百鬼夜行の
看不见的无线安全

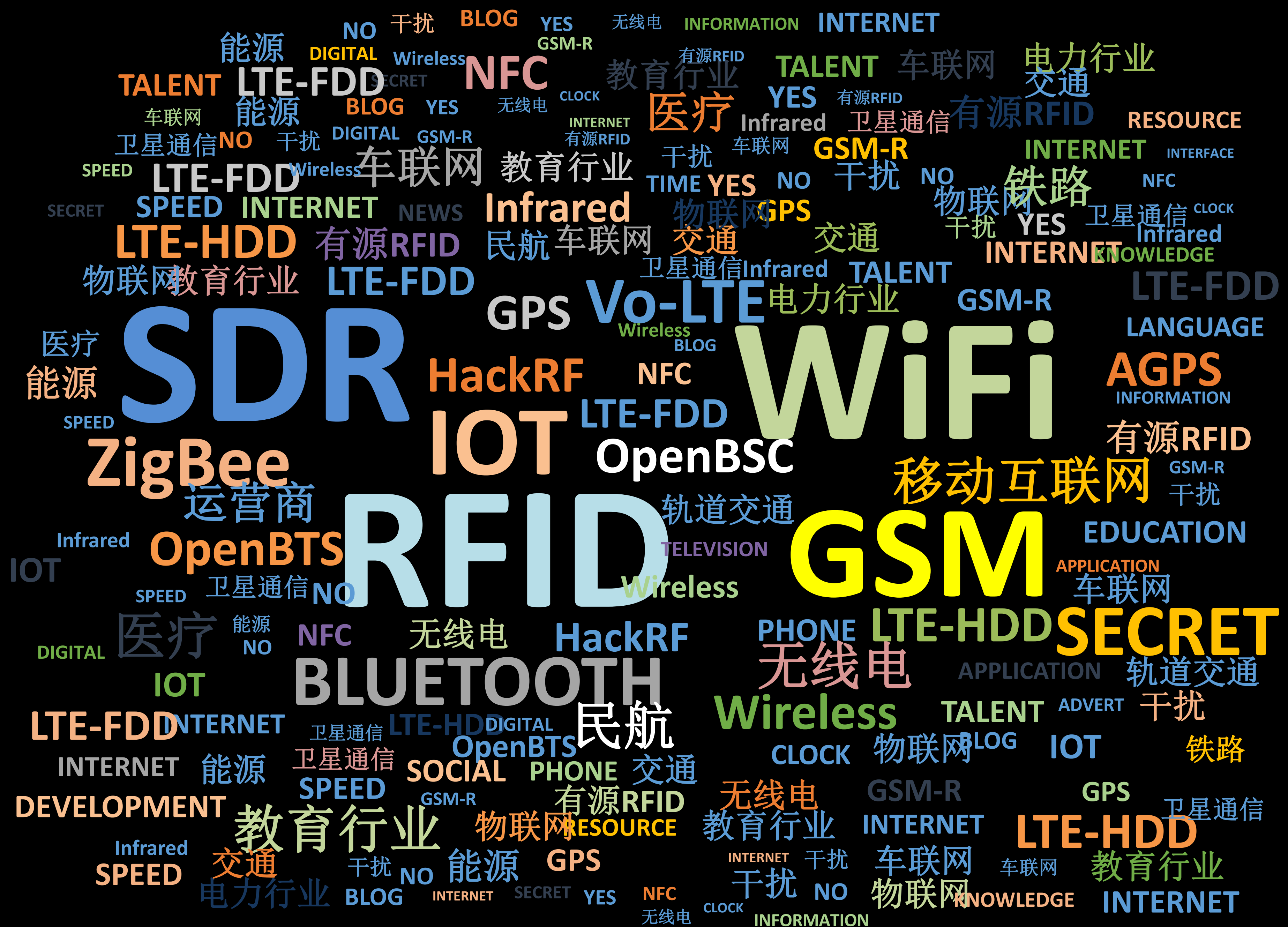
杨　哲 (Longas)
ZerOne无线安全研究

ZerOne无线安全研究组织

杨 哲 (Longas)

ZerOne
WirelessSec Research

- 成立于2006年，均为无线安全研究员/爱好者
- 成员来自安全公司、游戏公司、高校、公安及政府
- 历程与成果
  - 建立中国最大的Anywlan网站“无线安全”讨论区
  - 发起国内无线WPA加密分布式破解项目



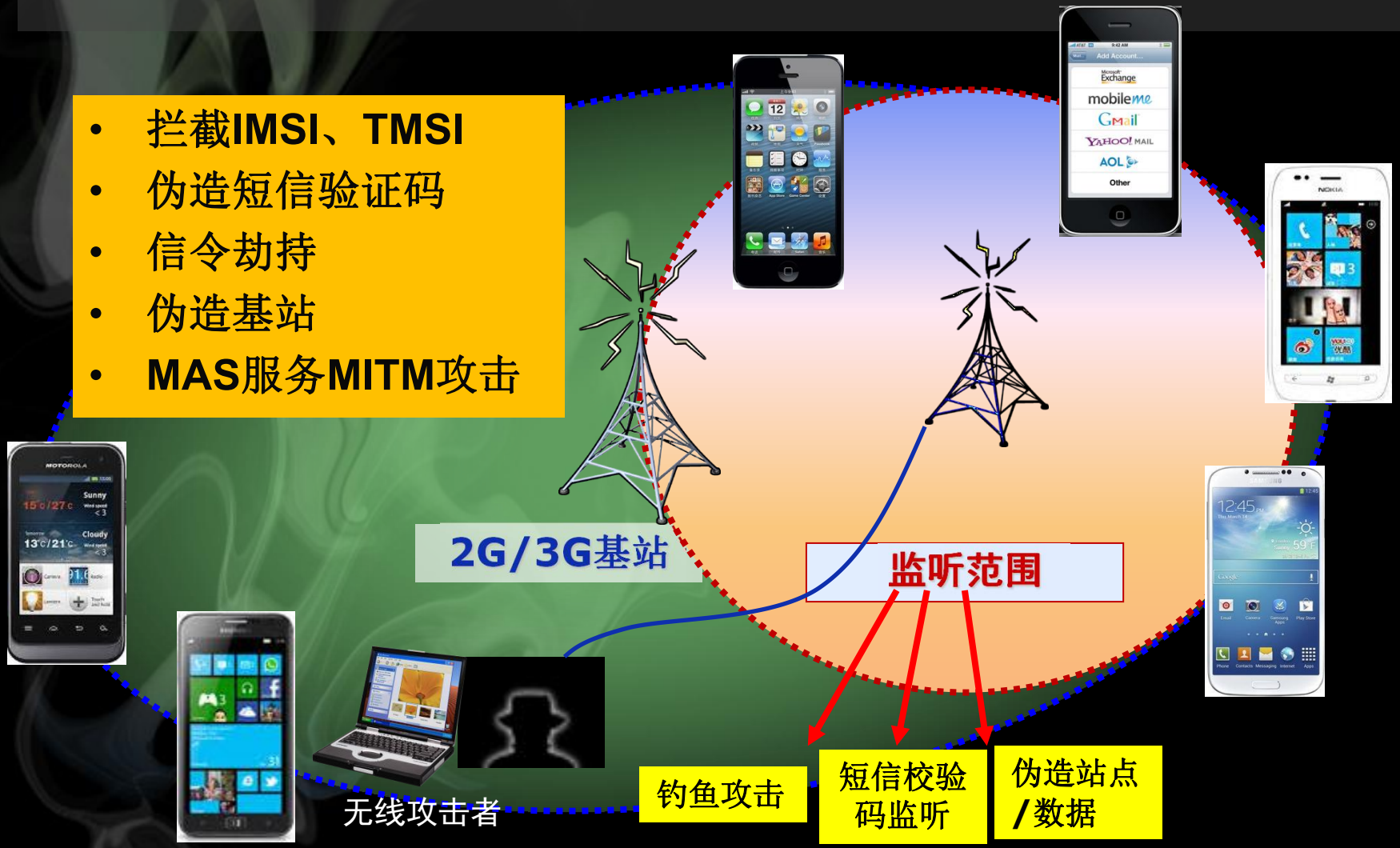
NO
干扰
BLOG
YES
无线电
INFORMATION
INTERNET
能源
DIGITAL
Wireless
GSM-R
有源RFID
TALENT
车联网
电力行业
TALENT
LTE-FDD
SECRET
NFC
教育行业
交通
车联网
能源
BLOG
YES
无线电
CLOCK
医疗
YES
有源RFID
有源RFID
RESOURCE
卫星通信
NO
干扰
DIGITAL
GSM-R
INTERNET
有源RFID
Infrared
卫星通信
车联网
GSM-R
INTERNET
INTERFACE
SPEED
LTE-FDD
Wireless
车联网
教育行业
干扰
干扰
NO
NFC
TIME
YES
NO
铁路
SECRET
SPEED
INTERNET
NEWS
Infrared
物联网
GPS
物联网
卫星通信
CLOCK
LTE-HDD
有源RFID
民航
车联网
交通
交通
干扰
YES
Infrared
INTERNET
KNOWLEDGE
物联网
教育行业
LTE-FDD
卫星通信
Infrared
TALENT
LTE-FDD
Vo-LTE
电力行业
GSM-R
SDR
GPS
Wireless
BLOG
WiFi
LANGUAGE
医疗
能源
HackRF
NFC
AGPS
INFORMATION
SPEED
LTE-FDD
有源RFID
IOT
ZigBee
OpenBSC
移动互联网
GSM-R
运营商
轨道交通
干扰
RFID
GSM
EDUCATION
Infrared
OpenBTS
TELEVISION
IOT
APPLICATION
SPEED
卫星通信
NO
Wireless
车联网
医疗
能源
NO
NFC
无线电
HackRF
PHONE
LTE-HDD
SECRET
DIGITAL
无线电
BLUETOOTH
APPLICATION
轨道交通
IOT
Wireless
TALENT
ADVERT
干扰
LTE-FDD
INTERNET
卫星通信
LTE-HDD
DIGITAL
民航
INTERNET
OpenBTS
CLOCK
物联网
BLOG
IOT
铁路
能源
卫星通信
SOCIAL
PHONE
交通
DEVELOPMENT
SPEED
GSM-R
有源RFID
无线电
GSM-R
GPS
卫星通信
教育行业
物联网
RESOURCE
教育行业
INTERNET
LTE-HDD
Infrared
交通
干扰
能源
GPS
INTERNET
干扰
车联网
车联网
教育行业
SPEED
NO
干扰
电力行业
BLOG
INTERNET
SECRET
YES
NFC
NO
物联网
KNOWLEDGE
INTERNET
无线电
CLOCK
INFORMATION

- 2G/3G/4G安全
- 伪基站分析
- 短信群发/钓鱼

谈谈伪基站

针对2G/3G/4G通信的高级MITM实现

- 拦截IMSI、TMSI
- 伪造短信验证码
- 信令劫持
- 伪造基站
- MAS服务MITM攻击



2015~2016：运营商3G/4G业务模拟攻击

OpenBTS

OpenSIM

Asterisk

osmocomBB

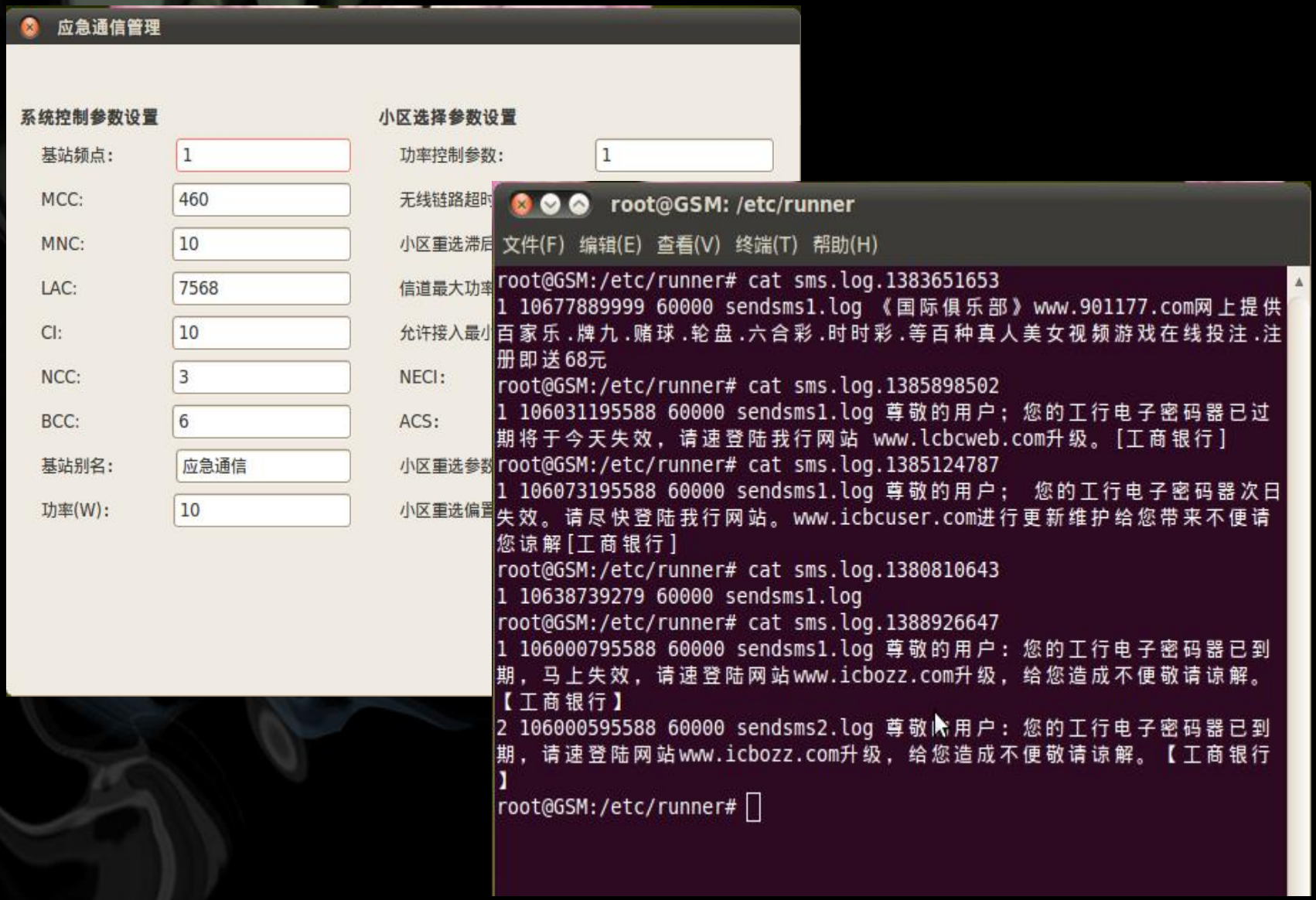
OPENSOURCEIMS core

伪基站小时代

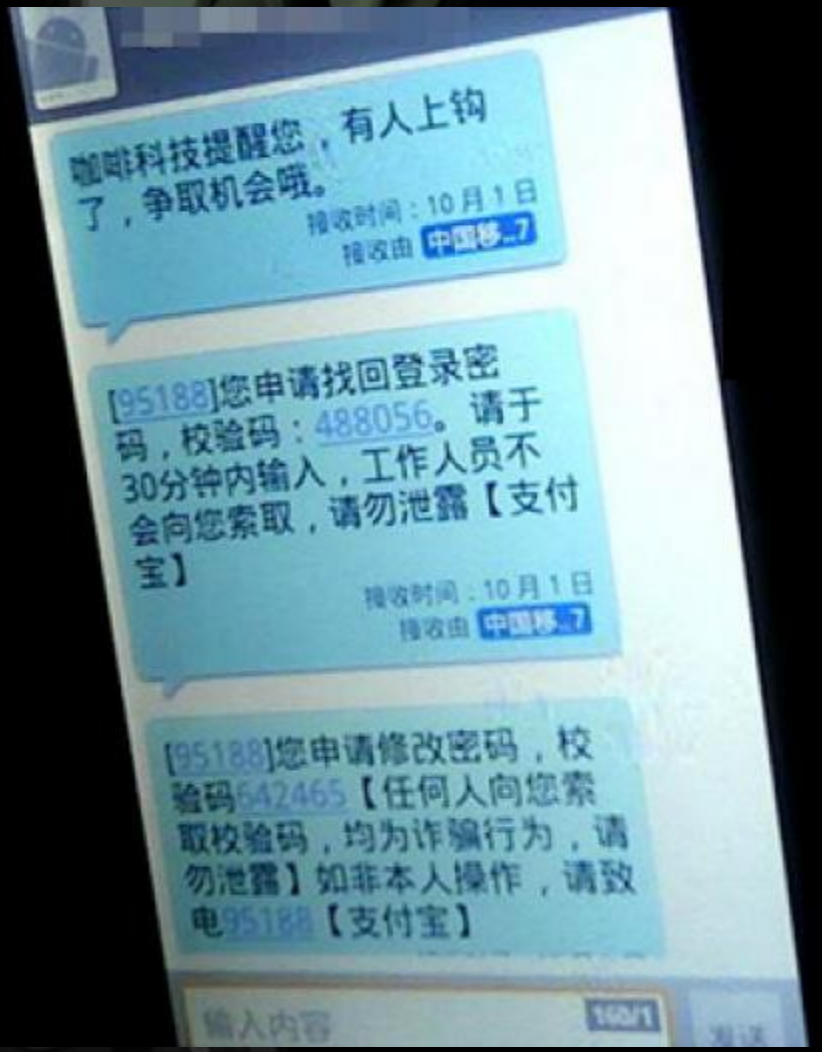
- OpenBTS
- USRP
- RAD-1

解剖“伪基站”

解剖“伪基站”


应急通信管理
系统控制参数设置
基站频点:
1
MCC:
460
MNC:
10
LAC:
7568
CI:
10
NCC:
3
BCC:
6
基站别名:
应急通信
功率(W):
10
小区选择参数设置
功率控制参数:
1
无线链路超时
小区重选滞后
信道最大功率
允许接入最小
NECI:
ACS:
小区重选参数
小区重选偏置
root@GSM: /etc/runner
文件(F) 编辑(E) 查看(V) 终端(T) 帮助(H)
root@GSM:/etc/runner# cat sms.log.1383651653
1 10677889999 60000 sendsms1.log 《国际俱乐部》www.901177.com网上提供百家乐.牌九.赌球.轮盘.六合彩.时时彩.等百种真人美女视频游戏在线投注.注册即送68元
root@GSM:/etc/runner# cat sms.log.1385898502
1 106031195588 60000 sendsms1.log 尊敬的用户；您的工行电子密码器已过期将于今天失效，请速登陆我行网站 www.lcbcweb.com升级。[工商银行]
root@GSM:/etc/runner# cat sms.log.1385124787
1 106073195588 60000 sendsms1.log 尊敬的用户； 您的工行电子密码器次日失效。请尽快登陆我行网站。www.icbcuser.com进行更新维护给您带来不便请您谅解[工商银行]
root@GSM:/etc/runner# cat sms.log.1380810643
1 10638739279 60000 sendsms1.log
root@GSM:/etc/runner# cat sms.log.1388926647
1 106000795588 60000 sendsms1.log 尊敬的用户：您的工行电子密码器已到期，马上失效，请速登陆网站www.icbozz.com升级，给您造成不便敬请谅解。【工商银行】
2 106000595588 60000 sendsms2.log 尊敬的用户：您的工行电子密码器已到期，请速登陆网站www.icbozz.com升级，给您造成不便敬请谅解。【工商银行】
root@GSM:/etc/runner#

典型手机短信钓鱼示例


咖啡科技提醒您，有人上钩了，争取机会哦。
接收时间：10月1日
接收由 中国移...7
[95188]您申请找回登录密码，校验码：488056。请于30分钟内输入，工作人员不会向您索取，请勿泄露【支付宝】
接收时间：10月1日
接收由 中国移...7
[95188]您申请修改密码，校验码642465【任何人向您索取校验码，均为诈骗行为，请勿泄露】如非本人操作，请致电95188【支付宝】
输入内容
160/1

- 短信群发
- 短信验证
- 伪造短信
- 短信监听
- **GSM气数已尽？**

再见短信？

短信群发的几种形式

- 短信猫 **SMS Modem**
  - SIM Card
  - RS232、USB
- **企信通**
  - 由于限制严格，多数已转向电信小灵通发送SMS
- **移动MAS**
  - 收发短信，WAPPush
  - Java+Tomcat+Hibernate+My
  - OA增值功能
- **Other Ways**
- 黑色产业链设备

短信验证的悲哀

- 短信验证场景
  - 网银登录手机校验码
  - 公共场所WiFi访问密码
  - 企业内部802.1X认证环境访问密码
  - 在线交易校验码
  - 邮箱密码丢失验证码
  - 临时验证码

手机验证码/交易过程面临的安全威胁

单一化手机验证流程机制，已在国内绝大部分银行、银联、运营商、商业论坛、邮箱服务提供商等广泛使用

现有安全策略：

1、重新发送时间限制：2分钟内不能点击“重新发送”

2、基于手机号码自身的身份验证

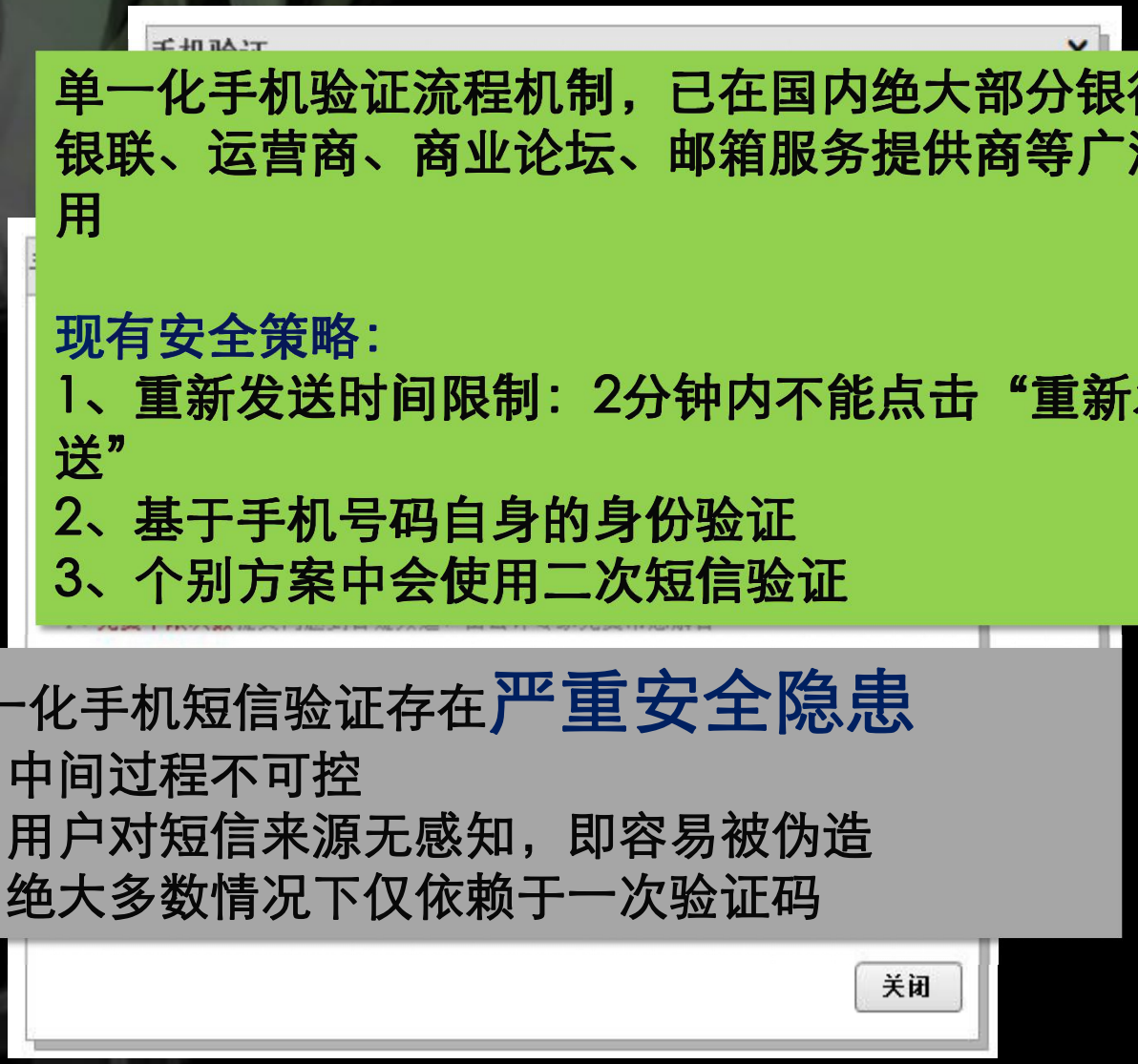
3、个别方案中会使用二次短信验证

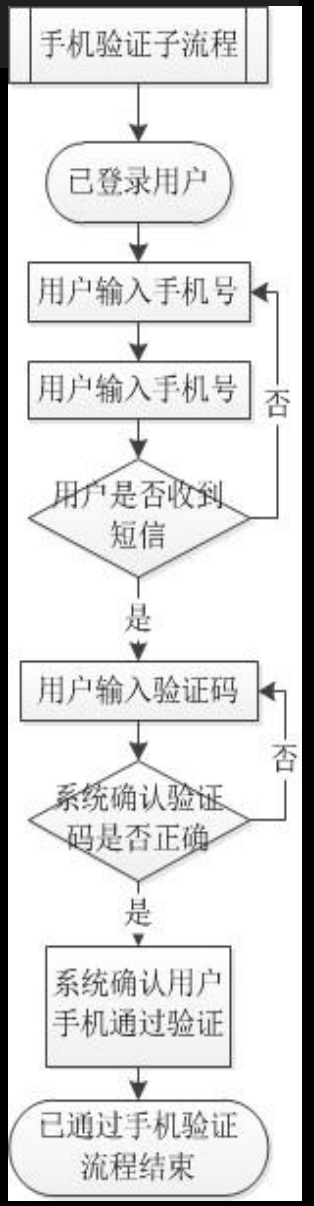
单一化手机短信验证存在**严重安全隐患**

1、中间过程不可控

2、用户对短信来源无感知，即容易被伪造

3、绝大多数情况下仅依赖于一次验证码






03月08日17:29，你使用支付宝付款122.60元，校验码是：937132[工作人员不会向您索取，请勿泄露]。【支付宝】
尊敬的褚[redacted]孜客户，您末位3519的订单，支付金额10.00元，验证码：459840，请即时输入。[建设银行]
交通银行手机动态密码：7325e8，密码序号：88。您正在进行网上支付，支付金额为：0.93元【交通银行】
国航知音会员开通手机号为登录账户信息验证码:4789【中国国航】
您在西安移动，订单尾号062[redacted]35，金额100.00元的交易，支付验证码为473280，请勿泄露！【中国银联】
您好！您已开通每月20小时的WLAN免费体验套餐，即时生效，帐号：137164[redacted]30，密码：9t5d5k。该套餐将于2013年
OK
您本次网上支付的动态密码是sqmchv，金额29.00元，订单号900[redacted]810，商户名支付宝(中国)网络技术有限公司。【浦发银行】
您在铁道部清算中心，订单尾号325[redacted]70，金额406.50元的交易，支付验证码为646628，请勿泄露！【中国银联】
933347（微信验证码）【腾讯科技】
您于01:51开通尾号9715的建设银行卡快捷支付，验证码367106。（机密信息，请勿泄露）【财付通】
注册成功，您的通行证账号[mp[redacted]7107]，密码[127765]，您也可以直接使用当前手机号登录或找回密码【斯[redacted]网络】
星巴克无线密码: 6631，7日有效.
OK

咖啡厅的WiFi验证SMS

- AT&T、T-Mobile与星巴克合作
- 中移动：CMCC-Starbucks
  - 以前依靠单纯的WPA-PSK密码
  - 现在通过手机发送无线密码SMS

- 安全威胁：
  - 一周内以注册用户身份使用WiFi
  - 对指定对象伪造攻击的可能
  - 用户对短信的盲目信赖感

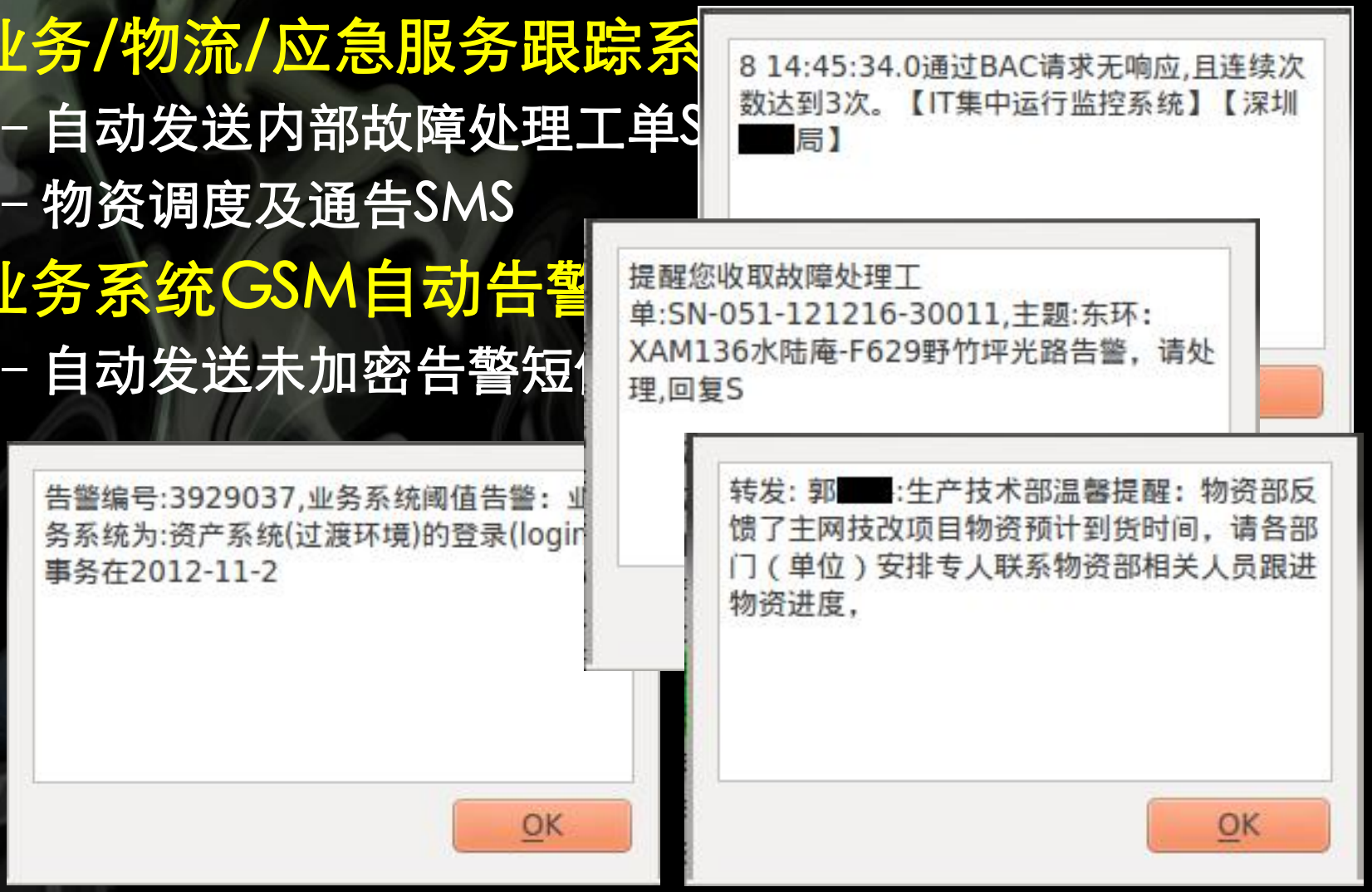
机场的WiFi环境验证SMS

- 国内机场
  - SSID：“Airport WiFi Free”
  - 伪造AP的天堂

- 安全威胁：
  - 以他人身份使用WiFi
  - 此类短信多数以1065、1069之类开头的号码发送
  - 使用特定短信工具可轻松实现欺骗攻击

工业控制领域の无线安全

- 业务/物流/应急服务跟踪系
  - 自动发送内部故障处理工单S
  - 物资调度及通告SMS
- 业务系统GSM自动告警
  - 自动发送未加密告警短



多重手机验证流程机制并不能从根本上解决安全威胁

思路1：在流程中增加额外需填写信息

思路2：通过不同通道验证码加强验证

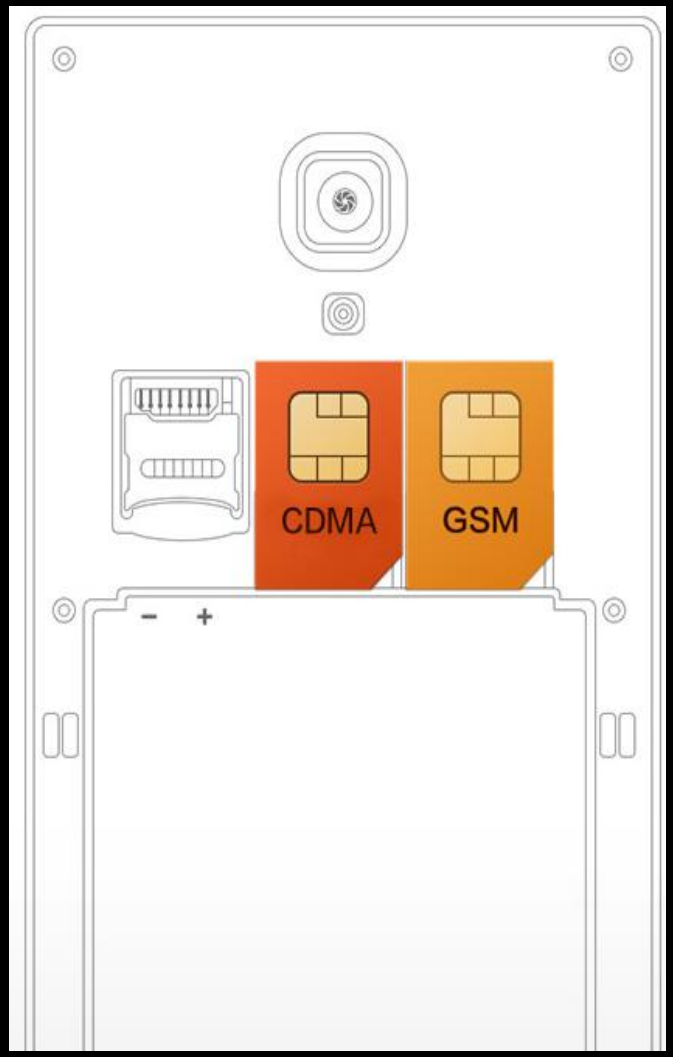
思路3：更换验证方式

犯罪实施的低成本化、机动化与多样化

- 低成本化
  - 68元SIM卡 + 200元GSM手机
  - 用完即换
- 机动化
  - 随身多张SIM卡
  - GSM手机用完即扔
  - 黑卡
- 多样化
  - 多卡多待
  - 一卡多号，最多可达12个号码
  - SIM卡复制应用更广

GSM真的气数已尽？

- 从双卡双待到全网通
  - GSM / CDMA
  - GSM / WCDMA
  - GSM / TD-SCDMA
  - GSM / TD-LTE
  - ……
  - 必有一卡支持GSM
- 个人持有手机号码
  - 双号
  - 3个以上



SMS，隐私暴露的必然

- 银行交易信息
  - 工资到账
  - 转账记录
  - 银行卡开户行
  - 银行卡后4位
- 差旅信息
  - 航班信息
  - 酒店预订信息
  - 签证信息

Only 3 Months

- 在线提示信息
  - 证券交易
  - 期货交易
  - 网校注册
  - 邮箱注册
- 其它提示
  - 未接来电提醒
  - 流量提示信息
  - 学校通知信息

来自中移动的数据

- 截至2016年3月，中国移动用户总数为**8.34亿户**
- 其中，2G、3G、4G用户分别占到**50.5%**、26.3%、23.2%。

- 粗略计算，国内至少约有**3亿户**仍在使用GSM。换句话说，国内至少还有3亿户面临威胁GSM空口数据威胁。

- 参考中移动的网络融合速度、新用户增长速度、资费套餐设计及市场粗略判断，大幅度解决此安全隐患，至少还需要**3~4年**。

一个简单的思路

- 针对双卡槽智能手机的特定病毒（Android）
  - 自动识别两个卡槽中SIM卡类型
  - 可根据多种方式远程激活（微信、短信等）
  - 主要功能：

    强制切换GSM的SIM卡为默认主卡

    或者

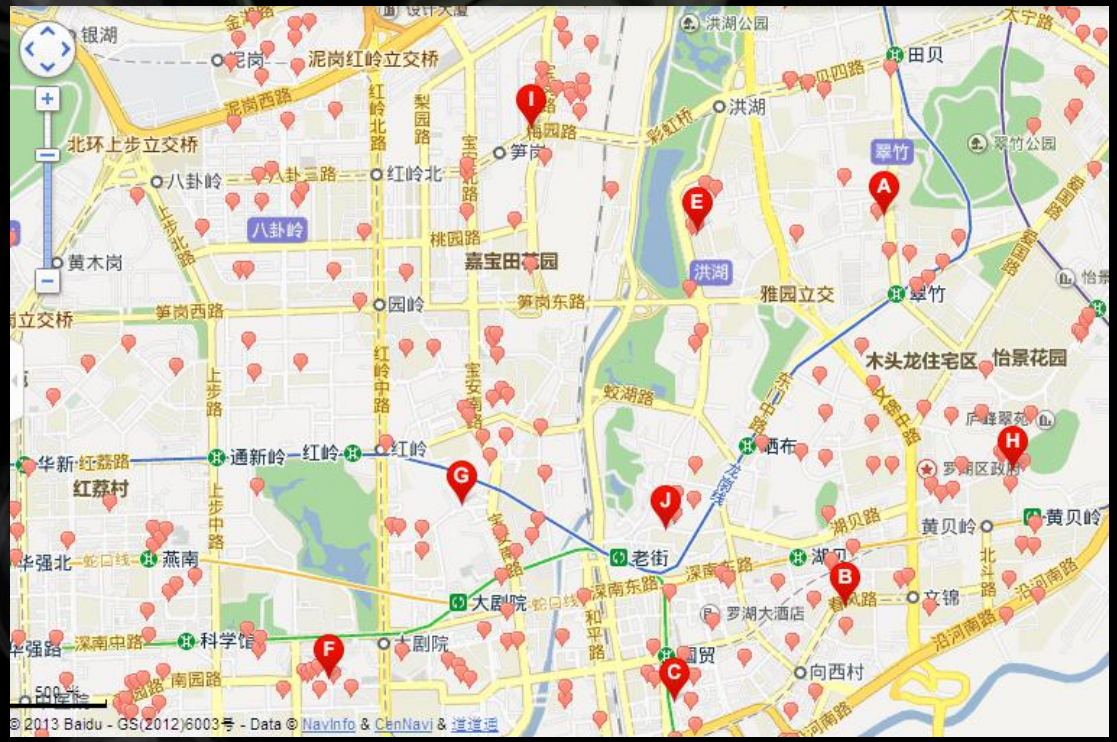
    免激活非GSM的SIM卡

- GPS 卫星定位
- CPS 基站定位
- WPS WiFi定位
- 监听模块定位
- SS7 信令定位
- 第三方APP

手机定位

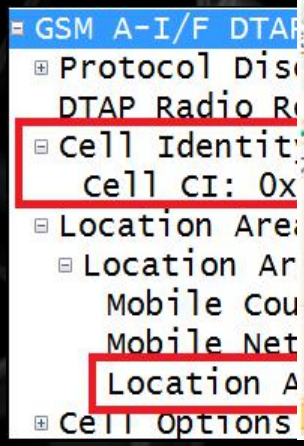
GPS卫星定位

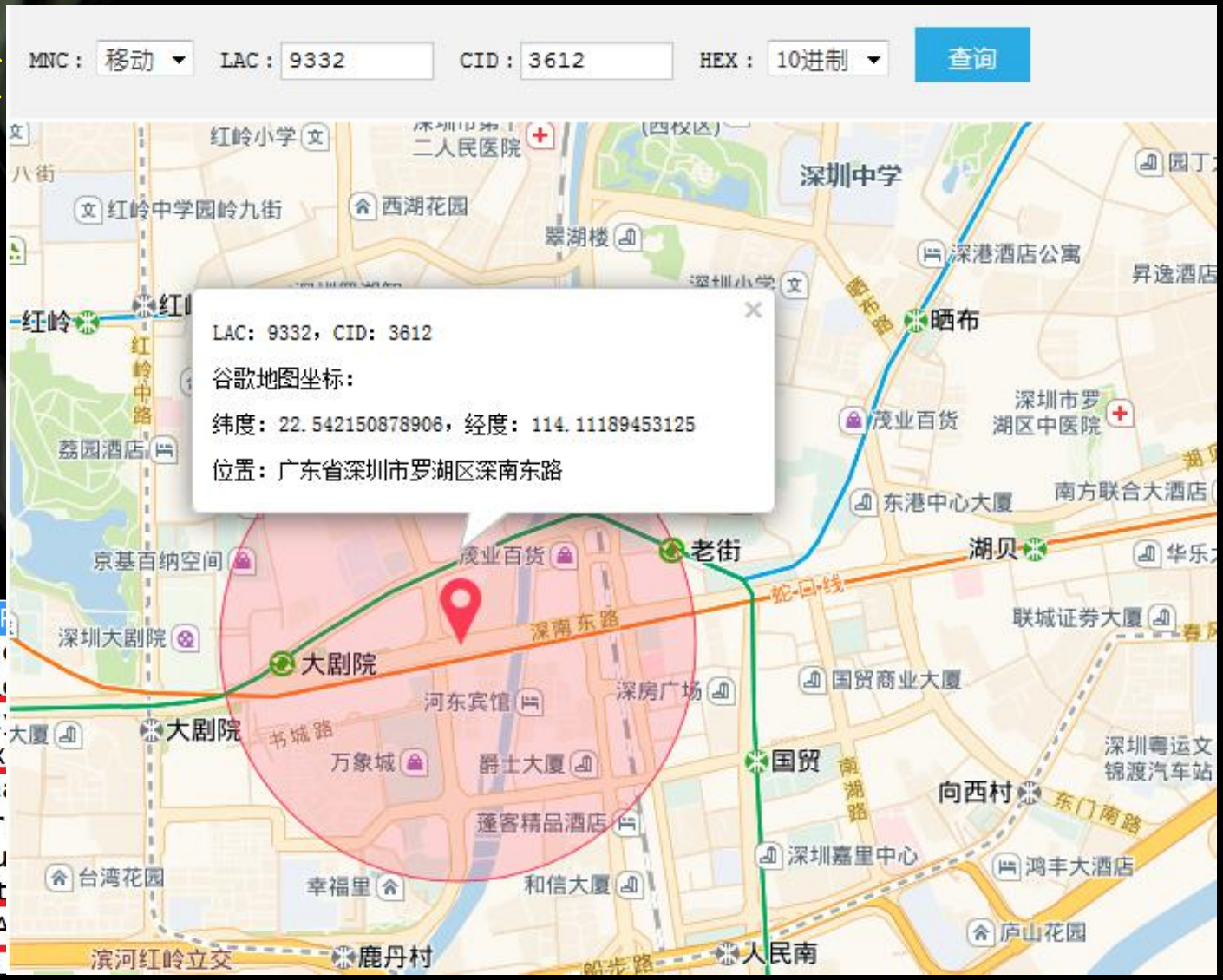
- 可根据设备内置的GPS模块锁定当前位置
- 第三方APP读取GPS数据



CPS基站定位

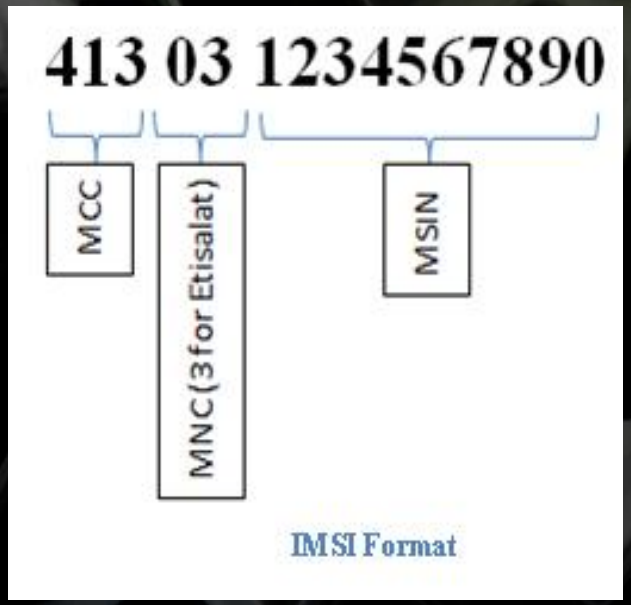
- 可根据空
  - MCC，
  - MNC，
  - LAC，
  - CID，
  - LAT，
  - LNG，





IMSI的意义

- IMSI：国际移动用户识别码
  - 15位， MCC+MNC+MSIN




```
2013.09.02 12:45:19 - TMSI/P-TMSI - 0x3196874c
2013.09.02 12:45:27 - TMSI/P-TMSI - 0x729c843d
2013.09.02 12:45:31 - TMSI/P-TMSI - 0xa01e8b9e
2013.09.02 12:45:31 - TMSI/P-TMSI - 0x4cc18296

2013.09.02 12:43:19 - IMSI - 15229  XXX(460022293425302)
2013.09.02 12:43:45 - IMSI - 18729  XXX(460027290117428)
2013.09.02 12:44:15 - IMSI - 13991  XXX(460001184924500)
2013.09.02 12:44:20 - IMSI - 15291  XXX(460022915557187)
2013.09.02 12:44:27 - IMSI - 13402  XXX(460020029685343)
2013.09.02 12:44:36 - IMSI - 13659  XXX(460009201573802)
2013.09.02 12:44:39 - IMSI - 15229  XXX(460022293620505)
2013.09.02 12:44:42 - IMSI - 13572  XXX(460002590791805)
2013.09.02 12:44:50 - IMSI - 15929  XXX(460029294561848)
2013.09.02 12:44:54 - IMSI - 13484  XXX(460020848270940)
2013.09.02 12:45:03 - IMSI - 13792  XXX(460009287018047)
2013.09.02 12:45:03 - IMSI - 13468  XXX(460020688344423)
2013.09.02 12:45:05 - IMSI - 13991  XXX(460001154924420)
2013.09.02 12:45:07 - IMSI - 13572  XXX(460002550794668)
2013.09.02 12:45:29 - IMSI - 15114  XXX(460021148842143)
2013.09.02 12:45:33 - IMSI - 18806  XXX(460078068703244)
2013.09.02 12:45:39 - IMSI - 13619  XXX(460009241116767)
```

不止是运营商

经度	纬度	CI	CELL	IMSI	STARTTI
104.0656	30.62311	7814	[redacted]	[redacted]	04-12月-14 07.17.25.937000 上午
104.0656	30.62311	7814	[redacted]	[redacted]	04-12月-14 07.09.36.859000 上午
104					
104					

用户上下班行为轨迹图

VIP用户*从家到公司有两种出行方案

家和公司业务量最多站点详细信息

地理位置	行政归属	小区中文名称	LAC	CI
公司	浦东新区	金桥园区办公研发楼14		
家	闵行区	水清北_3(0)		

反跟踪技巧：IMSI会告诉你~

-
-

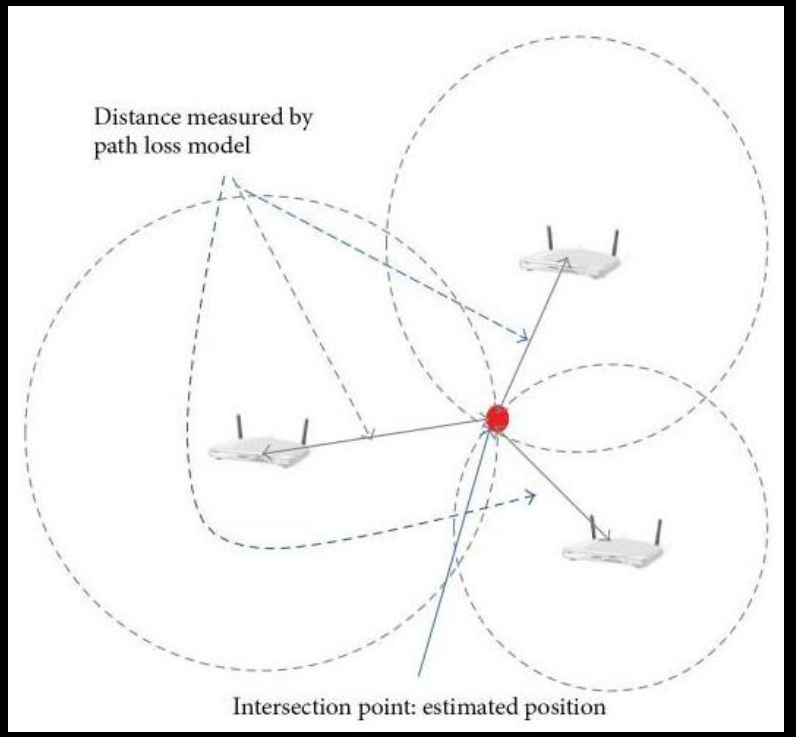
```
23:31:01 - IMSI - 460004492108950(1371449XXXX)
23:31:01 - IMSI - 455033101361019(Macao,China)
23:31:05 - IMSI - 455030100093221(Macao,China)
23:31:11 - IMSI - 460016160010829(1300616XXXX)
23:31:12 - IMSI - 460000450882693(1358045XXXX)
23:31:13 - IMSI - 460014432902591(1312443XXXX)
23:31:13 - IMSI - 455033200242898(Macao,China)
23:31:16 - IMSI - 455033200127445(Macao,China)
23:31:18 - IMSI - 455033200033774(Macao,China)
23:31:24 - IMSI - 455033200139340(Macao,China)
23:31:26 - IMSI - 222995307589879(Italy)
23:31:27 - IMSI - 455033200235157(Macao,China)
                                 59(Hong Kong,Ch
                                  9(Macao,China)
                                  0(Macao,China)
                                  5(1396583XXXX)
                                  2(Macao,China)
                                  0(1341452XXXX)
                                  0(Macao,China)
                                  3(Hong Kong,Ch
                                  4(Macao,China)
                                  0(1363108XXXX)
                                  8(Korea (Repub
                                  7(Macao,China)
                                  2(1316262XXXX)
```


```
2013.11.20 01:05:29 - IMSI - 460028118360642(1581183XXXX)
2013.11.20 01:06:22 - IMSI - 460000750638067(1356075XXXX)
2013.11.20 01:06:37 - IMSI - 460023999299010(1509992XXXX)
2013.11.20 01:07:19 - IMSI - 460021192453331(1511924XXXX)
2013.11.20 01:07:33 - IMSI - 460004594255393(1392459XXXX)
2013.11.20 01:07:55 - IMSI - 460078582900389(1885829XXXX)
2013.11.20 01:08:20 - IMSI - 460023192226911(1501922XXXX)
2013.11.20 01:08:27 - IMSI - 460004760541323(1355476XXXX)
2013.11.20 01:08:53 - IMSI - 460002319510390(1390231XXXX)
2013.11.20 01:09:14 - IMSI - 460029157468844(1591574XXXX)
2013.11.20 01:09:20 - IMSI - 460022202254718(1522022XXXX)
2013.11.20 01:09:31 - IMSI - 460016596289655(1360659XXXX)
2013.11.20 01:09:31 - IMSI - 460016698266187(1380669XXXX)
2013.11.20 01:09:35 - IMSI - 460015517609121(1867551XXXX)
2013.11.20 01:09:36 - IMSI - 460014894277822(1340489XXXX)
2013.11.20 01:10:03 - IMSI - 460010152603790(1862015XXXX)
2013.11.20 01:10:09 - IMSI - 460016688286665(1380668XXXX)
2013.11.20 01:10:14 - IMSI - 460079145837264(1471458XXXX)
2013.11.20 01:10:16 - IMSI - 460017992088689(1320799XXXX)
2013.11.20 01:10:19 - IMSI - 460014796908607(1316479XXXX)
2013.11.20 01:10:20 - IMSI - 460009012221711(1372901XXXX)
2013.11.20 01:10:25 - IMSI - 460016052612393(1862605XXXX)
2013.11.20 01:10:36 - IMSI - 460017982045551(1320798XXXX)
2013.11.20 01:10:43 - IMSI - 460078237045974(1882370XXXX)
2013.11.20 01:10:43 - IMSI - 460010362608108(1862036XXXX)
```

WPS WiFi定位

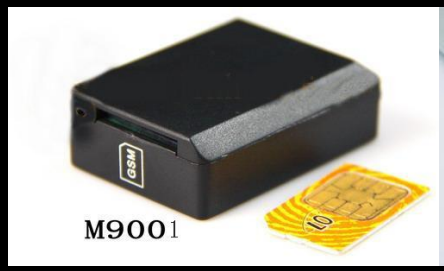
- **WiFi RSSI指纹库**
  - 基于WarDriving采集
  - BSSID
  - RSSI，接收的信号强度指示

- **WPS局限性**
  - 目标手机必须开启WiFi
  - MAC与手机号码的匹配问题



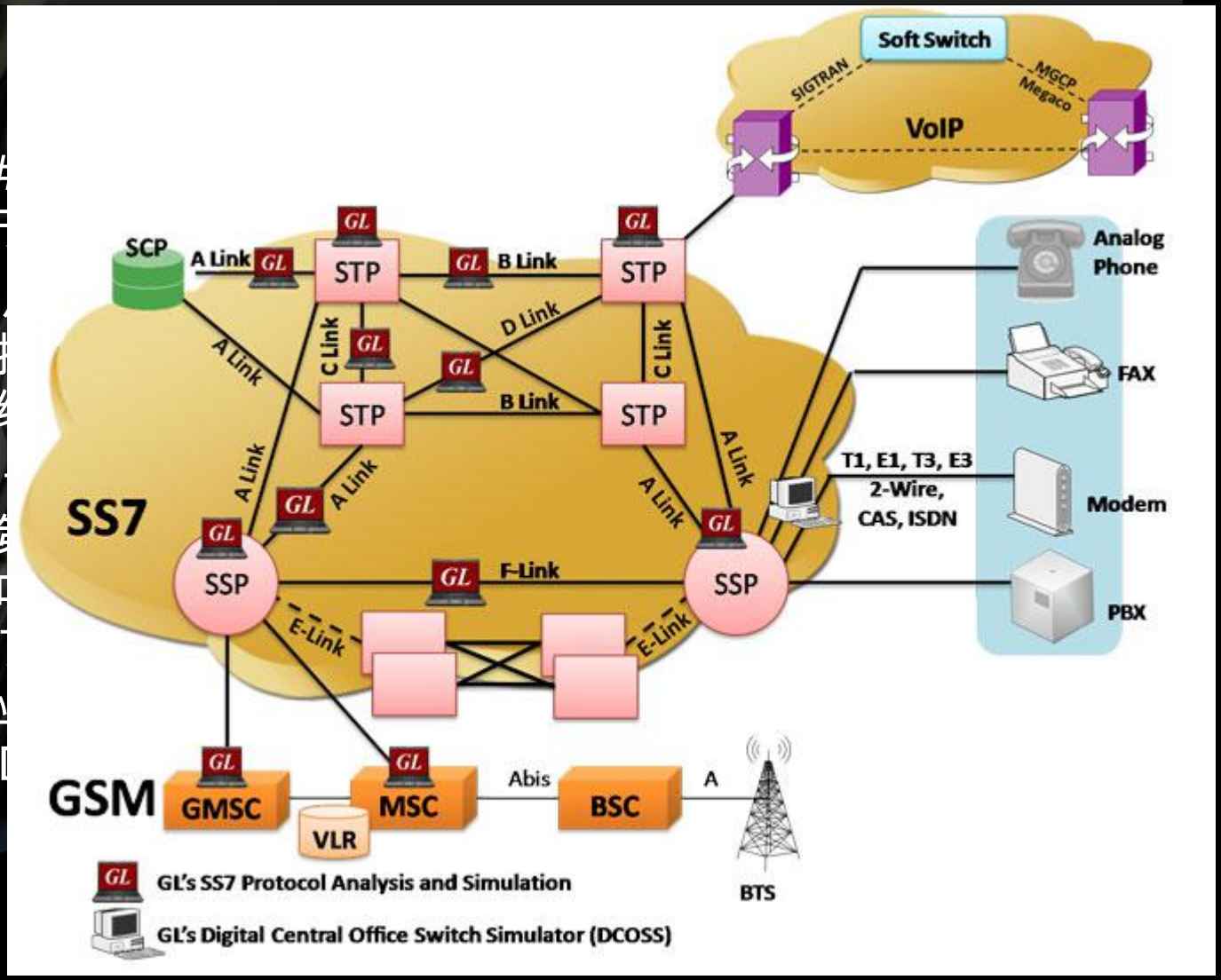
监听模块定位

- 基本功能
  - 监听功能
  - 声控功能
  - 支持短信参数设置
    - 激活监听模式
    - 目标定位
- 特点
  - 支持GSM
  - 待机一周以上
  - 外型多样化



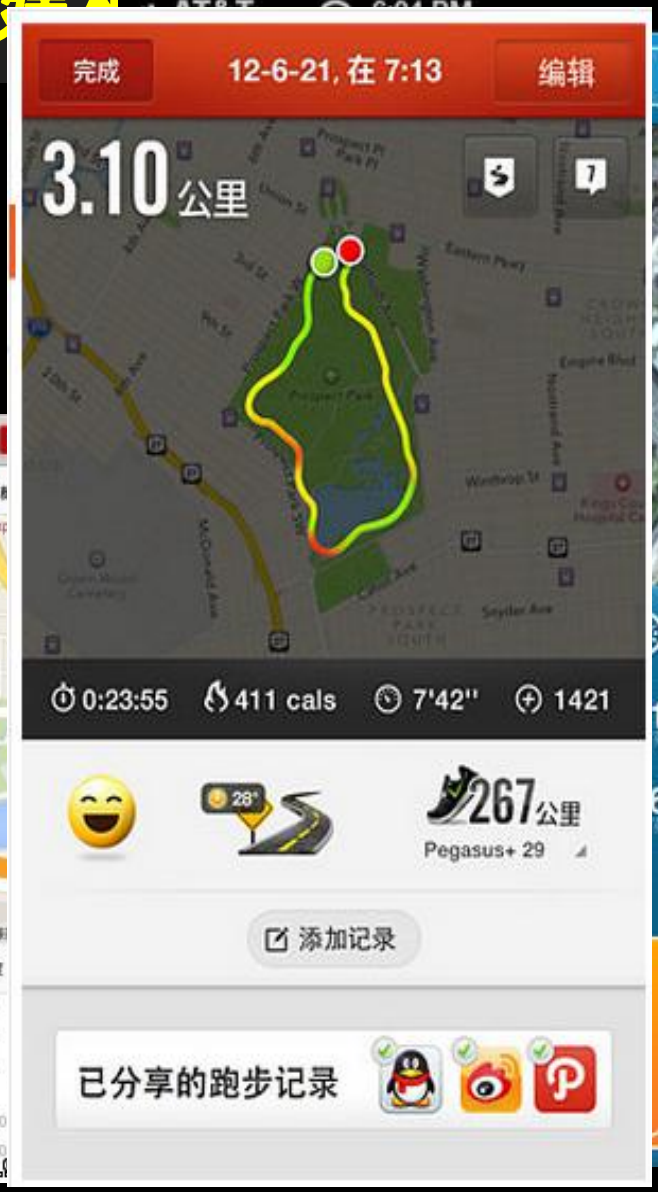
SS7

- SS7
  - 信令系统#
    ，主要用
  - SS7 中采
    带外信令
    组交换网
  - SS7 起源
    后期，是
    为电话呼
    功能包含
    作和综合
    Services



第三方APP：个人行动规律建模

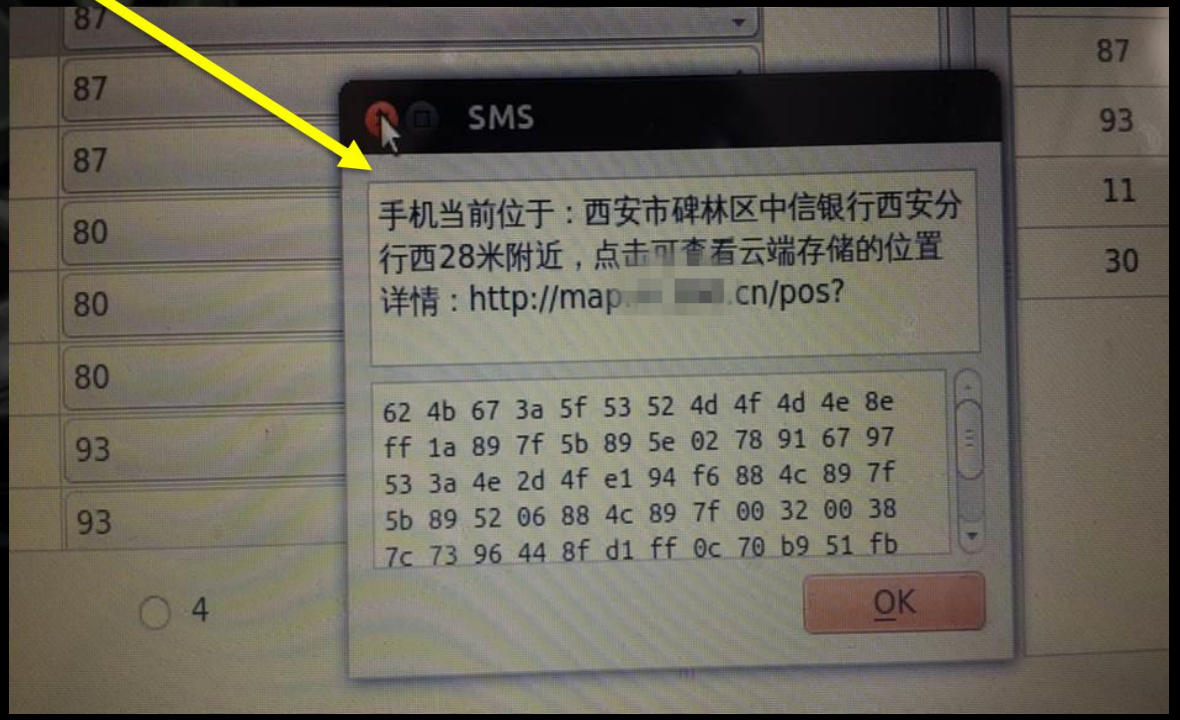
- 家庭住址？公司地址？很难么
- 不，这和社工没关系
- APP会告诉你



云存储类APP的手机定位

1：服务器端远程备份短信联系人等资料。
2：远程锁定/擦除手机所有数据。
3：支持通话转移功能。
4：发送地图信息点到手机/电脑
5：定位你的手机

APP主要功能

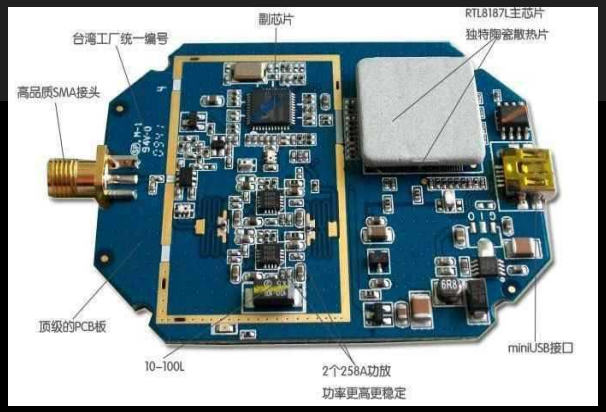


- 国内WiFi Hack历史
- 无线主流Crack技术
- 反物质平台

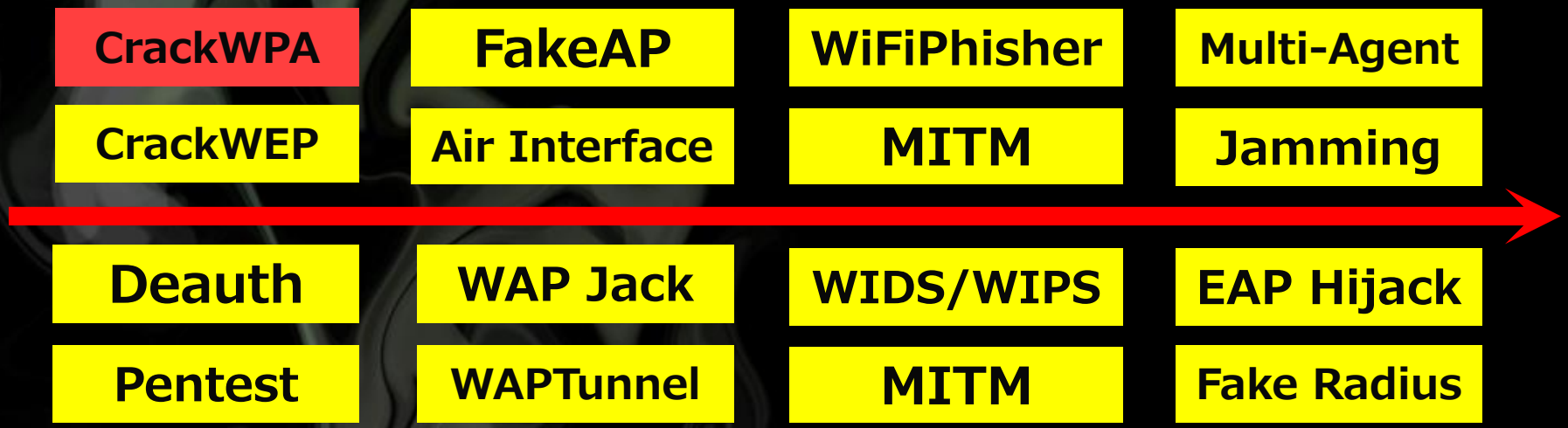
WiFi重灾区

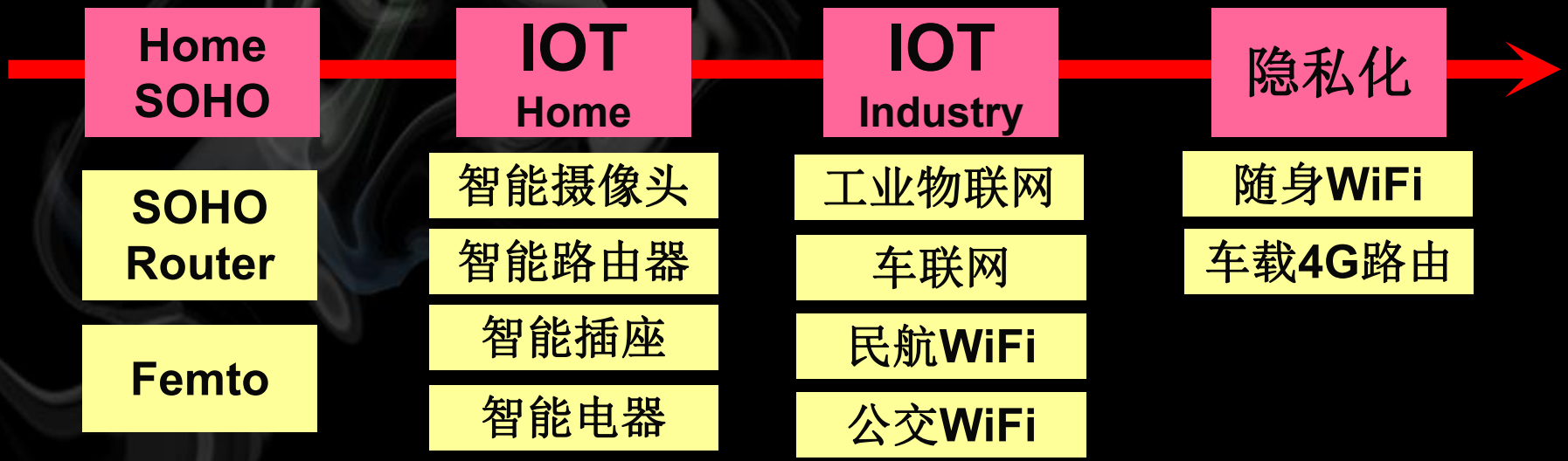
国内WiFi Hacking 历史

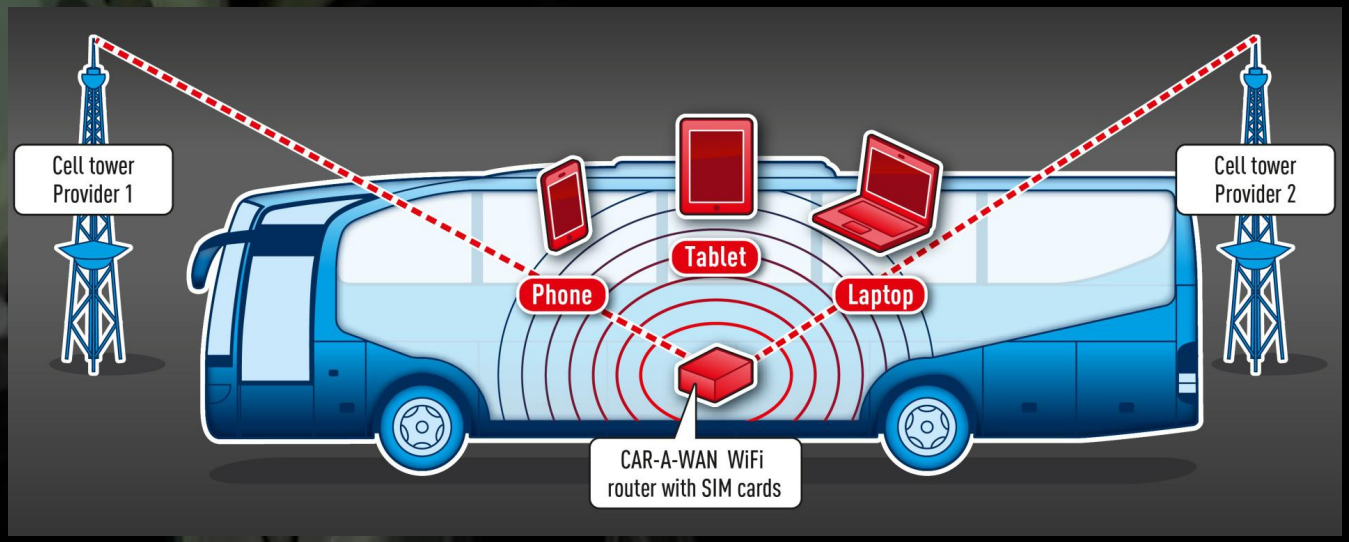
- 2006~2007 觉醒时期
- 2008~2009 蹭网卡鼎盛时期
- 2009~2011 “多国杀”时期
  - 创造奇迹的RTL8187
  - 永无止境的发射功率
  - 悲催的蚂蚁战车
  - SpoonWEP/SpoonWPA
  - 黑色产业链的形成
- 2010~2012 GPU时期
  - EWSA
- 2012~2014 移动破解时期
- 2015~2016 云破解时期+回归

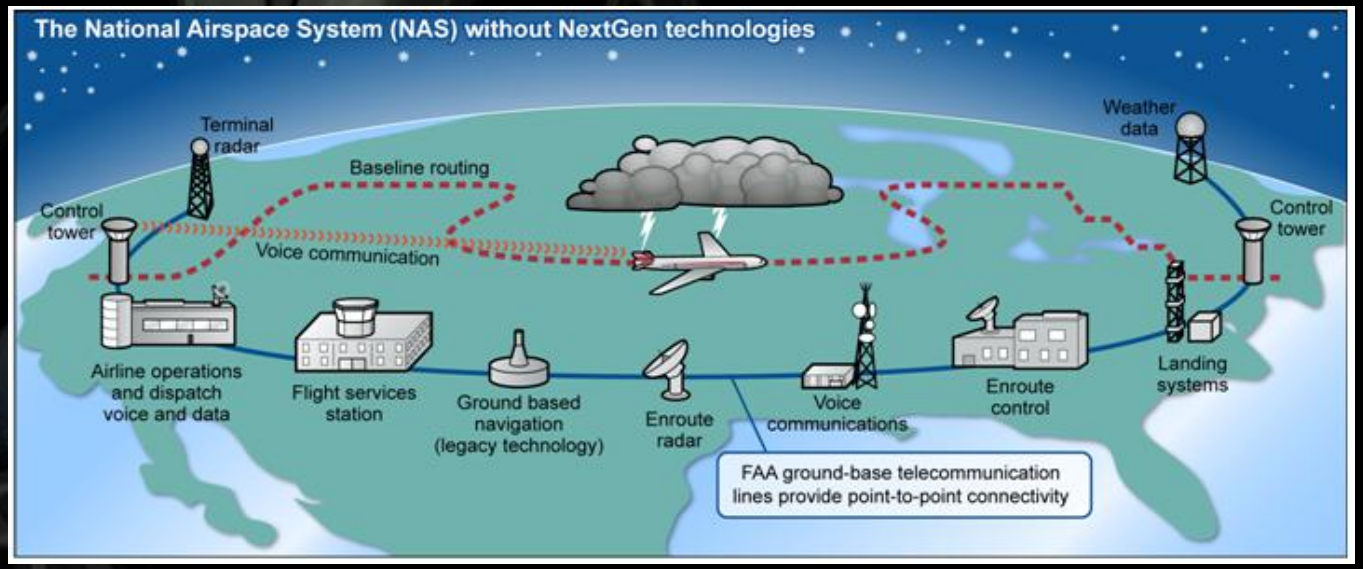


WiFi Attackの趋势



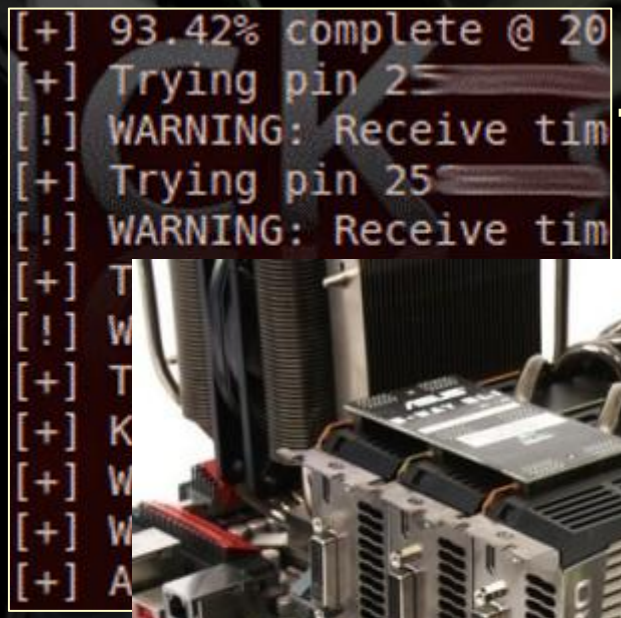



Cell tower
Provider 1
Cell tower
Provider 2
Phone
Tablet
Laptop
CAR-A-WAN WiFi
router with SIM cards


The National Airspace System (NAS) without NextGen technologies
Terminal
radar
Baseline routing
Control
tower
Voice communication
Weather
data
Control
tower
Airline operations
and dispatch
voice and data
Flight services
station
Ground based
navigation
(legacy technology)
Enroute
radar
Voice
communications
Enroute
control
Landing
systems
FAA ground-base telecommunication
lines provide point-to-point connectivity

Crack
#主流

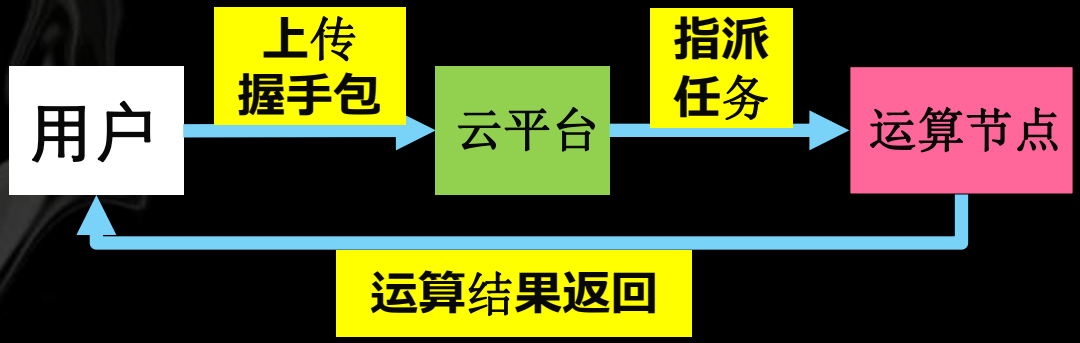
- Dictionary
- WPA PMK Hash
- WPS Online / Offline
- Distributed
- GPU
- Cloud



Cloud based のWiFi Crack Platform

{反物质}无线安全评估云平台

AntiMatter
Kill Password is our job



组合	40,000,000,000,000
样本	5,000

```
 [0:08:09] listening for handshake...
 [0:00:11] handshake captured! saved as "hs/nossid_78-44-76-
F5-E6-82.cap"

 [+] 1 attack completed:

 [+] 1/1 WPA attacks succeeded
        nossid (78:44:76:F5:E6:82) handshake captured
        saved as hs/nossid_78-44-76-F5-E6-82.cap

 [+] starting AntiMatter Cloud Compute on 1 handshake
 [!] Now activating handshake upload process....
 [*] 2 - Upload capfile now
 [*] 1 - Upload and upload other Failed capfile --- wait for
 :)
 [*] 0 - exit
[*] Select number and Enter:>2

 [*]- Check Client API_KEY now...
OK
 [*] Found...:  /hs/nossid_78-44-76-F5-E6-82.cap
 [*] Upload...:  /hs/nossid_78-44-76-F5-E6-82.cap
[*] Upload Done:  /hs/nossid_78-44-76-F5-E6-82.cap
```


AntiMatte
Kill Password is our job
123321
Gold: 0
首页
任务中心
新建任务
管理任务
成功记录
留言/回复
新建留言
我的留言
安全中心
修改密码
登录记录
安全退出
状态
结果
运行中
已完成
第 1 轮-未
第 1 轮-已
第 2 轮-未
第 2 轮-已
10659226
10658309
+86 170 52.
106901571.
+86 158 29.
106575251.
106902281.
新建
【反物质】运算成功:
SSID:TP-LINK_lan 密
码:hakuramatata
06:32
【反物质】运算成功:
SSID:123456qq 密
码:susu0709
07:16
2015/07/27 星期一
【反物质】运算成功:
SSID:Tenda_190A70
密码:23234098
22:33
输入内容

应用领域

内部安检　安全评估　无线渗透　边界防护

RP分割线

家庭防窥　隔壁老王　邻家妹纸　小区鲜肉

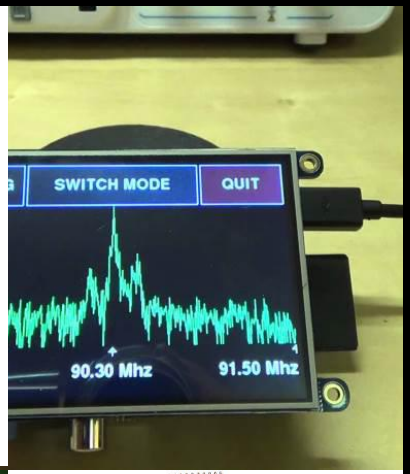



- SDR
- WiFi
- ZigBee
- Car-Hacking
- IOT
- SmartDevice
- AirLine

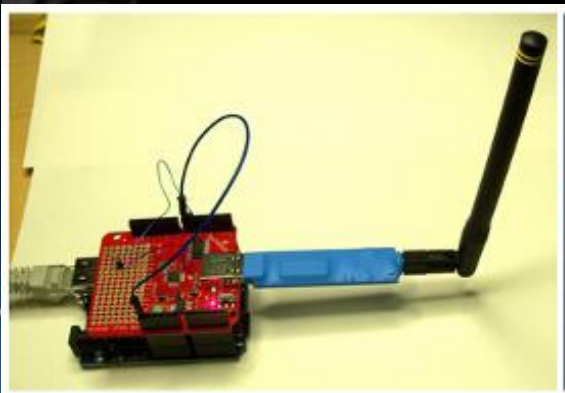
More


© IOActive/Ian Amit


QINMING
Qinming 2312M SSI
IS-1 unipolar
SN 25
Made in
QINMING
Qinming 2312S SSI
IS-1 unipolar / bipolar
SN 200014
Made in China


SWITCH MODE
QUIT
90.30 Mhz
91.50 Mhz


Aircraft Hacking
Practical Aero Series




Meter ID
kWh Reading

杨　哲
(Longas)
ZerOne无线安全研究组织
longaslast@126.com

ZerOne
WirelessSec Research

Thanks !!