Wireless Security
犹七年之病求三年之艾

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

“今之欲王者，犹七年之病，求三年之艾也。”

战国·邹·《孟子·离娄上》

“云无心以出岫亦为诗,若无心花月亦不苦。没有七年之病，不用三年之艾。 困欲眠时昼亦眠，醒欲起时夜亦起。 若无登九品莲台之欲，亦无堕八万地狱之罪。”

日本战国名将　前田庆次·《无苦庵记》

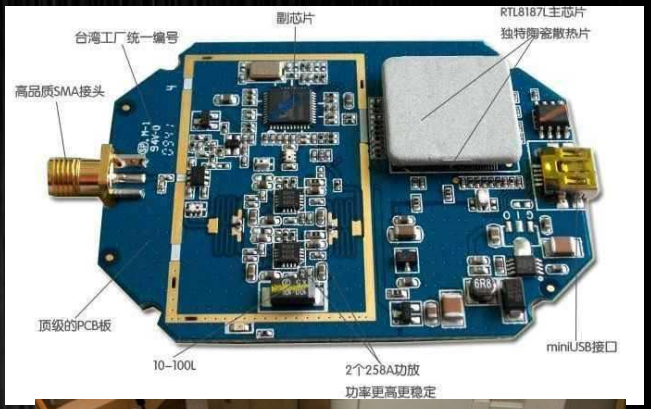
七年之病.01

三年之艾.02

一路泥泞.03

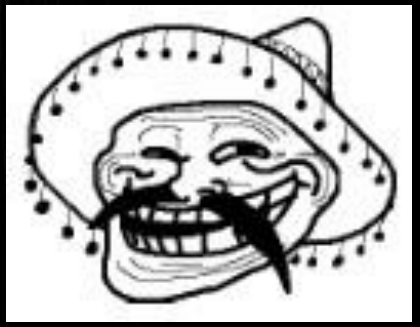
相见不如怀念的WiFi Hacking

- 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
- 2012~2013 移动破解时期
  - Dsploit之类

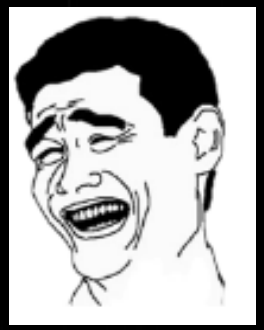


愈发险恶的江湖：欢迎来“蹭”

- 入门级挖坑 / 钓鱼
  - 常见SSID or 包含“免费”字样
  - 空密码 or 弱WEP
- 老手级挖坑 / 钓鱼
  - 一定要WPA-PSK + 10分钟能破解出来的密码
  - 一定要开WPS
- 无痕级挖坑 / 钓鱼
  - 桥接AP
  - SSL中间人



2011：国内无线安全研究的岔路口



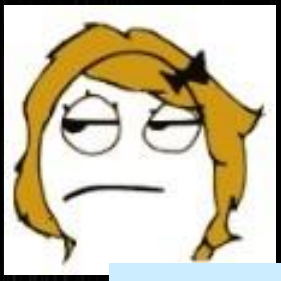
GNU Radio

软件无线电

RFID

PM3

NFC



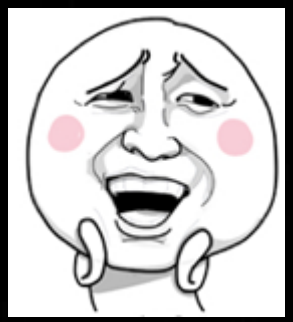
BT

被遗忘的

GSM

OpenBTS

OsmocomBB



信令研究

运营商业务流

OpenIMS

疲软的WLAN

802.1X

无线取证

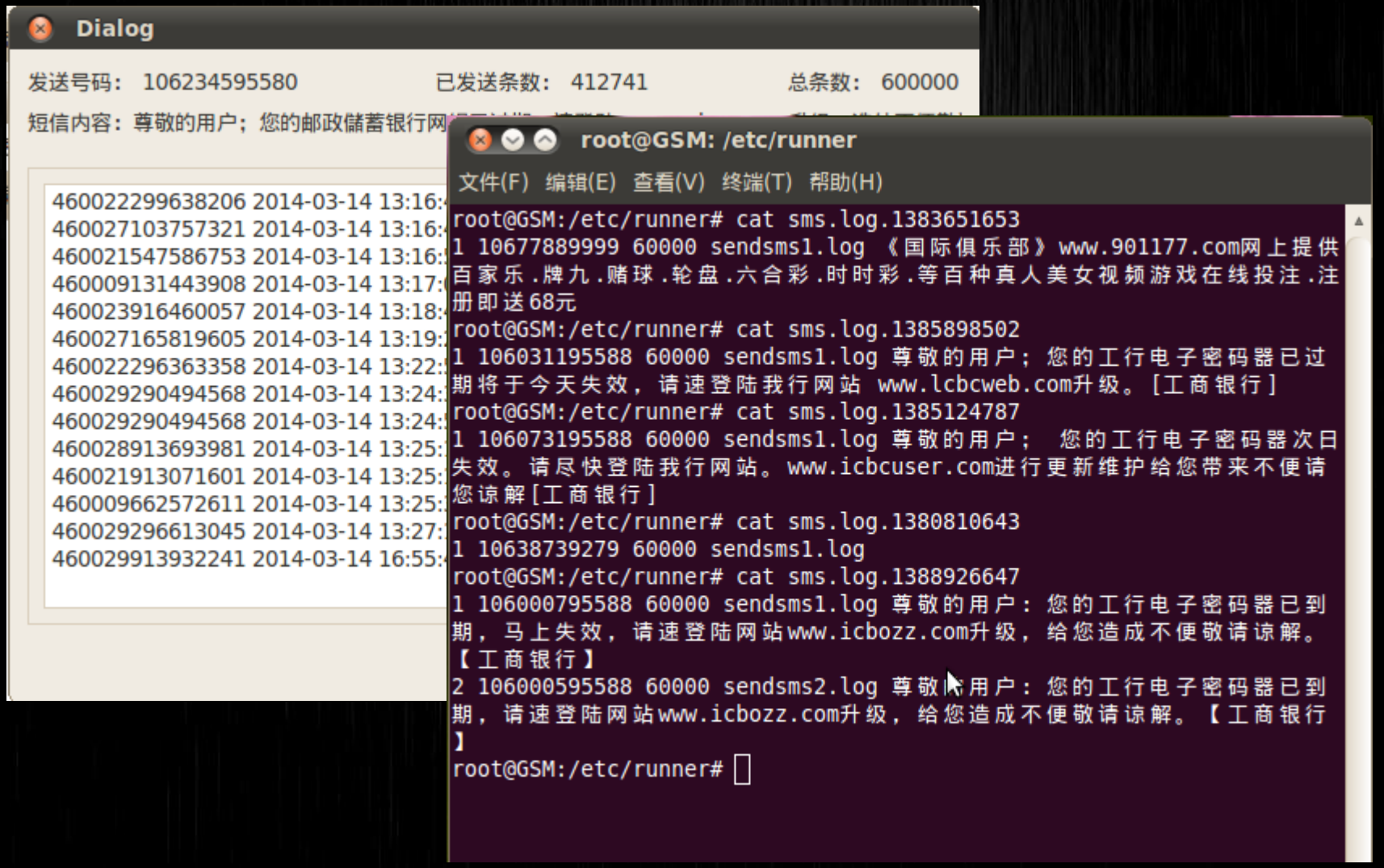
BYOD

深入研究

伪基站小时代

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

解剖“伪基站”


Dialog
发送号码： 106234595580
已发送条数： 412741
总条数： 600000
短信内容：尊敬的用户；您的邮政储蓄银行网
460022299638206 2014-03-14 13:16:
460027103757321 2014-03-14 13:16:
460021547586753 2014-03-14 13:16:
460009131443908 2014-03-14 13:17:
460023916460057 2014-03-14 13:18:
460027165819605 2014-03-14 13:19:
460022296363358 2014-03-14 13:22:
460029290494568 2014-03-14 13:24:
460029290494568 2014-03-14 13:24:
460028913693981 2014-03-14 13:25:
460021913071601 2014-03-14 13:25:
460009662572611 2014-03-14 13:25:
460029296613045 2014-03-14 13:27:
460029913932241 2014-03-14 16:55:
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#

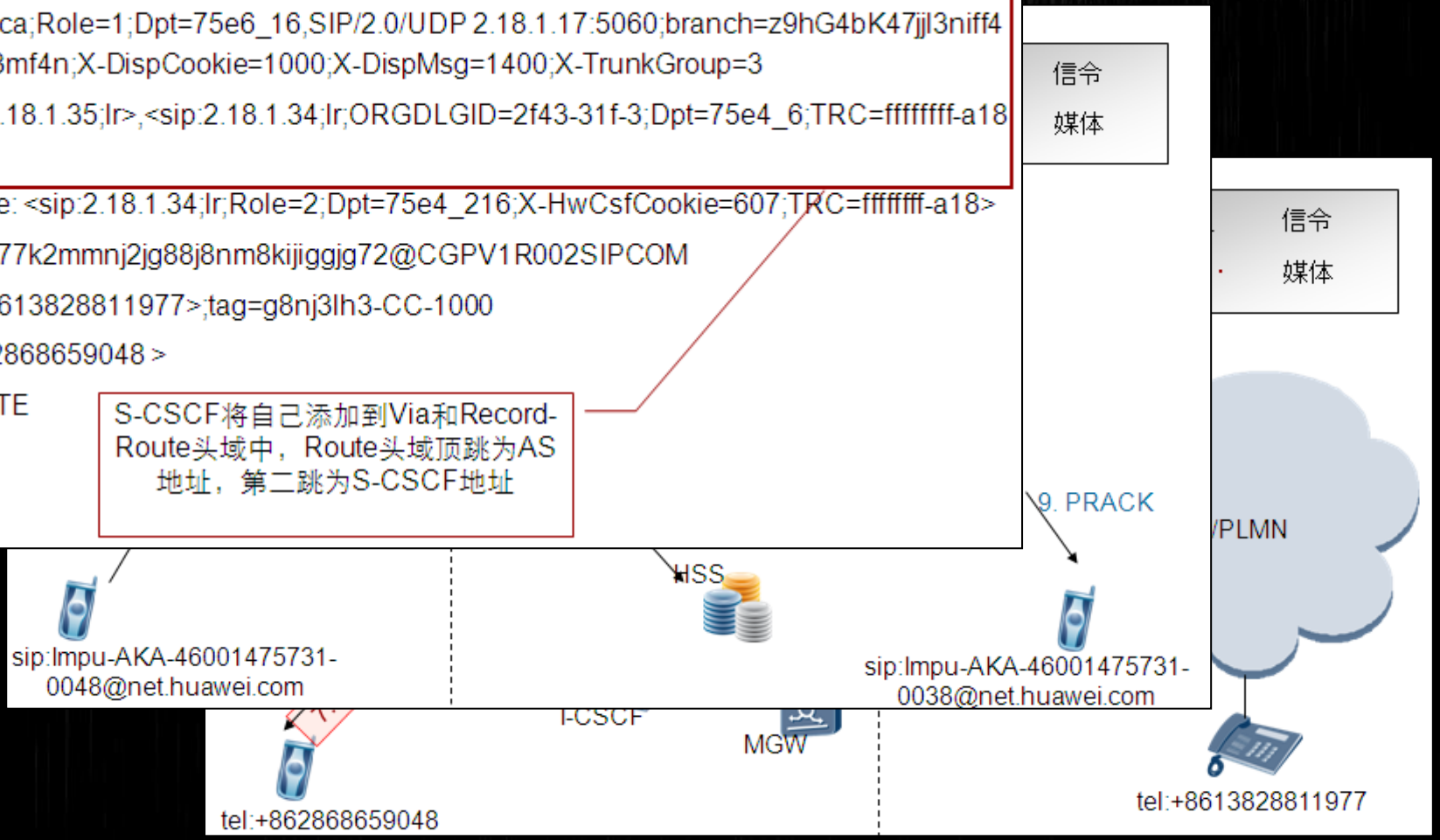
Fake AP +OpenBTS

- 国内机场
  - SSID： “Airport WiFi Free”
  - 伪造AP的天堂
- 增加的真实感：
  - 登录页面的短信发送伪造
  - 难以识别的账户短信

运营商通信业务流安全研究@IMS

- INVITE tel:+862868659048 SIP/2.0
- Via: SIP/2.0/UDP 2.18.1.34:5060;branch=z9hG4bKfoxbs8q1yoss1qtdj8fbcptub;Role=2;Dpt=75e4_16;sc=31f-4a4;TRC=ffffffff-a18,SIP/2.0/UDP 2.18.1.33:5060;branch=z9hG4bK8quabc1uqdfquoafdst88atca;Role=1;Dpt=75e6_16,SIP/2.0/UDP 2.18.1.17:5060;branch=z9hG4bK47jjl3niff44m7hm55k53mf4n;X-DispCookie=1000;X-DispMsg=1400;X-TrunkGroup=3
- Route: <sip:2.18.1.35;lr>,<sip:2.18.1.34;lr;ORGDLGID=2f43-31f-3;Dpt=75e4_6;TRC=ffffffff-a18>
- Record-Route: <sip:2.18.1.34;lr;Role=2;Dpt=75e4_216;X-HwCsfCookie=607;TRC=ffffffff-a18>
- Call-ID: 12g477k2mmnj2jg88j8nm8kijiggjg72@CGPV1R002SIPCOM
- From: <tel:+8613828811977>;tag=g8nj3lh3-CC-1000
- To: < tel:+862868659048 >
- CSeq: 1 INVITE

S-CSCF将自己添加到Via和Record-Route头域中，Route头域顶跳为AS地址，第二跳为S-CSCF地址



七年之病.01

三年之艾.02

一路泥泞.03

一波几折的WIDS

- “XX入侵检测与管理系统支持扩展无线安全模块，可准确识别各类无线安全攻击事件，按不同安全级别实时告警，并据此生成多种统计报表，为您提供有线、无线网络攻击检测整体解决方案。”

---摘自国内某一线安全厂商产品说明

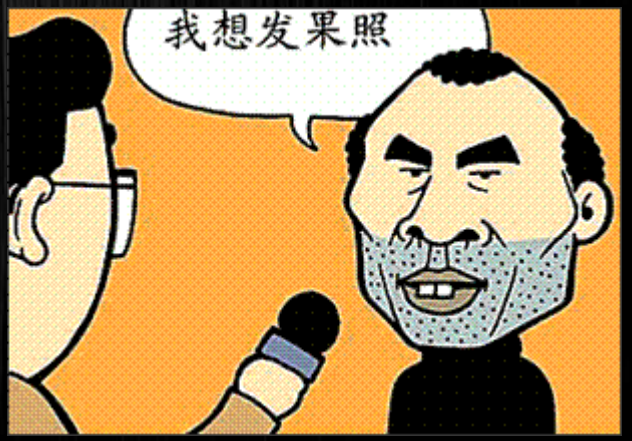
- 最大的局限：部署方式
- 最简单的组合
  - Kismet + OpenWRT + Snort

所谓的“无线安全审计系统”

- 国内某著名安全厂商悄悄推出XX无线安全审计产品

- Aircrack-ng + GPU + WPA PMK Hash Table
- BT4/5 or Kali Linux

- 无评估体系或架构指导
- 仅仅是开源工具的单纯堆叠
- 缺乏深入技术研究
- 专业性欠缺



GSM真的气数已尽？#01

- 双卡双待
  - GSM / CDMA
  - GSM / WCDMA
  - GSM / TD-SCDMA
  - ……
  - 必有一卡支持GSM
- 双号使用调查
  - 广东省的全部全球通用户中，使用两个以上手机号码的占11%～15%
  - 江苏省的100名商旅用户中，两个号码拥有者占40%
  - 四川省的118名和福建省的300名随机选取的全球通用户中，双号用户分别占34%和50%。

GSM真的气数已尽？ #02

- 4G智能手机
  - 必同时支持4G、3G和GSM
  - 若支持双卡，则必有一卡支持GSM
- 3G智能手机
  - 同上亦然

来自中移动的数据

- 中国移动公布2014年1月份运营数据，当月中国移动净增客户数466万户，其中3G用户净增1424.3万户。
- 截至2014年1月底，中国国内客户总数累计达7.71866亿户，其中3G客户总数达2.05866亿户。

- 粗略计算，国内至少约有5.5亿户仍在使用GSM。
- 换句话说，国内至少还有5.5亿户面临威胁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4~5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：

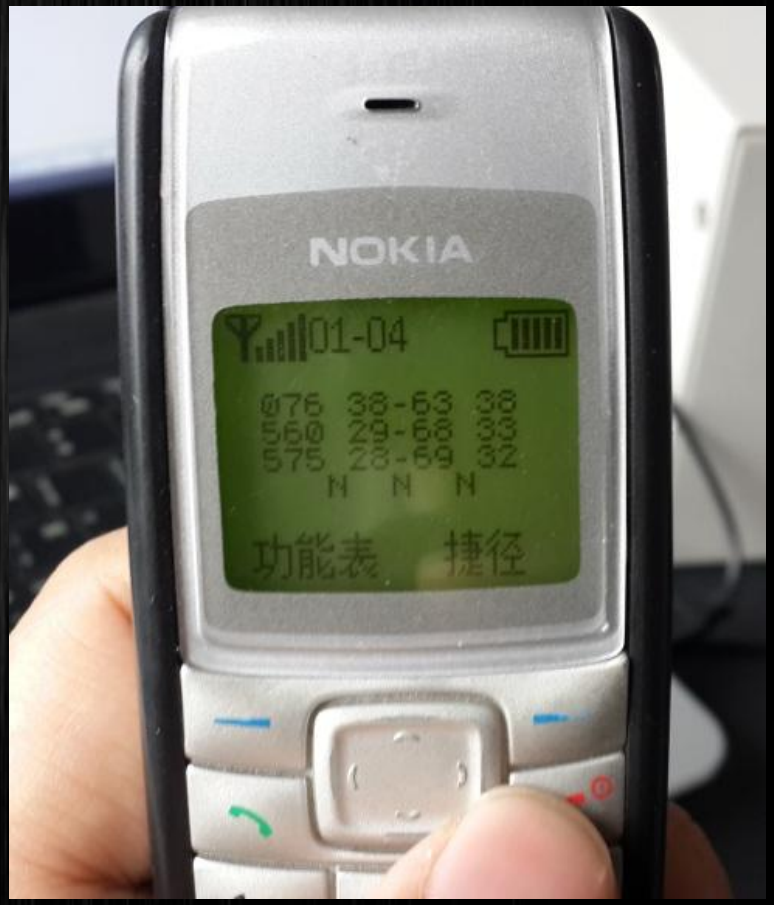
    强制切换GSM的SIM卡为默认主卡

    或者

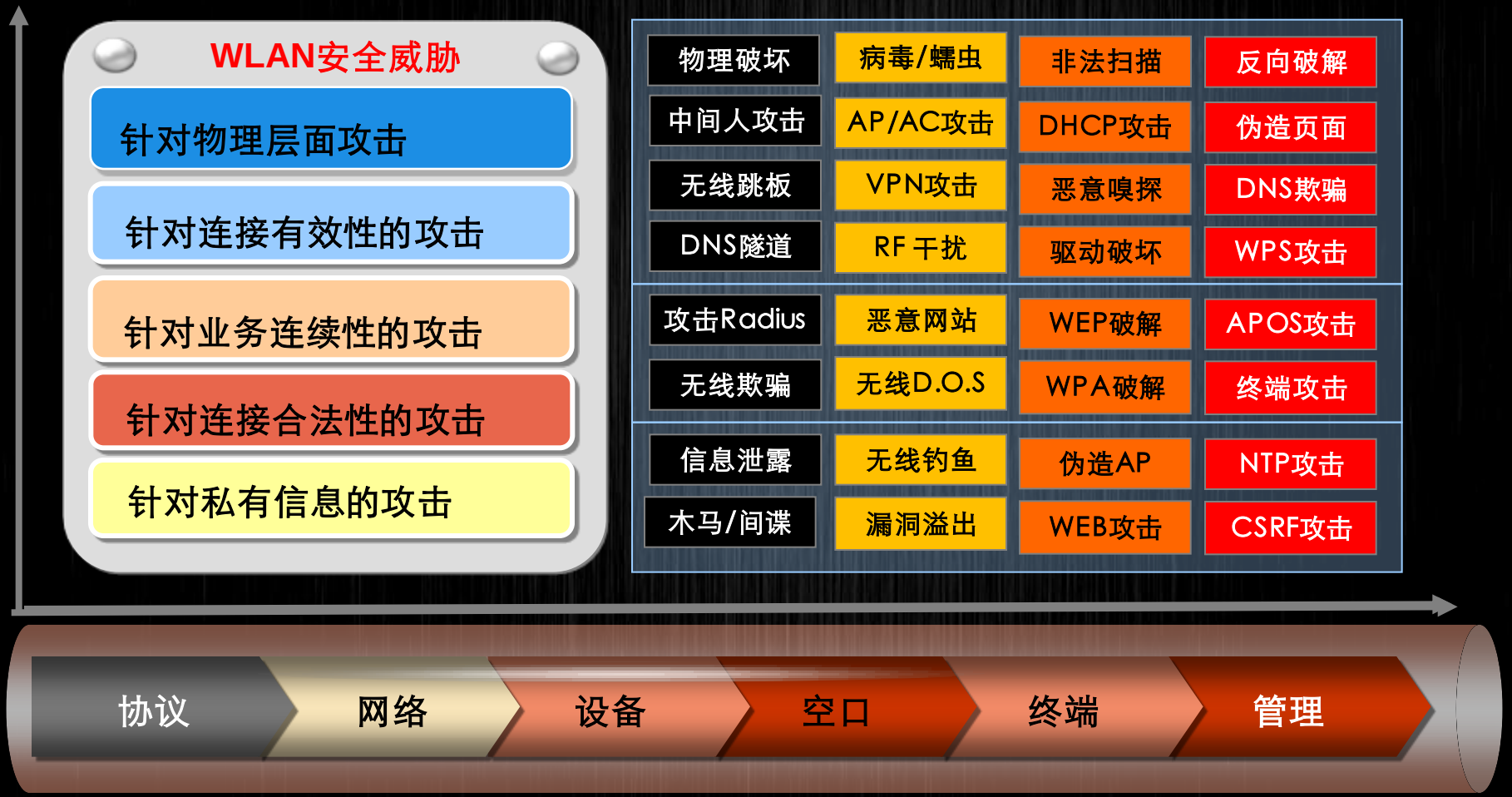
    免激活非GSM的SIM卡

伪基站的识别

- 几大明显的特征：
  - 伪基站功率过大
  - LAC 的频繁变化
  - C2 相关参数设路极端
  - 强制用户进入伪基站服务，会导致用户无法正常使用运营商提供业务（即脱网）



WLAN安全“6面5层”评估体系



WLAN安全研究的转向：设备安全

BlackHat 2009
- Cisco IOS Router Exploitation

BlackHat 2010
- How to Hack Millions of Routers
- Bad Memories

Defcon 2011
- Vodafone Femto was hacked by THC

BlackHat 2011
- Routers using OSPF open to attacks
- Owning the Routing Table: New OSPF Attacks
- Killing the Myth of Cisco IOS Diversity

Defcon 2012
- Embedded Device Firmware Vulnerability Hunting Using FRAK

BlackHat 2012
- SQL Injection to MIPS Overflows: Rooting SOHO Routers
- Huawei Router Security

Wooyun2013
- Tenda腾达某无线路由登陆密码绕过
- TP LINK无线路由器后台使用不安全的密码框
- 水星无线路由器在某中条件下能实现入侵泄露WIFI密码
- 移动CMCC网络之百万台路由交换设配任意登陆+弱密码

2009 2010 2011 2012 2013 2014

Exploits
- DLINK被曝光大量无线/有线设备漏洞
- 华为AR18和AR29路由器爆严重安全漏洞

Manufacturers
- 市面主流WLAN设备厂商均无良好的安全响应机制
- 部分国外厂商有相应安全部门

Fix & Update
- 绝大多数无线设备厂商没有响应
- 没有及时发布补丁或者安全通告

WLAN设备安全评估研究

- 主要针对企业用AP、AC及SOHO无线路由器的安全评估
- 评测模型示例：

- Level 1 级技术点包括：
  - 登录/身份验证评估
  - 交互界面评估
  - 主要服务/接口评估
  - Session安全评估
  - 通信数据安全评估
  - 日志安全评估
  - 固件安全评估
  - 本地数据安全评估
  - ……

- Level 2级技术点包含：
  - WEB服务评估
  - NTP功能评估
  - DHCP功能评估
  - SSH安全评估
  - FTP安全评估
  - Telnet安全评估
  - UPNP安全评估
  - 认证服务评估
  - 隐匿服务评估
  - ……

- Level 3级技术点包含：
  - UPNP服务基本信息读取测试
  - UPNP服务深入信息读取测试
  - UPNP外部探查测试
  - UPNP映射测试
  - ……

下一个交火区：谁将“占领客厅”

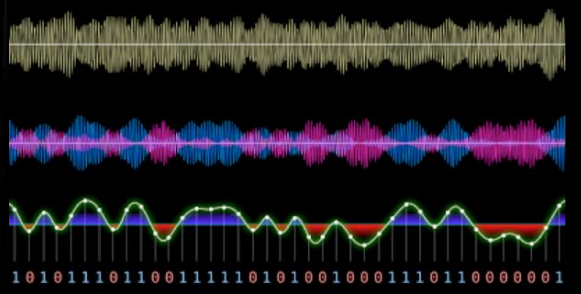
- TV + OTT盒子 + Wireless？
- 智能家居?

- 某粮食厂商
  - XX电视
  - XX盒子
  - XX路由

七年之病.01
三年之艾.02
一路泥泞.03

2014：受“关注”的交通行业

- X-ray行李安全检测仪
  - 名为Threat Image Projection (TIP)的训练函数调用，可被用于注入各类违禁品的 bmp 图像，如枪或刀等。
  - 该函数可以被操纵在反向操作，即将乘客随身携带的违禁品图片替换成无武器的正常行李图像。
- FM-RDS
  - 通过解码无线电信号来获取有关巴士运输相关信息
- Car-Hacking
  - CAN Hacking Tools（CHT）
  - 侵入 CAN可控制灯光、门锁、转向甚至刹车
  - 这套硬件的成本仅需 20 美元



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

ZerOne
WirelessSec Research

Thanks !!