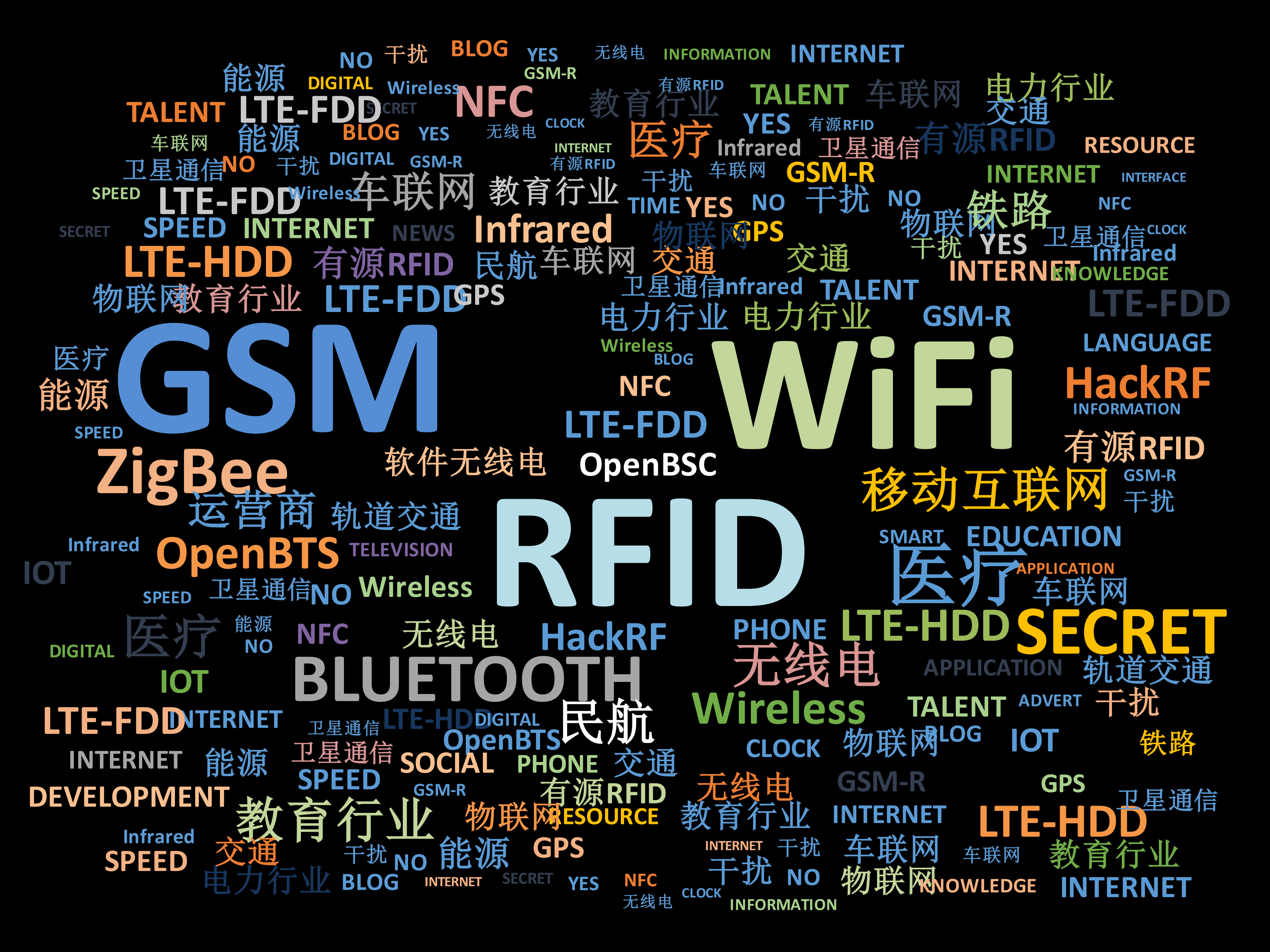
XDef 2014

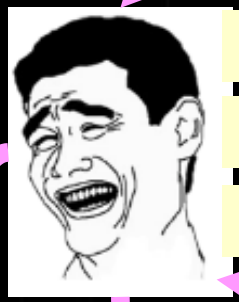
无线安全@幸忧参半的2015

杨　哲 (Longas)
ZerOne无线安全研究组织
ZerOne WirelessSec Research



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

2007~2014：国内无线安全研究



GNU Radio

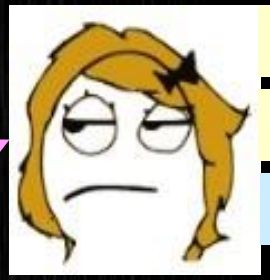
HackRF

USRP

RFID

PM3

NFC



Bluetooth

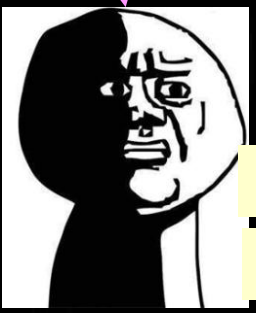
Ubertooth

被遗忘的

GSM

OpenBTS

OscomBB



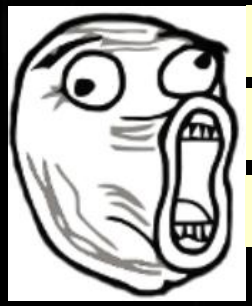
车联网

GPS

WLAN

蹭网卡

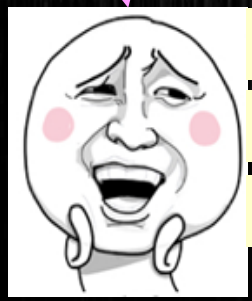
BT3 /4/5



物联网

ZigBee

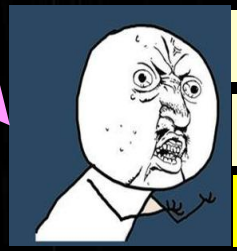
智能家居



信令研究

运营商业务流

OpenIMS



802.1X

BYOD/BYOA

深入研究

无线监听: 一直存在

对象

- WLAN
- 2G/3G/4G
- Bluetooth
- ZigBee
- 民用无线电
- ……

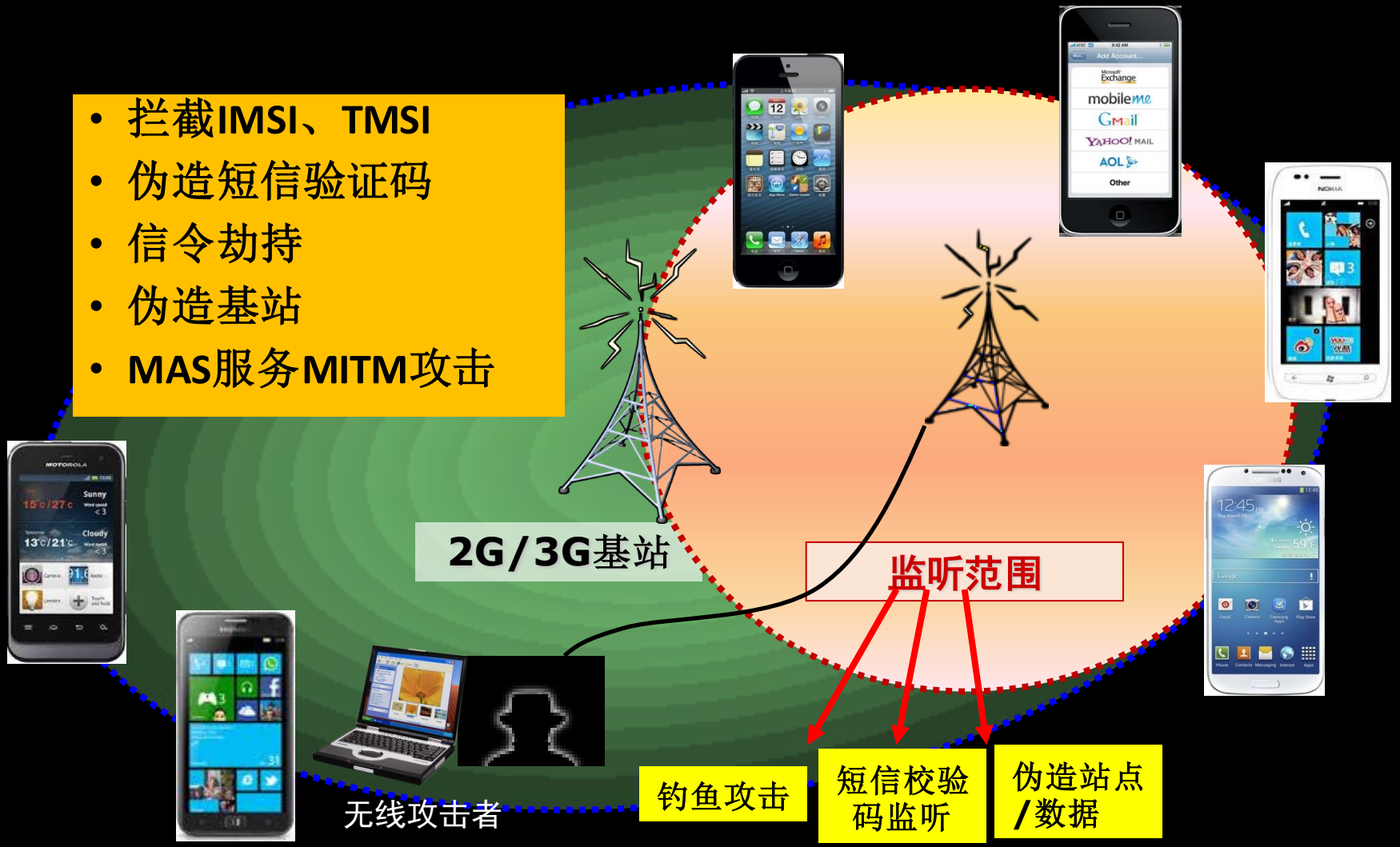
方式

- 出口镜像设备
- 监听解决方案
- 单点空口监听
- 区域空口监听

- 改装类设备
- 整合类设备
- 音频放大器
- 专用窃听工具

针对2G/3G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



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


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

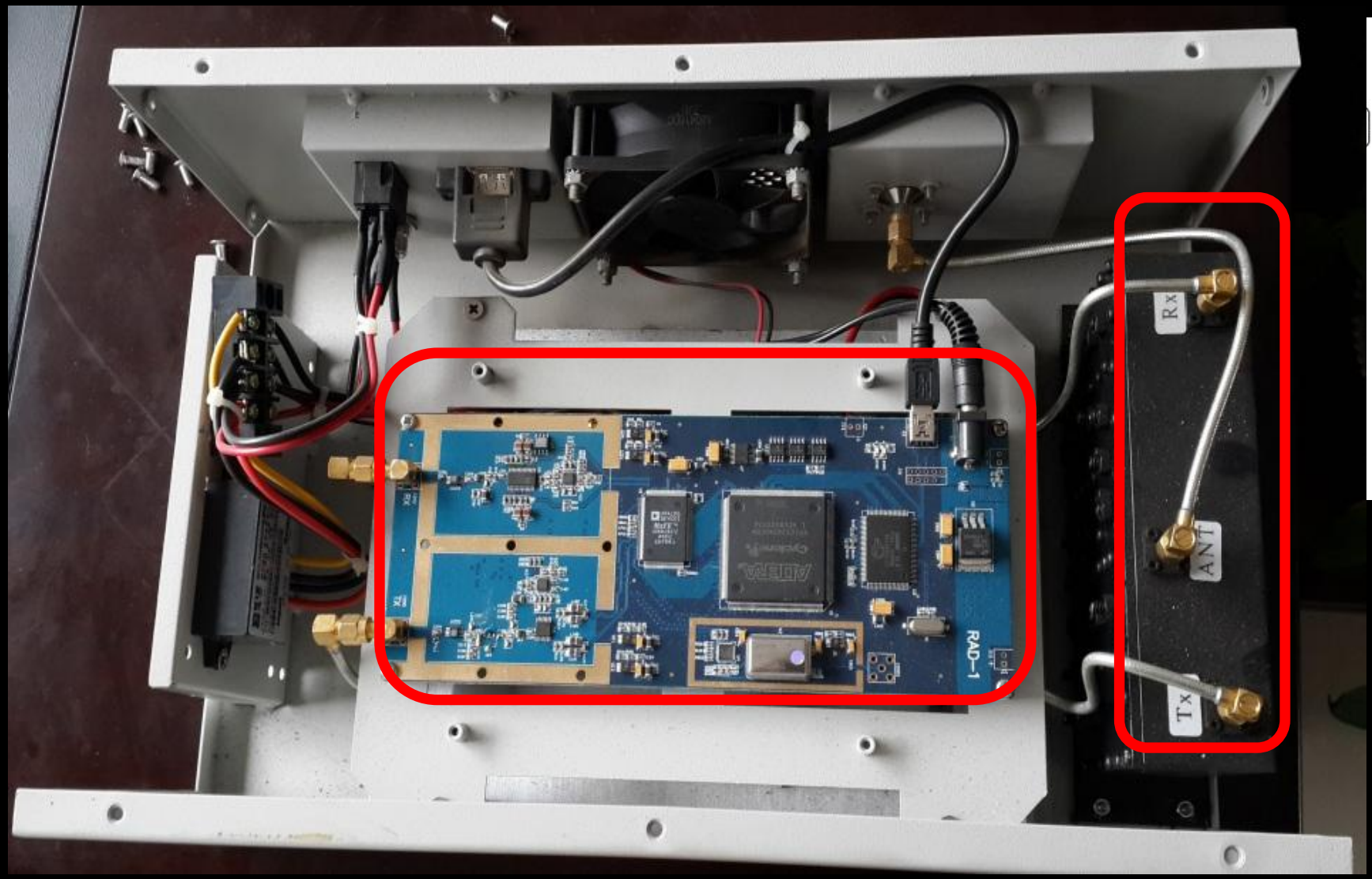
Fake AP +OpenBTS

- 以前
  - Fake ESSID
  - Fake BSSID
  - Fake DHCP
- 现在
  - Fake AP
  - DNS Spoof
  - Fake SMS
- 增加的真实感：
  - 登录页面的短信发送
  - 难以识别的账户短信

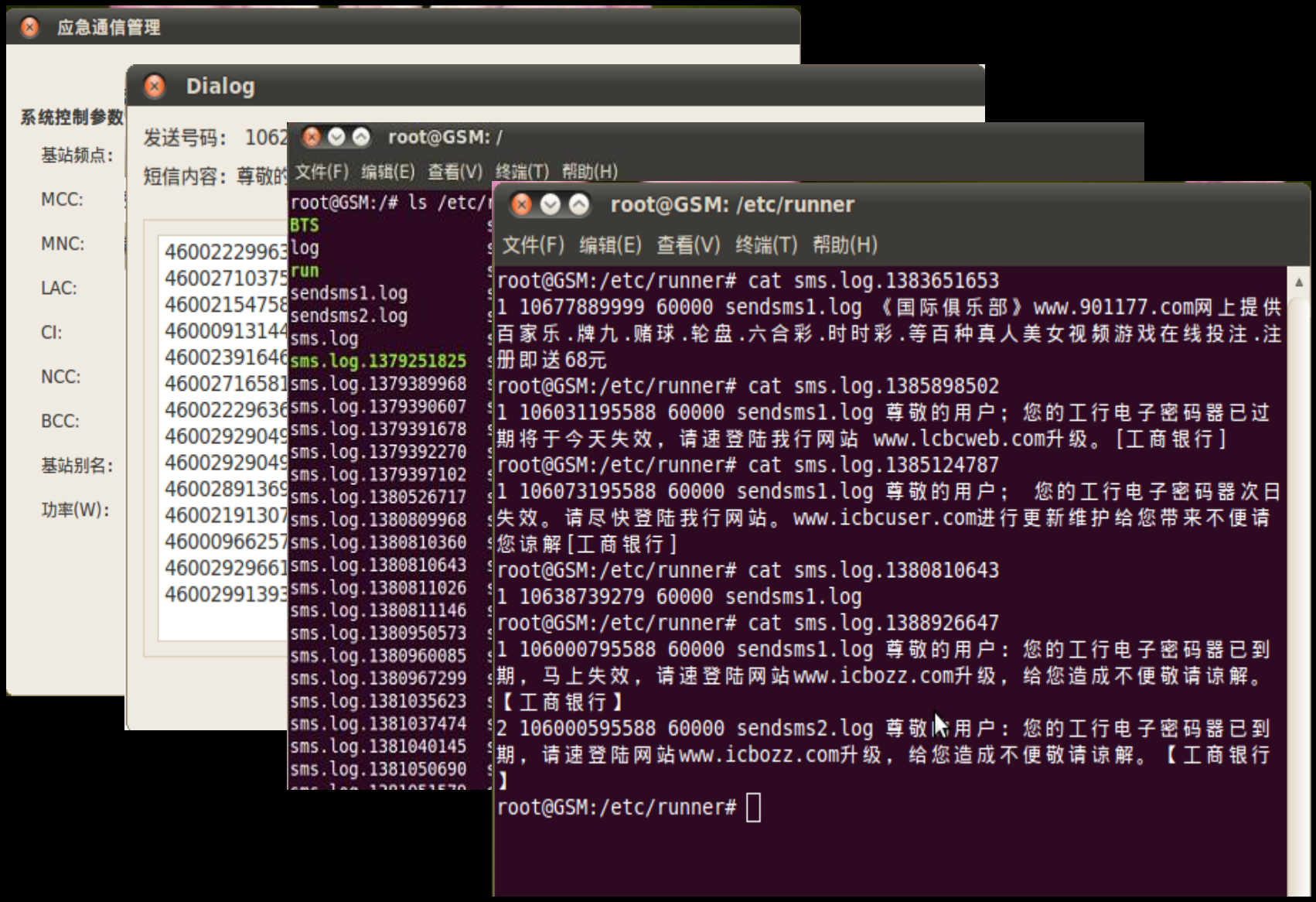
伪基站小时代

- OpenBTS
- ~~USRP ?~~
- RAD-1

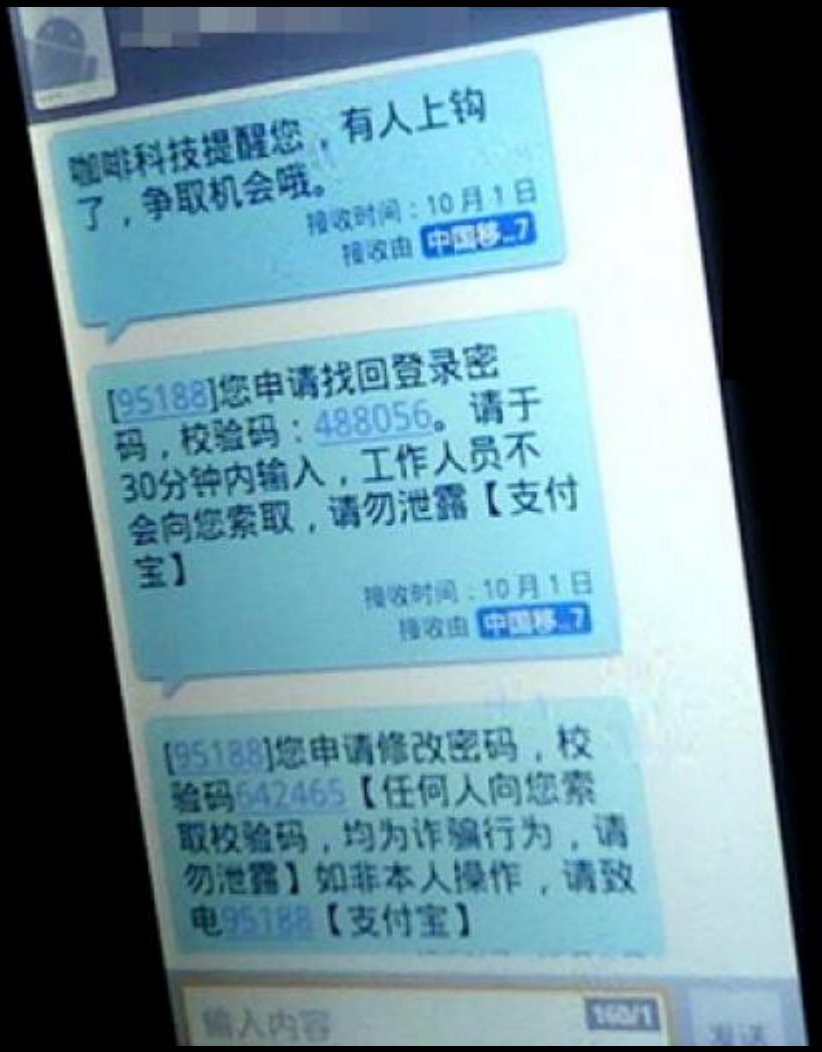
“伪基站”取证（硬件部分）



“伪基站”取证（软件部分）

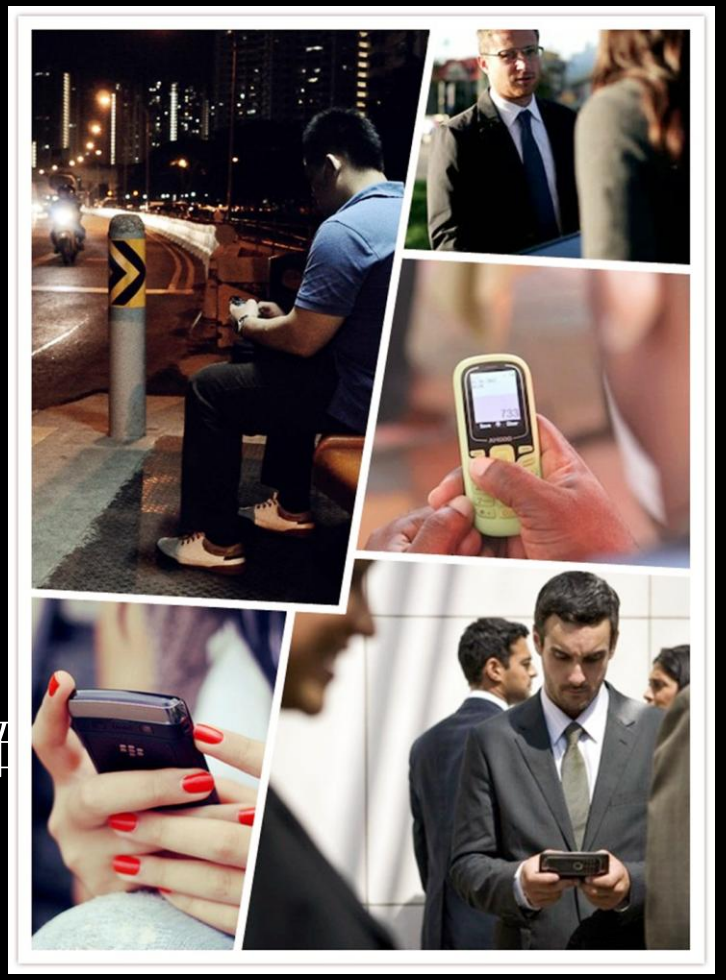

应急通信管理
系统控制参数
基站频点:
MCC:
MNC:
LAC:
CI:
NCC:
BCC:
基站别名:
功率(W):
Dialog
发送号码: 1062
短信内容: 尊敬的
root@GSM: /
文件(F) 编辑(E) 查看(V) 终端(T) 帮助(H)
root@GSM:/# ls /etc/
BTS
log
run
sendsms1.log
sendsms2.log
sms.log
sms.log.1379251825
sms.log.1379389968
sms.log.1379390607
sms.log.1379391678
sms.log.1379392270
sms.log.1379397102
sms.log.1380526717
sms.log.1380809968
sms.log.1380810360
sms.log.1380810643
sms.log.1380811026
sms.log.1380811146
sms.log.1380950573
sms.log.1380960085
sms.log.1380967299
sms.log.1381035623
sms.log.1381037474
sms.log.1381040145
sms.log.1381050690
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

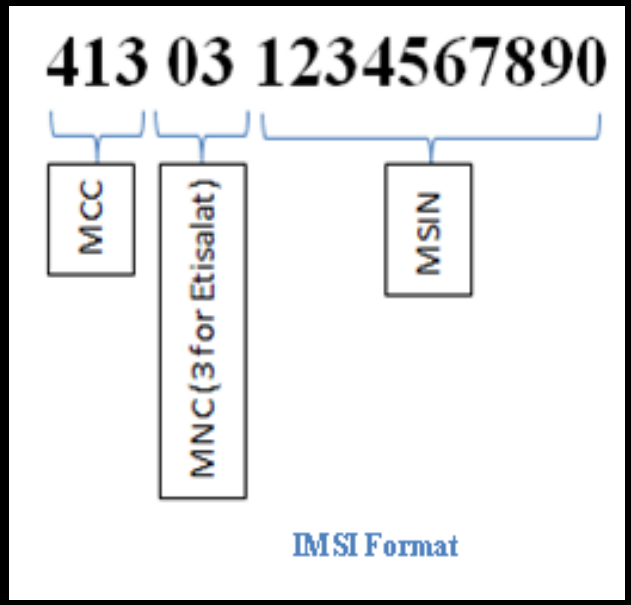
犯罪实施的低成本化、机动化与多样化

- 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
- 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



关于IMSI

- IMSI：国际移动用户识别码
  - 15位， MCC+MNC+MSIN
- 常态化个人路线建模
  - 工作、生活
- 重复率筛选
  - 手机所在位置区识别号LAI
  - 记下最近1个月出现率最高的全部IMSI，添加到黑名单列表中
  - 排除熟人/同路/沿线住址



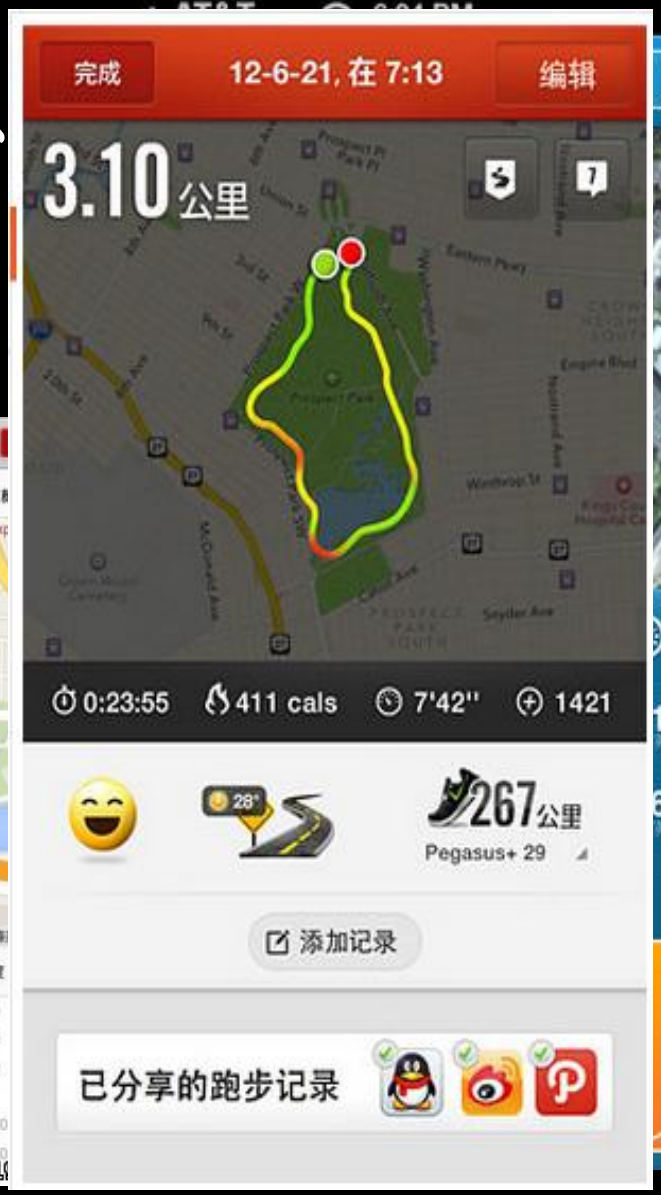
IMSI会告诉你

```
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)
                                 9(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)
```

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
- 你说对了，APP会告诉你



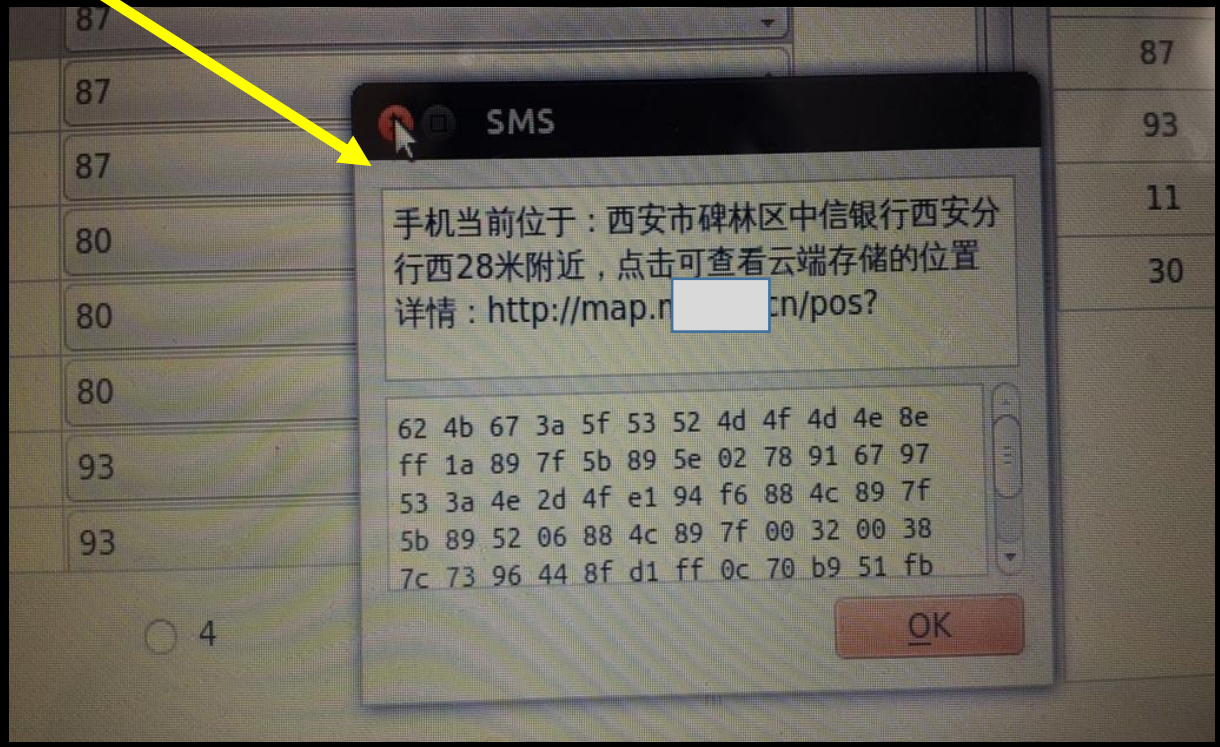
云存储类APP的手机定位

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

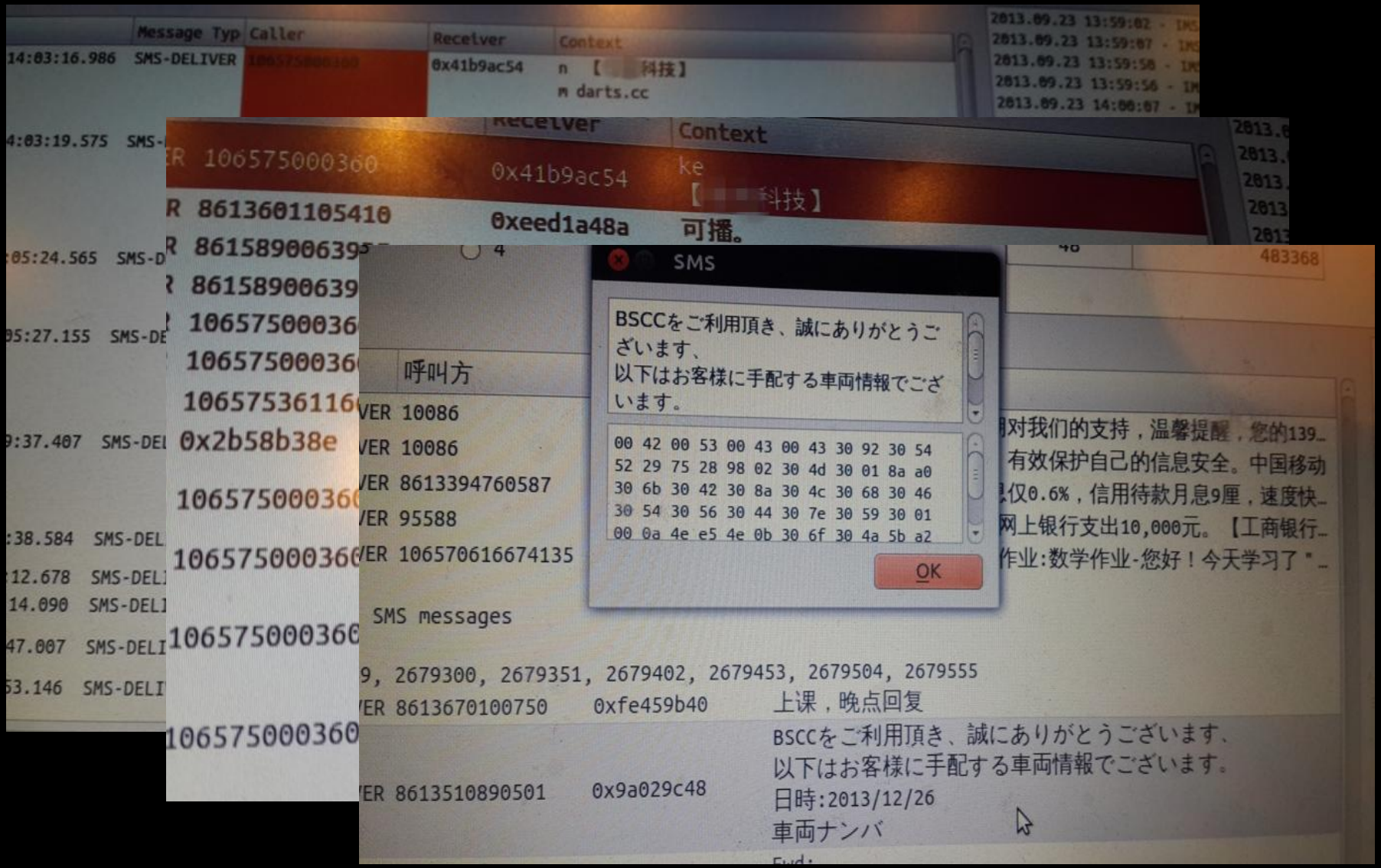
APP主要功能

APP厂商列表

百度云
360云盘
苹果iCloud 云存储
腾讯手机管家
360手机卫士
LBE安全大师



XX安全会议现场の隔墙斩获



人多 == 适宜RFID/BT/WiFi Hacking

STIX：网络空间威胁情报分享标准

einstein
ANALYSIS PORTAL

powered by the
NetSA
Security Suite

Portal

« July » « 2006 »

Su	Mo	Tu	We	Th	Fr	Sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

11:00

hour **day** week month

linear **log**

Views

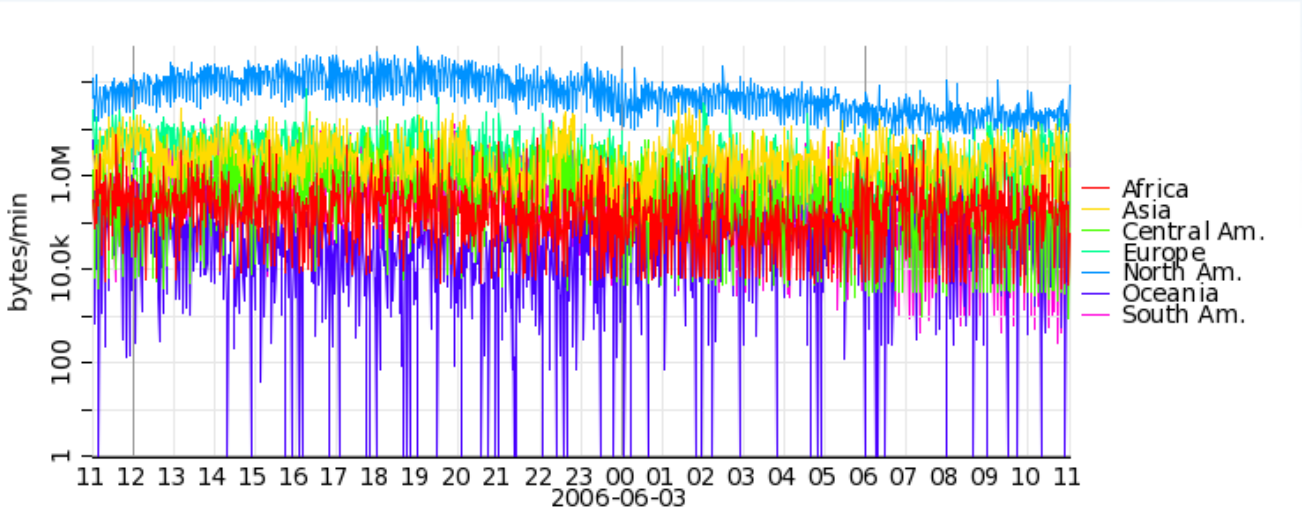
Geographic (In / Out)
Server ports (In / Out)
Client ports (In / Out)
Protocols (In / Out)

Recent Events

06 Jul 2006 - 20:28

Geographic View (Outgoing)

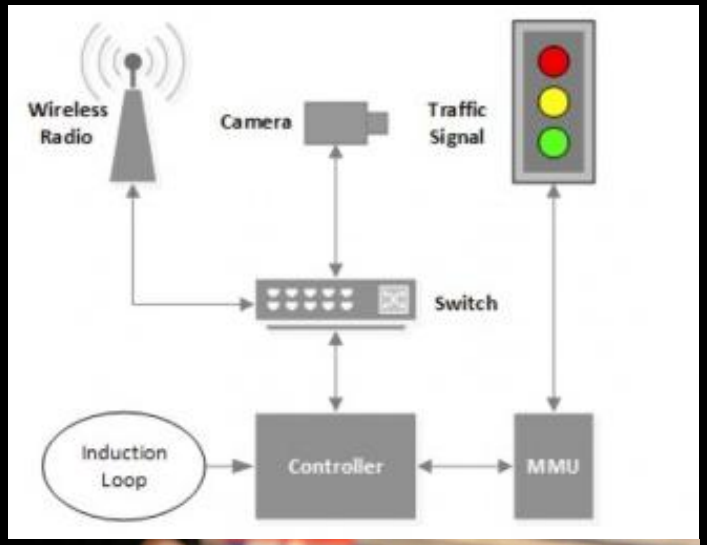
1 day starting Fri Jun 2 11:00:00 2006



Info2 Wireless

交通

- 交通指挥系统/交通灯局点
- 出租车/公交无线调度系统
- 车辆GPS定位系统
- 车辆无线电呼叫系统
- RFID地铁/公交卡
- 巴士车载视频接收系统



Car@Attack

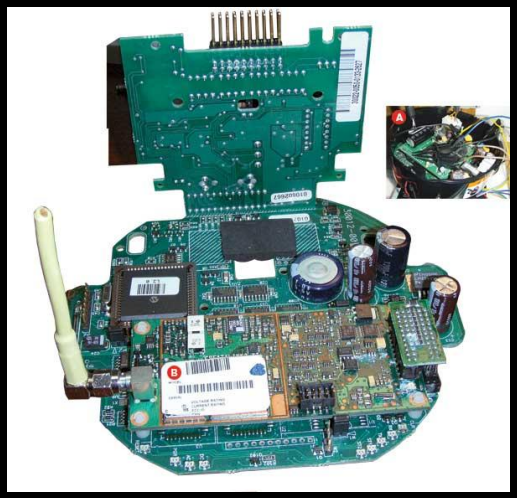
- 车辆智能辅驾系统/安全系统攻击
- 车辆外部信号破坏与干扰
- 车辆前部雷达探测干扰攻击……

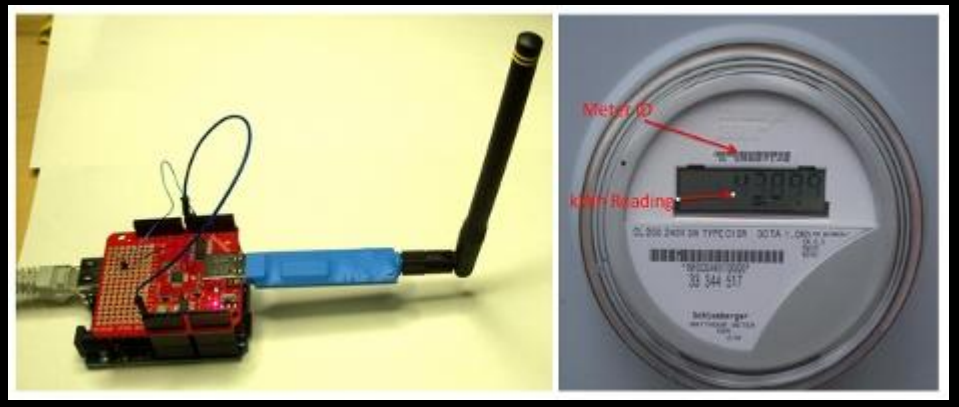
Info2 Wireless 民航

- ACARS通讯寻址与报告系统
- OMIS运行管理系统
- ADS-B播式自动监察系统
- FMS飞行管理系统
- 无线电通信
- 舱内WiFi应用
- GPS导航信号
- 非加密频段应用
- 厂商特殊设计通信
- 机场安检设备

电力

- 智能电表无线抄表
  - 国网645协议
  - 国网376.2协议
  - ANSI C12.18
  - ANSI C12.19
- 电网GPRS自动化数据采集
- PLC电力载波通信
- GSM无线报警系统
- 内部门禁系统



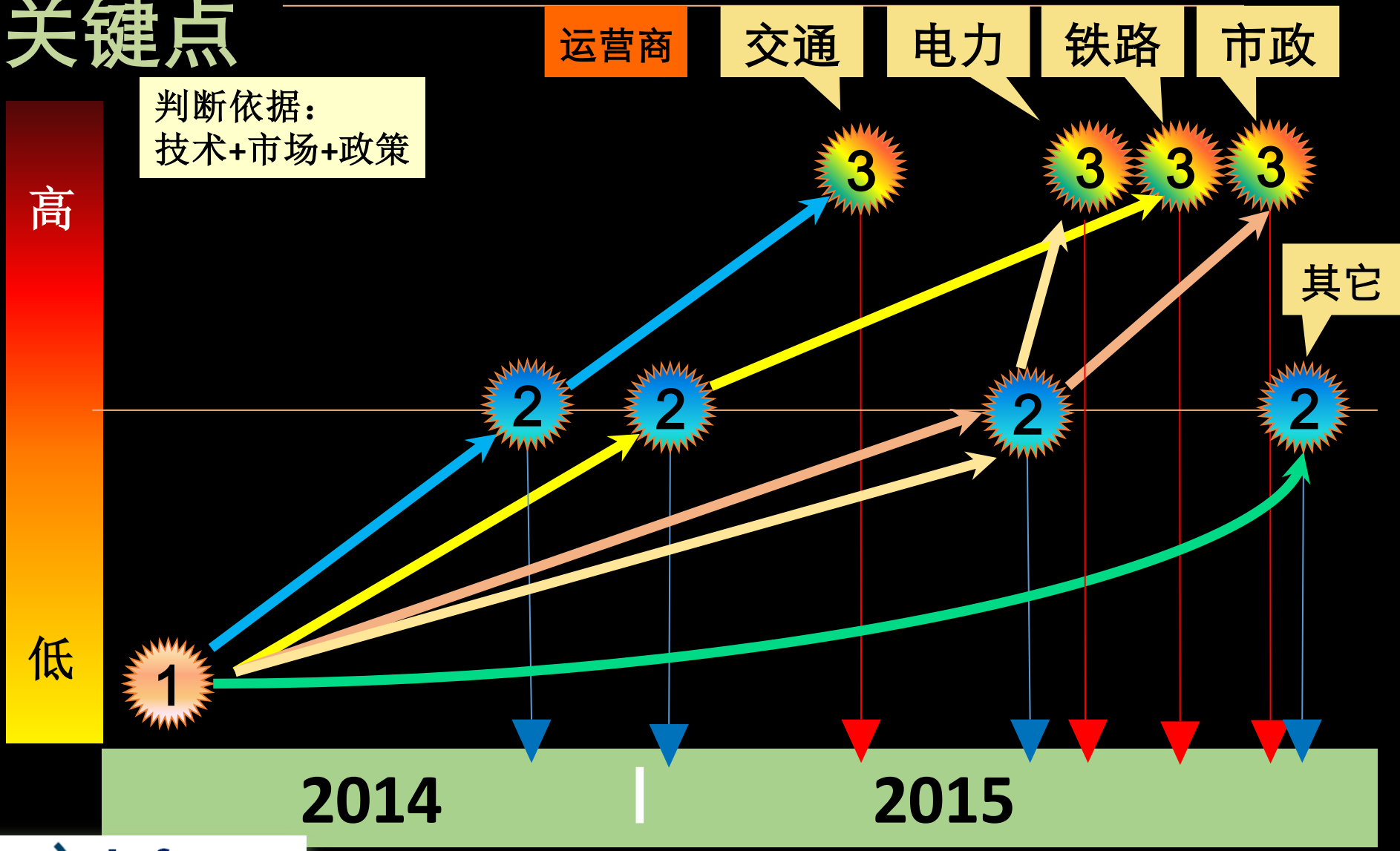


Info2 Wireless

医疗

- 个人健康自动化采集设备
  - 移动医疗终端
  - 可穿戴感应设备
- 个人健康自动化依赖设备
  - 植入式心脏起搏器/除颤器
  - 胰岛素泵
  - 神经监护系统
  - 自主呼吸系统
- 远程医疗/遥控手术机器人
- 医院内WiFi网络解决方案

关键点



Info2 Wireless

ZerOne无线前瞻性威胁研究小组

【ZerOne】Forward-Looking Threat Research Team

2015@喜忧参半

多维度空间安防

- 数年的社会应用积累与铺垫
- 与民生领域结合愈发紧密

→ 基础

- 相对低廉的入门要求
- 民间团体蜂拥的投入势头

→ 现状

- 炫耀型展示＋潜在心理优越感
- 拿来主义＋功利性研究

→ 心态

- 缺乏实时性情报参考支持
- 监管部门职能细节缺口较多

→ 约束

- 战略性安全规划不清晰
- 各自独立作战＋事件推动

→ 规划

- 反恐多样化隐蔽化趋势
- 存在大规模技术型扰乱隐患

→ 形势

多维度空间安防

联合
- 协同各行业推广无线安全
- 开展无线安全相关测评落地

引导
- 加大正面引导力度+法规建设
- 科研院所引领正确研究路线

鼓励
- 鼓励原创性研究＋技术深挖
- 发布实质性政策

提升
- 加强实时性技术情报跟踪
- 监管部门协商职能细节

规划
- 避免独立作战＋
- 建立安全事件及处理跟踪库

形势
- 加强技术型反恐研究
- 预设大规模技术型事件应急

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

ZerOne
WirelessSec Research

Thanks !!