DEFCON

百度安全
有AI更安全

反间谍计划：
自建基站与数据嗅探方法论



百度安全实验室 小灰灰

关于我



百度安全实验室 高级安全研究员

研究领域：IoT安全/AI安全/无人车安全

多次破解硬件设备

之前负责：

- BSRC、应急处置、0day分析
- 百度产品 安全评估
- 百度安全监控体系建设

大纲

- 联网IOT设备测试目的、测试方法
- 如何实现自动附着、MITM流量
- 如何搭建LTE测试基站
- 漏洞实例介绍
- 其他测试方法

目的及守则

- 目的：
  - 了解GSM的安全风险
  - 通过搭建测试基站，辅助IOT设备安全漏洞挖掘
  - 增强产品安全性
- 测试守则：
  - 严格遵守相关法律，不影响正常信道通信
    - 屏蔽器中/封闭地下室操作
    - 如实在条件限制，需**调低功率/衰减器直连**



测试目的

- 控制流量
  - 获取流量（敏感数据、接口分析、固件分析、远控&升级分析）
  - 修改流量（MITM中间人、DNS欺骗）
  - 访问（运营商侧interface访问设备 存在漏洞的端口）
- 控制短信
  - 短信下发指令（场景很少）

漏洞挖掘方法

- 获取云端接口
  - 攻击云端web漏洞（注入、升级FTP）
  - client重放、越权
- 获取通讯数据
  - 辅助理解流程
  - 加密信道：辅助分析获取加密密钥，获得加解密能力
  - 获取密码、token、session等关键key
  - 获取固件更新链接
- 修改数据
  - 修改配置参数、替换固件
  - 注入恶意代码，例如浏览器RCE
- 访问监听端口
  - 自身提供管理服务，例如telnet、adb、ssh
  - 分析监听bin，协议模拟/命令注入/溢出攻击
- 协议、基带Fuzz

看起来 基站辅助
测试是强需求
处处需要

有时是攻击前

有时在攻击中

两种测试基站需求场景

- 攻击前
  - 不需要任意client自动连入我们的攻击基站
  - 只需要目标client能够连入
  - 实现： 搭建GSM和LTE测试基站，特殊sim卡写卡实现认证
- 攻击中
  - 需要任意client自动从现网切换到我们的攻击基站
  - GSM网络存在认证问题，可能实现
  - 实现：搭建GSM攻击基站，通过强制小区重选 连接到攻击基站

我们先来实现难的-攻击中基站

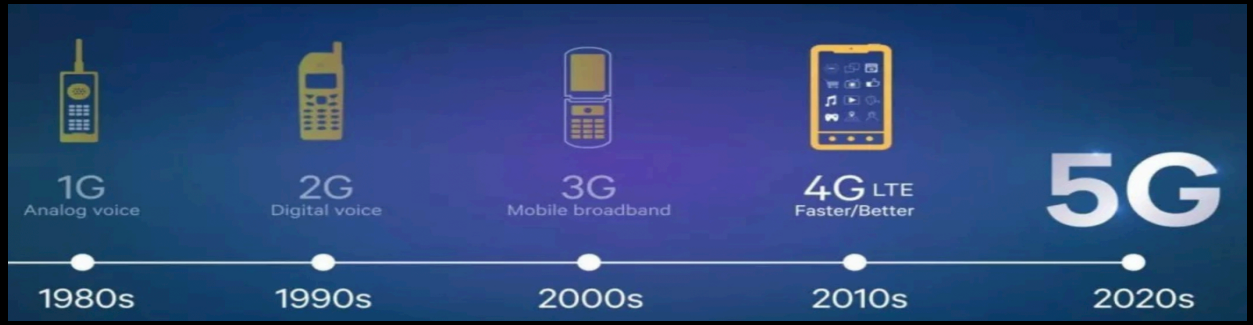
- 自动连入攻击基站，并且控制流量
- 看下腾讯KEEN LAB 攻击宝马车机系统的case

KEEN security lab

Remote Code Execution. After we implemented a stable GSM network using universal software radio peripheral (USRP) and OpenBTS, all the traffic from ConnectedDrive service were captured, and due to some insecure implementations of ConnectedDrive service in NBT, we also succeeded in intercepting network traffic from ConnectedDrive Service. After that, we were free to find the bugs in "DevCtrlBrowser_Bon". Then we exploited a memory corruption bug in "DevCtrlBrowser_Bon" and achieved remote code execution in the head unit with browser privilege. In the end, by leveraging the vulnerability mentioned earlier, we achieved root privilege escalation and got a remote root shell from NBT through a different path than 2.1.1.

G -- Generation

- 1G 模拟信号 大哥大
- 2G GSM/CDMA
- 3G 3GPP WCDMA/CDMA2000
- 4G LTE
- 5G 高速率 低延迟 切片 万物互联



	中国移动通信 CHINA MOBILE	China unicom 中国联通	中国电信 CHINA TELECOM
2G	GSM	GSM	CDMA 1X
3G	TD-SCDMA	WCDMA	CDMA2000
4G	TDD-LTE	TDD-LTE FDD-LTE	TDD-LTE FDD-LTE

泡泡网 PCPOP.COM

每个时代都有不同看法

2G ⬇



【超感人，老师时代】.txt

3G ⬇



【那些我们追过的老师】.jpg

4G ⬇



【老师的科学课】.avi

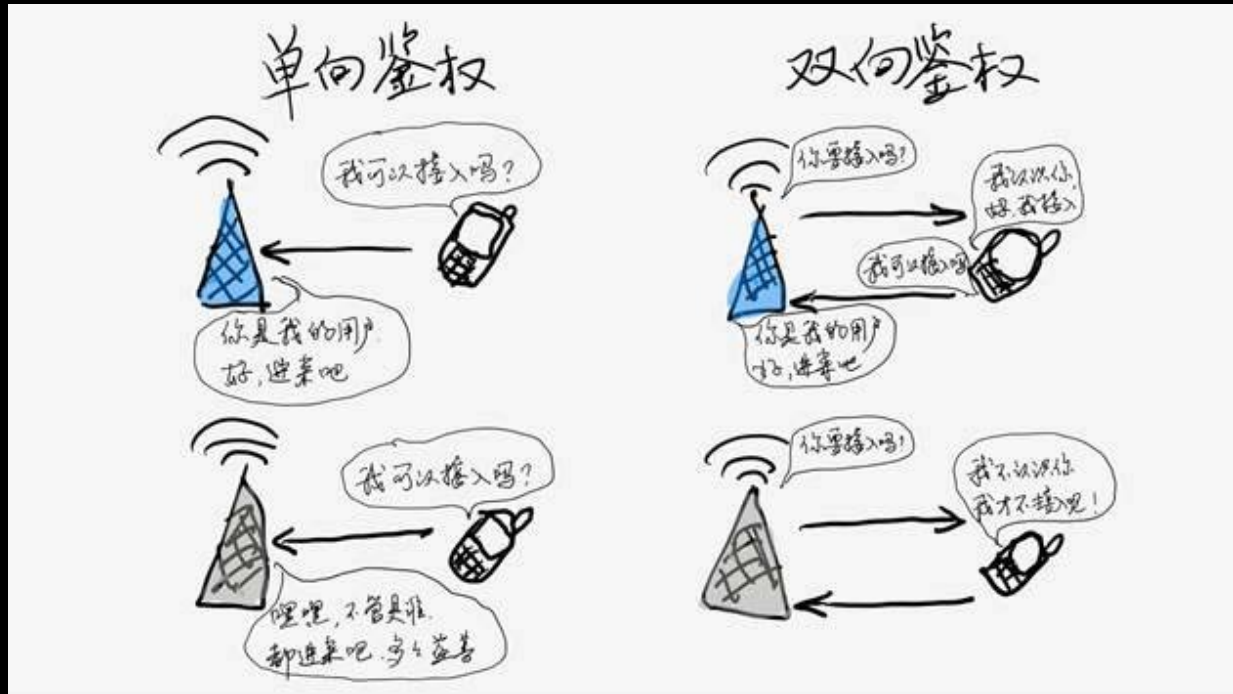
时代进步 -- > 技术升级

- 部分标准在设计之初没有考虑安全问题
  - 模拟已经不存在，不考虑
  - GSM存在问题，但部分地区已退网不支持2G
    - 问题已解决?
    - No
      - 所有手机都支持2G
      - 大部分物联网设备通讯模块都工作在2G下（不要求高速数据）

GSM安全问题

- 2G GSM网络，在设计之初就存在安全问题
  - 单向鉴权而非双向，即只有网络鉴定用户是否合法
  - 导致伪造基站的可能

如何实现
攻击中自动附着



伪基站应运而生











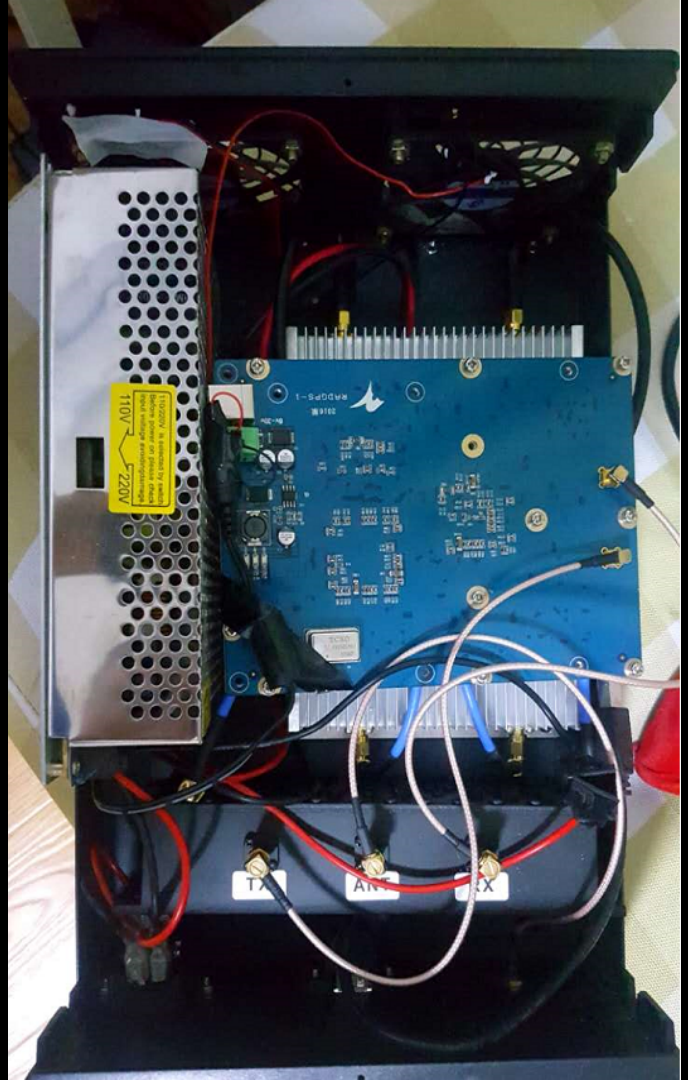


Just给你发了一个发送号码
和内容可以自定义的短信

伪基站内部探究

- 收发板（SDR软件无线电）
- 放大器（功率）
- 双工器、电源
- 外部笔记本+软件（Openbts 2.8）

通过软件模拟+收发设备实现GSM基站系统



伪基站都做了什么

- 用工程机 找个弱频点，设置MCC、MNC等参数和周围一样 LAC不一样
- 手机获知广播消息，C1C2还很大，呀！这得重选小区到这个伪基站。发现LAC变了！这得位置更新请求
- 手机傻乎乎的给鉴权信息，伪基站看也不看，来者不拒
- 手机在伪基站中，伪基站看IMSI（位置更新时获取的），嗯，刚刚没发过短信，发一条
- 伪基站利用完手机了，然后踢掉它
- 开始其他环节（钓鱼、种马、洗卡、售卖）

- Just给你发了一个发送号码和内容可以自定义的短信

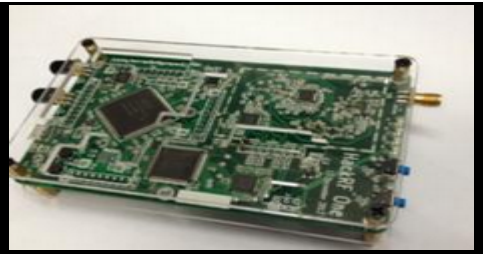
我们需要什么

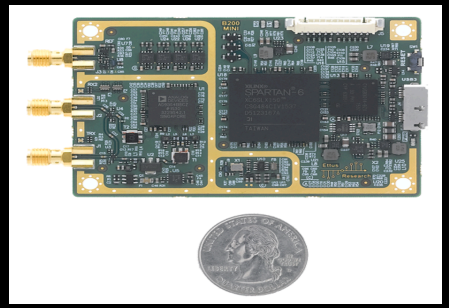
- 不可以滥发短信，不需要大功率，不可以干扰周边
- 只需要实现小区切换、自动附着
  - 实际上无需测试，请遵守法律法规
  - 通过修改开源BTS，增大C2
- 另外实现GPRS流量控制

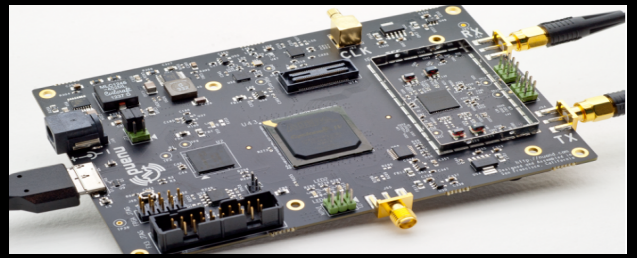
软件无线电介绍

- 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











开源GSM BTS



- 软件：
  - OpenBTS（难安装）
  - YateBTS（基于OpenBTS代码，可视化，容易安装）
  - OpenBSC(包含BTS，代码重写，规范，庞大，难安装)
- 硬件：
  - USRP系列（B系列偏频比较严重）
  - Bladerf x40（频率精准）
- So 我们选择YateBTS+Bladerf x40

如何实现

- BTS中小区重选参数C2无法设置或失效
  - 干脆代码里写死，最高值
- 基站配置参数
  - MMC、MNC需要与sim卡中一样
    - *#0011#
  - 获取较弱的频点
    - 使用工程机、GSM模块at指令
    - SDR扫描工具，例如kalibrate-rtl

GSML3RRElements.cpp

```
48
49
50  L3SI3RestOctets::L3SI3RestOctets()
51      :L3RestOctets(),
52      mHaveSI3RestOctets(false),
53      mHaveSelectionParameters(false),
54      mCBQ(0),mCELL_RESELECT_OFFSET(0),
55      mTEMPORARY_OFFSET(0),
56      mPENALTY_TIME(0),
57      mRA_COLOUR(0),
58      mHaveGPRS(false)
59  {
```

Mobile info refresh rate:

Disabled

Mobile location info (deprecated): LAC = c76 CID = 50b5

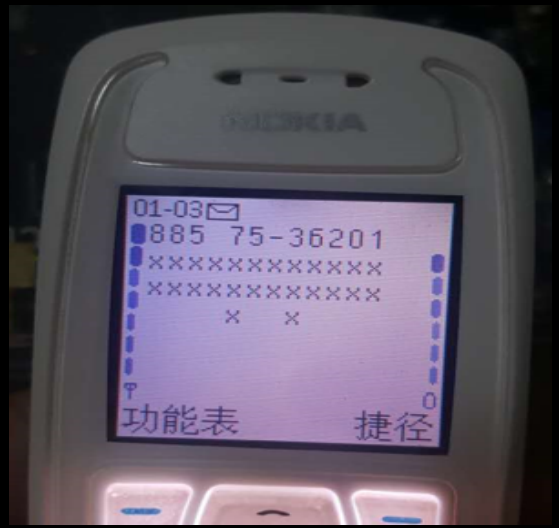
Neighbour mobile info (deprecated): [c765233@14] [c76e8c7@12] [c76e8c8@13] [c7650b6@14] [c765231@15]

All mobile measurement info:

GSM

SRV	MCC	MNC	LAC	CID	ARFCN	BSIC	RSSI
S	404	90	3190	20661	672	14	-73
	404	90	3190	21043	675	36	-85
	404	90	3190	59591	616	2	-89
	404	90	3190	59592	621	0	-87
	404	90	3190	20662	676	12	-85
	404	90	3190	21041	618	47	-83

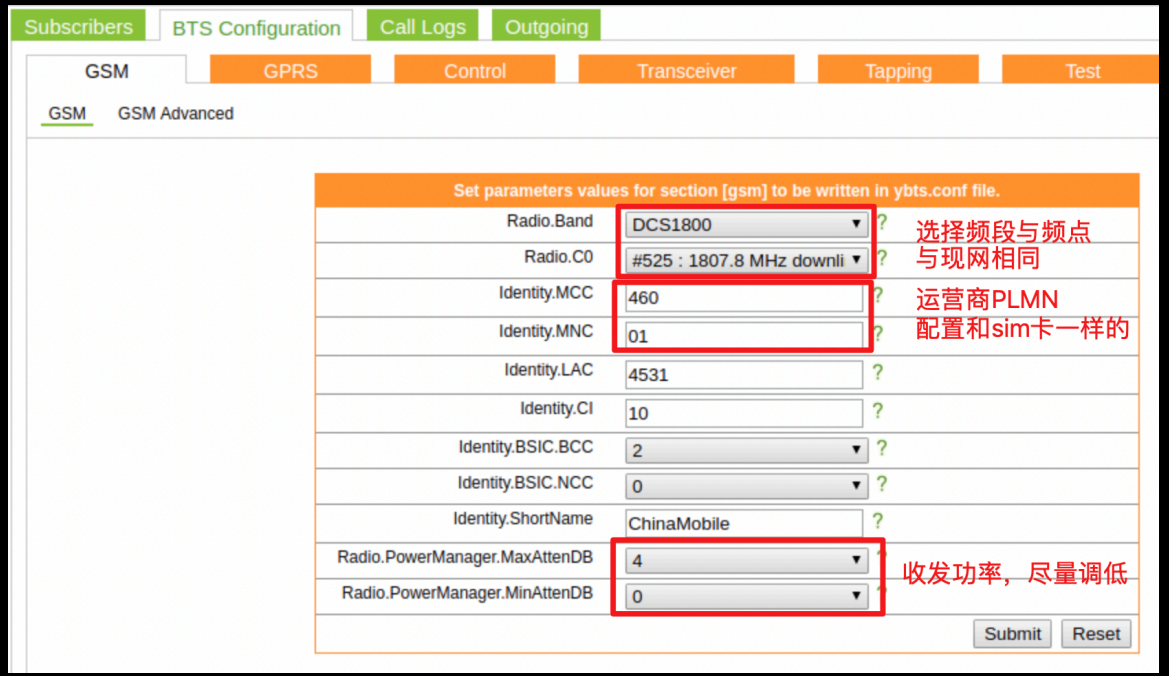
```
+CENG: 1,1

+CENG: 0,"0575,37,00,460,00,11,8dbb,13,00,11b2,255"
+CENG: 1,"0036,62,02,000a,460,00,a0f5"
+CENG: 2,"0571,32,44,8dba,460,00,11b2"
+CENG: 3,"0026,29,02,fbc4,460,00,11b2"
+CENG: 4,"0024,28,38,e65c,460,00,11b2"
+CENG: 5,"0029,24,61,e65b,460,00,11b2"
+CENG: 6,"0038,23,07,0e1a,460,00,11b2"

OK

+CMTI: "ME",11
AT+CENG?
+CENG: 1,1

+CENG: 0,"0036,51,01,460,00,02,000a,00,00,a0f5,255"
+CENG: 1,"0000,00,00,0000,,,0000"
+CENG: 2,"0000,00,00,0000,,,0000"
```




```
Using device 0: Generic RTL2832U OEM
Found Elonics E4000 tuner
Exact sample rate is: 270833.002142 Hz
Setting gain: 40.0 dB
kal: Scanning for DCS-1800 base stations.
DCS-1800:
        chan: 582 (1819.2MHz +  94Hz)   power: 511859.56
        chan: 590 (1820.8MHz -  43Hz)   power: 4439467.15
        chan: 615 (1825.8MHz +  57Hz)   power: 384392.76
        chan: 616 (1826.0MHz + 140Hz)   power: 663033.72
        chan: 618 (1826.4MHz +  50Hz)   power: 892936.25
        chan: 626 (1828.0MHz -  76Hz)   power: 2569451.64
        chan: 628 (1828.4MHz +  70Hz)   power: 5158224.62
        chan: 631 (1829.0MHz +  44Hz)   power: 1974235.05
        chan: 672 (1837.2MHz +  59Hz)   power: 1604471.91
        chan: 675 (1837.8MHz -  21Hz)   power: 1268341.27
        chan: 766 (1856.0MHz -  48Hz)   power: 789954.07
        chan: 768 (1856.4MHz + 139Hz)   power: 4244519.41
        chan: 770 (1856.8MHz -  93Hz)   power: 3517832.12
        chan: 772 (1857.2MHz +   7Hz)   power: 659372.12
```

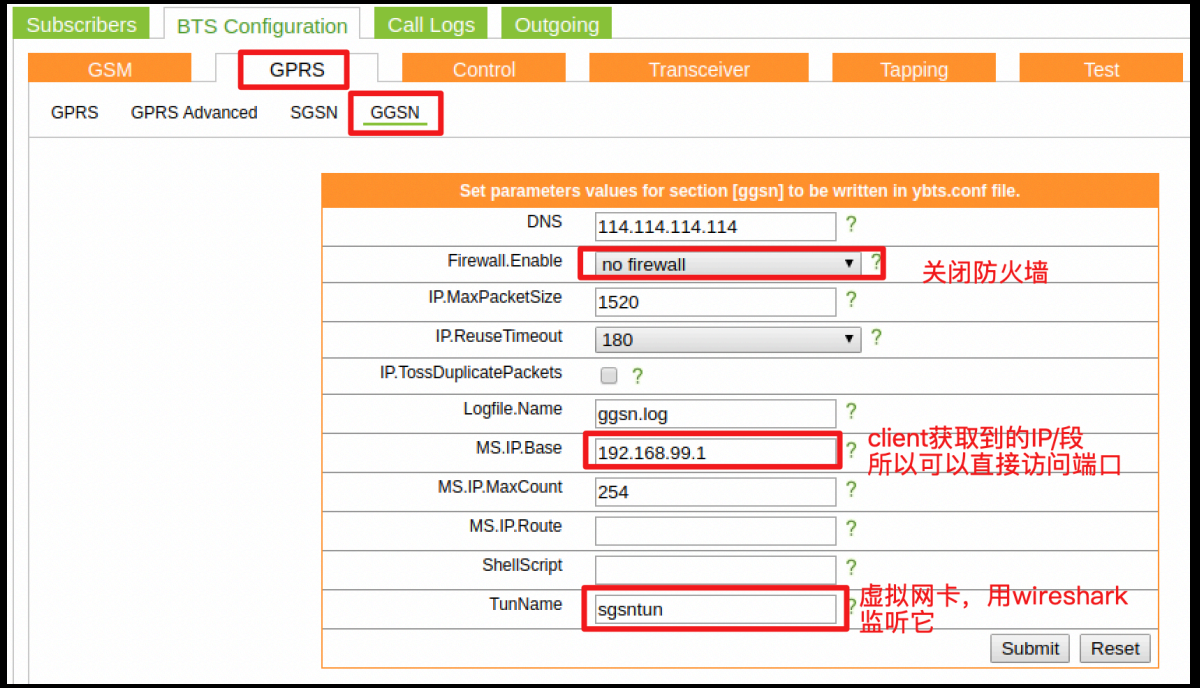
其他配置

- 基础配置
  - 选择频段与频点
  - 配置MCC、MNC
  - 配置功率参数



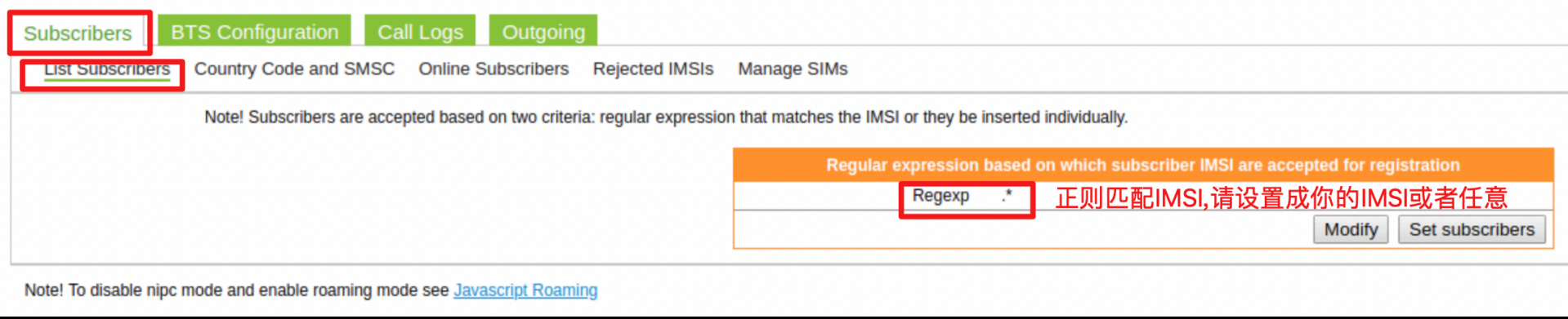
其他配置

- 网络配置
  - 关闭防火墙
  - 添加ip转发
  - 添加iptables策略



其他配置

- IMSI匹配
  - 配置具有哪些IMSI的sim卡可以入网



最小化影响

- 这套理论已经实践过，具有攻击场景，谨慎测试
  - MCC/MNC/频点的设置会影响周边设备通讯
- 推荐做法（快速附着）：
  - 无线信号屏蔽盒中测试
  - 有wifi/有线的 地下室中测试，例如小区地库
  - 重启下设备

万事具备，开始攻击

- 意义：拥有了控制现网GPRS流量的能力
- 方法：
  - 开启wireshark，记录分析流量
  - 使用burpsuite开启http/https代理，替换流量
    - 替换升级服务器
    - 注入浏览器漏洞
  - 直接访问ip端口
    - Exp
    - 管理工具（ADB、telnet、ssh、私有端口）

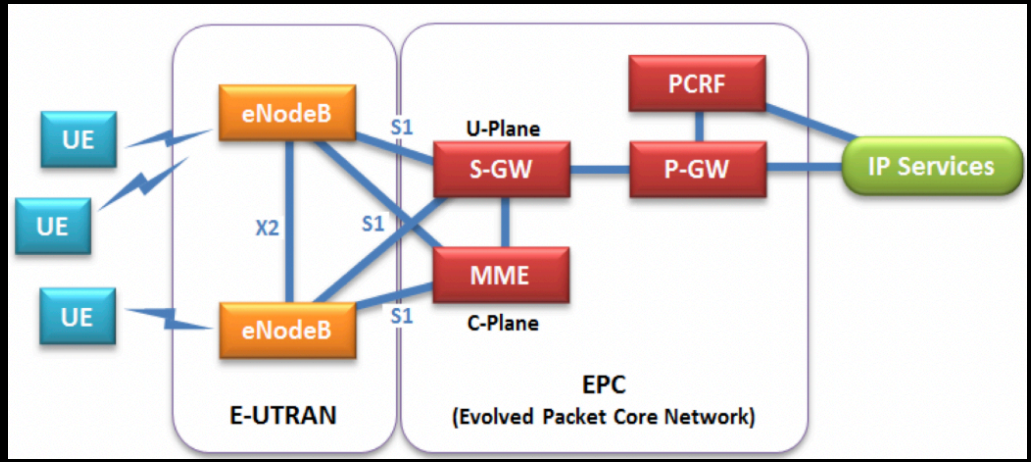
搭建LTE测试基站

- 当我们只需要获取流量做分析，不需要现场控制
- 简化搭建步骤
- 快速测试（例如快速扫描端口）

- LTE采用双向认证，不存在假基站
- 为了附着到网络，我们还需要解决认证问题

LTE系统介绍

- UE、EPC、eNodeB（ENB）
- 双向认证
- 开源SDR LTE：
  - OAI（过于复杂、安装困难）
  - srsLTE（安装使用简单，推荐）



SDR实现LTE测试基站

- srsLTE ENB、 EPC编译安装
- SDR硬件选择：
  - USRP B200/B210/B200 mini
  - Bladerf x40 xa4
  - LimeSDR

- 写卡
  - 可读写空白LTE sim 测试卡（仅限于测试使用）
  - 读卡器

配置参数

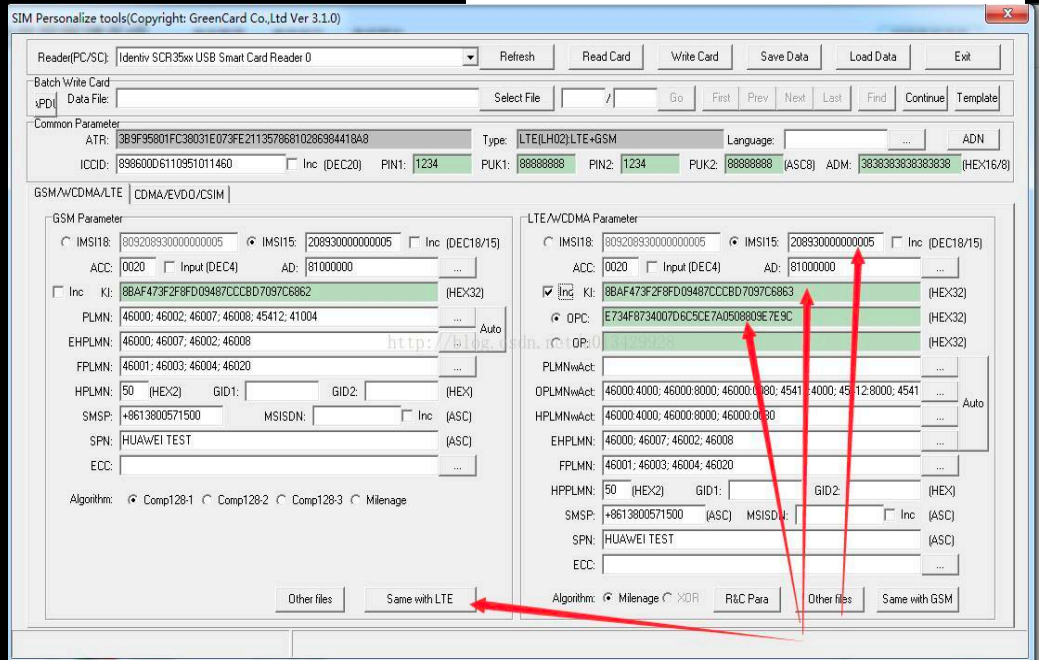
- PLMN （MCC、MNC）
- apn
- 频点（注意配置为设备支持的，例如Bind1、3、7)
- Ip转发、路由
- 写卡
  - IMSI Ki op/opc

OPENAIRINTERFACE- OAI 测试白卡

如何写卡

- 根据运营商填入IMSI
- 填入usr.csv中的KI、OP/OPC,替换IMSI
- 选择正确的算法
  - Mi or xor
- 现在，可以用手机主动搜索并且加入网络





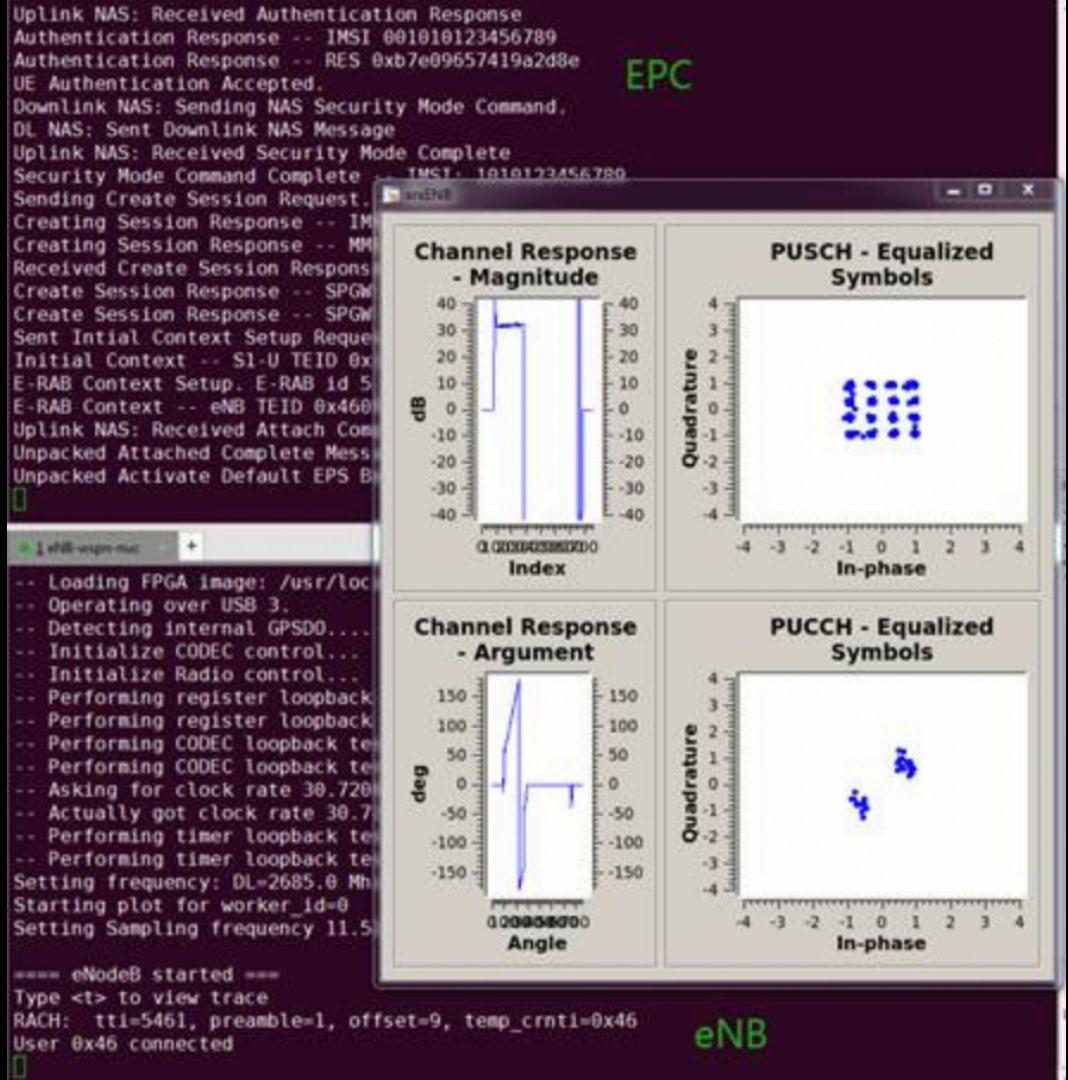
解决手动搜网、漫游、apn的问题

- 每次需要点手动搜网，且IOT设备很多无法手动搜
  - 配置和IMSI前5位一致的PLMN，且真实存在（这个同时会解决漫游状态问题）
  - 写卡配置HPLMN、EHPLMN、FPLMN等参数

- apn不匹配，导致无法建立IP链路
  - 配置为PLMN对应的apn，例如中国联通 46001，其通用apn为3gnet

Run !

- Start EPC
- Start ENB



各种带SIM卡的物联网设备















```
..{"Version":"00030000","SN":1074096116,"CID":10211,"PL":
{"Name":"863412030[redacted]","Password":"7805303461C5E33FC8[redacted]","Ty
pe":200,"machSerialNo":"15183/00035289"}}..{"RC":
1,"Version":"00030000","SN":1074096116,"PL":
{"EID":"B0C2116A04126B9122919095E6BA24FD","BIND":0,"GID":
["888B31A71E5B75376A97EBD8A0010429"],"GMT":"20170501184949080"},"CID":
10212,"SID":"89D4229CEB9C4128A0DC45F20BE7399B"}..{"CID":
80041,"Version":"00030000","SN":
```




```
PUST /gsmlock HTTP/1.1
Host:[redacted]fo.so
Content-Type: text/plain
Content-Length: 116
Cache-Control: no-cache

qlUAAQBPMUhCMTcxNDAzOTExAYA4r5S1QtHfGB7GxD44V9bml02K5xSxAhz3Mg2z00Lem9qIXY6eo
LEPTdYTRrEfQHT7EyG6TUPhBay44z5BeawX80YQHTTP/1.1 200 OK
Date: Fri, 04 Aug 2017 22:11:53 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 76
Connection: keep-alive
X-Powered-By: Express
ETag: W/"4c-o+ijHq59dUwrBdxcvODqDQ"

qlUAAQAvMUhCMTcxNDAzOTExAYAe+B0mKUwiwOgirvY5Sax1sLQy45XaioAu38M6gJxkpyYnAQ==
```

```python
    def decrypt(self,txt):
        key = hashlib.md5('[redacted]' + self.devide_id).hexdigest().decode("HEX")
        print key
        cryptor = AES.new(key, self.mode)

        plain_text = cryptor.decrypt(txt)
        return plain_text

aes_encrypt = AES_ENCRYPT()  # 初始化密钥
aes_encrypt.devide_id = '1HB1715[redacted]

print aes_encrypt.decrypt('d31d1ef31dcebad585ae71bd5a3c0365d66b5d6de92b320b18bd32cc6d332313'.decode('hex'))
```

key

Run aes_test

```
/opt/local/bin/python /Users/gaoshupeng/PycharmProjects/work/ofo/aes_test.py
n;?"??'?7 vG~Wy
□?1234□□□□□□□□Y? NY? N□□□□□□□□
```

解锁密码

某车载设备存在命令注入

```
20  addr_len = 16;
21  v3 = accept(dword_15230, &addr, &addr_len);
22  if ( v3 == -1 )
23  {
24    perror("accept error");
25  }
26  else
27  {
28    memset(&s, 0, 0x64u);
29    memset(&v10, 0, 0x64u);
30    v4 = getcwd(&s, 0x64u);
31    snprintf(&v10, 0x64u, "ls -l %s", v4);
32    v5 = popen(&v10, "r");
33    if ( v5 )
34    {
35      printf("pipe open successfully!, cmd is %s\n", &v10);
36      while ( 1 )
37      {
38        v6 = fgetc(v5);
39        putchar(v6);
40        write(v3, &v6, 1u);
41      }
42    }
43    puts("pipe open error in cmd_list");
44  }
45}
```

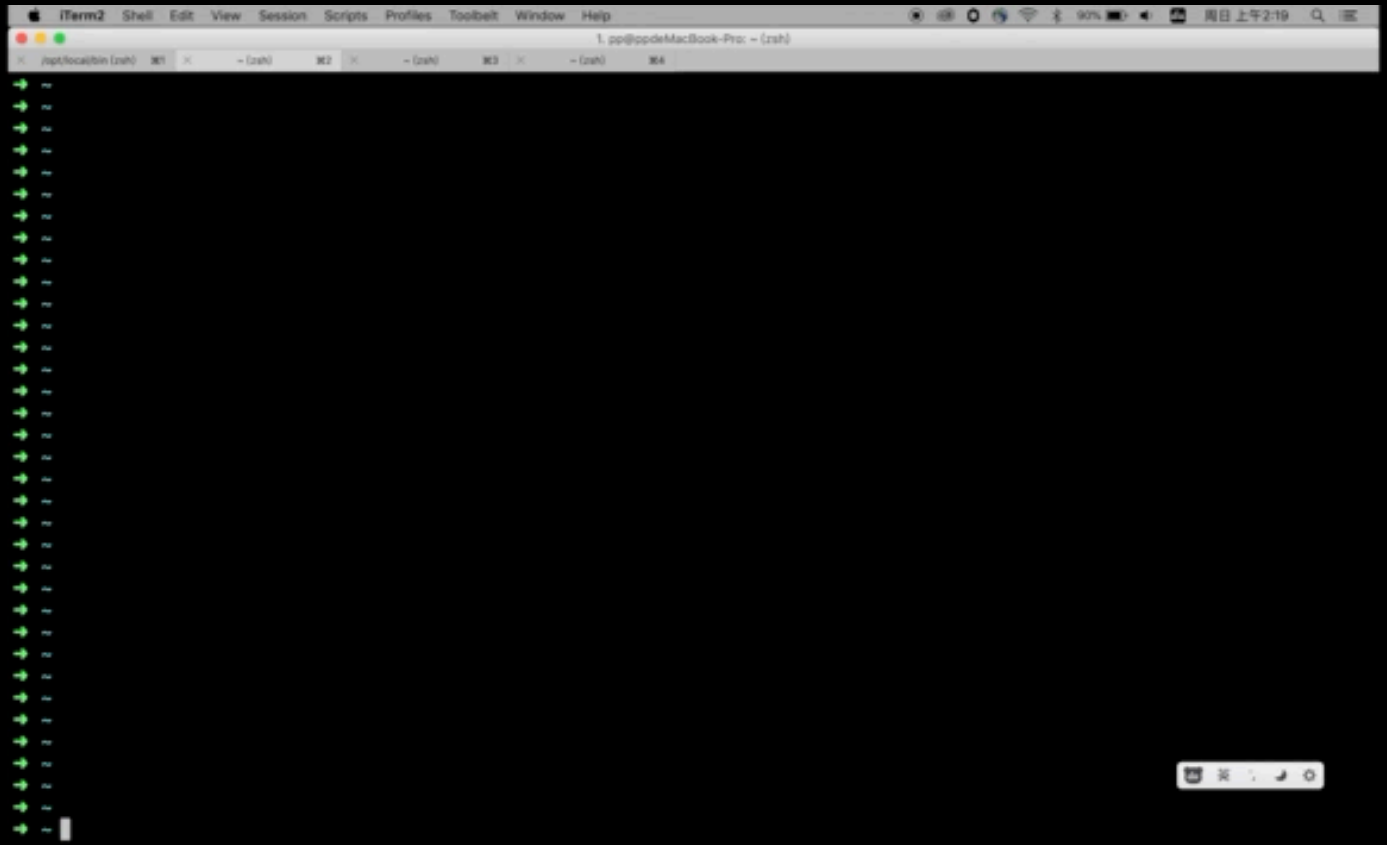
视频演示：LTE基站端口访问攻击



利用运营商内网

- 利用运营商内网进行端口间测试
  - 买两张同类型的4G卡，大概率会分配到一个内网
  - 如果是私有ANP，肯定会分配到同一内网
  - 如果实在条件限制，或者只做23、80等端口访问
    - 扫描一台开放5555等端口，从对方进行访问（未授权攻击，不推荐）
    - 在可控的私有APN内网中，这种方法OK

视频演示：利用运营商内网进行测试



其他

- 研究基带漏洞
  - Fuzz协议，调试基带
- 研究LTE 标准漏洞
  - Review、添加代码
  - 实际测试

Q&A