*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.26, NO.1, Feb. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.1.81

# USRP와 GNU Radio를 이용한 27MHz 무선 키보드 전자파 신호 분석*

김 호 연,[1†] 심 보 연,[2] 박 애 선,[2] 한 동 국[2‡]
[1]유비벨록스, [2]국민대학교

# Analysis of 27MHz Wireless Keyboard Electromagnetic Signal Using USRP and GNU Radio*

Ho-Yeon Kim,[1†] Bo-Yeon Sim,[2] Ae-Sun Park,[2] Dong-Guk Han[2‡]
[1]UBIVELOX, [2]Kookmin University

요 약

현재 전자기기가 없는 현실을 상상하기 어려울 만큼 각종 전자기기들이 우리 생활 속 깊숙한 곳까지 파고들어와 있다. 그중 높은 편의성과 휴대성을 가진 스마트폰, 태블릿 PC, 무선 키보드와 같은 무선 전자기기의 사용이 급격히 증가하고 있다. 또한 전자기기에서 중요한 개인정보 및 금융정보의 사용이 증가함에 따라 이를 탈취하기 위한 다양한 공격들이 보고되고 있다. 이에 본 논문에서는 대표적인 무선기기 중 27MHz 무선 키보드를 대상으로 취약성을 분석하고, 무선 키보드 분석 환경을 구축하였다. 뿐만 아니라 실생활에서 무선 키보드 사용 시 존재하는 취약성에 대한 실험을 수행하였다. 실험 결과는 향후 무선기기의 취약성 및 안전성 검증에 활용될 것으로 사료된다.

ABSTRACT

Nowadays, electronic device is in a close relationship with human life. Above all, the use of wireless electronic devices such as smart phone, tablet pc, and wireless keyboard is increasing owing to the high convenience and portability. Furthermore, according to the increasing use of sensitive personal and financial information from the electronic device, various attacks for stealing information are being reported. In this paper we do an analysis of 27MHz wireless keyboard vulnerability and set up an analysis environment. Moreover, we make an experiment and show that there are real vulnerabilities. An experimental result will be used for safety analysis and vulnerability verification of wireless electronic devices.

**Keywords:** GNU Radio, USRP, 27MHz Wireless Keyboard, Electromagnetic, Side Channel Analysis

## I. 서 론

현재 스마트폰, 태블릿 PC, 무선 키보드와 같은 전자기기의 사용이 급격히 증가하고 있을 뿐만 아니라, 이러한 전자기기에서 중요한 개인정보 및 금융정보의 사용이 증가하고 있다. 특히 인터넷 사용의 보편화로 인해 인터넷 뱅킹에 대한 수요는 해가 지날수록 늘어나고 있으며, 전자기기의 입력 장치인 키보드의 사용도 함께 증가하였다. 이에 따라 키보드를 공격하여 인터넷 뱅킹 정보를 탈취하려는 시도가 증가하고 있다. 따라서 악의적인 사용자로부터 사용자 인증정보를 보호하기 위해 국내 은행에서는 인터넷 뱅킹 수행 시 키보드 보안 모듈을 설치 및 실행하도록 하고 있다.

Received(11. 24. 2015), Modified(01. 11. 2016), Accepted(01. 31. 2016)
* 이 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(NRF-2013R1A1A2A10062137)
† 주저자, kimhy@ubivelox.com
‡ 교신저자, christa@kookmin.ac.kr(Corresponding author)

하지만 사용자가 무선 키보드를 이용하여 인터넷 뱅킹을 수행할 경우 키보드 보안 모듈은 무선키보드의 무선 통신 구간에 관한 보호를 제공하지 않는다. 더욱이 [3]을 통해 L사 27MHz 무선 키보드의 숫자 및 영문 키의 물리적 취약성이 이미 보고된 바 있다. 또한 [4]에서는 [3]에서 보고된 취약성을 이용해 동일 키보드의 단축키, 특수 문자 등에도 유사한 취약성이 존재함을 보였으며, 거리에 따른 누출 신호를 분석하여 실제 누출 신호를 4m 이상에서 분석할 수 있음을 보였다. 이러한 취약성에도 불구하고 근래에 들어 무선 키보드 점유율은 점차 증가하고 있으며, Fig.1.과 Fig.2.와 같이 2007년에 비해 약 6배 증가하였다[1]. 또한 태블릿 PC, 인터넷 TV(IPTV) 등과 같은 인터넷 사용 환경이 다양해짐에 따라 무선 키보드에 대한 수요가 앞으로도 꾸준히 증가 할 것으로 전망된다[2].

따라서 본 논문은 안전한 무선 키보드 사용 환경 구성에 앞서 더 많은 취약점을 파악하기 위해 기존 27MHz 무선 키보드 전자파 신호의 취약점을 이용하여 [3,4]에서 분석된 L사 27MHz 무선 키보드의 추가 글쇠 분석에 성공하였음을 보이고, M사 27MHz 무선 키보드에 대한 취약성을 분석함으로써 27MHz 무선 키보드 사용의 위험성을 보인다. 또한 통합 설치 관리, 공인인증서 보안, 키보드 보안, 개인 PC 방화벽 그리고 보안로그의 보안 프로그램을 제공하는 제 1 금융권의 4개의 은행을 선정하여 실제 인터넷 뱅킹 수행 시, 사용자 인증정보 탈취가 가능함을 실험을 통해 보인다.

본 논문의 구성은 다음과 같다. 2장에서는 기존 보고되었던 27MHz 무선 키보드의 물리적 취약성 동향을 언급한 후, 3장에서는 [3,4]의 선행연구를 기반으로 좀 더 확장된 글쇠를 분석한 실험 결과를 소개한다. 또한 기존 연구 대상인 L사 27MHz 무선 키보드 제품 외에 M사 제품에 대한 분석 결과를 설명한다. 4장에서는 이러한 취약성을 기반으로 실제 무선 키보드 제품을 대상으로 인터넷 뱅킹 수행 시 사용자 인증정보 탈취가 가능함을 실험을 통해 보인다. 5장에서는 본 논문의 결론으로 마무리 짓는다.

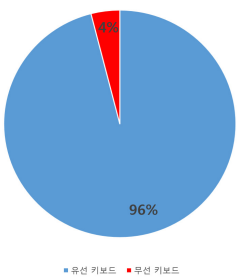



Fig. 1. market share 2007

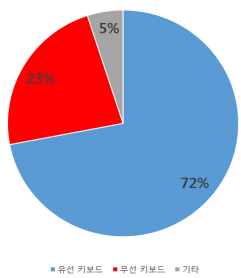



Fig. 2. market share 2014

## II. 기존 27MHz 무선 키보드 취약성 연구 동향

2011년 F$\ddot{a}$hnle은 27MHz L사 무선 키보드의 숫자 및 영문 키의 송·수신 신호를 분석하였다[3]. 본 장에서는 F$\ddot{a}$hnle에 의해 진행된 실험 및 환경에 대해 설명한다.

### 2.1 수신 신호 취약성 연구

L사 27MHz 무선 키보드 수신 신호 탐지 단계는 Fig.3.과 같이 5단계로 구성되며, 신호 탐지 시스템은 Fig.4.와 같이 구성된다. 즉, 사용자가 입력한 글쇠 정보가 아날로그 신호로 전송될 때, 공격자는 안테나를 이용해 이를 수신하고, PC에서 분석하여 글쇠 정보를 확인한다.

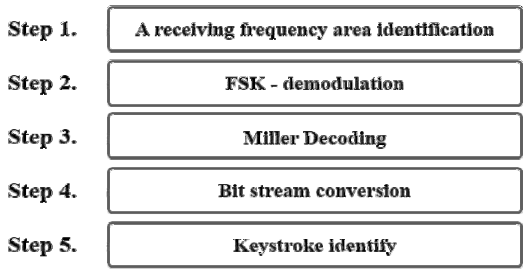



Fig. 3. Wireless Keyboard Signal Detection Phase

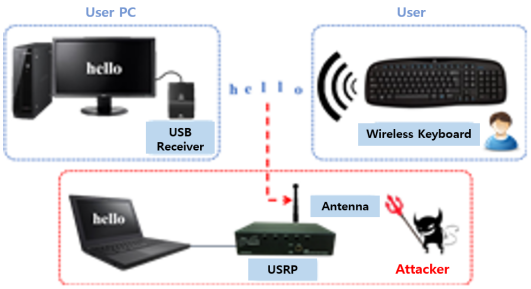



Fig. 4. Wireless Keyboard Signal Detection Environment

본 절에서는 수신 신호 분석에 대한 각 단계에 대해 간략히 언급한다. 보다 자세한 내용은 [3]에서 확인가능하다.

[1단계] 수신 주파수 영역 확인

[1단계]는 분석하고자하는 무선키보드의 주파수 대역을 파악하는 단계로, 주파수는 수신된 신호를 FFT 변환하여 파악 할 수 있다.

[2단계] FSK(Frequency Shift Keying) 복조

[2단계]에서는 [1단계]에서 확인된 주파수 대역의 신호를 수신하여 복조한다.

[3단계] 밀러 디코딩(Miller Decoding)

L사 무선 키보드는 밀러 디코딩 방식을 사용하여 통신한다. 신호 사이의 간격(=T)에 따라 밀러 디코딩을 적용하여 원하는 비트를 복구 할 수 있다. 밀러 디코딩은 다음의 Table 1.과 같이 수행된다.

[4단계] 신호의 비트 변환

[3단계]를 통해 T의 길이가 구분된 파형을 밀러 디코딩을 이용하여 비트 표현으로 변환 할 수 있다. Fig.5.는 신호 사이의 간격에 따라 수집한 신호를 비트로 표현한 그림이다. Table 2.는 Fig.5.의 네모 부분을 비트 스트림(Bit Stream)으로 나타낸 예제이다.

Table 1. Miller Decoding

| Signal period (=T) | | meaning |
|---|---|---|
| 1 | | identical with the previous bit |
| 2 | | next two bits are 01 |
| 1.5 | last bit | next bit |
| | 0 | '1' |
| | 1 | '00' |

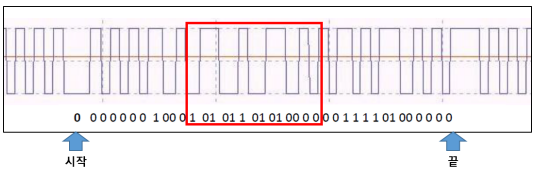



Fig. 5. Bit Stream

Table 2. Miller Decoding Example

| T | 1.5 | 2 | 2 | 1 | 2 | 2 | 1.5 | 1 | 1 |
|---|---|---|---|---|---|---|---|---|---|
| bit | 1 | 01 | 01 | 1 | 01 | 01 | 00 | 0 | 0 |

[5단계] 글쇠 확인

L사 27MHz 무선 키보드의 각 글쇠에 해당하는 비트 스트림을 모두 분석한 결과 L사 무선 키보드의 신호 패킷 구조는 Fig.6.과 같으며, DATA 영역을 통해 입력된 글쇠 정보를 확인한다.

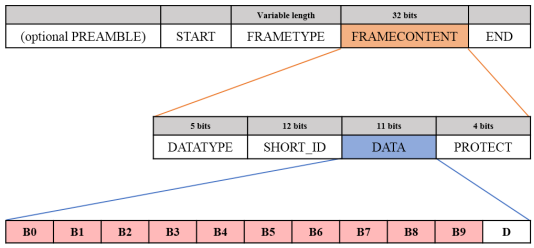



Fig. 6. 27MHz Wireless Keyboard Packet

## 2.2 송신 신호 취약성 연구

수신 신호의 분석을 통해 공격자가 사용자 컴퓨터에 임의의 정보를 사용자 모르게 입력 가능 하다.

본 절에서는 사용자 컴퓨터에 임의의 데이터를 전송하여 사용자 컴퓨터를 조작하는 단계에 대해 간략히 설명한다. 보다 자세한 내용은 [3]에서 확인 가능하다.

[1단계] 글쇠 입력

[1단계]에서는 삽입하고자 하는 L사 키보드의 글쇠 정보를 입력한다.

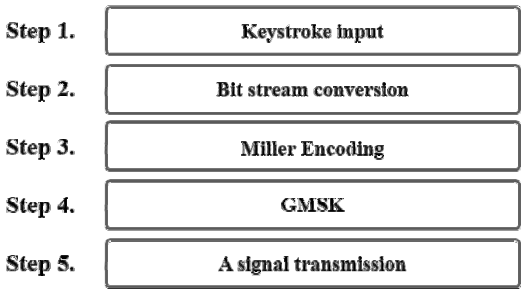



Fig. 7. L company Wireless Keyboard Signal Transmission Phase

〔2단계〕 비트 스트림 변환

〔2단계〕는 〔1단계〕에서 입력된 글쇠 정보를 이용하여 키보드 패킷에 맞추어 비트 스트림으로 표현하는 단계이다. 사전에 수신 신호 분석을 통해 L사 키보드의 각 글쇠 정보 및 패킷 정보를 분석해야 수행이 가능하다.

〔3단계〕 밀러 인코딩(Miller Encoding)

〔3단계〕에서는 〔2단계〕를 통해 표현된 비트들을 밀러 인코딩을 이용하여 디지털 신호로 나타낸다.

〔4단계〕 가우스 최소 편이 변조

〔4단계〕에서는 디지털 신호를 아날로그 신호 표현으로 변환한다.

〔5단계〕 수신 주파수 영역으로 신호 송신

마지막으로 〔5단계〕에서는 사용자 컴퓨터에 연결된 무선 키보드 리시버의 수신 주파수 영역으로 〔4단계〕에서 변환된 신호를 송신한다.

### 2.3 글쇠 추가 분석 결과

〔3〕에서는 제한된 범위의 키보드 송·수신 신호를 분석하였다. 그러나 높은 수준의 보안을 제공하기 위해 현재 인터넷 상에서는 대·소문자 영문, 특수문자로 구성된 비밀번호를 권장하고 있다. 따라서 이러한 글쇠는 추가적으로 분석되었다〔4〕.

- 수신 신호 글쇠 추가 분석

〔4〕에서는 Fig.9.와 같이 특수문자와 숫자패드 수신 신호를 추가 분석하였다. 이를 위해 우선 각 글쇠에 해당하는 아스키코드를 분석한 후, 프로그램에 추가하였다. 그리고 추가한 글쇠와 프로그램을 대응시켜 분석이 가능하도록 하였다. 이 때 특수문자는 기존 글쇠와 달리 2개 이상의 키보드 글쇠 조합으로 구성되어 있기 때문에 Shift Flag가 추가적으로 필요하다. 각 글쇠에 대한 추가 분석 결과에 대한 비트 스트림은 Table 3.으로 표현된다.

- 송신 신호 글쇠 추가 분석

본 논문에서는 Fig.9.와 같이 특수문자와 숫자패드 송신 신호 및 Table 4.와 같이 단축키 송신 신호를 추가 분석하였다. 이를 위해 먼저 추가 분석하고자 하는 글쇠에 해당하는 바이너리(binary) 표현

Table 3. Key Bit Stream

| Key | Bit Stream |
|---|---|
| 〔 | 0100110 |
| 〕 | 1100110 |
| ; | 1010001 |
| ‘ | 01100101 |
| , | 1100101 |
| . | 0010101 |
| / | 1010101 |
| ‘ | 1000100 |
| \ | 0111100 |
| f1 | 0100000 |
| f2 | 1100000 |
| f3 | 0010000 |
| f4 | 1010000 |
| f5 | 0110000 |
| f6 | 1110000 |
| f7 | 0001000 |
| f8 | 1001000 |
| f9 | 0101000 |
| … | … |

을 분석하였다. 그 후, 글쇠와 바이너리 표현을 대응시키는 프로그램을 추가하여 송신 신호를 추가 분석하였다. 수신 신호 글쇠 추가 분석과 동일하게 특수문자 송신을 위해 Shift Flag를 추가하였다.

Fig.8.의 GUI는 Fig.7. 1단계에 추가로 분석한 송신 신호를 추가하여 새로 구성하였다. 단축키는 송신하고자 하는 단축키를 Fig.8.의 GUI에서 클릭하여 송신하도록 구성하였다. 먼저 단축키에 사용되는 글쇠 바이너리 표현을 분석한 후, 이를 하나의 대푯값과 대응시킨다. 그리고 GUI의 단축키 목록에 이를 추가여 수행하면 Fig.7.의 단계를 따라 글쇠 신호가 송신된다. 즉, GUI에 나타난 Ctrl+C 단축키를 클릭하면 사용자 PC에서 복사하기를 수행 시킬 수 있다.

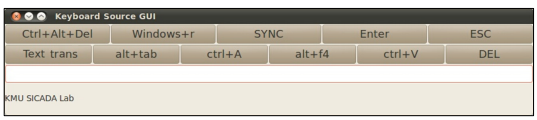



Fig. 8. Keyboard Signal Transmission GUI

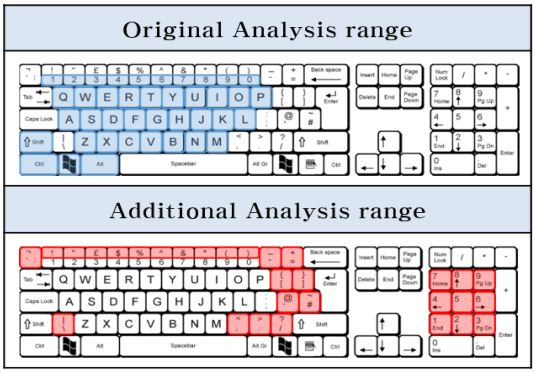



Fig. 9. Extended keyboard scope of analysis

Table 4. Extended keyboard shortcuts

| Keyboard Shortcuts | Description |
|---|---|
| Alt + Tab | Switch to another running program |
| Ctrl + A | Select all the items in the current window |
| Alt + F4 | Quit program |
| Ctrl + C(V) | Copy(Paste) |
| DEL | Delete |

## 2.4 거리에 따른 공격 가능성 실험 결과

L사 27MHz 무선 키보드를 대상으로 거리에 따른 송·수신 신호 분석 성공 여부를 판단하였다. 거리는 안테나의 성능에 따라 결정되며, Table 5.의 성능을 가진 범용 안테나를 사용하여 송·수신 신호 측정 가능 거리가 분석되었다[4]. 분석에 사용한 도터보드에 대한 자세한 설명은 [6,7]을 참고 하길 바란다.

수신 신호 분석 가능한 거리는 Table 7.과 같으며, 도터보드는 BasicRX와 LFRX 두 종류를 사용하였다. 도터보드는 분석하고자 하는 주파수 영역의 아날로그 신호를 디지털 신호로 변환해 주는 역할을 한다. 각 도터보드의 사양은 Table 6.과 같다. 두

Table 5. Antenna performance

| antenna | performance |
|---|---|
|  | 27MHz portable antenna 0.4M |
| | input : 10W |
| | impedance : 50Ω |
| | frequency range : 26 ~ 29MHz |
| | length : 40cm |

Table 6. Receiver Daughter Board

| Daughter Board | Frequency range |
|---|---|
| BasicRX | 1~250MHz |
| LFRX | 0~30MHz |

Table 7. Receiver signal distance

| Distance | BasicRX | LFRX |
|---|---|---|
| 0cm | ○ | ○ |
| 50cm | ○ | ○ |
| 100cm | ○ | ○ |
| 200cm | ○ | ○ |
| 300cm | ○ | ○ |
| 400cm | ○ | ○ |
| 450cm | △ | × |
| 500cm | × | × |

도터보드 모두 400cm 거리에서도 수신 신호 분석이 가능함을 확인하였다.

송신 신호 분석 가능한 거리는 Table 9.와 같으며, 도터보드는 BasicTX와 LFTX 두 종류를 사용하였다. 각 도터보드의 사양은 Table 8.과 같다. 두 도터보드 모두 500cm 거리에서도 송신 신호 분석이 가능하다.

분석 가능한 거리는 안테나의 성능 및 무선 통신이 이루어지는 환경에 따라 다를 것으로 예상된다. 실험적으로 무선 통신이 이루어지는 환경에 벽, 모니터 그리고 다른 무선기기가 있으면 분석 정확도가 떨어지는 것을 발견하였다.

Table 8. Transmitter Daughter Board

| Daughter Board | Frequency range |
|---|---|
| BasicTX | 1~250MHz |
| LFTX | 0~30MHz |

Table 9. transmitter signal distance

| Distance | BasicTX | LFTX |
|---|---|---|
| 0cm | ○ | ○ |
| 50cm | ○ | ○ |
| 100cm | ○ | ○ |
| 200cm | ○ | ○ |
| 300cm | ○ | ○ |
| 400cm | ○ | ○ |
| 500cm | ○ | ○ |
| 600cm | △ | △ |
| 650cm | × | × |

## III. 확장된 27MHz 무선 키보드 취약성 연구

본 논문에서는 M사 27MHz 무선 키보드의 한/영 글쇠를 추가적으로 분석했다. 또한 L사 27MHz 무선 키보드 분석 환경을 기반으로 M사 27MHz 무선 키보드에 대한 추가적인 실험 및 분석을 수행하였다. 따라서 본 장에서는 위 결과에 대해 설명한다.

### 3.1 L사 27MHz 무선 키보드 한/영 글쇠 분석

기존 L사 27MHz 무선 키보드 송신 신호 분석 환경에서는 알파벳 글자만 분석이 가능하였다. 본 논문에서는 이러한 제한적인 분석 환경을 한글 분석도 가능하도록 확장하였다. 따라서 L사 27MHz 무선 키보드에서 한/영 글쇠에 대한 송신 신호 분석을 수행하였다. Fig.8.에서 Text trans 버튼을 클릭하면 한글 입력과 영문 입력 신호에 대하여 구분되는 것을 확인할 수 있다.

결과적으로, 한/영 글쇠에 대한 추가 분석을 통해 국내 한글을 사용하는 환경에서도 공격자로부터의 위협이 존재함을 확인 하였다.

### 3.2 M사 27MHz 무선 키보드

본 절에서는 2장의 신호 분석 환경을 기반으로 M사 27MHz 무선 키보드를 분석하였다. 분석 단계는 Fig.3.과 동일하게 5단계로 구성하였고, 그 중 3단계 Decoding은 M사 환경에 맞게 새로 구성하였다.

〔1단계〕 수신 주파수 영역 확인

M사 27MHz 무선 키보드가 사용하는 주파수는 키보드 뒷면에 있는 FCC ID를 통해 확인 가능하며, FFT 파형을 통해서도 확인 가능하다. 본 논문에서는 Fig.10.과 같이 FFT 파형을 통해 27.195 MHz 근방의 주파수 대역을 수신하는 것을 확인하였다.

〔2단계〕 FSK 복조

〔1단계〕의 주파수 대역 신호를 수집하여 FSK 복조를 적용하여 Fig.11.과 같은 파형을 획득한다. 이후 고주파 제거를 통해 바이너리 표현으로 나타내기 용이하도록 정렬하면 Fig.12.의 파형을 얻을 수 있다.

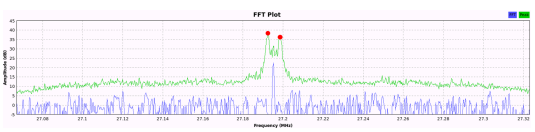



Fig. 10. M's Received frequency spectrum

M사 무선 키보드는 하나의 글쇠를 누른 경우에 대한 전체 파형 Fig.13.과 같이 세 부분으로 구분되어 나타나는 특징을 가지고 있다. 첫 번째 파형과 두 번째 파형은 동일한 파형으로 키보드의 글쇠에 따라 다르게 나타난다. 첫 번째와 두 번째 파형의 차이는 L사 키보드와 동일하게 글쇠의 down/up에 있다. 마지막 파형은 키보드의 글쇠 입력이 끝났음을 알리는 파형이다.

〔3단계〕 DDM 디코딩(DDM Decoding)

M사의 27MHz 무선 키보드 통신에서는 라인 부호화(Line coding) 기법으로 데이터 차이 변조(DDM, Data Difference Modulation)를 사용한다〔5〕. 따라서 수신 신호 분석 단계에서는 DDM 디코딩 방식을 통해 수신 신호를 바이너리 표현으로 나타낸다. 아래 Table 10.과 같이 신호 사이 간격(=T)을 기준으로 DDM 디코딩을 수행하므로 〔3단계〕에서는 FSK 복조 파형의 신호 사이 간격을 구분한다.

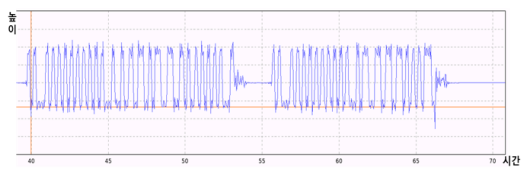



Fig. 11. M's FSK-Demodulation

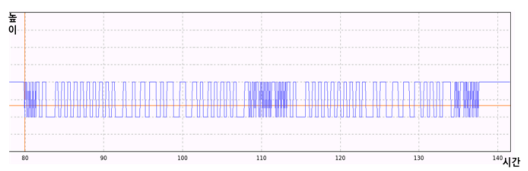



Fig. 12. Aligned FSK-Demodulation

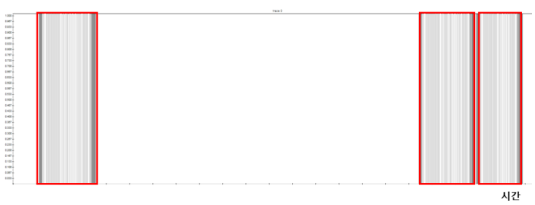



Fig. 13. Total receiver waveform of 1 key

Table 10. DDM Decoding

| Signal period (=T) | | meaning |
|---|---|---|
| 1 | | Contrary to the previous bit |
| 2 | last bit | next bit |
| | 0 | '00' |
| | 1 | '11' |
| 1.5 | last bit | next bit |
| | 0 | '01' |
| | 1 | '10' |

Table 11, Example of DDM Decoding

| T | last bit | 2 | 2 | 1 | 2 | 2 | 1.5 |
|---|---|---|---|---|---|---|---|
| bit | 0 | 00 | 00 | 1 | 11 | 11 | 10 |
| | 1 | 11 | 11 | 0 | 00 | 00 | 01 |

〔4단계〕 신호의 비트 변환

〔3단계〕를 통해 구분된 신호 사이 간격을 기준으로 DDM 디코딩을 수행하여 FSK 복조 파형을 비트 표현으로 변환한다.

Fig.13.의 세 번째 파형은 Table 12.와 같이 항상 동일한 비트 열으로 나타난다. 따라서 공격자는 세 번째 비트 열을 통해 글쇠 입력 상태가 마지막임을 알 수 있다.

〔5단계〕 글쇠 확인

키보드의 각 글쇠에 해당하는 비트를 분석한 결과 Fig.14.와 같이 M사 27MHz 무선 키보드의 신호 프레임 구조는 알파벳, 메타 글쇠 입력 경우로 나누어 분석되었다. 그리고 M사 27MHz 무선 키보드는 L사 27MHz 무선키보드와는 달리 connect 신호 내에 XOR KEY를 포함하여 통신에 사용한다.

포함된 XOR KEY는 송·수신 되는 알파벳 등 키보드에 입력되는 글쇠의 비트 스트림을 Xor 연산으로 안전하게 통신되도록 하는 역할을 한다.

M사의 무선 키보드는 XOR KEY가 고정적이지

Table 12. Last waveform bit stream

| Bit Stream |
|---|
| 010000000011110001010101 |

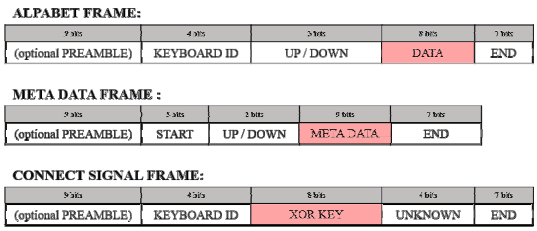



Fig. 14. M's 27MHz Wireless Keyboard Frame

않고 임의로 변경된다. 이러한 이유로 먼저 XOR KEY의 비트 스트림을 분석 한 후, 알파벳 a부터 차분(=Δ)을 계산하면 동일 XOR KEY에 대한 일정 차분을 분석 할 수 있다. 그런 후, 글쇠의 비트 스트림을 분석하면 글쇠 분석 결과의 정확도를 높일 수 있다.

Table 13. alphabet difference

| alphabet | Δ |
|---|---|
| b | ( 10000000, 0x80 ) |
| c | ( 01000000, 0x40 ) |
| d | ( 11000000, 0xC0 ) |
| e | ( 00110000, 0x30 ) |
| f | ( 10110000, 0xB0 ) |
| g | ( 01110000, 0x70 ) |
| h | ( 11110000, 0xF0 ) |
| i | ( 00010000, 0x10 ) |
| j | ( 10010000, 0x90 ) |
| k | ( 01010000, 0x50 ) |
| l | ( 11010000, 0xD0 ) |
| m | ( 00101000, 0x28 ) |
| n | ( 10101000, 0xA8 ) |
| o | ( 01101000, 0x68 ) |
| p | ( 11101000, 0xE8 ) |
| q | ( 00001000, 0x08 ) |
| r | ( 10001000, 0x88 ) |
| s | ( 01001000, 0x48 ) |
| t | ( 11001000, 0xC8 ) |
| u | ( 00111000, 0x38 ) |
| v | ( 10111000, 0xB8 ) |
| w | ( 01111000, 0x78 ) |
| x | ( 11111000, 0xF8 ) |
| y | ( 00011000, 0x18 ) |
| z | ( 10011000, 0x98 ) |

## IV. 실제 환경에서의 무선 키보드 취약성 검증

### 4.1 공격 가정

본 논문의 실험은 사용자가 국내 은행 인터넷 뱅킹 사용 시 27MHz 무선 키보드를 이용하여 사용자 인증정보를 입력 할 때 수행하였다. 또한 인증 수단으로 공인인증서와 보안 카드의 코드를 이용하는 경우 공격을 수행하였다.

공격 대상은 기본적으로 인터넷 뱅킹 수행 시 설치되는 통합 설치 관리, 공인인증서 보안, 키보드 보안, 개인 PC 방화벽 그리고 보안로그의 보안 프로그램을 제공하는 제 1 금융권의 4개의 은행을 선정하여 공격 가능성을 확인하였다.

### 4.2 공격 환경

무선 키보드 전자파 수신 신호 분석 환경은 Fig. 15.로 구성하였다. USRP(Universal Software Radio Peripheral)와 GNU Radio를 기반으로 SDR(Software Defined Radio) 시스템을 구축하였다. USRP 종류는 매우 다양하며, 본 논문에서는 Ettus사의 USRP1을 이용하여 환경을 구성하였다. PC에 Ubuntu, GNU Radio, GRC(GNU Radio Companion), UHD(USRP Hardware Driver)를 설치하고 공격 대상 키보드가 통신하는 주파수 영역을 송·수신할 수 있도록 실험환경을 구성하였다. 본 실험에서 사용자 컴퓨터 환경은 Window7을 지원하는 PC에 27MHz 무선 키보드를 연결한 환경에서 수행하였다. 그러나 본 실험은 키보드의 물리적 취약성을 이용한 실험이므로 사용자가 인터넷 뱅킹 사용 시 27Mhz 무선 키보드를 사용한다면 비밀 정보가 이와 유사한 방법으로 누출 될 수 있음이 명확하다.

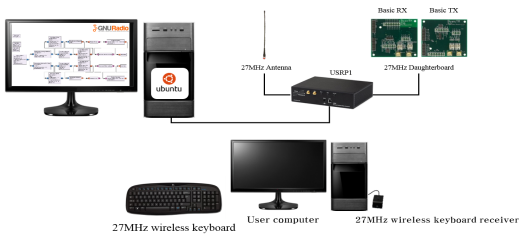



Fig. 15. Experiment environment

### 4.3 공격 과정

무선 키보드 전자파 수신 신호 분석 환경을 Fig. 15.로 구성한 후, 아래의 과정으로 공격을 수행하였다.

① 무선 키보드를 통해 입력된 입력 정보를 수신 신호 분석 과정을 통해 스니핑한 후, 텍스트 파일 형식으로 스니핑 정보를 저장한다.

② 저장된 스니핑 정보 파일을 Table 14.의 필터 키 워드를 이용하여 사용자가 수행하려는 인터넷 뱅킹 은행을 구분한다. 인터넷 뱅킹 처리 절차를 기반으로 Table 14.의 필터 키 워드 이후의 스니핑 정보를 모두 인증정보로 간주할 수 있다.

④ Fig.16.의 구분자를 이용하여 인터넷 뱅킹에 사용되는 각 단계의 인증정보를 구분한다.

Table 14. Filter keyword

| bank | filter keyword |
|---|---|
| A bank | "Internet Banking","A","ABank","ABank Internet Banking,"https://www.a_bank.com/" |
| B bank | "Internet Banking","B","BBank","BBank Internet Banking,"https://www.b_bank.com/" |
| C bank | "Internet Banking","C","CBank","CBank Internet Banking,"https://www.c_bank.com/" |
| D bank | "Internet Banking","D","DBank","DBank Internet Banking,"https://www.d_bank.com/" |

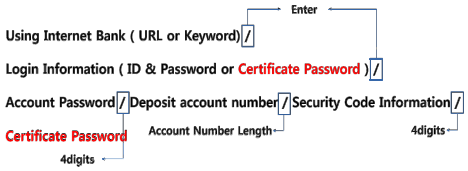



Fig. 16. User authentication method and separator

### 4.4 공격 결과

4개의 은행 인터넷 뱅킹에 대하여 무선 키보드 환

경에서 무선 키보드의 수신 신호 식별 가능성을 Table 15.로 나타내었다. 결과적으로 인터넷 뱅킹에 사용되는 인증정보는 스니핑이 가능하고, 이로부터 공격자가 각 인증단계에 사용되는 인증정보를 분석 할 수 있는 위협이 존재함을 확인하였다.

대표적으로 B 은행 인터넷 뱅킹 수행 시 입력하는 인증정보의 수신 신호에 대한 식별 공격을 수행하였다. 스니핑 정보로부터 Table 14.를 이용하여 사용자가 이용하는 은행정보를 Fig.17.로 나타내었다.

은행정보 다음의 스니핑 정보는 인터넷 뱅킹 인증 절차의 첫 번째 순서인 로그인 관련 정보이다. Fig. 18.에서 볼 수 있듯이 로그인 관련 정보를 획득할 수 있다.

로그인 정보 이후, 대부분의 인터넷 뱅킹 사용자들이 사용하는 계좌이체 입력 정보에 대해 스니핑을 수행하였다. 계좌이체 수행 시, 입력하는 계좌번호는 각 은행 또는 특성에 따라 길이가 다양하다, 이러한 이유로 입금 계좌번호는 마지막에 분석을 수행하였다.

먼저 인증서 암호와 보안카드 정보를 분석하였다. 인증서 암호는 로그인 시, 공인인증서 로그인을 수행할 때와 동일한 정보이다. 따라서 이와 같은 정보가 존재하는지 확인하여 분석 할 수 있다. 또는 보안카드 정보는 항상 4자리 숫자로 구성된다. 따라서 인증서 암호와 보안카드 정보는 계좌번호 및 계좌 비밀번호보다 먼저 분석이 가능하다.

Table 15. Sniffing possibility

| bank | keyboard security program | sniffing possibility |
|---|---|---|
| A bank | O | O |
| B bank | O | O |
| C bank | O | O |
| D bank | O | O |

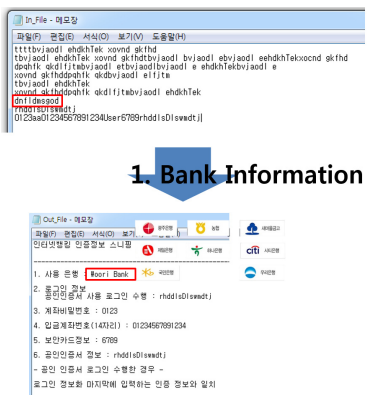



Fig. 17. bank information analysis

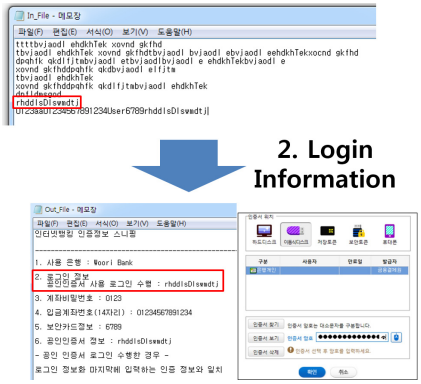



Fig. 18. login information analysis

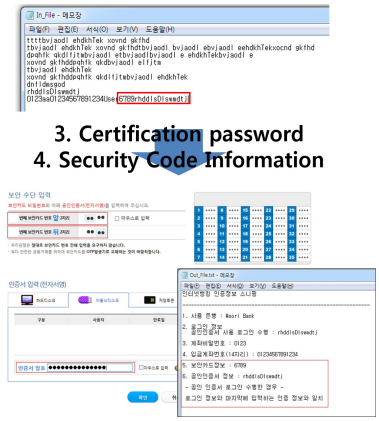



Fig. 19. Certification Password and Security Code

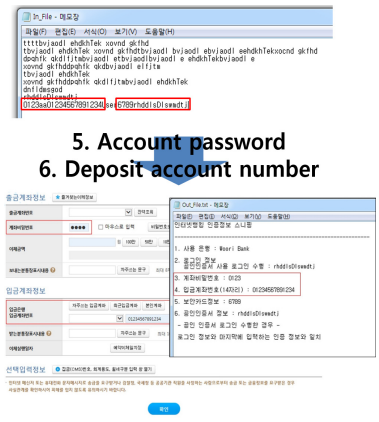



Fig. 20. Account password and Deposit Account Number

Fig.19.에서 인증서 암호와 보안카드 코드 정보를 분석한 후, 이 전에 입력된 스니핑 정보를 분석하면 Fig.20.과 같이 계좌 비밀번호와 입금 계좌번호를 분석 할 수 있다.

## V. 결 론

금융 및 개인정보 관련된 분야에서 전자기기의 사용이 증가함에 따라 이에 대한 위협도 함께 증가하고 있다. 그 중 전자기기에서 누출되는 전자파 신호를 통하여 금융 및 개인정보를 공격하는 위협에 대한 연구가 활발히 진행되고 있다.

본 논문에서는 일상생활에서 사용되는 무선 키보드의 전자파 누출 취약성을 분석하였다. 분석 대상으로는 27MHz 무선 키보드를 선정하였고 이에 대한 분석 환경을 구축하였다. 또한 이를 기반으로 무선 키보드 대표 회사인 L사 키보드의 확장 취약성 및 M사의 무선 키보드 송·수신 신호를 분석하였다.

이를 통하여 사용자가 입력하는 입력 글쇠가 스니핑 될 수 있는 취약성이 존재하는 것을 확인하였다. 또한 공격자가 임의의 글쇠 또는 단축키를 사용자의 PC에 전송하여 사용자 PC를 조작 할 수 있는 위협이 존재하는 것을 확인하였다. 더하여 인터넷 뱅킹을 수행할 때 악의적인 사용자로부터 사용자 인증정보를 보호하기 위해 국내 은행에서 키보드 보안 모듈을 설치 및 실행 하더라도 무선 키보드 사용 시 비밀 정보가 누출됨을 확인하였다.

무선 신호의 취약성에 대해 최근 연구된 대응 방안으로는 기존 무선 신호에 잡음을 섞어 통신하는 Jamming 방법이 있다[8]. 이는 잡음 패턴을 다양하게 하여 공격자가 전자파를 수집하여도 잡음과 중요 신호의 구분을 어렵게 만들어 정확한 분석을 어렵게 할 수 있다.

본 논문에서는 전자파를 이용한 공격이 유효함을 실험적으로 확인하였다. 또한 27MHz 무선 키보드 외에 다른 전자기기의 전자파 신호 분석을 통한 위협이 지속적으로 보고되고 있다. 따라서 전자기기에 대한 전자파 공격으로 실제 피해가 발생하기 전에 이에 대한 대책 마련이 시급할 것으로 예상된다.

## References


[1] danawa research. (2014). "Keyboard connection share, "http://prod.danawa.com/list/index.php?defSite=PC&cate1=861&cate2=881&cate3=0&cate4=0&mode=shot"

[2] J. Heo, "Take messy wires, IT home appliances wireless wide age," Korea Times, September 15, 2014.

[3] M, F$\ddot{a}$hnle 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, Feb. 2011.

[4] H.Y. Kim, S.J. Lee, A.S. Park and D.G. Han, "Enhanced Vulnerability Analysis on the Transmission module with electromagnetic leakage from wireless keyboard," CISC-S'14, pp.94, June. 2014.

[5] Microsoft Corporation, DATA PACKET TRANSMISSION FOR CHANNEL-SHARING COLLOCATED WIRELESS DEVICES, United States Patent, Mar. 2003.

[6] N. Manicka, GNU RADIO TESTBED, Spring, 2007.

[7] D. Shen, "Tutorial 4 : The USRP Board," University of Notre Dame, 2005.

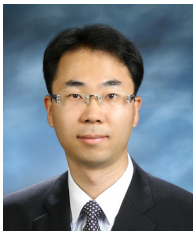
[8] Y. Suzuki, M. Masugi, K. Tajima and H. Yamane, "Countermeasures to Prevent Eavesdropping on Unintentional Emanations from Personal Computers," NTT Technical Review, Vol.6, No.10. Oct. 2008.

## 〈저자소개〉

김 호 연 (Ho-Yeon Kim) 정회원
2013년 2월: 국민대학교 수학과 졸업
2015년 2월: 국민대학교 금융정보보안학과 석사
2015년 3월~현재: 유비벨록스
〈관심분야〉 정보보호, 부채널 분석, 신호처리, 스마트 카드 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

박 애 선 (Ae-Sun 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



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