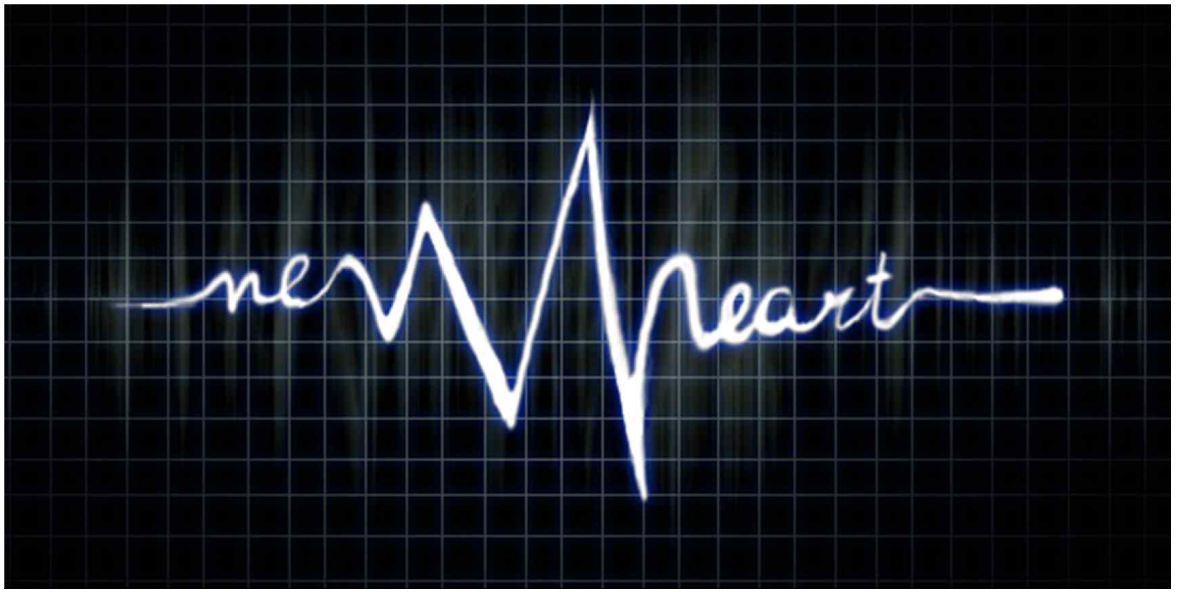
Wireless Keyboard(2.4 Ghz) Hacking



NewHeart

2012.01.01

남창현(hacktune)

hacktune@gmail.com

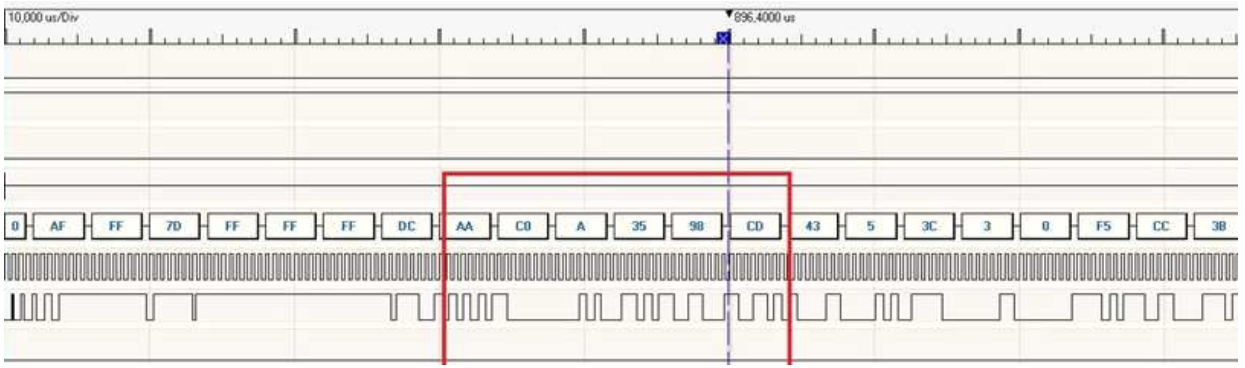
목차

1. 개념

무선 키보드가 USB 리시버와 송수신을 하는데, 이 신호의 패킷을 중간에 가로채는 것을 기본 원리로 한다.

전용 장비가 필요하며, ARM 코어를 기반으로 작동한다.

이 문서에서는 여러 가지 대역폭을 사용하는 키보드 중, 2.4Ghz 대역폭을 사용하는 Microsoft 社의 제품을 중점으로 논한다.



Device의 통신이 일어나는 Radio-Layer.

2. 원리 – 무선 패킷

오른쪽에 있는 그림이 2.4Ghz 대역폭을 사용하는 Microsoft 社의 무선 키보드의 패킷 구조이다. (무선 키보드 -> USB 리시버로 보내는 신호를 패킷화한 것.)

Key-Stroke가 일어날 때의 값은 위 패킷 구조중 HID코드를 포함한 CD 98 35 0A C0 부분에서 변화가 일어난다.

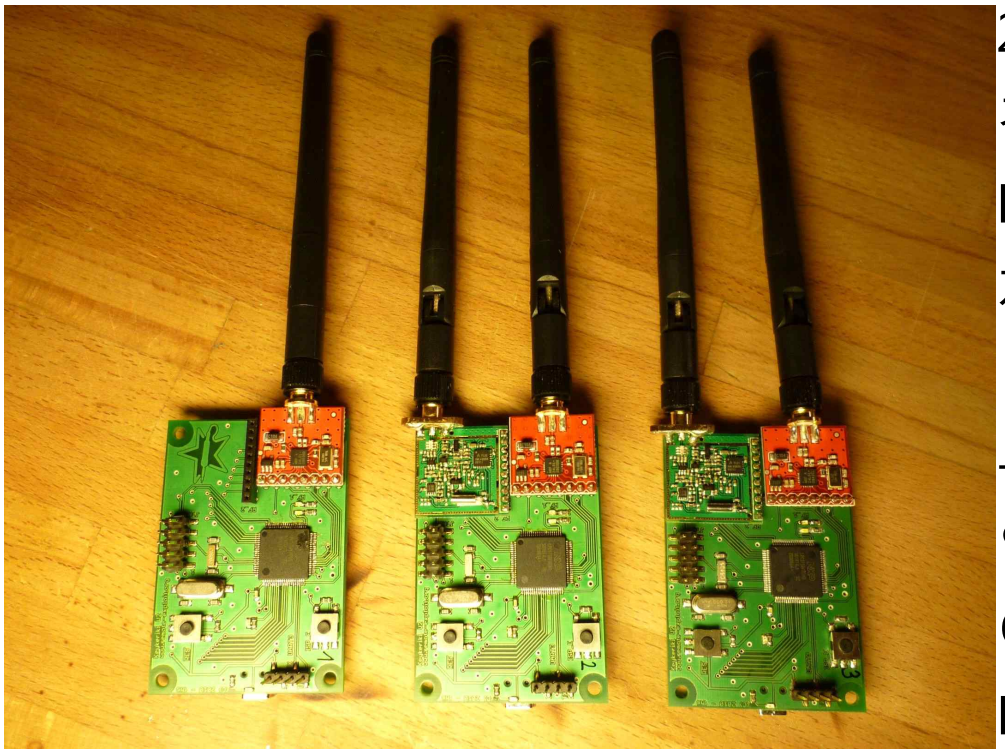
2. 원리 – 프로그램

Microsoft 社의 무선 키보드는 단방향 암호화가 아닌 양방향 암호화를 통해 암호화가 되어있다.

```
ctx->const_down= ctx->const_up= ~ctx->address[1];
...
cksum= ctx->const_down;
for(i=0;i<4;i++){
ctx->c_down[i] = ctx->p_down[i];
cksum^=ctx->p_down[i];}
for(i=4;i<15;i++){
cksum^= ctx->p_down[i];
ctx->c_down[i] = ctx->p_down[i] ^ ctx->secret[i % 5];}
ctx->c_down[15] = cksum;
```

반복문을 통해 패킷에서 Key-Stroke를 검출해 낼 수 있다.

2. 원리 – 하드웨어(디바이스)



2.4Ghz의 대역폭에서 무선 신호를 검출하고, 이를 패킷화 시켜서 PC로 전송시키거나 자체 Display에 출력시켜주는 장치.

무선 신호를 패킷으로 바꾸어주는 일련의 과정(fetch decode execute)이 일어나야 함으로, Device에 ARM Processor를 장착한다.

2.4Ghz의 통신에 사용하는 칩으로는 NRF24L01+ 규격을 사용한다.

3. 시연

http://youtu.be/LgeNj34awCI

http://player.vimeo.com/video/4990390?title=0&byline=0&portrait=0

위에서 언급한 Hardware Device와 Software를 이용해 실제로 무선 키보드의 Sniffing을 시연하는 동영상이다.

4. 위험성과 한계 및 대응 방안

가장 먼저 생각해 볼 수 있는 것은, 키보드를 통한 정보 유출이다.
한때 PC방 등에서 성행한 키로거처럼, 사용자의 신상정보를 포함한 개인정보의 유출될 수 있다.
그리고 비단 키보드에 국한된 것이 아니고, 전파를 사용하여 무선 통신을 하는 어떠한 장치가 있다면, 그 패킷을 해석하고 다시 내보낼 수만 있으면 통신을 하는 장치를 마음대로 조종하는 일이 가능할 것이다.
한계로는, 일정 거리에서만 사용할 수 있으며, 무선 신호를 검출하고 이를 해석하고 내보내 주어야 하기 때문에 필연적으로 하드웨어가 필요하고, 이 정보를 USB를 통해 재전송하기 때문에 발각되기가 매우 쉽다.
(반경 10m이내 정도에서만 검출이 가능하기 때문)
대응 방안으로는 키보드의 제작단계에서부터 리시버와의 통신을 할 때 리시버와 동기화 후 상호간의 어떤 약속을 통한 단방향 암호화라든가, 통신하는 주파수 대역폭을 실시간으로 변조해 주거나, 아니면 패킷 데이터에 페이크 데이터를 섞는 방법을 통한 방법을 생각해 볼 수 있다.

5. 참조

KeyKeriki v2.0 – 2.4GHz

Team – Remote Exploit

http://www.remote-exploit.org/?page_id=602

무선 키보드, 크래킹당할 위험 크다!

http://www.boannews.com/media/view.asp?idx=8355&kind=0