OWASP

Open Web Application Security Project

电磁波突破物理隔离技术

OWASP
Open Web Application Security Project

个人介绍

姓名：付鹏飞

研究方向：IOT，智能硬件，路由器0day。PC声卡，键盘，网卡等PC硬件的安全研究

爱好：DIY，制作各种机器人

参加了国际智能机器鼠大赛，获得国内最好的成绩。

OWASP
Open Web Application Security Project

个人介绍

姓名：孙浩然

曾为甲方公司进行src漏洞审核工作。多次参与国家重大会议安全保障工作，具有丰富的渗透测试经验。对App加固方式有深入研究。

研究方向：渗透测试、Android APP安全与逆向、Android恶意代码分析、机器学习与漏洞挖掘。

OWASP
Open Web Application Security Project

CONTENTS

OWASP

Open Web Application Security Project

1

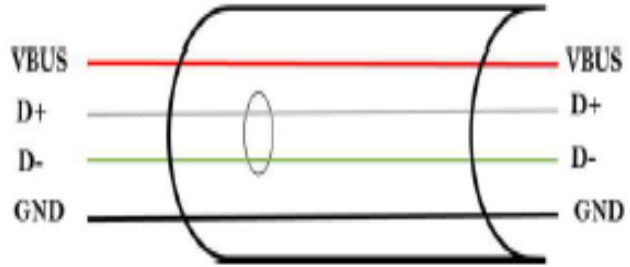
基本原理

电脑电磁波的产生

OWASP
Open Web Application Security Project

USBee？

无需USB插口




```
FILE *fp;
unsigned long  *buffer;
fp=fopen("\\.\PHYSICALDRIVE1","wb");
buffer=(unsigned long  *)malloc(4*100);
fill_buffer_freq(buffer,101,200);
fwrite(buffer,4,100,fp);
fclose(fp);
```

USB协议的NRZI编码方式

OWASP
Open Web Application
Security Project

接收设备

虚拟信道
（电磁辐射）

发射设备

通过利用电脑本身的电磁信号进行一个虚拟信道的搭建保证
了信息采集的隐秘性

OWASP

Open Web Application Security Project

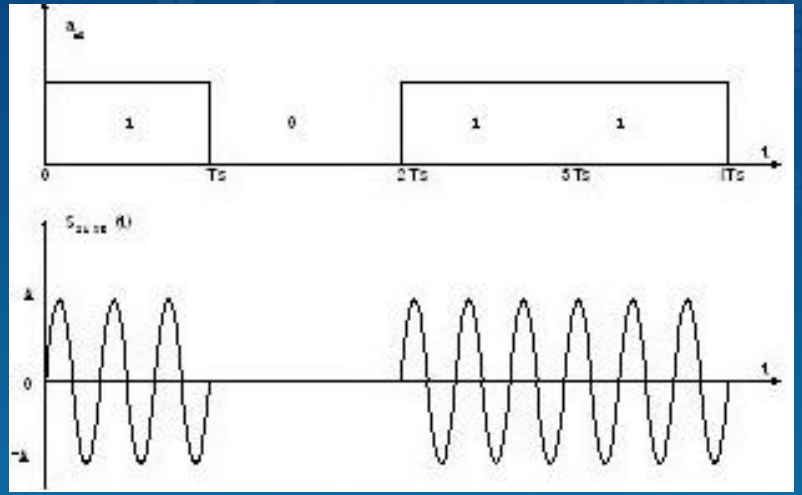
2

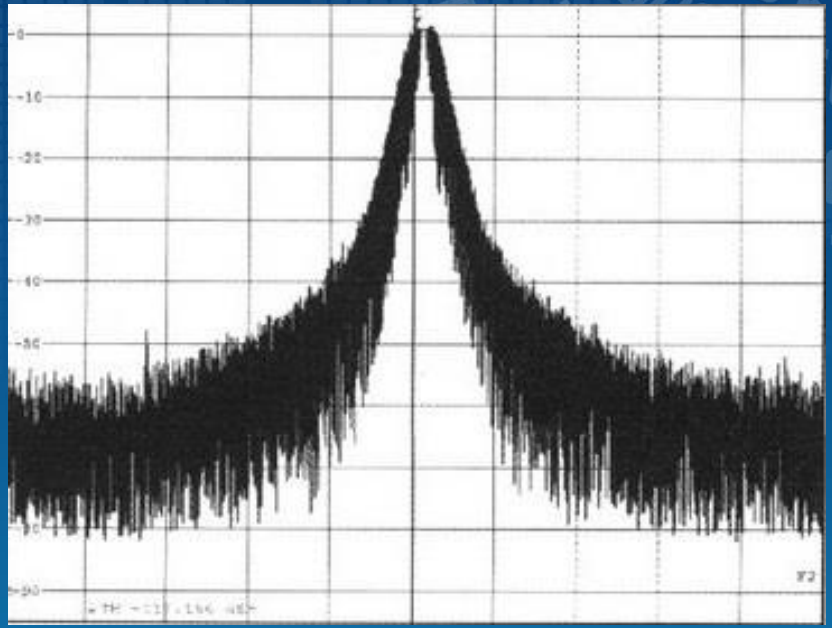
利用方法

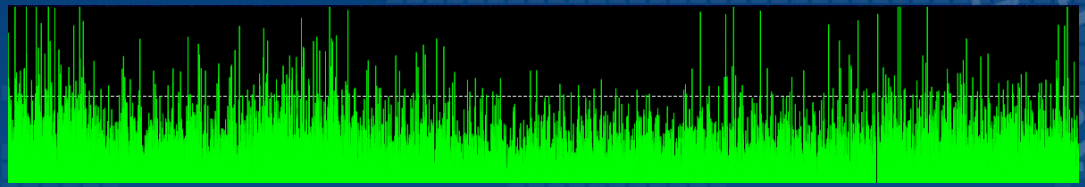
信号采集及利用的方法

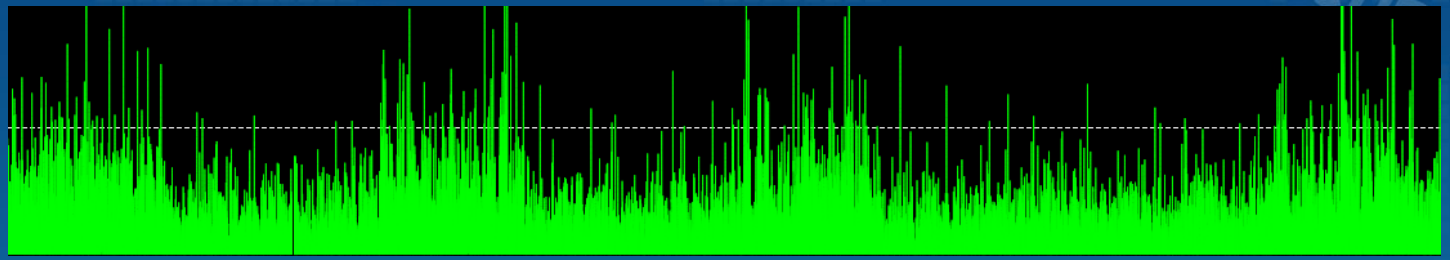
OWASP
Open Web Application Security Project

ASK调制





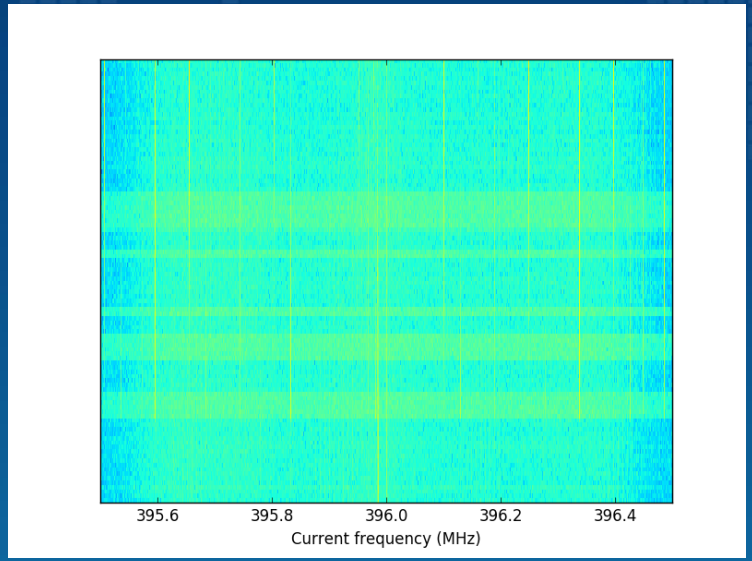


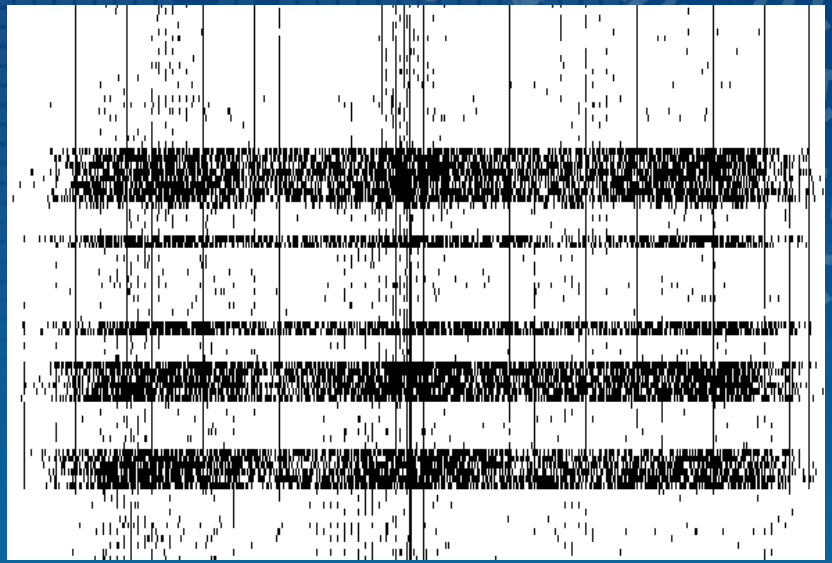


调制结果

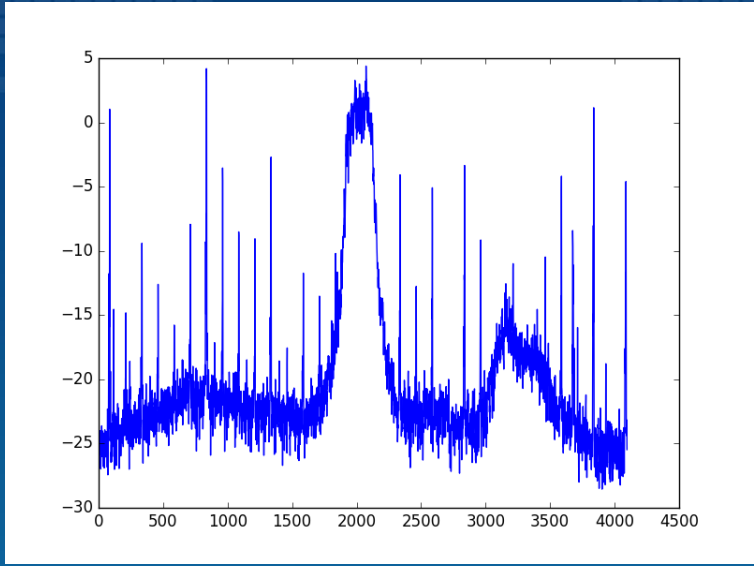
OWASP
Open Web Application
Security Project

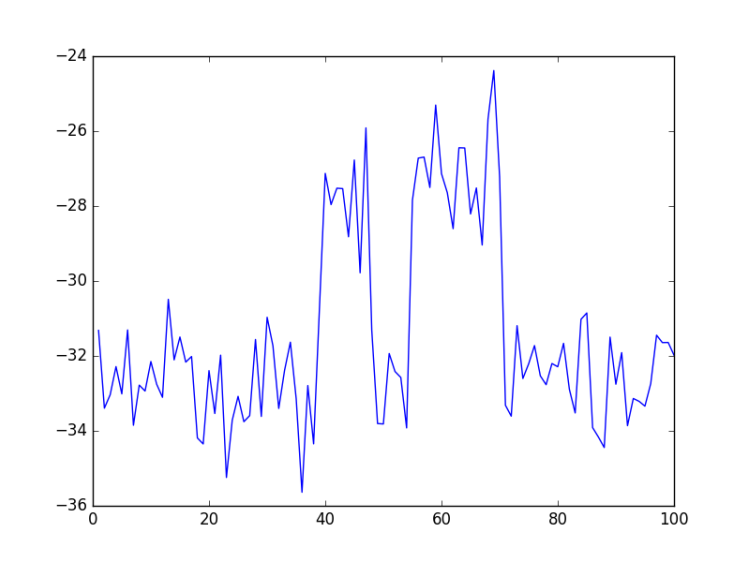
解调结果



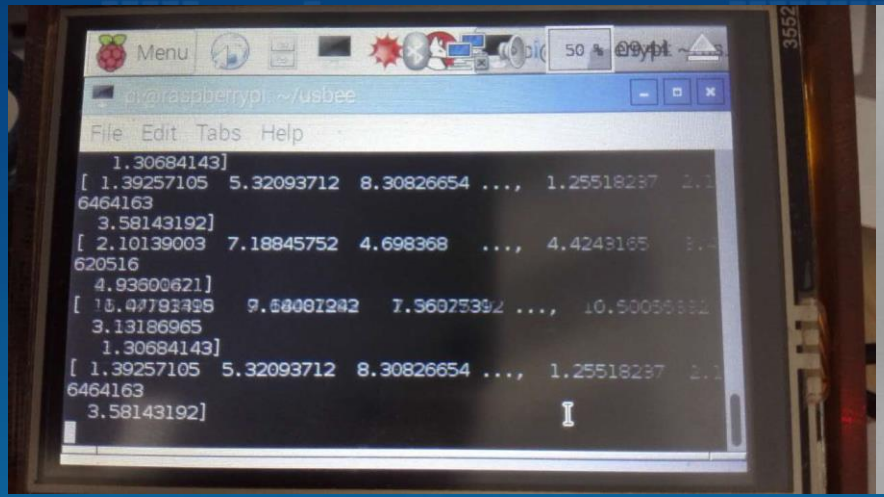


111 101000 101110 111


5
0
−5
−10
−15
−20
−25
−30
0
500
1000
1500
2000
2500
3000
3500
4000
4500


−24
−26
−28
−30
−32
−34
−36
0
20
40
60
80
100

实时数据的分析


Menu
File Edit Tabs Help
1.30684143]
[1.39257105 5.32093712 8.30826654 ..., 1.25518237
6464163
3.58143192]
[2.10139003 7.18845752 4.698368 ..., 4.4243165
620516
4.93600621]
3.13186965
1.30684143]
[1.39257105 5.32093712 8.30826654 ..., 1.25518237
6464163
3.58143192]

实物图设计

OWASP

Open Web Application Security Project

3

设计方案

电磁泄露利用的整体方案

OWASP

Open Web Application Security Project

调制

受‘污染’设备利用USB总线特点，写入数据产生特定频段的电磁辐射

通过RTL.SDR进行信号的的采集和传输

解调

微型手持仪使用卡片式微型电脑，应用软件无线电的方法进行信号的解调

微型手持电脑

主要进行无线电信号分析和信号的采集

无线电接收器

收集电磁信号并进行前段增益和滤波等

受到”污染”的电脑

通过特殊程序编码发送需要的数据，通过电磁辐射发送

OWASP

Open Web Application Security Project

其他类型技术

介绍其他类似电磁波技术的信息泄露技术

声卡产生超声波技术


```
70  sound proc near
71      push ax
72      push bx
73      push cx
74      push dx
75      push di
76      mov bx,3000
77      mov al,0b6h
78      out 43h,al
79      mov dx,12h
80      mov ax,34dch
81      div di
82      out 42h,al
83      mov al,ah
84      out 42h,al
85      in al,61h
86      mov ah,al
87      or al,3
88      out 61h,al
89  delay:mov cx,0ffffh
90  dl10ms:loop dl10ms
91      dec bx
92      jnz delay
93      mov al,ah
94      out 61h,al
95      pop di
96      pop dx
97      pop cx
98      pop bx
99      pop ax
00      ret
01  sound endp
02  code ends
```

声卡产生超声波技术