

# 来自空中的威胁

于旻@绿盟科技

yuyang@nsfocus.com



# 内容提要

- 无线安全包括的范围
- 各种无线技术简介
- 各领域无线安全存在的问题

# 什么是无线安全

- 广义上的无线安全
  - 各种无线信息交换技术中的安全技术
    - 通常指使用电磁波进行信息传递的技术
      - 无线电波、红外线
- 狭义上的无线安全
  - 802.11\*协议族无线部分所涉及的安全技术
- 更为狭义的无线安全概念
  - 无线局域网（Wi-Fi）涉及的安全技术

# 广义上的无线安全

- 无线数字语音及数据通信技术的安全问题
  - 无线网络、移动电话
- 信息设备无线控制技术的安全问题
  - 无线键盘、鼠标
- 无线个体识别技术的安全问题
  - 电子标签
- 其他和电磁波相关的信息安全问题
  - 电磁辐射的截取、还原技术

# 无线局域网 & 无线个人网

- 802.11
  - Wi-Fi (Wireless Fidelity)
  - 就是通常所说的“无线网络”
- 802.15
  - WPAN (Wireless Personal Area Network)
  - SIG (The Bluetooth Special Interest Group)
  - 目前主要指蓝牙 (BlueTooth)

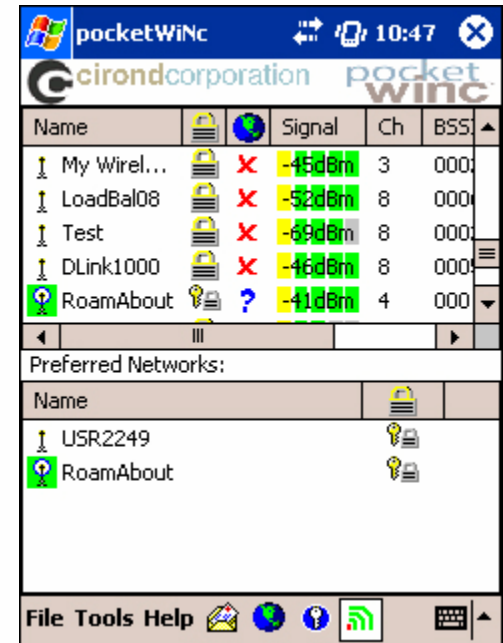


# WLAN ≠ Wi-Fi

- WLAN (Wireless Local Area Network)
  - Wi-Fi
  - BlueTooth
  - HomeRF
  - WMAN
- Wi-Fi (Wireless Fidelity)
  - 802.11协议族描述的无线组网技术
  - 802.11b、802.11a、802.11g

# Wi-Fi的安全问题

- 绝大多数接入点为开放式系统
- 大量接入点没有使用访问控制
- 脆弱的WEP加密方式
- 无线网络特有的一些安全问题
  - 假冒接入点
  - 无线中间人攻击
- 无线网络设备自身的安全问题



# 攻击WEP

- 40位WEP
  - 穷举攻击
  - 数分钟
- 104位WEP
  - 密钥弱点攻击
  - 收集尽可能多的数据包
    - 上百万个
    - 报文重放攻击
  - 半小时以内

```
[00:00:03] Tested 2 keys
depth  byte(vote)
0/ 1    D7( 93) 59( 15) D2(
0/ 1    57( 227) AE( 40) F7(
0/ 1    B7( 933) 9B( 27) 01(
0/ 1    C9( 330) 62( 39) E8(
0/ 1    A8( 475) 25( 69) 0F(
0/ 1    EB( 519) 75( 59) E2(
0/ 2    60( 171) 81( 135) 7F(
0/ 2    7E( 358) 17( 150) 16(
0/ 3    DB( 196) 8E( 101) BF(
0/ 1    86( 496) A7( 87) A8(
0/ 2    07( 283) 14( 120) 0E(
0/ 1    A4( 340) 19( 77) FE(
0/ 2    A4( 328) 4C( 187) 53(
KEY FOUND! [ D7:57:B7:C9:f
```

# 无线网络设备自身的问题

- 历史上传统网络设备曾出现过的问题都会在无线设备上重演一遍
  - 缓冲区溢出
  - 默认管理口令
  - SNMP默认共同体字符串
  - 认证绕过
  - 非授权访问
  - 拒绝服务

# 无线网络设备自身的问题

- 几个比较有代表性的漏洞
  - 无线接入认证绕过
    - Linksys WRT54GS
  - TFTP非授权访问
    - D-Link DWL-900AP+
  - 泄露WEP密码等信息
    - 3Com Wireless 11g AP 1.00.08
  - 远程管理接口验证绕过
    - Motorola WR850G 4.03

# 蓝牙的安全问题

- 蓝牙协议本身的安全问题
  - 劫持配对过程
  - 窃听、伪造蓝牙通信
- 蓝牙协议栈实现的安全问题
  - 无线网络绑定的是硬件层和协议层
  - 蓝牙直接绑定应用→相对复杂
  - BlueSnarf
  - Overflow

# 蜂窝通信网

- Cellular-Based Networks
  - 2G
    - GSM、CDMA.....
  - 2.5G
    - GPRS、GPRS/EDGE.....
  - 3G
    - EDGE、CDMA 2000、WCDMA.....

# 我们身边的移动通信安全

- GSM
  - 协议本身可以加密
    - A3、A8、A5
- CDMA
  - CDMA网络有加密措施
  - 相对安全
- 移动电话自身的安全问题
  - 最容易被人们忽视

# WiMAX & UWB

- 未来数年内的热点
- 802.16
  - WMAN (Wireless Metropolitan Area Network)
  - WiMAX (Worldwide Interoperability for Microwave Access)
- UWB (Ultra-Wide-Band)
  - 以千兆无线技术连接各种数字设备
  - 已经被纳入下一代蓝牙标准

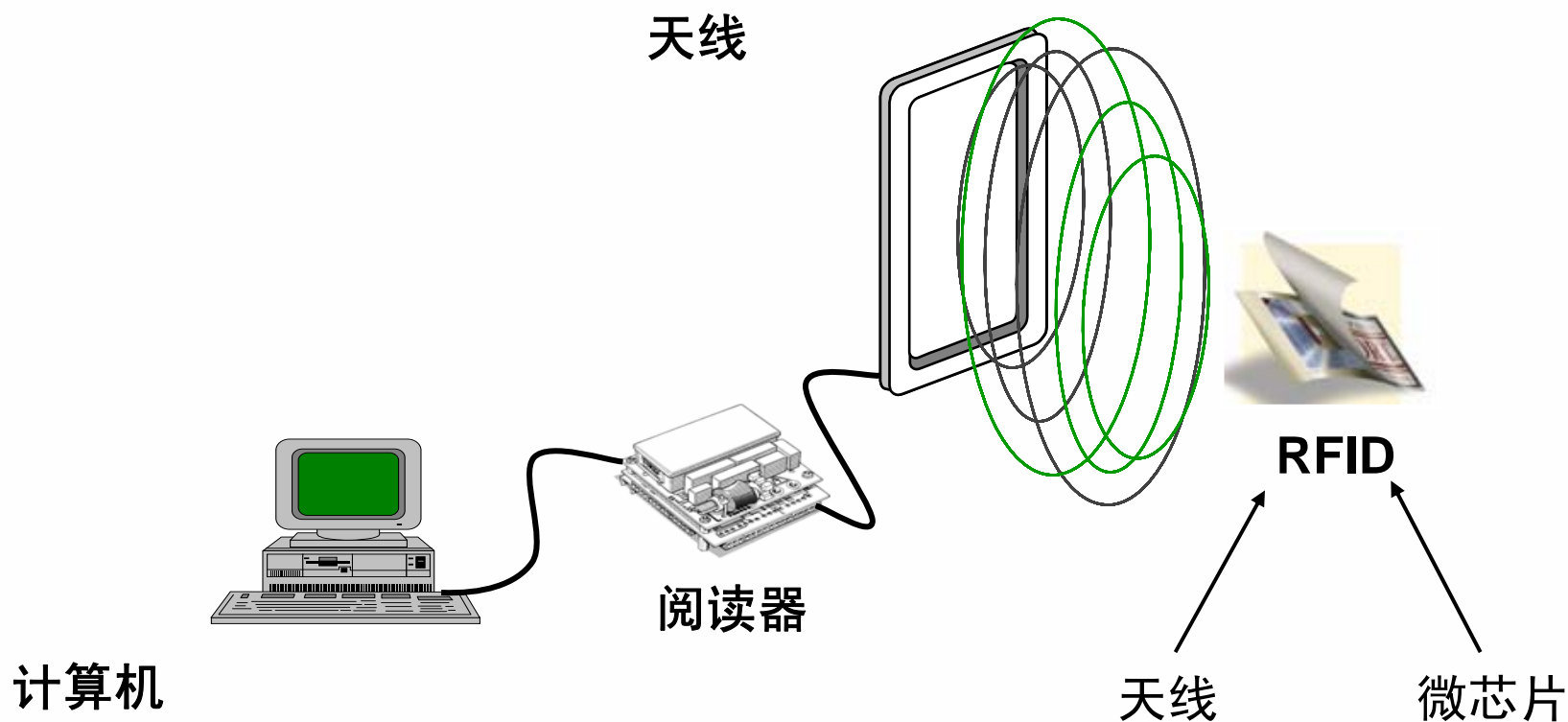
# 电子标签 (RFID)

- RFID (Radio Frequency Identification)



# RFID的工作原理

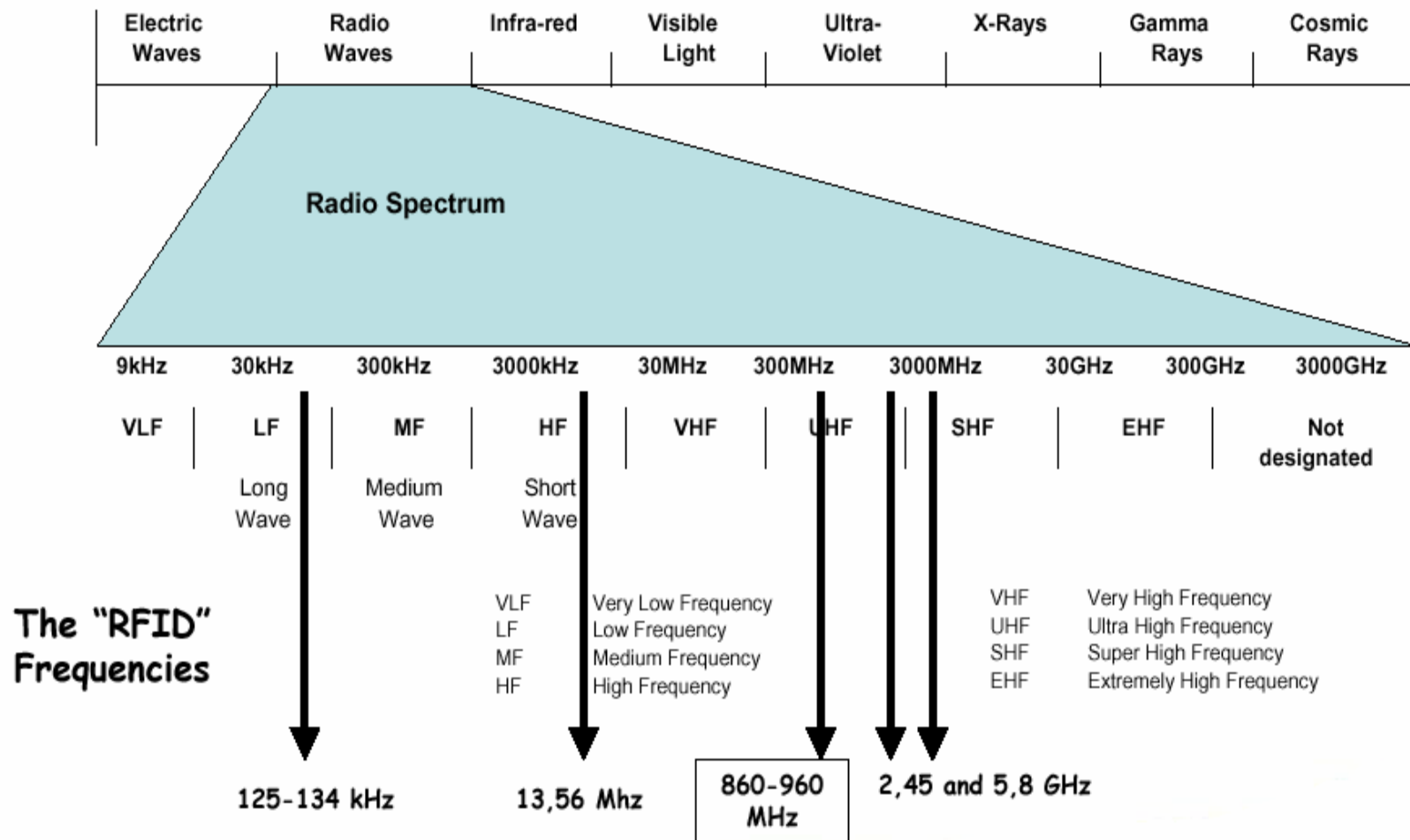
被动式RFID读写过程：



# RFID技术的现状和趋势

- 越来越多的应用
  - 原本只是以条形码的替代者面目出现
- 飞快的发展速度
- 小型化，低成本化
- 协议和标准泛滥
  - 目前共有117个不同的协议
  - 各国使用不同的标准不同的频段

# RFID使用的频段



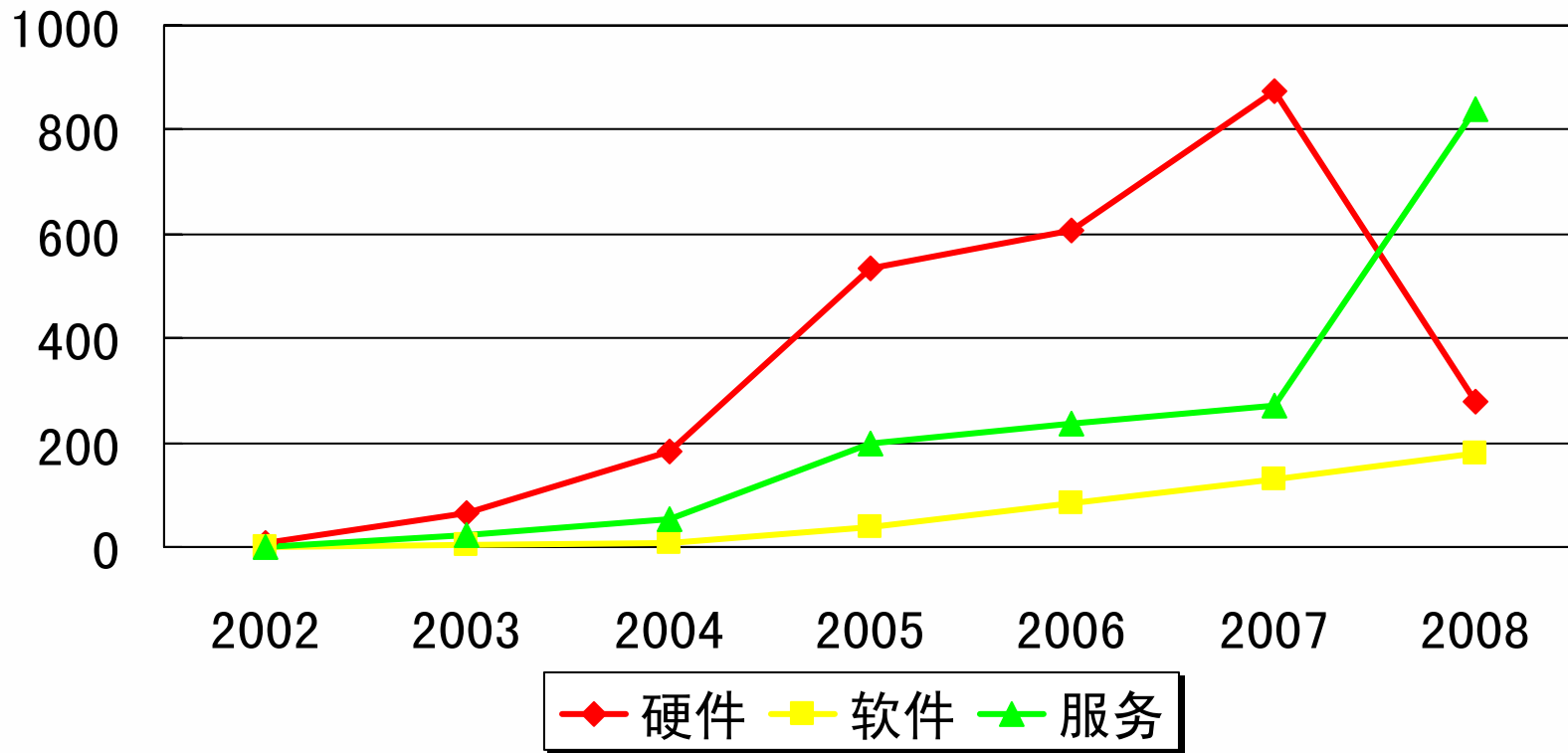
# RFID的应用领域

- 门禁管制
- 文档管理
- 安全管理
- 畜牧管理
- 交通运输
- 医疗管理
- 生产链
- 物流链
- 供应链



# RFID的未来

美国RFID消费支出统计及预测（百万美元）

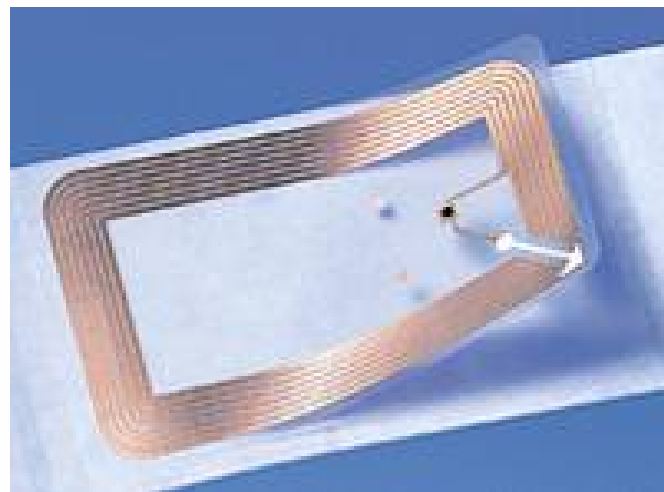


# RFID分类： 是否可写？

- 可读写卡（RW）
  - Read Write， 相当于CDRW
  - 第二代身份证
- 一次写入卡（WORM）
  - Write Once ,Read Many， 相当于CDR
- 只读卡（RO）
  - Read Only， 相当于CD
  - 门禁

# RFID分类：是否带电源？

- 无源RFID（Passive RFID）
  - 依靠和阅读器的电磁耦合供能
  - 读取距离取决于
    - 阅读器耦合线圈的尺寸
    - 工作频率
    - 阅读器的功率
      - 0.5W → 0.7m
      - 4W → 2m
      - 30W → 5.5m
  - 成本低，应用广泛



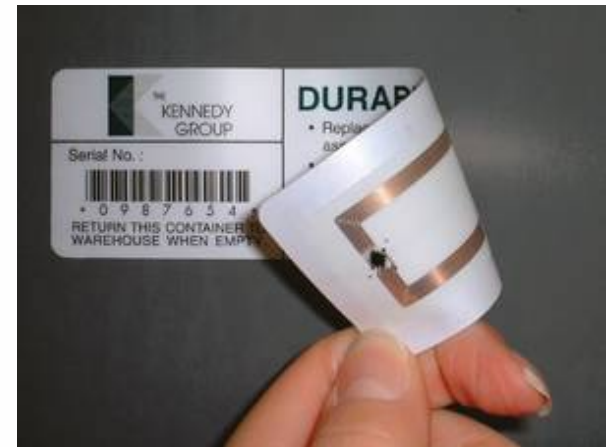
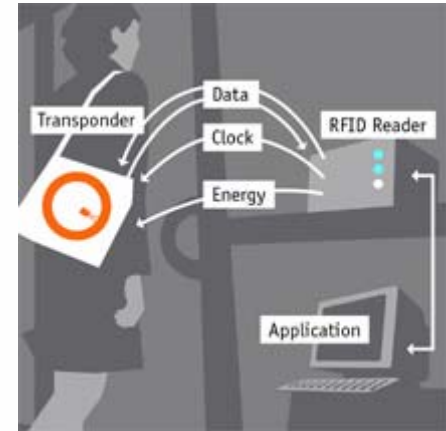
# RFID分类：是否带电源？

- 有源RFID（Active RFID）
  - 自带电源供电
    - 使用锂电池通常可工作3~10年
  - 读取距离10m~30m，或更远
  - 目前的应用相对无源ID要少
    - 需要远距离识别的场合
    - “手机钱包”



# RFID的隐患

- 伪造、假冒和非法篡改
- 泄露隐私
  - 我的口红里有RFID吗？
- 植入人体？
  - 技术上已经成熟
  - 美国国会通过了相关法律
- 《Enemy of the State》



# 我们身边的RFID

- 绿盟科技的门禁
  - 无源只读卡
  - 载波频率125KHz
- 第二代身份证
  - 无源读写卡
  - ISO 14443 TYPE B
  - 载波频率13.56 MHz、副载波频率847 KHz
  - 身份证号、姓名、性别、居住地址、照片……

# 无线键盘和无线鼠标

- 红外键盘鼠标
  - 唯一的访问控制就是红外设备的距离特性
    - 电影《小鬼当家》中的一个片段
- 无线鼠标键盘（不包括蓝牙鼠标/键盘）
  - 27MHz
  - 256个ID + 2个频道就是所有识别措施
- 蓝牙键盘鼠标
  - 安全性优于无线键盘鼠标，成本较高

# 电磁辐射泄露

- CRT显示器行场信息还原
  - 一个抛物面天线，一台电视机
  - 数百米到数公里
- 普通键盘和鼠标的电磁泄露问题



# The End

于旻@绿盟科技  
yuyang@nsfocus.com

