System for 2.4 GHz Wireless Keyboard Using an Android Smart Phone*

Su-Jin Lee,[1†] Aesun Park,[1] Bo-Yeon Sim,[1] Sang-su Kim,[2] Seung-Sup Oh,[2]
Dong-Guk Han[1‡]
[1]Kookmin University, [2]LIGnex1

요 약

PC의 입력 장치인 키보드 중 RF 신호를 이용한 무선 키보드의 사용은 꾸준히 증가하고 있다. 특히 2.4 GHz 대역을 사용하는 무선 키보드는 현재 가장 많이 사용되고 있으며 이에 대한 취약점이 2010년부터 보고되고 있다. 본 논문은 기존 연구되어진 마이크로소프트 2.4 GHz 무선 키보드 취약점을 기반으로 안드로이드 스마트폰을 이용한 2.4 GHz 무선 키보드 키 스트로크 분석 및 주입 기능을 모두 갖춘 원격 제어 시스템을 제안하고, 제안된 시스템을 이용해 실제 2.4 GHz 무선 키보드를 사용하는 사용자의 민감한 정보의 노출 위험성을 실험을 통해 보인다.

ABSTRACT

It has been steadily increasing to use a wireless keyboard via Radio Frequency which is the input device. Especially, wireless keyboards that use 2.4 GHz frequency band are the most common items and their vulnerabilities have been reported since 2010. In this paper, we propose a 2.4 GHz wireless keyboard keystroke analysis and injection system based on the existing vulnerability researches of the Microsoft 2.4 GHz wireless keyboards. This system is possible to control on the remote. We also show that, via experiments using our proposed system, sensitive information of user can be revealed in the real world when using a 2.4 GHz wireless keyboard.

Keywords: 2.4 GHz wireless keyboard Vulnerability, keystroke sniffing, keystroke injection, Electromagnetic

I. 서 론

전자기기의 사용 및 연결을 위해 유선 매체를 이용 했던 과거와는 달리, 최근에는 편의성, 휴대성 및 확장성 등의 이유로 무선 통신 기술이 급격히 발전함에 따라 무선 전자기기는 실생활에서 유용하게 사용되고 있다. 이러한 무선 통신 기술의 발달과 무선 전자기기의 사용 증가로 인해 무선 통신 환경에서의 정보보안은 더욱 더 이슈화 되고 있다. 또한 개인용 컴퓨터 및 그 주변기기로부터 뜻하지 않게 누설되는 미약한 전자파를 제3자가 수신하여 개인 정보를 빼내는 문제, 즉, 전자파 보안 문제도 중요한 이슈이다.

키보드는 전통적으로 사용되고 있는 대표적인 PC 입력 장치로 사용자가 입력하는 값을 컴퓨터 내부로 전달하는 기능을 갖는다. 이러한 키보드는 연결 방식을 기준으로 유선 키보드와 무선 키보드로 나눌 수

Received(06. 13. 2016), Accepted(07. 15. 2016)
* 본 연구는 2015년도 LIG넥스원의 연구비 지원으로 수행하였습니다.
† 주저자, leesuj28@kookmin.ac.kr
‡ 교신저자, christa@kookmin.ac.kr(Corresponding author)

있으며, 무선 키보드는 다시 적외선, 블루투스, 무선 주파수를 이용한 방식으로 나눌 수 있다.

그중 현재 널리 사용되고 있는 무선 주파수 통신 키보드의 물리적 취약점에 대한 다양한 연구들이 보고되고 있다[1~6,8,9]. 특히, 사용자가 27MHz 무선 주파수 통신 키보드를 사용할 때, GNU Radio[1]와 USRP(Universal Software Radio Peripheral)[2]를 이용해 각각의 글쇠에 따라 키보드에서 발생되는 고유한 전자파를 측정하여 입력된 글쇠 정보들을 획득하거나 임의의 글쇠 정보를 주입 시킬 수 있음이 발표되었다[1,2]. 또한 현재 많이 사용되고 있는 2.4 GHz 대역 무선 키보드의 취약성 연구가 2010년부터 진행되어 왔으며[3~6], 특히, KeySweeper는 2015년에 nRF24L01+와 아두이노 보드를 이용하여 원거리에서 마이크로소프트 2.4 GHz 무선 키보드 글쇠 분석이 가능한 공격 장비를 구축하였다[4]. 뿐만 아니라 USB 수신기의 취약점을 이용해 무선 마우스만 사용하고 있어도 키보드 신호를 사용자의 컴퓨터에 주입시키는 공격도 발표되는 등 무선 키보드 취약성에 대해 많은 연구가 이루어지고 있다[5]. 이 때, 글쇠 분석은 무선 키보드 통신 주파수 신호를 분석하여 사용자가 누른 글쇠 정보를 찾아내는 공격 방법이다. 글쇠 주입은 공격자가 임의의 글쇠에 대한 키보드 통신 주파수 신호를 구성하여 사용자 PC에 연결되어 있는 무선 키보드 리시버에 전송, 리시버가 이를 정상 사용자의 키보드가 보낸 것으로 인식하도록 하는 공격 방법이다.

기존 누설 전자파 분석 장비는 복잡하거나 고가의 장비였던 것과 달리, 최근에는 USRP처럼 상대적으로 저렴한 장비와 오픈소스를 이용한 무선 키보드 전자파 신호 분석이 가능해졌다. 또한 아두이노, nRF24L01+ 칩 등 누구나 사용가능하며 저렴한 장비들이 나날이 발달하고 있어 이를 이용한 무선 키보드 취약점 분석 시스템이 보고되고 있다[4]. 이렇게 분석에 필요한 하드웨어 및 안테나 등 분석 장비의 발달은 공격 장비의 소형화, 원거리 분석/주입 장비 구성 등을 보다 쉽게 만든다.

특히 마이크로소프트 2.4 GHz 무선 키보드의 취약성 연구는 2010년 KeyKeriki v2.0 프로젝트[3]가 발표된 이후 2011년 Travis에 의해 2개의 모듈을 사용하던 기존 방법과 달리 하나의 모듈을 이용한 분석 장비가 제안되었다[6]. 그러나 이 장비들은 모두 공격자가 항상 공격 장비 근처에 있어야 한다는 단점이 존재한다. 이러한 단점을 보완하기 위해 KeySweeper는 아두이노 보드와 GSM 통신 모듈이 장착된 보드를 이용하여, 공격자가 공격 장비 근처에 없어도 키보드의 글쇠 분석이 가능하도록 하였다[4]. 그러나 KeySweeper는 글쇠 주입 시스템을 구성하지 않았고, GSM 통신이 가능한 환경에서만 원거리 공격이 가능하다는 제약이 존재한다.

이러한 단점을 극복하기 위해 본 논문은 안드로이드 스마트폰을 이용하여 원거리에서 키보드 글쇠 분석과 주입이 모두 가능한 공격 시스템을 제안한다. 기존 글쇠 주입 공격과 달리 본 논문의 공격 시스템은 원거리 글쇠 주입이 가능한, 즉, 공격자가 공격 장비와 떨어져 있는 곳에서도 글쇠 주입이 가능한 시스템이다. 또한, 안드로이드 스마트폰의 무선랜, LTE 모듈을 이용함으로써 공격 적용 가능 범위를 넓혔다. 즉, GSM 모듈을 사용하지 않는 국내·외 환경에서도 공격이 가능하도록 구성하였다.

더불어 본 시스템을 이용해 2.4 GHz 무선 키보드 사용자가 금융서비스를 이용할 경우, 로그인 정보와 같은 민감한 정보를 원거리에서 탈취할 수 있고, 사용자의 컴퓨터를 조작할 수 있음을 실제 응용 서비스 환경에 적용한 결과를 통해 보인다.

본 논문의 구성은 다음과 같다. 2장에서는 기존에 연구되어진 2.4 GHz 무선 키보드 분석 동향을 언급 후, 3장에서 제안하는 시스템을 설명한다. 이후 4장에서 제안된 시스템을 이용하여 실제 무선 키보드 제품 사용 시 발생할 수 있는 민감 정보 노출에 관한 실험결과를 보이고, 5장에서 결론으로 마무리 짓는다.

II. 2.4 GHz 무선 키보드 분석 동향

본 장에서는 기존 연구된 마이크로소프트사 2.4 GHz 무선 키보드 취약성 분석 연구에 대해 서술한다. 분석 대상 무선 키보드는 무선 통신을 할 때 Nordic 사의 nRF24L 시리즈를 사용한다. nRF24L 시리즈는 2.4 GHz 대역을 사용하는 무선 키보드에 많이 사용되는 트랜시버이며, 칩에 대한 자세한 사양은 설명서가 공개되어 있기 때문에 정보를 쉽게 얻을 수 있다[7]. 칩 설명서를 통해 Fig. 1.과 같이 통신 패킷 구조를 확인할 수 있다.

1) 소프트웨어에 기반 무선 통신 시스템을 연구하고, 만들고, 제작하기 위한 툴
2) GNU Radio와 종속적인 관계로 USRP에서 신호를 송·수신하여 GNU Radio로 전달하는 장비

1 byte	5 bytes	9 bits	0~32 bytes	1~2 bytes
PREAMBLE	MAC ADDRESS	PACKET CONTROL	PAYLOAD	CRC

Fig. 1. Enhanced ShockBurst™ packet format of nRF24L chip

2.1 KeyKeriki v2.0 프로젝트

KeyKeriki v2.0 프로젝트는 2.4 GHz 마이크로소프트 무선 키보드에 대한 취약점을 연구한 프로젝트로 2010년 CanSecWest 보안 컨퍼런스에서 최초로 발표되었다[3].

공격자는 Fig. 1.과 같이 패킷 구조를 알고 있다 하더라도 패킷의 페이로드(payload) 부분은 각 제조사들의 구현에 의존하며 비공개 되어 있기 때문에 페이로드 구조를 분석해야한다. 이를 위해 KeyKeriki v2.0 프로젝트에서는 Amiccom A7125 모듈을 이용하여 분석 대상 2.4 GHz 무선 키보드의 유효한 신호를 수신한 후 패킷의 페이로드 구조, 체크섬(checksum) 계산방법을 분석했다. 또한 페이로드 암호화 방식을 분석하고 공격 대상 키보드 신호 송·수신에 필요한 MAC 주소 값을 획득하였다.

Fig. 2.는 분석 대상 키보드의 페이로드 구성을 보여주고 있다. 헤더(HEADER) 부분에는 디바이스, 패킷, 키보드 모델 ID 등의 내용이 포함되어 있으며, SEQUENCE ID부터 DATA까지 총 11바이트는 키보드의 MAC 주소 값을 이용하여 XOR 암호화 한 결과로 채워진다. 그중 눌린 키의 HID (Human Interface Device) 코드는 DATA 영역의 2번째 바이트에서 확인 할 수 있다[3].

4 bytes	2 bytes	2 bytes	7bytes	1 byte
HEADER	SEQUENCE ID	METAKEY FLAGS	DATA	CHECKSUM

Fig. 2. MicroSoft 2.4 GHz wireless keyboard Payload format

2.2 NHB12

2011년 Travis는 Amiccom A7125, nRF24L01+ 두 개의 모듈을 사용해 2.4 GHz 무선 키보드 신호를 송·수신하는 KeyKeriki v2.0과는 달리 하나의 nRF24L01+ 칩만을 사용해 신호를 송·수신할 수 있는 장비 NHB12를 구성하였다[6].

nRF24L01+ 칩을 사용해 무선 키보드 신호를 수신할 경우, 무선 키보드에 설정 되어 있는 nRF24L01+ 칩의 MAC 주소 값을 알아야한다. 하지만 nRF24L01+ 칩은 수신한 패킷의 페이로드 부분만을 공격자가 볼 수 있도록 전달하기 때문에 공격자는 키보드의 MAC 주소 값을 확인하기 어렵다. 이러한 문제를 해결하기 위해 KeyKeriki v2.0에서는 Amiccom A7125 모듈을 사용하여 MAC 주소 값을 직접 확인하는 방법을 사용하였다. 그러나 Travis는 nRF24L01+ 칩의 취약성을 이용해 별도의 다른 수신 모듈 없이 MAC 주소 값을 확인 할 수 있는 방법을 제안하였다.

nRF24L01+ 칩의 설명서에 따르면, MAC 주소의 길이는 3, 4 또는 5바이트로 구성할 수 있다. 이때 MAC 주소의 길이는 AW라는 크기가 2비트인 레지스터에 따라 정해지는데 $00_{(2)}$값으로 설정하면 MAC 주소 길이를 2 바이트로 인식하는 현상이 발생한다. 따라서 이 현상을 이용하기 위해 공격 장비의 AW 레지스터 값을 $00_{(2)}$으로 설정한다. 그리고 패킷의 CRC 값을 확인하지 않도록 설정하고, MAC 주소 값을 0x00AA 또는 0x0055로 설정한 후 키보드 신호를 수신한다. 이때 nRF24L01+ 모듈 노이즈 신호에는 0xAA, 0x55, 0x00, 0xFF가 많이 포함되어 있어 노이즈를 포함한 패킷을 정당한 패킷 구조로 인식 하는 경우가 빈번히 발생하게 된다. 따라서 공격 장비는 MAC 주소 영역을 페이로드 영역으로 인식하여 공격자의 MCU(Micro Controller Unit)로 전달하므로 MAC 주소 값을 획득 할 수 있다.

2.3 KeySweeper

KeySweeper는 KeyKeriki v2.0과 NHB12의 내용을 토대로 아두이노 보드, nRF24L01+ 칩, GSM 통신 모듈이 장착된 Adafruit FONA 보드를 이용하여 무선 키보드 신호를 수신한 후 SMS로 전송하는 장비를 구성하였다[4]. 앞 선 두 개의 장비는 PC와 공격 장비가 연결되어 있어야 공격을 수행할 수 있다. 이는 공격자가 항상 공격 장비 근처에 존재하여야 함을 의미한다. 그러나 KeySweeper는 GSM 통신 모듈을 사용하여 아두이노 보드에서 분석된 키보드 글쇠 정보를 원거리에서 확인 가능하도록 하였다. 즉, 공격자는 공격 장비의 위치에 상관없이 키보드 글쇠를 분석 할 수 있다.

그러나 KeySweeper에서 사용한 아두이노 보드

는 사용 할 수 있는 RAM 용량이 제한적이기 때문에 키보드 글쇠 분석과 주입이 한 장치에서 이루어지지 않는 단점이 존재한다.

III. 제안하는 글쇠 분석 및 주입 시스템

KeyKeriki v2.0과 NHB12는 PC의 자원을 활용하기 때문에 공격 장비와 PC가 항상 연결되어 있어야 키보드 글쇠 분석 및 주입이 가능하다. 이것은 공격자가 항상 공격 장비 근처에 있어야 함을 의미하며, 이는 실제 공격에서 단점이 된다. 이러한 단점을 극복하는 KeySweeper는 PC 대신 아두이노 보드의 자원을 사용하여 공격 장비가 단독으로 실행 가능하도록 구성하였다. 또한 GSM 통신 모듈이 장착된 보드를 통해 공격자가 공격 장비 근처에 없어도 원거리에서 키보드 글쇠 분석이 가능하다. 그러나 KeySweeper는 아두이노의 RAM 용량의 한계로 인해 키보드 글쇠 분석과 주입이 한 장치에서 이루어지지 못한다는 단점이 존재한다.

따라서 본 논문에서는 알려진 마이크로소프트 2.4 GHz 무선 키보드 취약점을 기반으로 안드로이드 스마트폰을 이용하여 원거리에서 키보드 글쇠 분석과 주입이 모두 가능한 공격 시스템을 제안한다. 본 논문의 공격 시스템은 기존 글쇠 주입 공격과 달리 원거리 글쇠 주입이 가능한 것이 특징이며, 안드로이드 스마트폰의 무선랜, LTE 모듈을 이용함으로써 공격 적용 가능 범위를 넓혔다.

3.1 시스템 구성

본 절에서는 제안하는 키보드 글쇠 분석 및 주입 시스템 구성 및 이를 위해 필요한 각 장비에 대해 간략히 설명한다. Fig. 3.은 제안하는 키보드 글쇠 분석 및 주입 시스템 구조를 도식화 한 것이다. 안드로이드 스마트폰, 아두이노, nRF24L01+칩으로 구성된 공격 장비는 마이크로소프트 2.4 GHz 무선 키보드를 사용하는 사용자가 있는 장소에 함께 존재한다. 그러나 공격자와 웹 서버는 이와 상관없는 곳, 즉, 마이크로소프트 2.4 GHz 무선 키보드와 서로 다른 공간에 존재하며 공격 장비는 무선랜 또는 LTE 망을 통해 분석된 키보드 글쇠를 웹 서버에 전송하거나 웹 서버의 문자열을 사용자 PC에 주입하는 역할을 한다.

공격 장비에 사용 된 아두이노는 주로 Atmel사의 AVR을 사용하는 오픈소스 마이크로컨트롤러 보드로, nRF24L01+ 칩과 안드로이드 스마트폰을 제어하고 키보드 패킷을 분석한다. 그리고 인터넷 통신 관련 제어는 안드로이드가 수행하기 때문에 아두이노 보드에서 GSM 통신 모듈을 제어하였던 KeySweeper와는 달리 아두이노의 RAM 용량 제한으로 인한 문제없이 키보드 글쇠 주입 공격을 동일 장비에서 수행할 수 있다.

nRF24L01+ 칩은 2.4 GHz의 주파수를 통하여 데이터를 송·수신을 할 수 있도록 지원해주는 칩으로, SPI통신을 사용해 키보드로부터 방출되는 입력 정보를 받아들여 패킷의 페이로드 부분을 아두이노에 전달하는 역할을 한다. 또한 아두이노에서 전달받은 키보드 주입 신호 페이로드를 Fig. 1.과 같이 구성하여 2.4 GHz 주파수를 통해 무선 키보드 리시버에 전달하는 역할을 한다.

안드로이드 스마트폰은 어플리케이션을 이용해 분석된 키보드 글쇠 정보를 웹 서버로 보내 주거나 웹 서버에서 문자열을 받아 아두이노에 보내주는 역할을 한다. 이 때 인터넷 연결은 무선랜 또는 LTE 모듈을 이용한다.

KeyKeriki v2.0과 NHB12의 경우 공격자가 탈취한 키보드 입력 값을 확인하기 위해서는 공격 장비와 연결되어 있는 컴퓨터를 통해 입력 값을 직접 확인해야 한다. 이 경우, 공격자가 항상 공격 장비 근처에 있기 때문에 사용자에게 들킬 수 있다. 하지만 KeySweeper와 본 논문의 장비는 공격자가 공격 장비의 근처에 없어도 탈취한 입력 값을 확인할 수 있어 기존의 장비들보다 더 현실적인 공격을 수행 할 수 있다. 이뿐만 아니라 아두이노 플랫폼을 사용하기 때문에 부피가 작은 다른 종류의 아두이노 보드로 쉽게 최적화 할 수 있다. 이 경우 공격 장비를 소형화하여 사용자 눈에 띄지 않도록 숨기기 쉽기 때문에 더욱 현실적인 공격을 수행 할 수 있다. 또한, 본 논문의 장비는 GSM 통신 모듈을 사용하는 KeySweeper와 달리 무선랜 또는 LTE를 사용하기 때문에 국내 환경에서도 공격이 가능하며, 공격 적용 가능 범위가 넓어졌다. 이에 더불어 키보드 글쇠 분석 및 주입이 하나의 공격 장비에서 가능하다는 장점을 지닌다.

3.2 키보드 글쇠 분석 및 주입 시스템

3.2.1 사전 정보 탐색

일반적으로 키보드 글쇠 분석 또는 주입 공격을 수행하기 위하여 공격자는 공격 대상 키보드의 통신 주파수 등 필요한 정보를 획득하여야 한다. 공격 대상이 정해지면 통신 가능 주파수 대역, 통신 속도 및 통신 대역폭은 공개되어 있는 정보이므로 쉽게 확인 가능하다. 본 논문의 공격 대상인 마이크로소프트 2.4 GHz 무선 키보드는 MAC 주소 값을 이용해 데이터를 암호화 하고, 리시버는 고정 MAC 주소 값을 가진 신호만 수신한다. 따라서 신호 분석 및 주입을 위해 MAC 주소 값을 획득하여야 하는데 이 과정은 실제 공격이 이루어지기 전에 아래와 같은 방법으로 탐색한다. 실제 이 과정은 공격 대상이 정해지면 최초에 한번만 실행하면 된다.

〔1단계〕 사용 가능한 주파수 대역, 통신 속도 및 통신 대역폭 확인

키보드가 사용 가능한 모든 주파수 대역은 키보드의 FCC ID를 통해 확인 할 수 있다. FCC ID는 분석 대상 키보드의 제조사 홈페이지에서 제공하는 기술 데이터시트 또는 분석 대상 키보드와 동일한 키보드 뒷면에서 확인가능하다. 본 논문의 분석 대상 키보드는 FCC ID가 C3K1394이므로 FCC ID를 찾는 사이트를 통해 통신 가능한 주파수 영역이 2.403GHz ~ 2.480GHz 임을 확인 할 수 있다.

무선 키보드 신호 분석 및 주입을 위해 통신 속도 및 통신 대역폭을 알아야하는데, 분석 대상 키보드는 nRF24L01+ 칩을 사용하고 있기 때문에 칩 설명서에 의해 사용 가능한 통신 속도 및 통신 대역폭을 확인 할 수 있다. 이후 실험을 통해 키보드의 실제 통신 속도 및 통신 대역폭을 확인한다.

〔2단계〕 MAC 주소 획득 및 통신 주파수 확인

MAC 주소는 NHB12의 방법과 같은 방법으로 진행된다. 즉, nRF24L01+ 칩의 MAC 주소 길이 설정 값을 $00_{(2)}$로 설정하고, 패킷의 CRC 값을 확인하지 않도록 설정한다. 그리고 MAC 주소 값을 0x00AA 또는 0x0055로 설정한 후 키보드 신호를 수신한다. 이때 키보드가 사용 가능한 모든 주파수로 변경하면서 주파수를 변경할 때마다 정상 데이터가 수신되는지 조사한다. 따라서 정상 데이터가 수신될 때의 주파수를 통신 주파수로 설정하고, 수신된 데이터 패킷에서 MAC 주소 값을 확인한다.

3.2.2 글쇠 분석 시스템

사용자가 무선 키보드를 이용해 입력한 글쇠 정보는 아날로그 신호로 리시버에 전송된다. 이때 nRF24L01+ 칩은 키보드로부터 방출된 신호를 받아 패

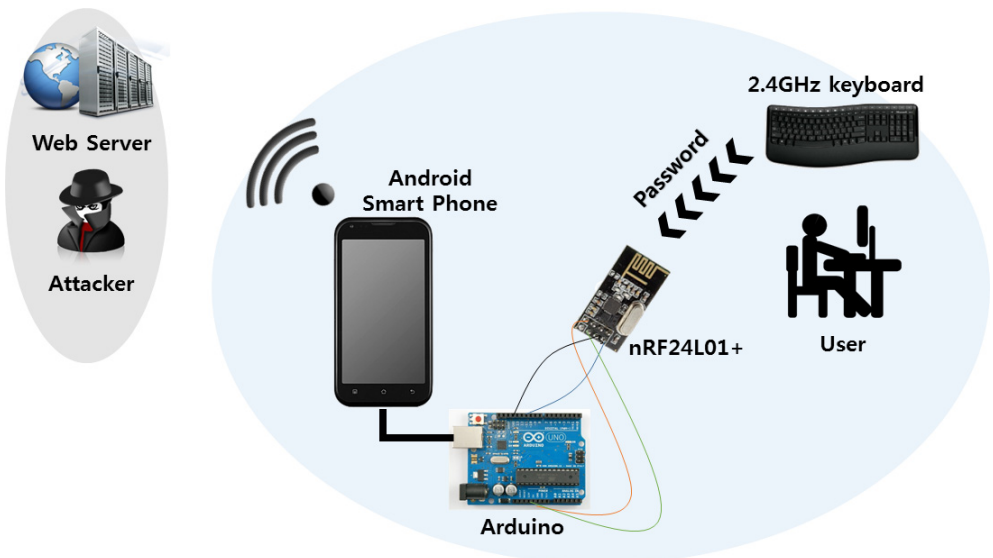


Fig. 3. The proposed attack system

킷의 암호화 된 페이로드 부분을 아두이노에 전달한다. 이후, 아두이노는 전달 받은 페이로드를 복호화해 어떤 키보드 글쇠가 눌렸는지 판단하여 안드로이드 스마트폰의 어플리케이션에 글쇠 정보를 전달하면 어플리케이션은 웹 서버에 전송함으로 키보드 글쇠 분석은 완료된다.

Fig. 4.는 2.4 GHz 무선 키보드의 눌린 글쇠에 대한 분석 과정을 간략히 나타낸 그림이다. 각 단계에 대한 자세한 내용은 다음과 같다.

〔1단계〕 nRF24L01+ 칩 설정

사전 확인 된 MAC 주소와 통신 주파수를 공격 장비 nRF24L01+ 칩의 MAC 주소 및 주파수로 설정한다. 이 단계는 공격 대상 키보드 별로 최초에 한번만 실행하면 된다.

〔2단계〕 패킷 데이터 수신 및 패킷 분석

〔1단계〕를 통해 nRF24L01+ 칩은 유효한 패킷을 확인 후 페이로드 부분을 아두이노로 전송한다. 전송 받은 페이로드 신호는 MAC 주소로 암호화 된 데이터 이므로 아두이노에서 암호화 된 데이터를 MAC 주소를 이용해 배타적 논리합(exclusive OR)으로 복호화 후 HID 코드를 확인한다.

〔3단계〕 웹 서버로 결과 전송

마지막 단계는 분석된 HID 코드를 통해 사용자가 입력한 글쇠 정보를 확인한 후 웹 서버로 전송하는 단계이다. 이 때, 엔터키를 기준으로 전송하며, 공격자는 공격 장비와 떨어져 있는 곳에서도 사용자가 누른 키보드 글쇠를 분석 할 수 있다.

3.2.3 글쇠 주입 시스템

본 항에서는 2.4 GHz 무선 키보드 신호를 생성하여 사용자의 PC에 주입하는 시스템을 설명한다.

공격 장비는 안드로이드 스마트폰의 어플리케이션을 이용하여 웹 서버로부터 받은 문자열들을 확인한 후 아두이노로 전송하면 아두이노는 문자열을 하나의 키보드 글쇠 단위(keystroke)로 분해한다. 이후 각 글쇠에 해당하는 페이로드를 생성하여 이를 MAC 주소로 암호화한다. 이렇게 생성된 암호화된 페이로드를 설정이 끝난 nRF24L01+ 칩을 이용하여 유효한 패킷으로 구성한 후 키보드 리시버로 전송한다.

Fig. 5.는 2.4 GHz 무선 키보드 글쇠 주입 과정을 간략히 나타낸 그림이다. 각 단계에 대한 자세한 내용은 다음과 같다.

〔1단계〕 nRF24L01+ 칩 설정

본 단계는 글쇠 분석의 〔1단계〕와 동일하다. 단지 본 논문 공격 장비의 nRF24L01+ 칩은 기본적으로 수신 상태로 설정되어있어 키보드를 조작하기 위해서는 일시적으로 송신 상태로 설정해야 한다. 그리고 글쇠 주입이 끝나면 바로 글쇠 분석이 가능하도록 다시 수신 상태로 설정한다.

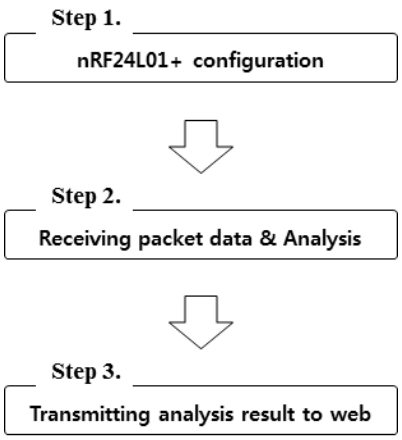


Fig. 4. Wireless Keyboard keystroke analysis Phase

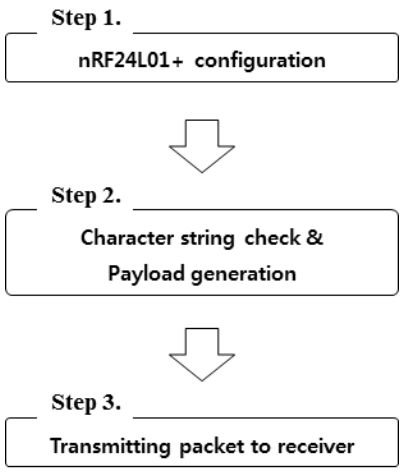


Fig. 5. Wireless Keyboard Signal Transmission Phase

〔2단계〕 문자열 확인 및 페이로드 생성

아두이노가 안드로이드 스마트폰으로부터 사용자 PC에 전송 할 문자열을 전송받으면 이를 키보드 글쇠 단위로 분해한다. 이후 각 글쇠의 HID 코드를 확인한 뒤 페이로드를 생성하고, MAC 주소를 이용하여 암호화한다. 생성된 페이로드는 nRF24L01+ 칩으로 전송된다.

〔3단계〕 리시버로 패킷 전송

〔1단계〕에서 송신 상태로 설정이 끝난 nRF24L01+ 칩을 이용하여 아두이노로 부터 받은 암호화된 페이로드를 유효 패킷으로 변형한 후 사용자의 키보드 리시버에 전송함으로 키보드 글쇠 주입 공격을 완성한다.

IV. 실제 환경에서의 공격사례

본 장에서는 실제 2.4 GHz 무선키보드를 사용하는 환경에서 제안하는 시스템을 통하여 원격에서 취약점을 이용한 공격이 가능함을 실험을 통해 보인다.

4.1 공격자 가정

공격 장비는 무선 키보드를 사용하는 사용자와 통신이 가능한 범위, 즉 사용자의 무선 키보드가 제대로 동작되는 거리 안에 존재한다고 가정한다. 단, 공격자는 공격 장비의 위치와는 무관한 곳에 존재한다. 또한 무선 인터넷이 가능한 환경이거나 안드로이드 스마트폰의 유심(USIM)이 활성화 되어 있어 LTE 모듈을 사용할 수 있다 가정한다.

4.2 글쇠 분석 공격사례

4.2.1 주요 포털 사이트의 로그인 정보 획득 공격

본 항에서는 3.2.2의 글쇠 분석 시스템을 기반으로 사용자가 2.4 GHz 무선 키보드를 사용하여 국내 유명 포털사이트에 로그인 할 때 키보드 입력 값을 탈취하는 시나리오와 시나리오에 따른 결과에 대해 설명한다. 사용자는 포털 사이트의 서비스를 이용하기 위해 다음의 시나리오를 따른다고 가정한다.

우선 사용자는 메일 조회 등 포털 사이트의 서비스를 이용하기 위해 해당 사이트에 접속해야 하므로 키보드를 사용하여 주소창에 직접 해당 포털의 URL 또는 키워드를 입력하는 것으로 가정한다. 그리고 URL을 이용하여 직접 접속을 하거나 키워드로 검색 할 때 대부분의 사용자들은 엔터키를 누른다. 따라서 사이트 정보는 서비스 이용 시 웹서버에 가장 처음 전송된 데이터에 존재한다는 가정한다.

이후 사용자는 메일 등의 확인을 위해 홈페이지에 로그인하는 과정을 거치게 되며, 이때 키보드를 사용하여 사용자 아이디와 비밀번호를 입력한 후 대부분의 사용자들은 엔터키로 로그인을 시행한다. 따라서 로그인 정보인 사용자 아이디와 비밀번호는 두 번째 전송된 데이터로부터 추출이 가능하다. 본 논문의 실험에서는 사용자 아이디 입력 후 탭(Tab)키를 이용하여 비밀번호 입력 창으로 이동한다고 가정하였으며 탭키 신호를 받으면 space+\t+space 신호로 전환하여 표시하도록 하였다. 만약 마우스 클릭으로 비밀번호 입력 창으로 이동하였다 하더라도 아이디와 비밀번호를 어렵지 않게 구분 할 수 있다.

Fig. 6.은 포털 사이트 로그인 시 사용되는 사용자의 키보드 신호를 받아 공격 장비가 웹 서버에 보내준 정보를 순차적으로 보여주고 있다. 공격자는 웹 서버의 정보를 통해 로그인 정보를 분석한다. Fig. 7.은 웹 서버에 전송된 데이터로부터 포털 사이트의 로그인 정보를 분석한 결과이다. 가장 처음에 전송된 데이터인 '스니핑 데이터 1'에 사이트 정보가 있으므로 키워드를 사용하여 사용자가 Fig. 7.의 ①처럼 어떤 사이트에 접속하였는지 알아낼 수 있다. 또한 두

Sniffing log

date	text
Fri, 20 May 16 15:04:57 +0900	shrtodckdid ₩t votmdnjem
Fri, 20 May 16 15:04:43 +0900	spdlqj

Fig. 6. sniffing data of Portal login

==========

포털사이트 로그인정보 스니핑

==========

스니핑 데이터 1 : spdlqj
스니핑 데이터 2 : shrtodckdid ₩t votmdnjem

"[redacted]" 접속 ①

ID : shrtodckdid ②

PassWord : votmdnjem ③

Fig. 7. Portal login data analysis

번째로 전송받은 '스니핑 데이터 2'에 포함된 ②, ③ 로그인 정보를 쉽게 획득 할 수 있음을 알 수 있다.

최근 많은 사람들이 아마존, 페이팔 결제 기반의 이베이 등 해외 구매 사이트를 통해 해외직구를 이용한다. 이러한 사이트는 결제 카드를 등록한 후 비밀번호와 아이디만 안다면 쉽게 결제를 할 수 있다. 따라서 이처럼 사용자의 아이디와 비밀번호 획득 사례는 사용자에게 금전적인 손해를 입힐 수 있는 공격으로 이에 대한 대응책이 모색 되어야 할 것이다.

4.2.2 공인인증서 비밀번호 획득 공격

본 항에서는 3.2.2의 글쇠 분석 시스템을 토대로 사용자가 2.4 GHz 무선 키보드를 사용하여 인터넷 뱅킹을 사용 할 때 입력 정보를 탈취하는 과정과 그 결과에 대해 설명한다. 인터넷 뱅킹을 사용 할 때 사용자는 다음의 시나리오에 따라 ○○○ 은행 계좌이체를 수행한다고 가정한다.

사용자가 인터넷 뱅킹을 사용하기 위해서는 주소창에 직접 은행 홈페이지 URL 또는 키워드를 입력한다. 4.2절의 포털 사이트와 마찬가지로 대부분의 사용자는 URL 또는 키워드를 입력한 후 엔터키를 입력하므로 은행 정보는 가장 처음 전송된 데이터에 존재하게 될 것이다.

이 후, 계좌를 조회하거나 이체하기 위해 홈페이지에 로그인을 하는 단계를 수행하며 이때 키보드를 사용하여 아이디와 비밀번호 혹은 공인인증서 비밀번호를 입력한 후 엔터키를 누른다. 따라서 로그인 정보는 두 번째 전송된 데이터로부터 추출 할 수 있다.

사용자가 은행 홈페이지에 로그인을 하면 인터넷 뱅킹을 이용하여 계좌이체를 하게 되는데, 이 때 총 3단계를 거친다. 거래 내용을 작성하는 정보입력단계, 거래내용 부인 방지를 위하여 본인인증이 진행되는 입력확인단계, 마지막으로 이체결과를 보여주는 이체확인단계이다. 여기에서 마지막으로 전송된 데이터는 정보작성단계와 입력확인단계에서의 무선키보드 입력 값을 담고 있다.

본 실험에서는 Fig. 8.의 왼쪽 그림처럼 정보입력단계에서 이체금액은 마우스로 입력 받고, 추가적인 통장 내용 표시부분은 입력하지 않는 것으로 가정한다. 또한 Fig. 8.의 오른쪽 ③처럼 입력확인단계에서 사용되는 1회용 비밀번호는 OTP를 이용하는 것으로 가정한다. 물론 OTP 발생번호가 아닌 보안카드의 정보를 사용 하는 경우라도 관련 정보를 쉽게 추출 가능하다. 이 때, ①~④ 정보는 순차적으로 입력된다고 가정한다.

Fig. 9.는 인터넷 뱅킹 정보가 포함되어 있는 데이터로 웹 서버에 전송된 데이터의 일부이다. 내림차순으로 정렬되어 있으며, 점선 네모 박스안의 text 정보는 앞에서 언급한 시나리오로 인터넷 뱅킹 수행 시 발생되는 글쇠정보를 담고 있다. 본 실험은 Fig. 9.와 같이 인터넷 뱅킹에 사용된 글쇠 정보뿐만 아니라 여러 가지 다른 글쇠 정보가 섞여 있는 스니핑 데이터를 이용해 비밀정보를 추출한다.

Fig. 10.은 웹 서버에 전송된 데이터로부터 사용자와 관련된 민감 정보를 분석한 결과이다. '스니핑 데이터 1'로부터 사용 은행을 분석 할 수 있으며, '스니핑 데이터 2'를 이용해 로그인 정보를 추출 할 수 있다. 마지막으로 '스니핑 데이터 3'을 통해 출금 계좌 비밀번호 등을 알 수 있다.

'스니핑 데이터 3'은 정보입력단계와 입력확인단계에서의 무선 키보드 입력 정보가 담겨있다. 출금 계

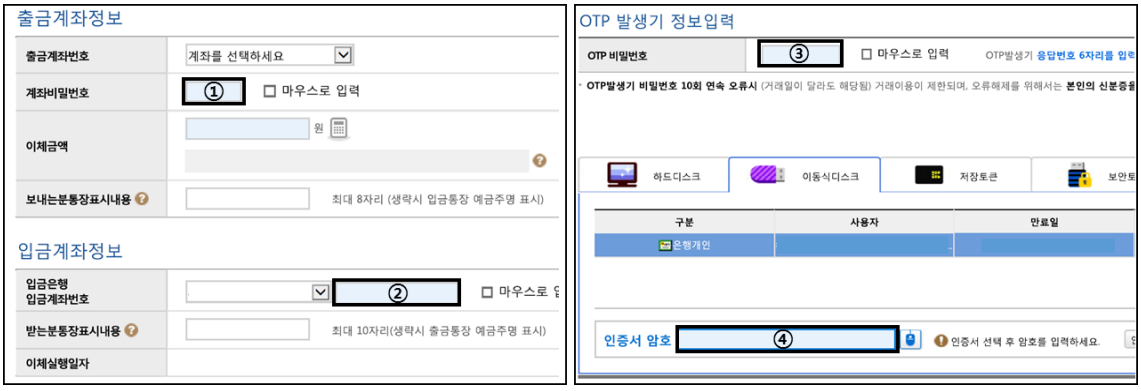


Fig. 8. Information input stage (Left) and Information confirm stage in ○○○ bank (Right)

Sniffing log

date	text
Mon, 23 May 16 15:41:29 +0900	0509100214381405172825 7yoo1990811@
Mon, 23 May 16 15:40:10 +0900	yoo1990811@
Mon, 23 May 16 15:39:56 +0900	dnfldmsgod
Mon, 23 May 16 15:39:22 +0900	xovnd gkfhddpqhfk qkdlfjtmbvjaodl ehdkhTek

Fig. 9. sniffing data

인터넷뱅킹 인증정보 스니핑

스니핑 데이터 1 : dnfldmsgod ①

스니핑 데이터 2 : yoo1990811@ ②

스니핑 데이터 3 : 0509100214381405172825 7yoo1990811@

③ ④ ⑤ ⑥

1. 사용 은행 : [redacted] Bank
2. 로그인 정보
   공인인증서 사용 로그인 수행 : yoo1990811@
3. 계좌비밀번호 : 0509
4. 입금계좌번호(13자리) : 1002143814051
5. OTP 정보 : 728257
6. 공인인증서 정보 : yoo1990811@

Fig. 10. authentication certificate data analysis

좌비밀번호는 4자리의 숫자로 항상 정해져 있기 때문에, Fig. 10.의 '스니핑 데이터 3'에서 가장 먼저 알아 낼 수 있는 정보③은 정보입력단계의 출금 계좌 비밀번호이다. 그리고 사용자들이 인터넷뱅킹을 이용할 때 대부분 공인 인증서를 이용하여 로그인하기 때문에 ②와 ⑥을 비교하면 입력확인단계의 공인인증서의 비밀번호를 쉽게 추출 할 수 있다. 또한 입력확인단계 중 OTP 발생번호는 보통 공인인증서로 거래내역을 서명하기 전에 먼저 키보드로부터 6자리의 숫자를 입력 받는다. 따라서 Fig. 10. ⑥의 앞 6자리의 숫자인 ⑤가 OTP 발생번호인 것을 알 수 있다. 마지막으로 남은 정보④는 정보입력단계의 입금계좌번호임을 알 수 있다.

이러한 공격을 통하여 공격자는 사용자의 공인인증서 비밀번호 및 계좌 비밀 번호를 획득 할 수 있다.

4.3 글쇠 주입 공격사례

4.3.1 드라이브 포맷 공격

본 항에서는 3.2.3의 글쇠 주입 시스템을 토대로 사용자가 2.4 GHz 무선 키보드를 사용할 때, 사용자 PC에 임의의 글쇠를 주입하는 과정과 그 결과에 대해 설명한다. 이 때, 사용자 PC에는 운영체제가 설치되어 있는 드라이브 외에 한 개 이상의 드라이브가 연결되어 있다고 가정한다.

운영체제가 설치되어 있지 않은 드라이브를 e 드라이브라 가정하고, 드라이브 포맷 명령어를 실행시키기 위해 cmd 창을 이용한다. 이 때, 사용자 PC의 cmd 창을 실행시키기 위해 Fig. 11.의 위쪽 그림 ①과 ②처럼 웹 서버를 통해 공격 장비로 Window 글쇠 신호를 전송한 후 'c', 'm', 'd', '\n' 글쇠를 순차적으로 주입하라는 문자열을 전송한다. 이 후 웹 서버에서는 e 드라이브를 포맷시키기 위한 "format e: /q\n" 명령어에 대한 글쇠를 순차적으로 주입하라는 문자열을 ③과 같이 공격 장비로 전송한다. 마지막으로 포맷을 정상적으로 진행하기 위해 ④와 같이 '\n', '\n', 'y', '\n', '\n' 글쇠를 순차적으로 주입하라는 문자열을 전송한다.

Fig. 11.의 아래 그림은 실제 사용자 PC에 ①~④ 글쇠 정보가 주입된 화면이고, Fig. 12.의 왼쪽 그림은 e 드라이브 포맷 명령어가 실행되기 전, 오른쪽 그림은 e 드라이브 포맷 명령어가 실행된 결과이다. 이와 같은 공격을 통해 공격자는 임의의 글쇠를 사용자 PC에 주입할 수 있으며, 사용자에게 심각한 피해를 입힐 수 있다.

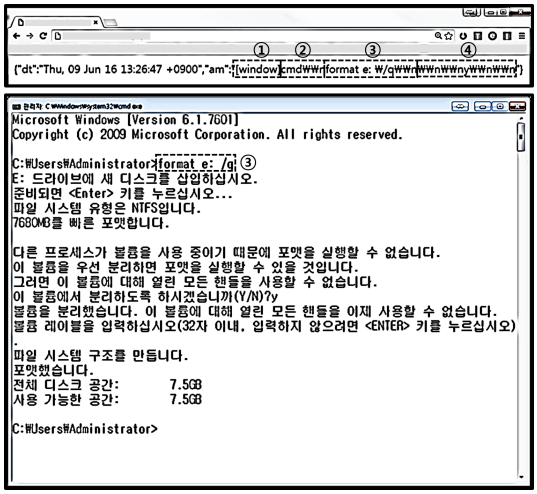


Fig. 11. injection data(Up) and User's PC screen (Down)

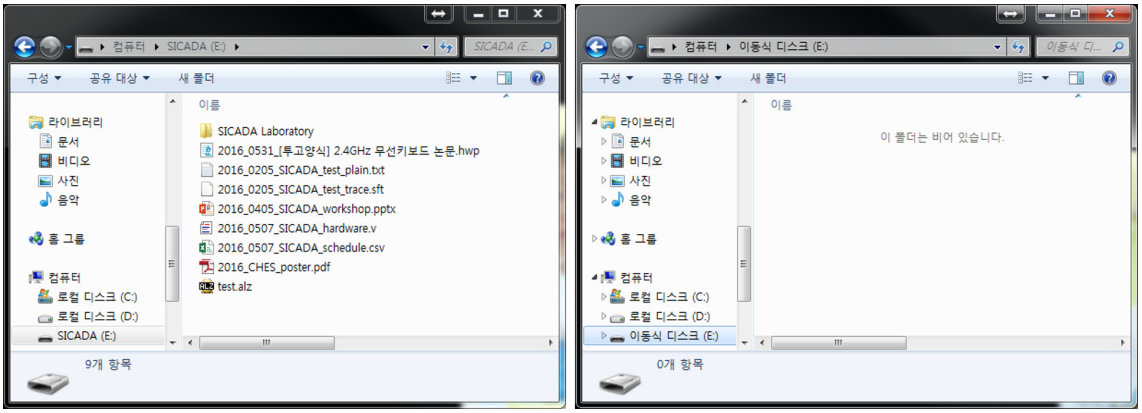


Fig. 12. Before keystroke injection attack (Left) and after keystroke injection attack (Right)

V. 제안하는 공격 시스템의 장·단점

Table 1.은 제안하는 공격 장비와 이전 공격 장비의 특징 및 장·단점을 정리해 놓은 표이다. 본 논문에서 제안하는 공격 시스템은 기존 공격들과 달리 안드로이드 스마트폰을 이용하여 원거리에서 키보드 글쇠 분석과 주입이 모두 가능하다는 것이 특징이다. 즉, 키보드 글쇠 분석 및 주입이 하나의 공격 장비에서 가능하며, 공격자가 공격 장비 근처에 없어도 공격이 가능하다는 장점을 지닌다. 또한 본 논문의 공

Table 1. advantages and disadvantages of each attack device

	feature	advantage	disadvantage
KeyKeriki v2.0 (2010)	• Packet format check - Payload format - Payload encryption - Checksum algorithm	• Receiving raw data using Amiccom A7125 - obtain MAC Address	• use different modules to transmitter and receiver - transmitter : Amiccom A7125 - receiver : nRF24L01+ • need a PCB board • need a PC to control the transmitter and receiver
NHB12 (2011)	• Obtain MAC Address using nRF24L01+ chip	• Transmitter and receiver integration	• need a PCB board • need a PC to control the transmitter and receiver
KeySweeper (2015)	• portable attack device - using resources of Arduino	• Don't need a PC to control the receiver	• attack can only apply to the GSM communication environment. • only receiving function
Our proposed attack device (2016)	• portable attack device - using resources of Android smart phone and Arduino • ranged transmit	• Transmitter and receiver integration • Don't need a PC to control the receiver and transmitter • Use wireless LAN or LTE module	• need to build a web server

격 장비는 무선랜 또는 LTE를 사용하기 때문에 국내 환경에서도 공격이 가능하고, 그 공격 적용 가능 범위가 넓어졌다는 장점이 있다. 단점으로는 웹 서버를 구축해야 하는 점이 있다.

VI. 결 론

본 논문은 기존 연구되어진 마이크로소프트의 2.4 GHz 무선 키보드 취약점을 토대로 원격에서 제어 가능한 2.4 GHz 무선 키보드 글쇠 분석 및 주입 시스템을 제안하였다. 기존 글쇠 주입 공격과 달리 본 논문의 공격 시스템은 원거리 글쇠 주입이 가능하며, 사용자의 키보드 입력정보를 웹 서버로 전송하는 기능을 추가함으로써 공격자가 장소에 구애받지 않고 공격 결과를 확인 할 수 있도록 하였다. 또한 무선랜 또는 LTE 환경에서 통신이 가능하도록 구성하여 국내 환경에서도 공격의 적용이 가능하다. 더불어 안드로이드 스마트폰을 활용하여 장비는 작게 유지하고 글쇠 분석과 주입이 모두 가능하도록 하였다. 그리고 본 시스템을 이용해 실제 2.4 GHz 무선 키보드를 사용 할 때 웹 서버로 전달된 키보드 신호 분석 정보를 통해 사용자의 민감한 정보가 노출되어 짐을 실험을 통해 보였다.

최근 많은 소비자들이 해외직구 사이트를 이용하고 있으며, 해외직구 사이트는 결제 카드 등록 후 비밀번호와 아이디만으로 쉽게 결제 할 수 있도록 시스템이 운영되고 있다. 공인인증서의 경우, 이를 탈취하는 수법은 이미 해커들에서 널리 알려진 수법이 존재한다. 따라서 본 논문에서 보인 사용자의 아이디와 비밀번호 획득 및 공인인증서 비밀번호 탈취의 성공은 무시할 수 없는 결과 일 것이다. 즉, 직접적으로 소비자에게 금전적인 피해를 입힐 뿐만 아니라, 관리자의 공인인증서 탈취 및 권한 획득으로 인해 심각한 보안 사고를 유발할 수 있다. 따라서 가상 키보드만을 사용하여 비밀번호 등을 입력하는 등 본 취약점을 막을 수 있는 대응책에 대한 연구가 필요할 것이다.

References

[1] M, Fähnle and M, Hauff, "Analysis of unencrypted and encrypted wireless keyboard transmission implemented in GNU radio based software-defined radio," Hochschul Ulm, University of Applied Sciences Institute of Communication Technology, 2011

[2] Ho-Yeon Kim, Bo-Yeon Sim, Aesun Park and Dong-Guk Han, "Analysis of 27MHz Wireless Keyboard Electromagnetic Signal Using USRP and GNU Radio," Journal of the Korea Institute of Information Security and Cryptology, 26(1), pp. 81-91, Feb. 2016.

[3] T. Schröder and M. Moser, "KeyKeriki v2.0 - 2.4 GHz", CanSecWest 2010, http://www.remote-exploit.org/articles/keykeriki_v2_0__8211_2_4ghz/, 2010.

[4] S. Kamkar, "KeySweeper", http://samy.pl/keysweeper/, 2015.

[5] Bastille, "MouseJack", https://www.bastille.net/technical-details, 2016.

[6] Travis Goodspeed, "Promiscuity is the nRF24L01+'s Duty", http://travisgoodspeed.blogspot.kr/2011/02/promiscuity-is-nrf24l01s-duty.html, 2011.

[7] Semiconductor, Nordic. "nRF24L01 single chip 2.4 GHz transceiver product specification." http://www.nordicsemi.com/eng/Products/2.4GHz-RF/nRF24L01, 2007.

〈저자소개〉

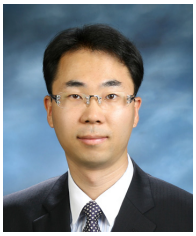
이 수 진 (Su-Jin Lee) 일반회원
2014년 2월: 국민대학교 수학과 졸업
2016년 2월: 국민대학교 금융정보보안학과 석사
〈관심분야〉 정보보호, 핀테크, 임베디드시스템, 부채널 분석

박 애 선 (Aesun Park) 학생회원
2011년 2월: 국민대학교 수학과 졸업
2013년 2월: 국민대학교 수학과 석사
2014년 3월~현재: 국민대학교 금융정보보안학과 박사과정
〈관심분야〉 부채널 분석 및 대응법, 신호처리, 스마트 카드 평가, Post-quantum cryptography 등

심 보 연 (Bo-Yeon Sim) 학생회원
2013년 2월: 국민대학교 수학과 졸업
2015년 2월: 국민대학교 금융정보보안학과 석사
2015년 3월~현재: 국민대학교 수학과 박사과정
〈관심분야〉 공개키 암호 시스템, 부채널 분석 및 대응기법 설계, 경량·저전력 정보보호 기술

김 상 수 (Sang-Su Kim) 일반회원
2008년 2월 : 성균관대학교 정보통신공학부 졸업
2007 년 12월~현재 : LIG넥스원 선임연구원
〈관심분야〉 정보보호, 통신시스템, 신호분석

오 승 섭 (Seung-Sup Oh) 일반회원
1989년 2월 : 조선대학교 전자공학과 졸업
1989년 1월~현재 : LIG넥스원 수석연구원
〈관심분야〉 정보보호, 통신대역 신호분석 시스템 등



한 동 국 (Dong-Guk Han) 종신회원
1992년 2월: 고려대학교 수학과 졸업 (학사)
2002년 2월: 고려대학교 수학과 석사 (이학석사)
2005년 2월: 고려대학교 정보보호대학원 박사 (공학박사)
2004년 4월~2005년 4월: 일본 Kyushu Univ., 방문연구원
2005년 4월~2006년 4월: 일본 Future Univ.-Hakodate, Post.Doc.
2006년 6월~2009년 2월: 한국전자통신연구원 정보보호연구단 선임연구원
2009년 3월~현재: 국민대학교 수학과 부교수
〈관심분야〉 공개키 암호시스템 안전성 분석 및 고속 구현, 부채널 분석 및 대응법 설계, IoT 정보보호 기술