THE JOURNAL OF KOREAN INSTITUTE OF ELECTROMAGNETIC ENGINEERING AND SCIENCE. 2016 Dec.; 27(12), 1075～1083.

http://dx.doi.org/10.5515/KJKIEES.2016.27.12.1075
ISSN 1226-3133 (Print) · ISSN 2288-226X (Online)

2.4 GHz 무선 키보드/마우스 전자파 신호 분석 및 조작 시스템 구축

Implementation of 2.4 GHz Wireless Keyboard and Mouse Electromagnetic Signal Analysis and Manipulate Systems

김 상 수 · 오 승 섭 · 나 인 석

Sang-Su Kim · Seung-Sub Oh · In-Seok Na

요 약

최근 높은 편의성과 휴대성을 바탕으로 무선 입력 장비들의 사용이 증가하고 있다. 특히 2.4 GHz 주파수 대역을 사용하는 무선 키보드와 무선 마우스가 가장 많이 사용되고 있지만, 무선 장비의 경우 누설되는 전자파를 제3자가 수신하여 개인정보를 획득하기가 용이하기 때문에, 보안에 대한 취약점 또한 꾸준히 보고되고 있다. 본 논문에서는 2.4 GHz 무선 키보드와 무선 마우스의 취약점을 검증하기 위해 USRP 장비와 GNU 라디오(Radio) 패키지를 사용하여 2.4 GHz 무선 키보드와 무선 마우스의 패킷을 분석하고, 이를 조작하는 시스템을 구현하였다. 구축한 시스템을 이용하여 해당 장비의 통신 프로토콜 및 패킷 구조를 분석하여 장비 고유 주소(Address)와 입력 키 정보를 획득하였고, 임의의 키를 송신하여 원거리에서 사용자 PC를 조작할 수 있다는 것을 증명하였다.

Abstract

Nowadays, the use of wireless input devices has been increasing on the basis of high convenience and portability. In particular the most widely used wireless keyboard and the mouse to use the 2.4 GHz frequency band, but due to the third party receives the electromagnetic wave from leaking when the radio equipment it is easy to obtain the personal information and the vulnerability is also being reported consistently. In this paper, implement a system to analyze and manipulate the packets of 2.4 GHz wireless keyboard and mouse using USRP device and GNU Radio package for verify the vulnerability of 2.4 GHz wireless keyboard and mouse. Using the construction system has attained a equipment specific address and key information by analyzing the communication protocol and the packet structure of the device was proved that a user can operate the PC to send the random key from long distance.

Key words: Wireless Keyboard, Wireless Mouse, nRF24L01, USRP, GNU Radio

Ⅰ. 서 론

과거 개인용 PC의 입력장치는 PS/2 키보드와 USB 키보드 등의 유선 장치가 주로 사용되었다. 하지만 최근에는 편의성과 휴대성을 바탕으로 무선 통신 기술이 발전되어 개인용 컴퓨터를 비롯한 태블릿 PC, 휴대폰 및 IPTV 등과 같은 다양한 매체에서 무선 키보드와 무선 마우스가 활발하게 사용되고 있다. 하지만 무선 통신의 경우, 장비에서 누설되는 전자파를 제3자가 수신하여 개인정보를 유출할 가능성이 있기 때문에 이에 대한 취약점에 대한 문제가 꾸준히 제기되고 있다.

가장 최초에 사용된 27 MHz 대역 무선 키보드의 경우,

LIG 넥스원 전자전연구센터(Electronic Warfare R&D Lab., LIG Nex1)
· Manuscript received August 30, 2016 ; Revised October 21, 2016 ; Accepted December 9, 2016. (ID No. 20160830-094)
· Corresponding Author: Sang-Su Kim (e-mail: sangsu.kim82@lignex1.com)

각 키의 입력에 따라 키보드에서 발생하는 전자파를 측정하고, 통신 패킷을 분석하여 입력된 키 값을 획득하고, 임의의 키 정보를 전달할 수 있다는 것이 발표되었다[1].

또한 현재 가장 대중적으로 사용되고 있는 2.4 GHz 무선 키보드의 경우도 보안 취약성 문제와 관련한 연구가 지속적으로 발표되고 있다[2]~[5]. 대표적인 예로 2010년 CanSecWest 보안 컨퍼런스에서 발표된 KeyKerki v2.0 프로젝트가 있다. 이 프로젝트에서는 Microsoft 사의 2.4 GHz 무선 키보드에 대한 보안 취약점에 대해 보고하였다. 무선 키보드의 통신 패킷 구조 분석을 위해 Amiccom A7125 모듈을 이용하여 무선 키보드의 유효한 신호를 수신한 후, 패킷 구조를 분석하였다. 무선 키보드의 페이로드 암호화 방식을 분석하고, 해당 장비의 주소 값을 획득하여 입력된 키를 분석할 수 있다는 것을 발표하였다[2].

2015년 발표된 KeySweeper는 아두이노 보드와 GSM 통신이 가능한 모듈을 이용하여 공격자가 대상 장비 근처에 없어도 무선 키보드 분석이 가능한 장비를 구현하였다. 이 장비는 아두이노 보드와 2.4 GHz 무선 키보드의 송수신 모듈인 Nordic 사의 nRF24L01+칩(chip)과 GSM 통신이 가능한 Adafruit FONA 칩(chip)을 사용하여 무선 키보드 신호를 수신한 후, SMS로 키 정보를 전송할 수 있는 장비이다. 해당 장비가 PC와 연결되어 있지 않아도 상용 전원과 배터리 전원을 이용하여 무선 키보드의 정보를 수신할 수 있어, 원거리에서도 장시간 사용 가능한 장점이 있다. 하지만 아두이노 보드의 메모리 용량 제한으로 무선 키보드 분석만 가능하다는 단점이 존재한다[4].

최근에 발표된 MouseJack 프로젝트에서는 AES 암호화 무선 키보드도 조작할 수 있는 시스템을 구현하였다. 무선 마우스가 암호화되지 않은 약점을 이용하여 무선 마우스의 통신 패킷을 분석하고, 상대방의 USB 동글 수신기와 공격자의 송신모듈을 강제 동기화시킴으로써 원하는 키를 입력하여 조작할 수 있는 시스템을 구현하였다[5].

본 논문에서는 기존 보고된 연구들의 내용을 검증하기 위해 무선 입력장치 중 가장 보편적으로 사용되는 2.4 GHz 무선 키보드와 무선 마우스의 전자파 신호를 분석하여 입력되는 정보를 확인하고, 임의의 신호를 송신하여 상대방 PC를 조작할 수 있는 시스템을 구현하였다.

해당 시스템은 소프트웨어 라디오 범용 하드웨어인

그림 1. USRP N200 장비
Fig. 1. USRP N200 equipment.

USRP N200 장비와 오픈 소스 소프트웨어 라디오 개발 툴킷인 GNU Radio 패키지를 사용하여 구현하였다. USRP 장비는 ADC, DAC, DUC, DDC로 구성되어 있으며, RF 신호를 송수신하고, 기저 대역의 신호를 IF 대역 또는 RF 대역으로 변환하거나, 반대로 RF 또는 IF 대역의 신호를 기저 대역의 데이터로 변환하는 기능을 수행한다[7],[9]. USRP N200 장비의 형상은 그림 1과 같다.

GNU Radio는 신호 처리 블록을 제공하는 무료 소프트웨어 개발 툴로 저렴한 가격의 외부 RF 하드웨어와 프로세서를 이용하여 쉽게 소프트웨어 라디오를 구현할 수 있는 장비이다. GNU Radio는 주로 Python 언어로 작성되지만, 성능이 중요시되는 신호 처리 경로는 C++로 수행한다. 이로 인해 개발자는 간편하고 신속한 개발 환경에서 실시간 무선 처리 시스템을 구현할 수 있다[8].

Ⅱ. 무선 키보드/마우스 전자파 신호 분석

본 장에서는 Microsoft 사의 Wireless Comfort Desktop 5000 무선 키보드와 무선 마우스 제품에 대한 전자파 신호 분석 과정에 대해 설명한다. 무선 키보드와 무선 마우스의 분석 과정은 그림 2와 같이 주파수 영역 확인 단계, GFSK 복조 단계, 패킷 분석 단계, 입력 정보 확인 단계로 구성된다.

그림 2. 무선 키보드/마우스 신호 분석 단계
Fig. 2. Signal analysis step of wireless keyboard/mouse.

2-1 [1단계] 주파수 영역 확인

1단계에서는 분석 대상 무선 키보드와 무선 마우스의 통신 주파수 영역을 확인한다. 해당 장치의 통신 정보는 장치 뒷면에 있는 FCC ID(미국연방통신위원회 인증 고유 번호)를 통해 확인할 수 있다[10]. 시험 대상 무선 키보드와 무선 마우스는 2,403~2,480 MHz의 주파수 대역을 2 MHz의 대역폭으로 사용하고, GFSK 변조 기법을 사용하는 것을 확인할 수 있다. 또한, 각 장치별로 24개의 주파수 채널을 4개씩 묶어 총 6개의 부분집합이 사용되는 것을 확인하였다. 상세 정보는 표 1과 같다.

이를 참고하여 무선 키보드/마우스 누설 전자파 신호를 주파수 영역에서 측정한 결과는 그림 3과 같다. 수신 장비는 USRP N200과 송수신 모듈(UBX-40) 및 수신 안테나(ANT2400Y12-WR)로 구성하였고, GNU Radio S/W에서 제공하는 "WX GUI FFT Sink" 블록으로 해당 결과를 도시하였다. 확인 결과, 해당 장비는 2,480 MHz 채널을 사용하는 Subset B 장비인 것을 확인할 수 있었다.

2-2 [2단계] GFSK 복조

2단계에서는 1단계에서 필터링된 아날로그 신호를 GFSK 복조기법을 적용하여 디지털 신호로 변환하는 기능을 수행한다. GFSK 복조 기능은 GNU Radio S/W에서 제공하는 "GMSK Demod" 블록을 이용하여 구현하였다.

표 1. 무선 키보드/마우스 통신 주파수 채널
Table 1. Channel of wireless keyboard & mouse communication frequency.

Channel group	Channel	Frequency (MHz)	Channel group	Channel	Frequency (MHz)
Subset A	0	2,403	Subset D	12	2,405
	1	2,419		13	2,425
	2	2,478		14	2,444
	3	2,468		15	2,452
Subset B	4	2,429	Subset E	16	2,423
	5	2,450		17	2,446
	6	2,470		18	2,456
	7	2,480		19	2,474
Subset C	8	2,421	Subset F	20	2,417
	9	2,431		21	2,427
	10	2,472		22	2,448
	11	2,454		23	2,476

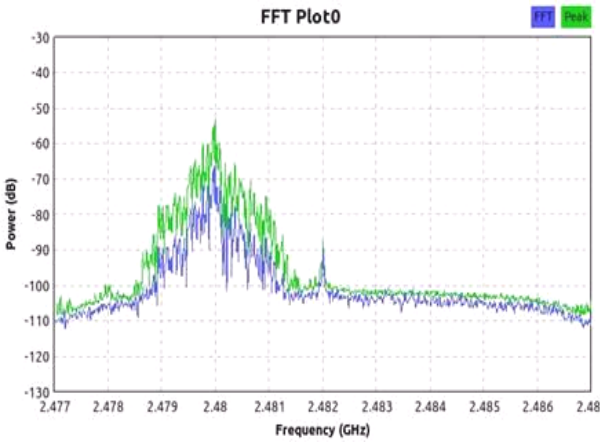

그림 3. 무선 키보드/마우스 RF 신호
Fig. 3. RF signal of the wireless keyboard/mouse.

2-3 [3단계] 패킷 분석

3단계에서는 복조된 디지털 신호를 바탕으로 무선 키보드와 무선 마우스 패킷을 분석한다. 해당 장비는 FCC ID 내부 형상 자료를 통해 Nordic 사의 nRF24L01 송수신 칩을 사용하는 것을 확인할 수 있다[10]. nRF24L01은 Enhanced ShockBurst™ 통신 프로토콜 엔진을 사용하는데, 이는 1~32 바이트(byte)의 가변적인 페이로드를 가진다. 상세 프로토콜 구성은 그림 4와 같다[6].

프리앰블(Preamble)은 패킷의 첫 번째 영역으로 , 주소(Address)의 첫 번째 비트값이 1이면 "10101010" 값을, 0이면 "01010101" 값을 자동으로 가진다. 주소 값은 무선 키보드와 무선 마우스의 고유 주소를 나타내며, 수신기에 유효한 패킷이 감지되었는지를 보증한다.

패킷 제어 필드(Packet Control Field)는 6 비트의 페이로드 길이(Payload length), 2 비트의 PID(Packet Identify),

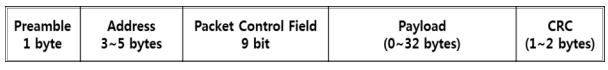

그림 4. Enhanced ShockBurst™ 패킷 구조
Fig. 4. Enhanced ShockBurst™ packet format.

Payload length 6 bit	PID 2 bit	NO_ACK 1bit

그림 5. 패킷 제어 필드 구조
Fig. 5. Packet control field format.

1 비트의 NO_ACK flag로 구성된다. 페이로드 길이 값은 0~32 바이트의 페이로드 길이를 결정하는데, “000000”일 경우 0 바이트(ACK 패킷)를 나타내고, “100000”일 경우 32 바이트를 나타낸다. PID는 수신한 패킷이 신규 패킷인지, 재전송 패킷인지를 감지하는데 사용된다. PID는 각 신규 패킷이 전송될 때마다 값이 증가되어 같은 페이로드가 MCU로 여러 번 전송되는 것을 막는다. NO_ACK는 자동 긍정 응답(Auto Acknowledgement) 기능을 제어한다. 상세 패킷 제어 필드 구성은 그림 5와 같다[6].

CRC(Cyclic Redundancy Check)값은 패킷의 오류를 검출하는 기법으로 주소, 패킷 제어 필드, 페이로드를 계산하여 정상 패킷 유무를 확인한다.

무선 키보드의 누설 전자파를 분석한 결과, 주소는 5 바이트로 구성되고, 마지막 바이트 값은 항상 “0xCD”임을 확인하였다. 페이로드 길이는 키 입력 시(Key Down)와 키 해제 시(Key Up)는 16 바이트, 키를 누르고 있을 경우(Key Idle)는 8 바이트로 구성된 것을 확인하였다[11].

키 입력 시 송신 패킷이 순차적으로 발생되고, 각 패킷마다 수신부에서 ACK 패킷을 전송하여 응답한다. 패킷이 발생할 때마다 각 PID 값이 증가되는 것을 확인할 수 있고, 패킷의 상세흐름은 그림 6과 같다.

무선 마우스의 경우, 주소 값은 키보드와 동일하게 5 바이트이지만, 마지막 바이트 값이 “0x66”으로 다른 것을 확인하였다. 페이로드 길이의 경우, 마우스 버튼 클릭 시는 19 바이트, 버튼을 누르고 있을 경우는 무선 키보드와 동일하게 8 바이트임을 확인하였다.

2-4 [4단계] 입력 정보 확인

4단계는 패킷의 페이로드를 분석하여 입력된 정보를 확인하는 단계이다. 무선 키보드의 키 입력 패킷을 분석한 결과, 그림 7과 같이 4바이트의 헤더(Header), 2바이트의 시퀀스 아이디(Sequence ID), 2바이트의 메타키 플래그(Metakey flags), 7바이트의 데이터, 1바이트의 검사합(Checksum)으로 구성되어 있는 것을 확인하였다[11]. 검사합 값은 전체 페이로드 데이터의 정확성을 검사하기 위한 용도로 사용된다.

앞서 소개한 KeyKerki v2.0 프로젝트를 통해 Microsoft 사 무선 키보드의 페이로드가 그림 8과 같이 암호화 되어 있는 것을 확인하였다. 전체 페이로드 중 시퀀스 아이디 영역에서 데이터 영역까지 11 바이트값이 패킷의 주소 값과 각각 XOR을 취해 암호화되어 있는 것을 확인하였다[2].

이를 참고하여 무선 키보드의 영소문자 ‘a’를 입력했을 때, 실제 장비에서 누설되는 신호를 측정하여 페이로드를

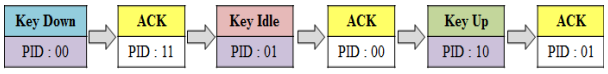

그림 6. 무선 키보드 키 입력 시 발생하는 패킷
Fig. 6. Packet generated when wireless keyboard key input.

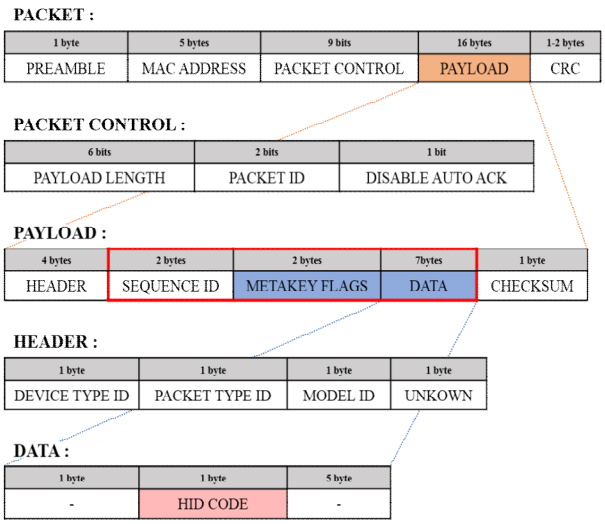

그림 7. 키 입력 패킷 페이로드 구조 분석
Fig. 7. Analysis of key down packet payload format.

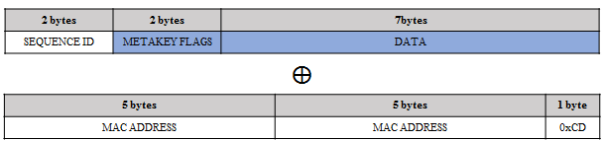

그림 8. 무선 키보드 페이로드 암호화 구조
Fig. 8. Format of wireless keyboard payload encryption.

구분		HEADER				SEQUENCE ID		METAKEY FLAGS		DATA							CHECKSUM
		4 bytes				2 bytes		2 bytes		7bytes							1 byte
Key Down (16 Bytes)	Packet	0A	78	09	01	80	29	2E	39	A8	C9	29	6D	39	A8	CD	A6
	MAC					CD	29	6D	39	A8	CD	29	6D	39	A8	CD	(~29 = D6)
	XOR Packet	0A	78	09	01	4D	0	43	0	0	4	0	0	0	0	0	A6
Key Idle (8 Bytes)	Packet	0A	38	09	01	80	29	6D									B1
	MAC					CD	29	6D									(~39 = C6)
	XOR Packet	0A	38	09	01	4D	0	0									B1
Key Up (16 Bytes)	Packet	0A	78	09	01	83	29	2E	39	A8	CD	29	6D	39	A8	CD	A1
	MAC					CD	29	6D	39	A8	CD	29	6D	39	A8	CD	(~29 = D6)
	XOR Packet	0A	78	09	01	4E	0	43	0	0	0	0	0	0	0	0	A1

그림 9. 무선 키보드 'a' 키 분석 결과
Fig. 9. Result of wireless keyboard key 'a' analysis.

분석해 보았다. 그 결과는 그림 9와 같다.

헤더 영역의 첫 번째 값은 장비 유형으로 무선 키보드의 경우는 "0x0A", 무선 마우스의 경우는 "0x08" 값을 가진다. 두 번째 값은 패킷 유형으로 키 입력 또는 해제 시는 "0x78" 값을, 키를 누르고 있을 시 "0x38" 값을, 마우스 click 시 "0x90" 값을 가진다. 세 번째 값은 모델 정보로 해당 무선 키보드는 "0x09", 무선 마우스는 "0x03" 값을 가진다. 시퀀스 아이디 영역은 카운터 역할을 하며, 새로운 키를 전송할 때마다 순차적으로 증가한다. 메타키 플래그 영역에는 Shift, Alt, Ctrl 키와 같은 특수키의 입력여부에 대한 정보가 포함되어 있다. 시험을 통해 획득한 메타키 플래그 값에 따른 키 정보는 표 2와 같다.

데이터 영역에는 입력된 키의 USB HID 코드 정보가 암호화되어 저장되어 있다. 복호화 결과 데이터 영역의 2번째 값만 유효한 정보를 가지며, 이 값은 입력된 키의 HID 코드 값과 일치한다(0x04='a').

검사합 값은 전체 페이로드 값을 검사하여 정상 유무를 확인하는 값이다. 복호화된 페이로드 값을 XOR하고 이 값과 주소의 4번째 값(0x29)의 역수를 XOR 취하여 구한다(0A ^ 78 ^ 09 ^ 01 ^ 4D ^ 43 ^ 04 ^ D6(~29) = A6).

표 2. 메타키 플래그 키 정보
Table 2. Key information of Metakey flags.

Metakey flags	키
0x4300	-
0x4301	Ctrl(left)
0x4302	Shift(left)
0x4304	Alt(left)
0x4305	Window

구분	HEADER				SEQUENCE ID		METAKEY FLAGS	DATA											CHECKSUM
	4 bytes				2 bytes		1 bytes	11 bytes											1 byte
Left click (19 Bytes)	08	90	03	01	2C	20	40	00	01	00	00	00	00	00	00	00	00	01	29 (2C^20^40^1^1^65)
Right click (19 Bytes)	08	90	03	01	C7	15	40	00	02	00	00	00	00	00	00	00	00	01	F4 (C7^15^40^2^1^65)

그림 10. 무선 마우스 페이로드 분석 결과
Fig. 10. Result of wireless mouse payload analysis.

무선 마우스의 경우, 페이로드 분석 결과, 무선 키보드와 다르게 주소값과 XOR을 이용한 암호화가 적용되어 있지 않은 것을 확인하였다. 버튼 클릭 시 누설되는 신호를 측정하여 분석한 결과는 그림 10과 같다. 분석 결과, 무선 마우스의 페이로드는 데이터 영역이 11 바이트로 이루어져 있고, 2번째 값이 "0x01"일 경우 좌 클릭, "0x02"일 경우 우 클릭이 실행된 것을 알 수 있다. 마우스를 움직일 경우에는 데이터 영역의 나머지 값들이 좌표에 따라 변하는 것을 확인하였다. 무선 마우스의 검사합 값은 헤더를 제외한 페이로드 값을 XOR하고, 이 값과 "0x65" 값을 XOR 취하여 구한다.

2-5 무선 키보드/마우스 전자파 신호 분석 결과 확인

앞에서 분석한 패킷 구조를 바탕으로 GNU Radio Companion 개발 툴을 이용하여 분석 소프트웨어를 구현하였다. 분석 대상 장비의 주소 값을 획득하면 무선 키보드의 입력 키 값과 무선 마우스의 클릭 여부를 실시간으로 확인할 수 있고, 다중 환경에서도 원하는 장비의 입력키를

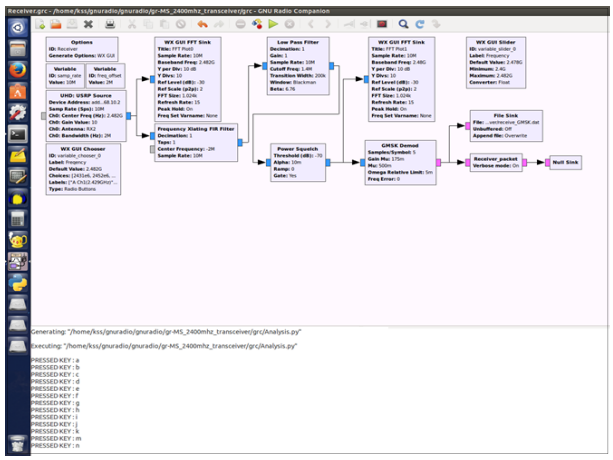

그림 11. GNU radio를 이용한 분석 소프트웨어 구현
Fig. 11. Implementation of GNU radio analysis software.

구분해서 확인할 수 있다. 구현한 시스템으로 무선 키보드 입력 키 분석 시 최대 7 m 이격된 거리에서 95 % 이상의 인식률을 검증할 수 있었다.

Ⅲ. 무선 키보드/마우스 전자파 신호 조작

본 장에서는 무선 키보드와 무선 마우스의 신호 복원을 통한 전자파 신호 조작 과정을 설명한다. 무선 키보드와 무선 마우스의 신호 조작 과정은 그림 12와 같이 주소 확인 단계, 송신 패킷 구성 단계, GFSK 변조 단계, RF 신호 송신 단계로 구성된다.

3-1 [1단계] Address 확인

1단계에서는 조작 대상 무선 키보드와 무선 마우스의 통신 주소를 확인한다. Ⅱ장의 분석 과정을 통해 파악한 각 장비들의 주소를 파일명으로 저장하여 각 무선 키보드를 구분한다.

3-2 [2단계] 송신 패킷 구성

2단계에서는 조작을 위한 송신 패킷을 구성한다. 무선 키보드의 경우, 조작 키는 아스키 코드 형태로 변환하여 처리하는데, 아스키 코드에 없는 특수 키와 주요 단축키의 경우도 조작할 수 있도록 그림 14와 같이 구현하였다.

해당 조작 키의 HID 코드 정보를 데이터 영역에 배치하고, 주소값과 XOR하여 암호화된 페이로드 및 검사합

그림 12. 무선 키보드/마우스 신호 조작 단계
Fig. 12. Step of wireless keyboard/mouse signal manipulate.

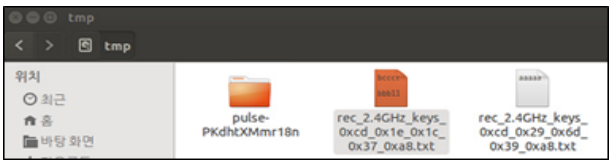

그림 13. 통신 주소 확인
Fig. 13. Confirmation of communication address.

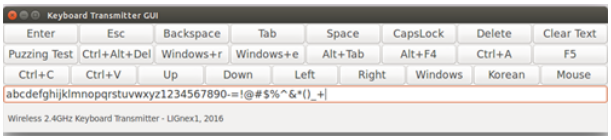

그림 14. 조작 신호 송신 프로그램
Fig. 14. Manipulate signal transmission program.

값을 생성한다. 패킷 제어 필드, CRC를 구성하여 패킷을 완성하고, 키 입력, 키 정지, 키 해제 각 패킷 사이에 적절한 지연시간을 추가하여 수신부에서 인식될 수 있도록 구현하였다. 무선 마우스는 좌클릭, 우클릭 패킷을 구성하여 각각 송신할 수 있도록 구현하였다.

3-3 [3단계] GFSK 변조

3단계에서는 2단계에서 구성된 패킷을 GFSK 변조기법을 사용하여 디지털 신호에서 아날로그 신호로 변환한다. GFSK 변조 기능은 GNU Radio Companion S/W에서 제공하는 “GMSK Mod” 블록을 이용하여 구현하였다.

3-4 [4단계] RF 신호 송신

4단계에서는 3단계에서 변환된 아날로그 신호를 송신 안테나를 통해 방사한다. 분석 단계에서 확인한 해당 무선키보드와 무선 마우스의 주파수 채널(2,403~2,480 MHz)로 변환하여 RF 신호로 송신한다.

3-5 무선 키보드/마우스 전자파 신호 조작 결과 확인

앞에서 재구성한 송신 패킷 구조를 바탕으로 조작 소프트웨어를 구현하였다. 조작 대상 장비의 주소 값과 통신 주파수를 설정하여 송신하면, 다중 환경에서도 원하는 정보를 각 해당 장비로 전송하여 조작할 수 있다. 조작 정확도를 향상시키기 위해 조작 정보를 파일로 저장하여 송신할 수 있도록 그림 15와 같이 구현하였다.

이를 이용하여 상대방 PC 내 임의의 폴더와 내부 파일을 삭제해 보았다. “실행” 창 단축키(Windows+r)를 입력하고, ‘cmd’를 입력하여 관리자 창을 실행한다. C 드라이브 내 임의의 폴더(Test_demo)를 삭제하는 명령어인(rd c:\Test_demo)를 수행하고, 그 결과를 확인하였다. 이와 유

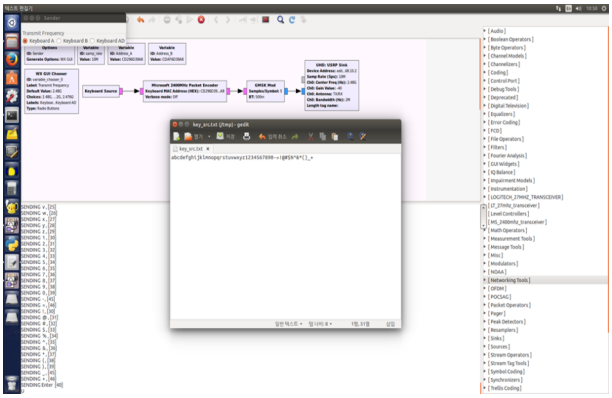

그림 15. 조작 소프트웨어 구현
Fig. 15. Implementation of manipulate software.

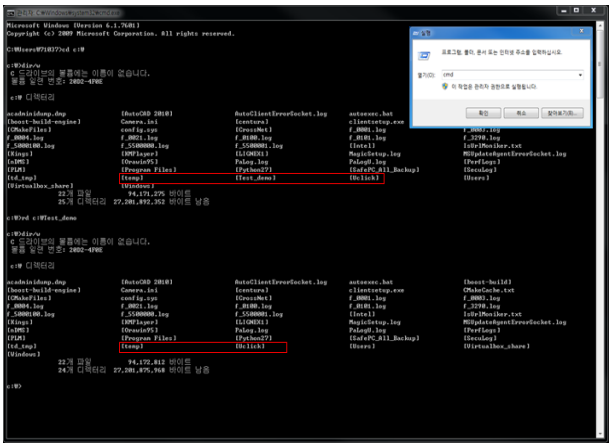

그림 16. 폴더 삭제 조작 결과
Fig. 16. Manipulate result of delete the folder.

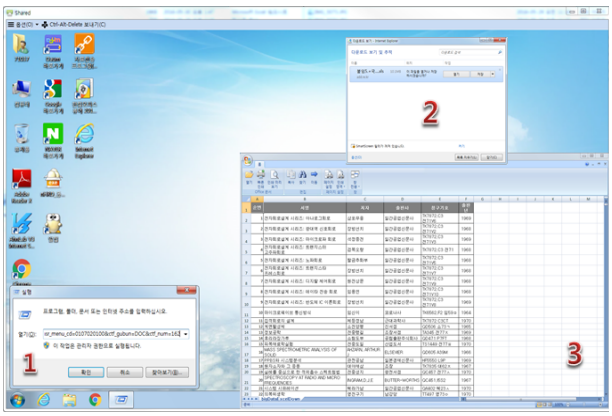

그림 17. 파일 다운로드 및 실행 결과
Fig. 17. Result of download and execute the file.

사하게 드라이브 전체를 삭제하거나, 포맷하는 것도 가능한 것을 시험을 통해 확인하였다.

인터넷이 연결된 PC의 경우, 조작을 통해 인터넷상의 임의 파일을 다운로드하여 저장하고 실행할 수 있다. “실행” 창 단축키(Windows+r)를 입력하고, 파일이 저장된 주소를 입력하면 해당 파일을 실행할 수 있다. 이를 이용하면 상대방 PC에 원하는 악성코드 파일을 실행하여 감염시킬 수 있다.

Ⅳ. 분석 및 조작 시스템 구축

본 장에서는 Ⅱ~Ⅲ장을 바탕으로 구축한 무선 키보드와 무선 마우스의 분석 및 조작 시스템의 성능에 대해 소개한다. 분석 및 조작 시스템 구성도는 그림 18과 같다.

4-1 시스템 분석 및 조작 성능

운용자 PC에서 사용 중인 무선 키보드의 누설 신호를 안테나를 통해 측정하고, 신호 분석기와 운용 컴퓨터를 이용하여 해당 장비의 주소값과 주파수 채널을 분석한다. 운용 컴퓨터와 조작신호 발생기를 이용하여 분석한 정보로 송신 패킷을 재구성하고, 안테나로 RF 신호를 송신하여 운용자 PC를 조작한다. 실제 구축한 분석 및 조작 시스템은 그림 19와 같다.

구축한 시스템의 분석 및 조작 성능을 측정해 본 결과는 다음과 같다. 분석 성능은 약 8 m 이격된 거리에서 100개 문자 입력 시 100 % 분석되는 것을 확인하였고, 조작 성능의 경우 약 30 m 이격된 독립된 방에서도 100개의 문자가 100 % 조작되는 것을 시험을 통해 확인하였다.

4-2 최대 조작 가능 거리 분석

조작 시스템의 최대 조작 가능 거리는 자유 공간 기본

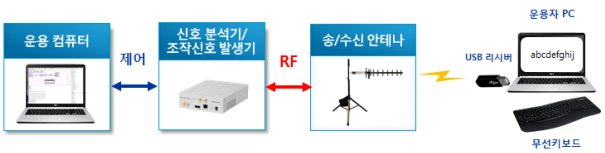

그림 18. 분석 및 조작 시스템 구성도
Fig. 18. Block diagram of analysis and manipulate system.

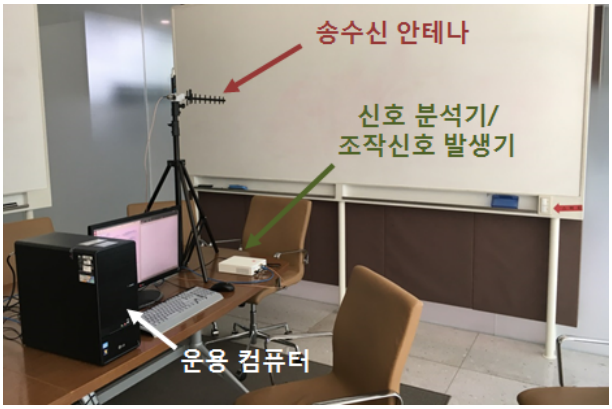

그림 19. 분석 및 조작 시스템
Fig. 19. Analysis and manipulate system.

전파 손실을 계산하는 식 (1)을 이용해 계산할 수 있다.

$$L_{df} = 10\log\left(\frac{4\pi df}{c}\right)^2 (\mathrm{dB}) \quad (1)$$

이 때, d는 거리, f는 주파수, c는 빛의 속도를 나타낸다. 무선 키보드의 경우, 최대 30 m 이격된 거리에서도 통신 가능한 것을 확인하였다. 식 (1)에 따르면 30 m 이격 시 자유공간에서 전파 손실은 약 69.87 dB이다. 무선 키보드의 송신 안테나 이득은 −2.03 dBi이고, 수신부의 안테나 이득은 −2.19 dBi 이므로, 송수신 칩의 최대 출력인 0 dBm으로 송신 시, 수신부에 입력되는 신호세기는 약 −74.09 dBm로 기타 손실이 약 7 dB 발생한 것으로 가정하면 수신기 수신감도인 −82 dBm를 만족함을 알 수 있다. 이를 이용하여 본 연구에서 구현한 시스템의 최대 조작 가능 거리를 계산해 보면, 1.5 km 이격 시 수신부에 입력되는 신호세기가 약 −81.04 dBm으로 방해물이 없는 야외일 경우, 약 1.5 km 이격된 거리에서도 조작이 가능할 것으로 판단된다. 무선 키보드와 조작신호 발생기 및 USB 수신기의 주요 RF 성능은 표 3과 같다.

표 3. 무선 키보드 및 조작 시스템 RF 성능
Table 3. RF specification of wireless keyboard and transmission system.

항 목	성 능
송신 주파수	2.48 GHz
조작신호 발생기 최대 송신 출력	20 dBm
무선 키보드 최대 송신 출력	0 dBm
송신 안테나 이득	12 dBi
무선 키보드 송신 안테나 이득	−2.03 dBi
무선 키보드 수신 안테나 이득	−2.19 dBi
기타 손실	약 7 dB
송수신 칩 수신 감도	−82 dBm

Ⅴ. 결 론

본 논문에서는 2.4 GHz 무선 키보드와 무선 마우스의 누설 전자파 신호를 분석하여 입력 키 정보를 확인하고, 임의의 신호를 송신하여 최대 1.5 km 이격된 거리에서 사용자 PC를 조작할 수 있는 시스템을 구현하였다. 해당 무선 키보드 무선 마우스 장비의 통신 프로토콜을 확인하고, 패킷 구조를 분석하여 장비 고유의 주소와 입력 키 정보를 획득하였고, 임의의 키를 송신하여 사용자 PC를 조작하였다. 이를 통하여 무선 키보드 및 무선 마우스를 사용하는 경우, 사용자가 입력하는 키 정보가 제 3자에 의해 스니핑(sniffing)될 수 있고, 또한 공격자에 의해 사용자 PC가 조작될 수 있는 위협이 존재하는 것을 확인하였다. 본 연구를 통해 일반 무선 키보드와 무선 마우스의 경우 보안에 취약한 것을 검증하였으므로 보안을 위해 유선 입력 장치 또는 블루투스 무선 키보드를 사용할 것을 권장한다.

References

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

[2] Schroeder, Moser, "Practical exploitation of modern wireless devices", CanSecWest, Mar. http://www.remote-exploit.org/content/keykeriki_v2_cansec_v1.1.pdf

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

[4] Samy Kamkar, "KeySweeper", 2015, http://samy.pl/key-

sweeper
[5] Mark Newlin, Bastille, "MouseJack", Feb. 2016, https://www.bastille.net/technical-details
[6] Semiconductor, Nordic, "nRF24L01+ single chip 2.4 GHz transceiver product specification", Jul. 2007, http://www.nordicsemi.com/eng/Products/2.4 GHz-RF/nRF24L01P
[7] Ettus USRP N200 Web page (https://www.ettus.com/product/details/UN200-KIT)
[8] GNU Radio Web page (http://gnuradio.org/redmine/projects/gnuradio/wiki)
[9] 박대현, 김영식, "USRP와 GNU Radio를 이용한 IEEE 802.15.4 물리 계층 소프트웨어 라디오 시스템 구현", 한국전자파학회논문지 21(11), pp. 1214-1219, 2010년 11월.
[10] FCC ID Application Database Web page (https://fccid.io)
[11] 김상수, 오승섭, 정창민, "GNURadio를 이용한 2.4 GHz 무선키보드 전자파 신호 분석", 2016 한국군사과학기술학회 종합학술대회, p. 208, 2016년 6월.
[12] 곽경훈, 신봉득, 박동욱, 어윤성, 오혁준, "USRP RIO SDR을 이용한 5G 밀리터리파 LTE-TDD HD 비디오 스트리밍 시스템 설계 및 구현", 한국전자파학회논문지, 27(5), pp. 445-453, 2016년 5월.

김 상 수

2008년 2월: 성균관대학교 정보통신공학부 (공학사)
2007년 12월～현재: LIG넥스원 선임연구원
[주 관심분야] 통신대역 신호분석

오 승 섭

1989년 2월: 조선대학교 전자공학과 (공학사)
1989년 1월～현재: LIG넥스원 수석연구원
[주 관심분야] 통신대역 신호분석 시스템, 고출력 RF 시스템

나 인 석

1993년 2월: 성균관대학교 전자공학과 (공학사)
2012년 8월: 아주대학교 전자공학과 (공학석사)
1993년 1월～현재: LIG넥스원 수석연구원
[주 관심분야] 전자전, 통신 시스템