



移动互联网安全

第四章 移动通信与物联网安全综述

黄 珂



内容提纲

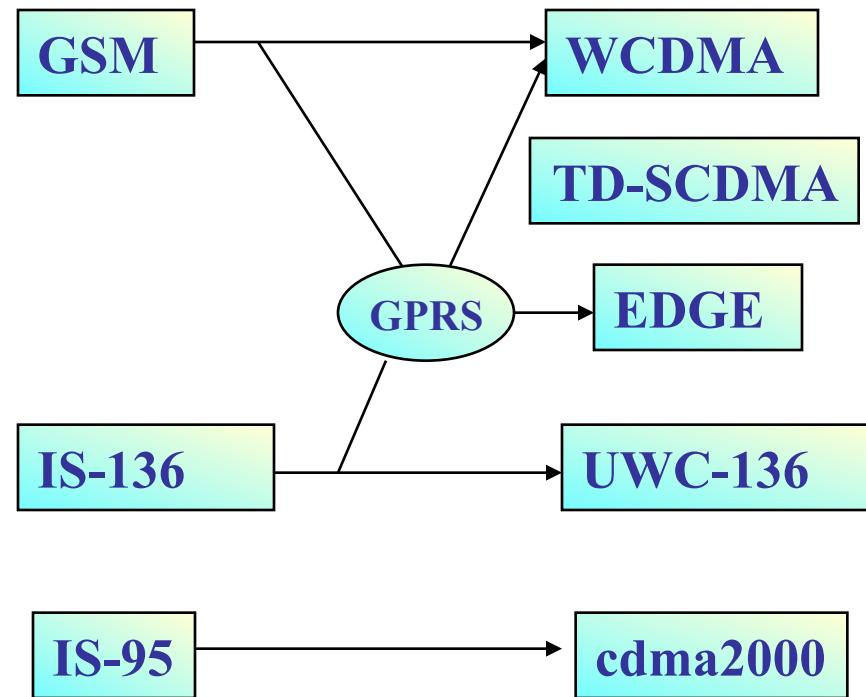
- 2G / 2.5G
- 3G / 4G / 5G
- 物联网安全
- 蓝牙安全
- “智能”硬件
- 广义无线网络安全



移动通信系统演进里程碑

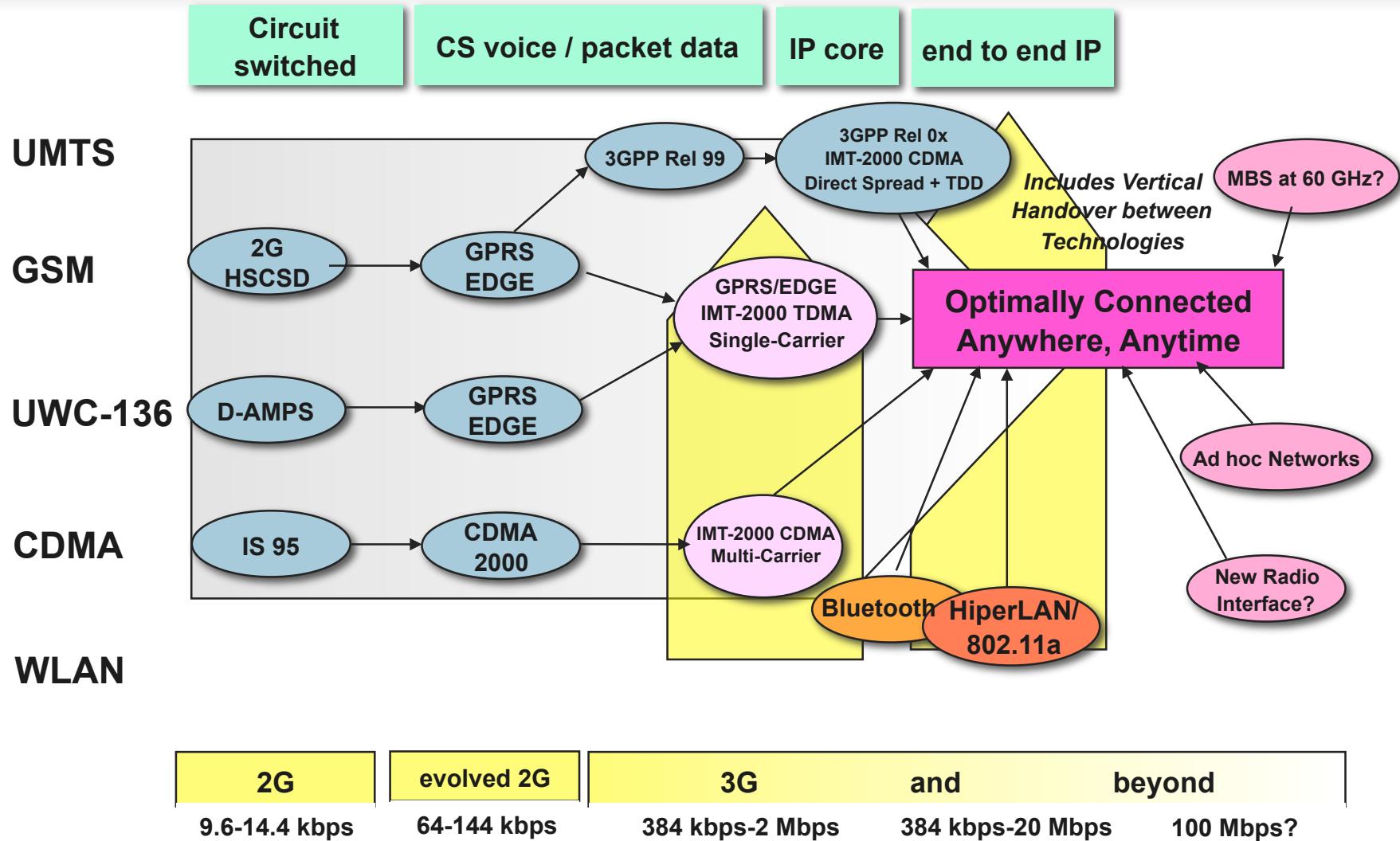


模拟系统





移动通信技术发展历程





移动通信各代典型系统特点

	典型代表	技术	特性
第一代	AMPS	小区制蜂窝系统	模拟话音
第二代	GSM	数字蜂窝 (TDMA)	数字话音, 数据速率 13Kbps(12.2kbps)
第二代半	GPRS	通用分组数字蜂窝	数据速率 115Kbps , 数 据在线连接
第三代	W-CDMA	宽带码分多址, 实 现宽带多媒体业务	数据速率最高达 2Mbps , 数据在线连接宽带数据 业务
后三代



蜂窝通信网

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



蜂窝通信网

- Cellular Based Networks
 - 3.5G
 - WiMax、HSPA
 - 4G
 - TDD-LTE、FDD-LTE
 - 5G
 - 标准研究制订过程中，无正式商用案例



GSM 网络概述

- HPLMN (Home Public Land Mobile Network)
GSM的网管、票据处理和安全业务由Home网操作
- HLR (Home Location Register) 处理本地实时认证和接入控制，永久注册。保存用户的基本信息，如你的SIM的卡号、手机号码、签约信息等，和动态信息，如当前的位置、是否已经关机等



GSM 网络概述

- VLR (Visitor Location Register) 处理本地实时认证和接入控制，临时注册。保存的是用户的动态信息和状态信息，以及从HLR下载的用户的签约信息
- SIM (Subscriber Identity Module) 用户标识卡
 - ICCID (序列号)
 - IMSI
 - 秘钥Ki (加密使用的主秘钥！) 和加密算法



GSM 网络概述

- MS (Mobile Station) 移动终端，例如手机
- MSC (Mobile Switching Center) 移动交换中心，移动网络完成呼叫连接、过区切换控制、无线信道管理等功能的设备，同时也是移动网与公用电话交换网(PSTN)、综合业务数字网(ISDN)等固定网的接口设备
- IMSI (International Mobile Subscriber Identity) 跨国移动用户标识，是TD系统分给用户的唯一标识号，它存储在SIM卡、HLR/VLR中，最多由15个数字组成
- IMEI (International Mobile Equipment Identity) 跨国移动设备标识，MS的唯一标识



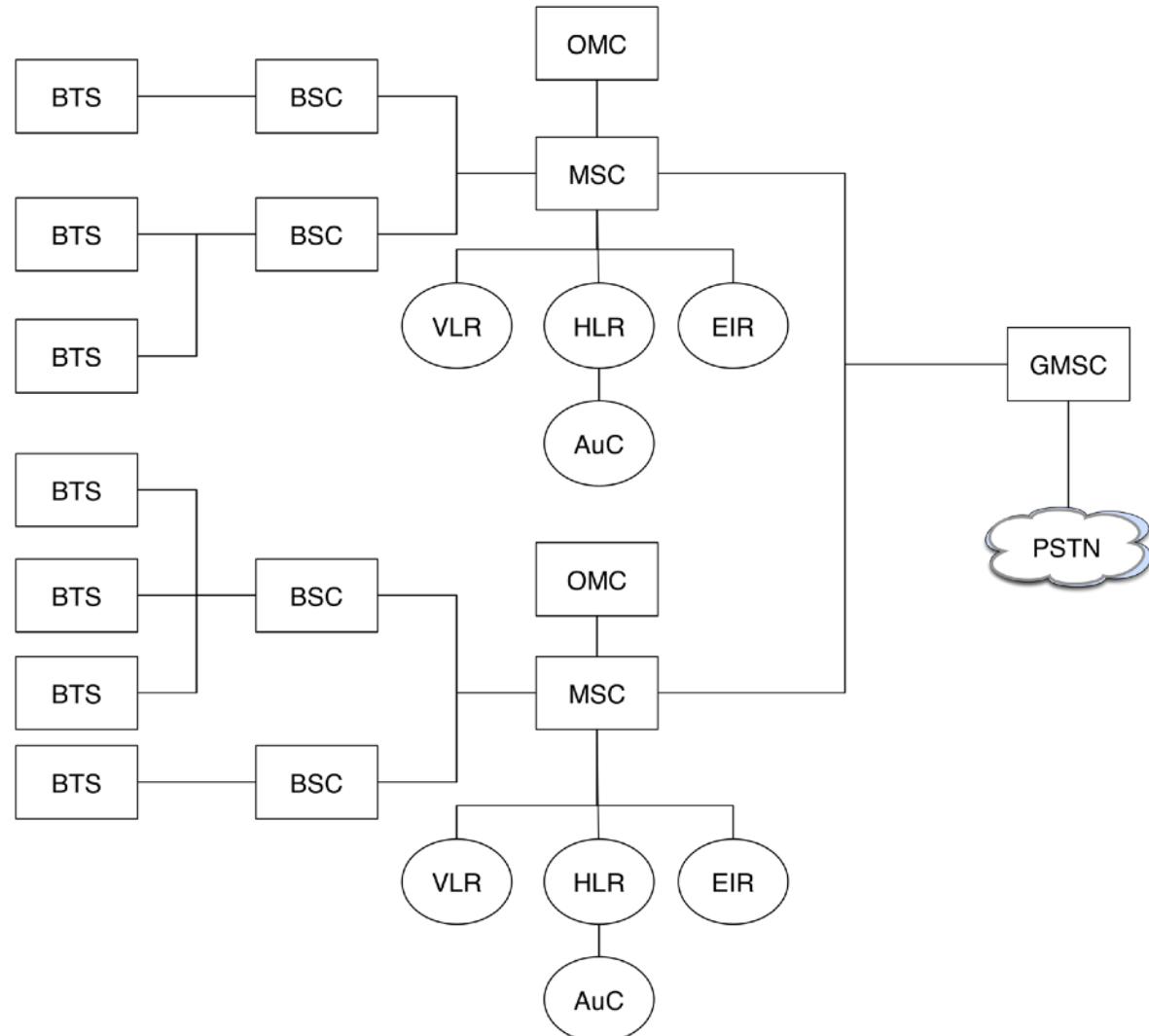
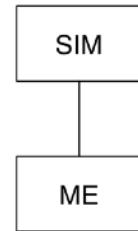
GSM 网络概述

- TMSI (Temporary Mobile Subscriber Identity)
临时用户身份
 - 用户在呼叫/被呼叫前，其身份必须为网络知道
 - IMSI 仅在初次接入，或 VLR 中数据丢失时使用
 - 目的是防止攻击者得到用户的进网信息，防止用户位置跟踪



GSM 网络体系结构组成

- 带有SIM卡的移动设备: ME
- 归属位置登记数据库: HLR
- 访问位置登记数据库: VLR
- 设备标识注册数据库: EIR
- 基站(收发信台): BTS
- 基站(控制器): BSC
- 移动交换中心: MSC
- 认证中心: AuC
- 运营管理中心: OMC
- 有线固话网络: PSTN





GSM安全目标

- 获得和PSTN (Public Switched Telephone Network) 等价的安全性
 - 基于电磁信号传输方式难免传输过程中的监听和传输链路劫持风险
 - GSM协议设计时主要针对上述2大类风险进行了威胁建模和安全机制设计



相关密码学算法

- GSM用到的密码学算法是对称密钥加密体制
 - A3：移动设备到GSM网络认证
 - A5：语音和数据的分组加密算法
 - A8：产生A5算法中用到的（会话）对称密钥的密钥生成算法



相关密码学算法

- Ki用于A3、A8的用户认证密钥
 - 与HLR共享，128bit的秘密数据
- A3为认证算法，单向散列函数
 - 对于HLR的询问产生32bit响应SRES
 - $SRES = A3(Ki, RAND)$
- A5是分组加密算法，会话秘钥Kc的长度为64bit
- A8为生成Kc的单向散列函数
 - $Kc = A8(Ki, RAND)$



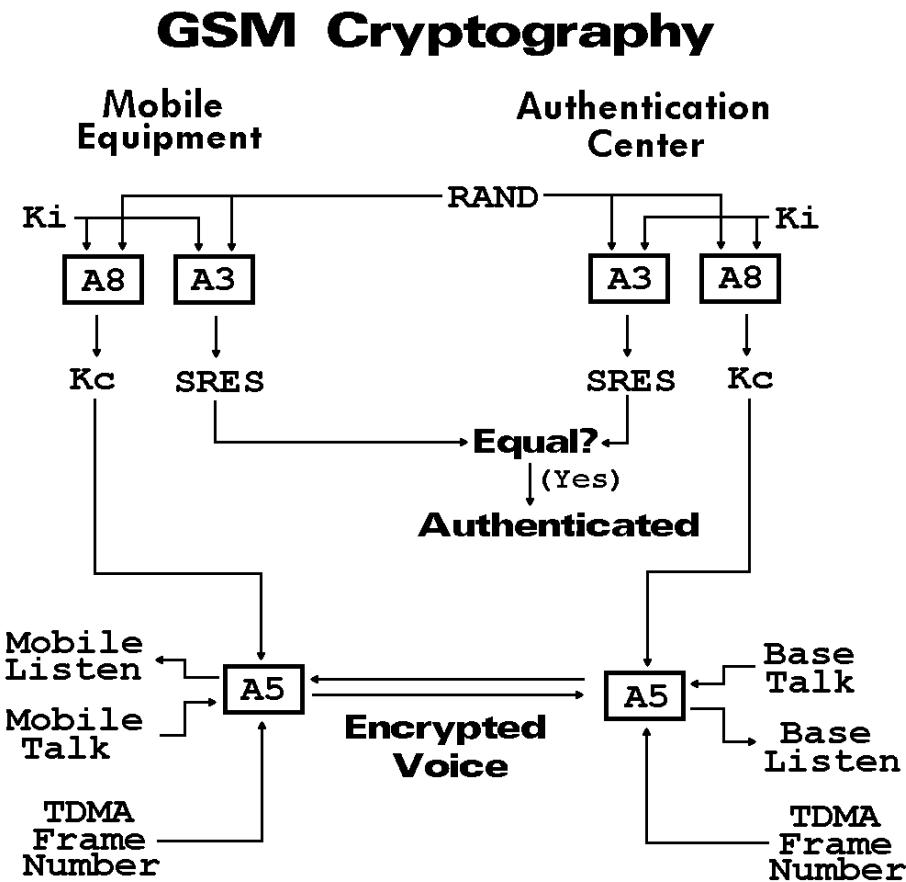
相关密码学算法

- A3和A8算法内置于SIM
 - 由运营商选择A3/A8
 - COMP-128是A3和A8的一种典型实现
 - 终端漫游时用于安全的传输(RAND,SRES,Kc)
- A5内置于终端设备
 - A5/1 - 安全性较好
 - A5/2 - 安全性较差
 - 不加密



GSM安全机制——认证

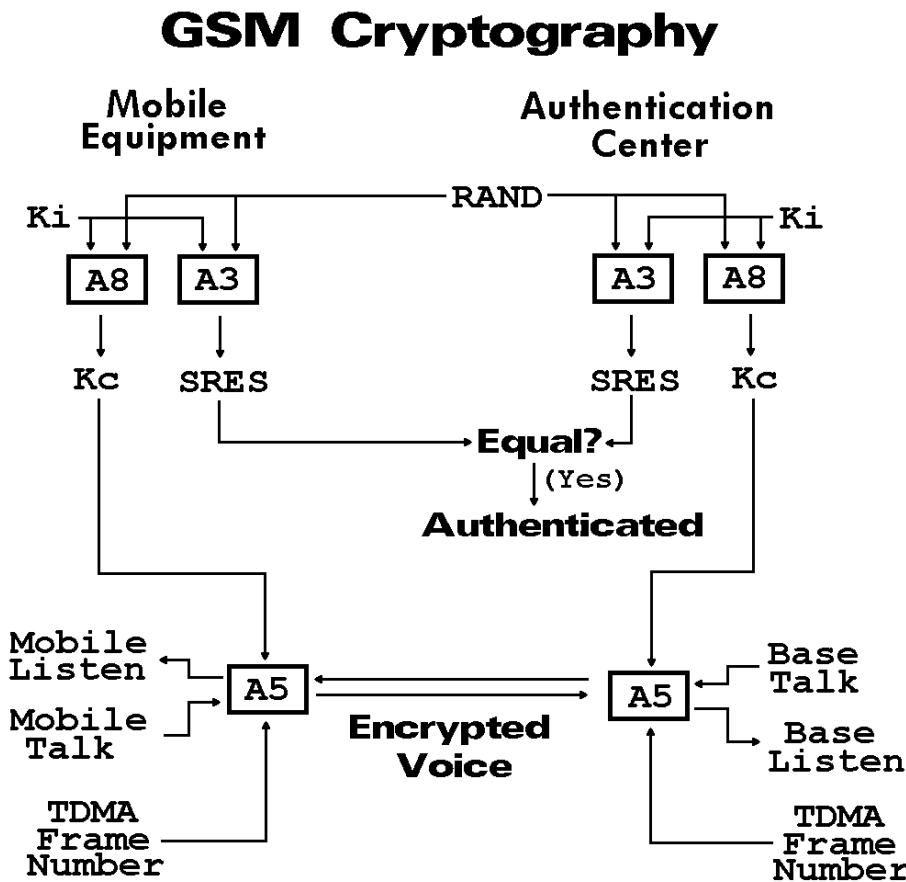
- 手机终端接受随机验证码
- 手机终端使用密钥Ki和A3认证算法加密验证码
- 手机终端返回挑战响应码（SRES）
- 蜂窝网络校验挑战响应码是否正确





GSM安全机制——用户数据和信令机密性

- A8算法产生Kc
- 使用Kc加密信令传输链路
- A5算法用于用户数据传输过程加密





GSM脆弱性

- COMP-128 算法会泄漏 Ki (1998.4)
- A8的有效密钥长度只有54 bits (最后10位全0)
- A5
 - 缺乏数据完整性验证机制
 - A5/1 (欧洲标准)
 - A5/2 (北美标准)
 - A5/0 (不加密, 比如我国)



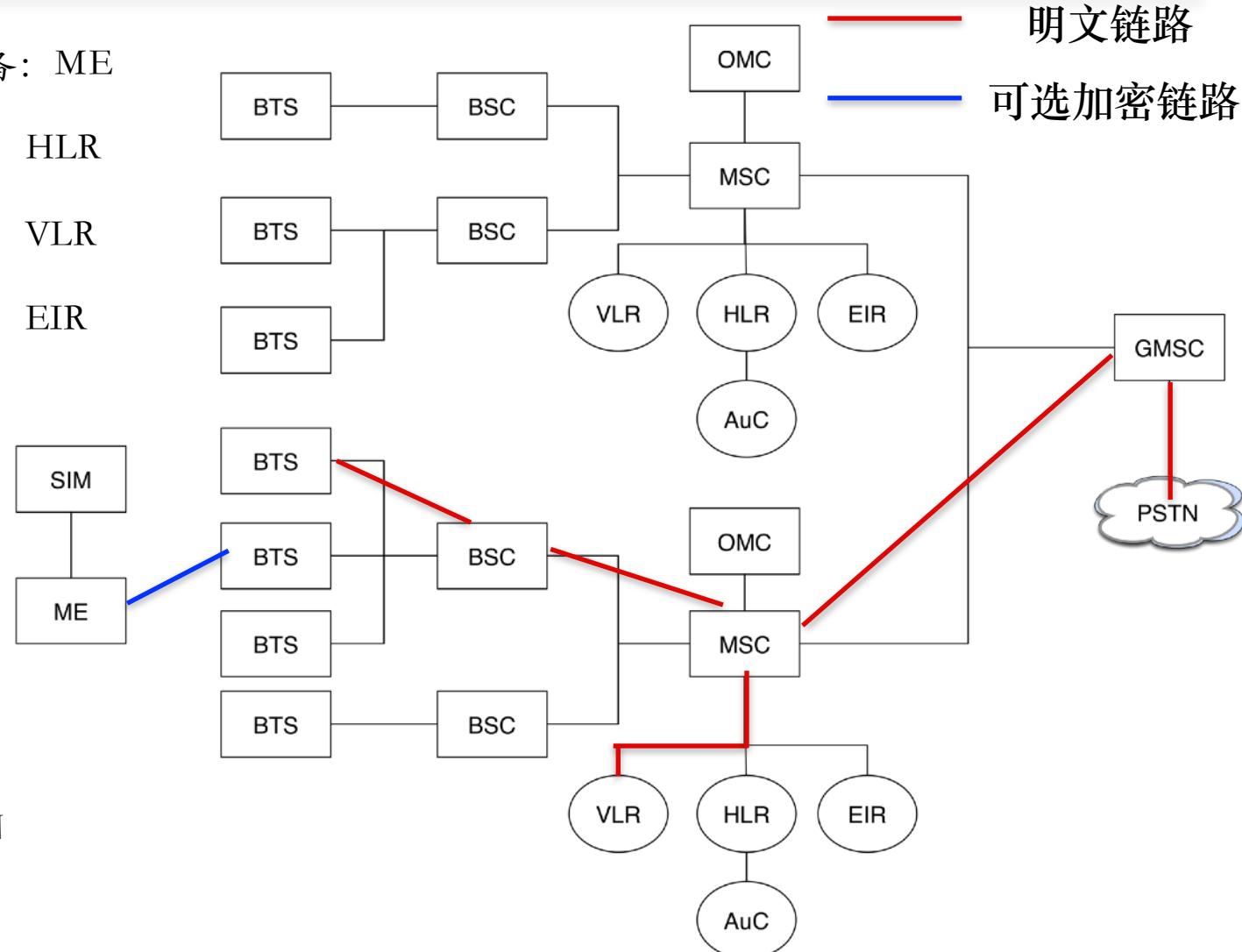
GSM脆弱性

- 伪基站
 - 只有基站认证用户，缺少用户对基站的认证
- 明文网络传输链路
 - 监听
 - （匿名）查询HLR/AuC
- Kc更新周期太长
- 算法和Ki均存储在SIM卡中，存在复制SIM卡的风险



GSM网络中的明文传输风险

- 带有SIM卡的移动设备：ME
- 归属位置登记数据库：HLR
- 访问位置登记数据库：VLR
- 设备标识注册数据库：EIR
- 基站收发信台：BTS
- 基站控制器：BSC
- 移动交换中心：MSC
- 认证中心：AuC
- 运营管理中心：OMC
- 有线固话网络：PSTN





GSM网络的中间人劫持（伪基站）风险

- MS（手机）向系统请求分配信令信道（SDCCH）
 - MS倾向信号更强的BTS，使用哪种算法由BTC决定
- MSC收到手机发来的IMSI可达消息
- MSC将IMSI可达信息再发送给VLR，VLR将IMSI不可达标记更新为IMSI可达
- VLR反馈MSC可达信息信号
- MSC再将反馈信号发给手机



真实世界中的GSM威胁——监听

The screenshot shows a Kali Linux desktop environment with several windows open:

- Terminal Window:** Shows a root shell with the command `root@kali: ~`.
- Wireshark Window:** Capturing from interface `lo` (port 4729) [Wireshark 1.8.5]. The filter is set to `gsm.sms`. The packet list shows two GSM SMS messages sent from 127.0.0.1 to 127.0.0.1. The details pane shows the message content: "尊敬的客户，您本次登录移动官网的动态密码为232525，请在10分钟内使用，广东移动！". The bytes pane displays the raw hex and ASCII data of the captured packets.
- File Manager Window:** Shows a file browser with a list of files and folders.
- System Tray:** Shows icons for network, battery, and system status.



真实世界中的GSM威胁——伪基站



名师传授（扑克，麻将，牌九绝技）任意一副牌随意洗叠就能得到自己想要的好牌如235变AAA，东风变八万另有高科技产品电话[13693054780](#)

发送者：[10086100065](#)

接收时间：9月 23 日

归属地：未知



CDMA安全综述

- CDMA系统使用蜂窝认证和语音加密（CAVE, Cellular Authentication and Voice Encryption）算法
- CDMA网络的安全同样采用对称加密体制（单钥体制）
- CDMA采用64bit的对称密钥（A-Key）来认证。出售手机时，运营者用程序将这个密钥输入到用户手机内，同时运营商也将此密钥保存在数据库中



CDMA安全综述

- 如同GSM中的Ki一样，A-Key也应该妥善保存
- A-Key不直接用于认证和加密，而用于产生子密钥，因此其安全性要高于GSM
- 为了使A-Key泄露的风险降到最低，CDMA采用A-Key生成动态的随机数来进行认证。该随机数称为安全共享密钥（SSD）。它是使用3个数值计算出来的



CDMA安全综述

- CAVE算法产生2个64bit的散列值，即SSD_A和SSD_B
- SSD_A用来认证，SSD_A等同于GSM的SRES(32bits)
- SSD_B用来加密，SSD_B等同于GSM的Kc(64bits)



CDMA安全综述

- CDMA的机密性建立在对称加密体系上
 - 与GSM类似的数据与语音加密机制
- CDMA的认证建立在挑战/响应机制上
- 2011年DEF CON 19上，Coderman演示了通过中间人攻击CDMA和4G监听数据的方法



3G/4G安全综述

- 3G/4G系统采用双向身份认证
 - 杜绝伪基站威胁
- 身份认证算法：MILENAGE算法基于AES-128+循环移位+异或
- 会话密钥更新周期大大缩短
- 缺陷
 - 没有采用用户数字签名技术，数据完整性保护存在缺陷
 - 密钥产生机制存在脆弱性
 - 认证协议仍然存在安全漏洞



USIM

- (U)SIM = (Universal) Subscriber Identity Module
 - 属于智能卡
- 存储的数据类似SIM，区别在于保存的秘钥信息不同
 - 主秘钥K和OPc, r1, r2, …, r5, c1, …, c5



USIM 已知安全问题

- SIM 卡制造商密钥数据库机密性保护能力
 - SIM 卡制造商金雅拓遭黑 嫌疑人是美英情报机构 2015.02.27
- 补卡攻击
 - 运营商营业厅身份认证不合规
 - 在线补卡/换卡业务流程考虑不周全
- 使用侧信道攻击技术复制 USIM 卡
 - Cloning 3G/4G SIM Cards with a PC and an Oscilloscope: Lessons Learned in Physical Security presented on Blackhat USA 2015 现场演示复制 USIM 卡获取验证码短信的视频



VoIP/VoLTE安全综述

- Caller ID伪造与欺骗更容易
 - 短信和来电号码是伪造的
- 针对呼叫终端/网关的拒绝服务攻击难度和成本大大降低
 - IP化网络攻击手段和工具
- 中间人劫持攻击方式多样化
 - IP化网络攻击手段和工具



物联网安全

广义无线网络安全

中国传媒大学



回顾第一章内容：无线网络是什么

- Wi-Fi? WLAN? 802.11? 蓝牙? NFC?
- 核心是：“无线”，相对于“有线”网络技术，无线技术使用肉眼不可见的传输介质
 - 电磁波



回顾第一章内容：WLAN ≠ Wi-Fi

- Wi-Fi
 - Wi-Fi 联盟制造商的商标可做为产品的品牌认证，最基础的认证条件是符合 IEEE 802.11 标准，此外还需缴纳认证授权费用
- WLAN
 - 不仅可以使用Wi-Fi设备来组网，蓝牙、ZigBee等技术都可以用于构建一个无线局域网
 - Wi-Fi是符合802.11标准的WLAN



回顾第一章内容：无线网络有什么（补充）

- AP? 路由器? 热点?
- 上网卡? 电力猫? 3G? 4G?
- 手机? 平板? 笔记本? 台式机? 空调? 插座?
- 无线键盘、无线鼠标、无线SD卡
- 电子标签
- 手机支付（公交卡、手机钱包等）



物联网概述

- 物联网（Internet of Things, IoT）是互联网、传统电信网等信息承载体，让所有能行使独立功能的普通物体实现**互联互通**的网络
- Machine To Machine
 - 依赖于“通信技术”
- 智能
 - 自动化（Autonomous）
 - 人工智能（Artificial Intelligence, AI）



物联网概述

- 泛在 (Ubiquitous) 网络: 具备4A级别通信能力
 - 4A: Anytime, Anywhere, Anyone, Anything
- 继承了IP网络基本组网和通信模型
 - 通信架构
 - 分层结构
 - 通信模式
 - 点对点, 组播, 广播, 任播



基于“近”距离通信传输技术的无线技术

- RFID (物联网的基础设施技术之一，可以通过蓝牙、NFC技术来实现)
- 蓝牙 (802.15.1)
- NFC (ISO 13157等)
- ZigBee (802.15.4)



电子标签 (RFID)

- Radio Frequency Identification
—射频标识
- 属于无线通信技术范畴
- 通过无线电信号识别特定目标并读写相关数据
无需识别系统与特定目标之间建立机械或光学接触



RFID的工作原理

- 无线电的信号是通过调成无线电频率的电磁场把数据从附着在物品上的标签上传送出去，以自动辨识与追踪该物品
- 某些标签在识别时从识别器发出的电磁场中就可以得到能量，并不需要电池——无源RFID
- 也有标签本身拥有电源，并可以主动发出无线电波（调成无线电频率的电磁场）——有源RFID
- 标签包含了电子存储的信息，数米之内都可以识别。与条形码不同的是，射频标签不需要处在识别器视线之内，也可以嵌入被追踪物体之内



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

频带	规章管理	读取范围	数据速度	备注	标签估价 (以2006年美元计算)
120到150千赫(低频)	无规定	10厘米	低速	动物识别, 工厂数据的收集	1元
13.56兆赫(高频)	全世界通用ISM频段	1米	低速到中速	小卡片	0.50元
433兆赫 (特高频)	近距离设备 SRD	1到100米	中速	国防应用 (主动式标签)	5元
868到870兆赫(欧洲) 902到928百万赫兹(北美) 特高频	ISM频段	1到2米	中速到高速	欧洲商品编码, 各种标准	0.15元 (被动式标签)
2450到5800兆赫(微波)	ISM频段	1到2米	高速	802.11WLAN (无线局域网), 蓝牙标准	25元(主动式)
3.1到10吉赫(微波)	超宽带	最高200米	高速	需要半主动或主动标签	设计为5元

ref: <http://zh.wikipedia.org/wiki/%E5%B0%84%E9%A2%91%E8%AF%86%E5%88%AB>



RFID的应用领域——物联网的基础

- 钞票及产品防伪技术
- 身份证、通行证（包括门票）
- 电子收费系统，如香港的八达通与台湾的悠游卡、台湾通、一卡通
- 家畜或野生动物识别
- 病人识别及电子病历
- 物流管理
- 行李分类
- 门禁系统



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
 - 一如航空行李标签、特殊身份证件标签等
- 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, 被动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，主动RFID)
 - 自带电源供能
 - 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
 - 高速公路ETC



RFID的安全风险

- 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

- 门禁
- 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
- 食堂饭卡、水卡、校园一卡通



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



电磁辐射泄漏

- 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



智能卡 (Smart Card)

- “智能”体现在
 - 内置“存储器”，对存储的数据可以进行访问控制，阻止未授权访问
 - 内置“微处理器”和RAM
 - 密码学计算
 - 可编程计算
 - 支持组件式架构
 - 指纹识别
 - OTP
 - 传感器





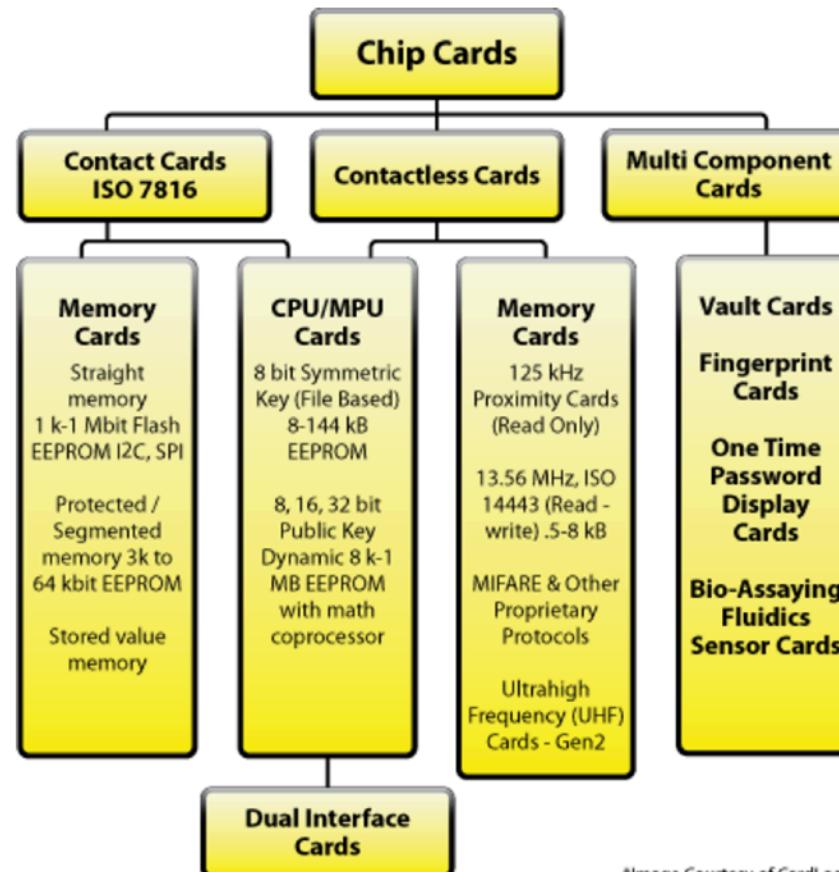
智能卡 (Smart Card)

- 与读卡器之间的通信方式

- 接触式

- 非接触式

- RFID为主



*Image Courtesy of CardLogix



USB令牌

- 除了接口和外观形状不同，其他物理和软件技术架构和智能卡无差异
- 一接口：使用USB，无需专用的“读卡设备”

- 常见产品



产品	产品实物图
二代 U盾 (LCD型)	
二代 U盾 (OLED型)	



智能卡主要应用场景

- 信息存储卡
 - 通常用于保存个人（隐私）信息，例如个人医疗记录卡
- 储值卡
 - 代替小额现金支付场景
 - 无需在线联网校验，直接读写卡内余额（次数）
自动贩卖机卡、预付费一次性电话卡、公交卡
- 认证令牌卡
 - 内置加密芯片，提供散列值、数字签名和加解密能力



智能卡主要应用场景

- 多功能卡
 - 内置操作系统
 - Windows for Smart Cards, MULTOS, Java Card
 - 支持灵活丰富的应用场景



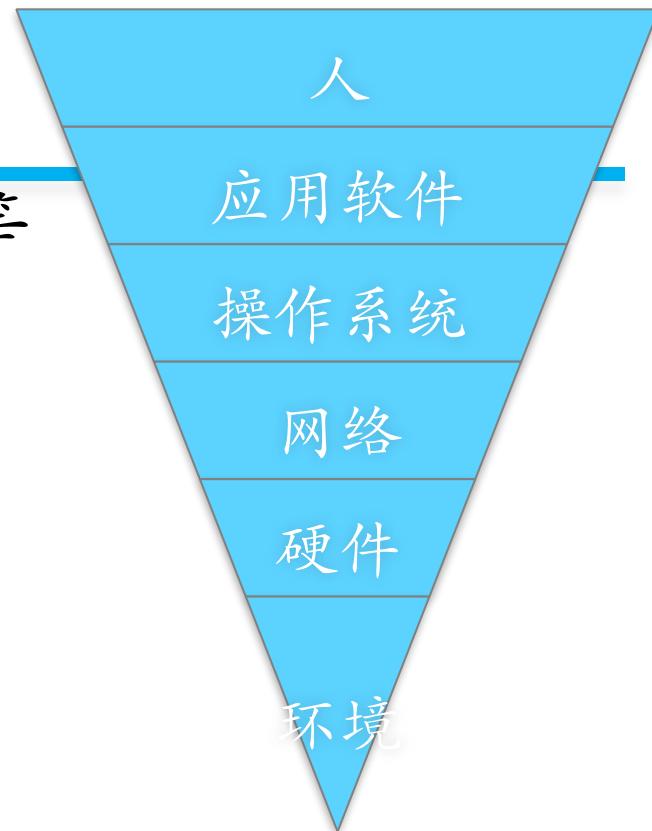
智能卡威胁

- 差分功耗分析 (Differential Power Analysis)
 - 基于密码学计算过程中的功耗变化统计数据来推导卡片上存储的密钥
- 计时攻击 (Timing Attacks)
 - 类似的攻击手段我们已在“SQL盲注攻击”中见识过
- 芯片逆向 (Reverse Engineering of the Chips)
 - 专家/富人/国家级研发能力和成本投入
- 设计/实现缺陷
 - 通用/缺省加密口令/密钥



智能卡威胁建模

- 人: 遗失、外借、设置PIN码等
- 软件: 软件设计与实现漏洞
 - 固定文件系统
 - 动态文件系统
- 网络: 明文传输风险, MITM, 嗅探器调试
- 硬件: 直接读取或破坏 (改变电压/温度/酸碱度/电路板重新焊接搭线等) EEPROM
- 环境: 钓鱼风险





智能卡操作系统安全

- 固定文件系统
 - 通常只被用于可信安全计算环境
 - 所有文件权限都是出厂时设置好无法修改的
 - 例如员工信息卡
- 动态文件系统
 - JavaCard®和MULTOS，操作系统和应用软件解耦
 - GSM的SIM卡，支持OTA更新
 - 适用于频繁需要更新数据/软件的场景，例如密钥协商

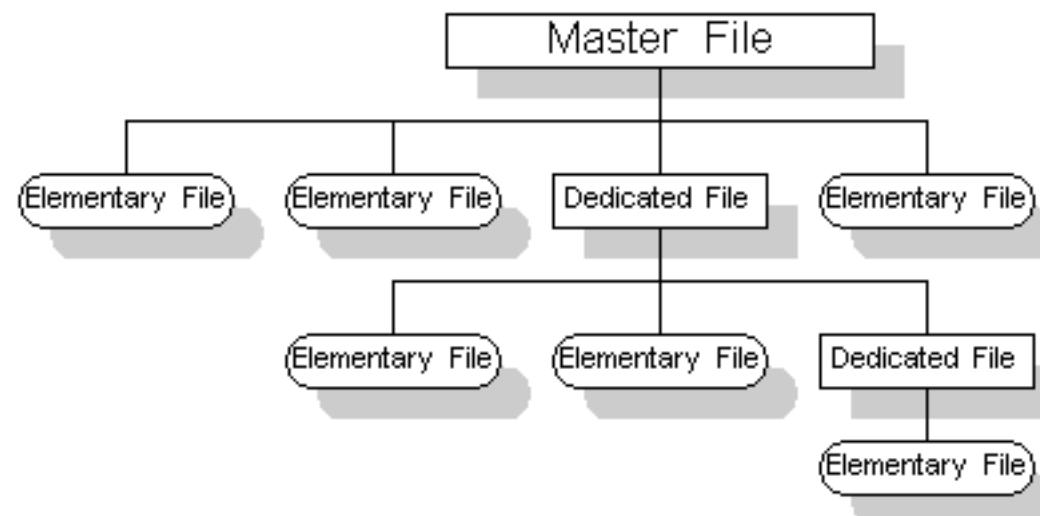


智能卡操作系统安全

- MF(Master File)和DF(Dedicated File)相当于“目录”，但DF依然可以独立存储数据
- EF(Elementary File)相当于“文件”
- MF/DF/EF的文件头包含安全属性（相当于访问控制信息）

—只要有“权限”就
可以遍历所有文件

—5类安全属性（权限）





智能卡文件系统安全属性

- Always(ALW)
- Card holder verification 1 (CHV1)
 - 使用PIN1验证， 用户设置的
- Card holder verification 2 (CHV2)
 - 使用PIN2验证， 设备商设置的用于解封设置（PIN1和PIN2是相互独立的PIN）
- Administrative (ADM)
- Never (NEV)



智能卡操作系统的PIN码安全机制

- 防暴力破解锁定机制

- 触发锁定的错误尝试认证次数和锁定时间取决于操作系统设置
 - PIN2用于解封PIN1被锁定状态
 - PIN2被锁定通常就只能返厂维修了
 - PIN1被锁定时所有文件均被设置CHV1属性，禁止访问



MIFARE

- MIFARE 是恩智浦半导体公司 (NXP Semiconductors) 在非接触式智能卡及近场感应卡领域的注册商标
- MIFARE是依循ISO/IEC 14443-A规格创建的非接触式智能卡，利用无线射频识别（频率为13.56MHz）来完成验证
- 近年来MIFARE已经普遍在日常生活当中使用，如大众运输系统付费、商店小额消费、门禁安全系统、借书证等



MIFARE产品线

	MIFARE Ultralight		MIFARE Classic	MIFARE Plus		MIFARE DESFire			
	MIFARE Ultralight EV1	MIFARE Ultralight C	MIFARE Classic EV1	MIFARE Plus (S/X)	MIFARE Plus SE	MIFARE DESFire EV1	MIFARE DESFire EV2		
射频接口	ISO/IEC 14443-2, TYPE A								
通信协议	ISO/IEC 14443-3			ISO/IEC 14443-3&4		ISO/IEC 14443-2			
UID码	UID: 7字节		UID: 7字节, RID: 4位组 (无UID)			UID: 7字节			
通信速度	106Kbps			106Kbps-848Kbps					
数据存储容量	48bytes	128bytes	144bytes	1K、4Kbytes	2K、4Kbytes	1Kbytes	2K、4K、8Kbytes		
验证密钥种类	无	TDES	Cryptot-1	Crypto-2、AES		TDES、AES			
机卡验证类型	无	三重认证							
机卡通信加密类型	无		Encrypted	Plain, Encrypted以及CMACed					
共同判据认证类型 (Common Criteria Certification)	无			EAL4	以CC认证为基 础	EAL4+	EAL5		



MIFARE Classic

- Unique Identifier(UID)只读
- 读取设备和卡片双向认证通过之后使用协商出的会话秘钥加密通信数据
- 使用私有的CRYPTO1加密算法（依赖于算法保密来“提升”密码学算法的安全性）
- 奇偶校验位混淆
- 仅硬件实现（依赖于硬件化“提升”防逆向能力）



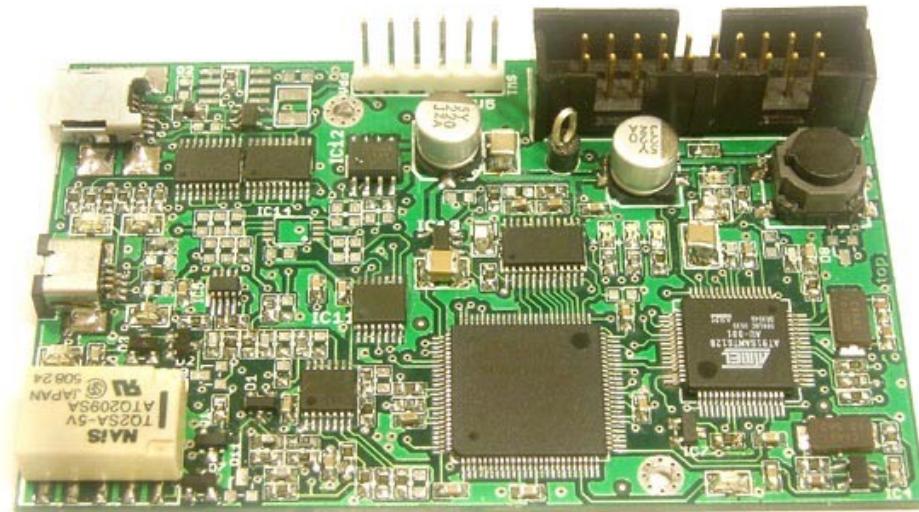
MIFARE的黑历史

- 2007年12月两个德国人Nohl 和 Plötz在 Chaos Communication Congress上展示了通过Crypto-1的一些缺陷部分逆向了其算法
- 2008年3月来自荷兰Radbond大学的研究者完全逆向了Crypto-1算法并予以公开
 - NXP试图通过法律途径禁止上述公开行为，但在2008年7月被当地法庭以言论自由原因驳回了申诉
- 2008年10月Radbond大学以GNU GPL v2协议开源了Crypto-1算法代码
- 大量针对MIFARE Classic卡的黑客工具被公开



Proxmark3

- Jonathan Westhues设计并且开发的开源硬件，其主要用RFID的嗅探、读取以及克隆等的操作
 - 低频(125kHz)～高频(13.56MHz)
- 可类比802.11类嗅探和注入实验





开放式讨论

- 接触式智能卡比非接触式智能卡更安全？更不安全？
 - 调试和逆向工具的完备性、成本
 - 卡片设计安全性
 - 卡片制造与实现安全性
- 类似的：无线网络和有线网络谁更安全？

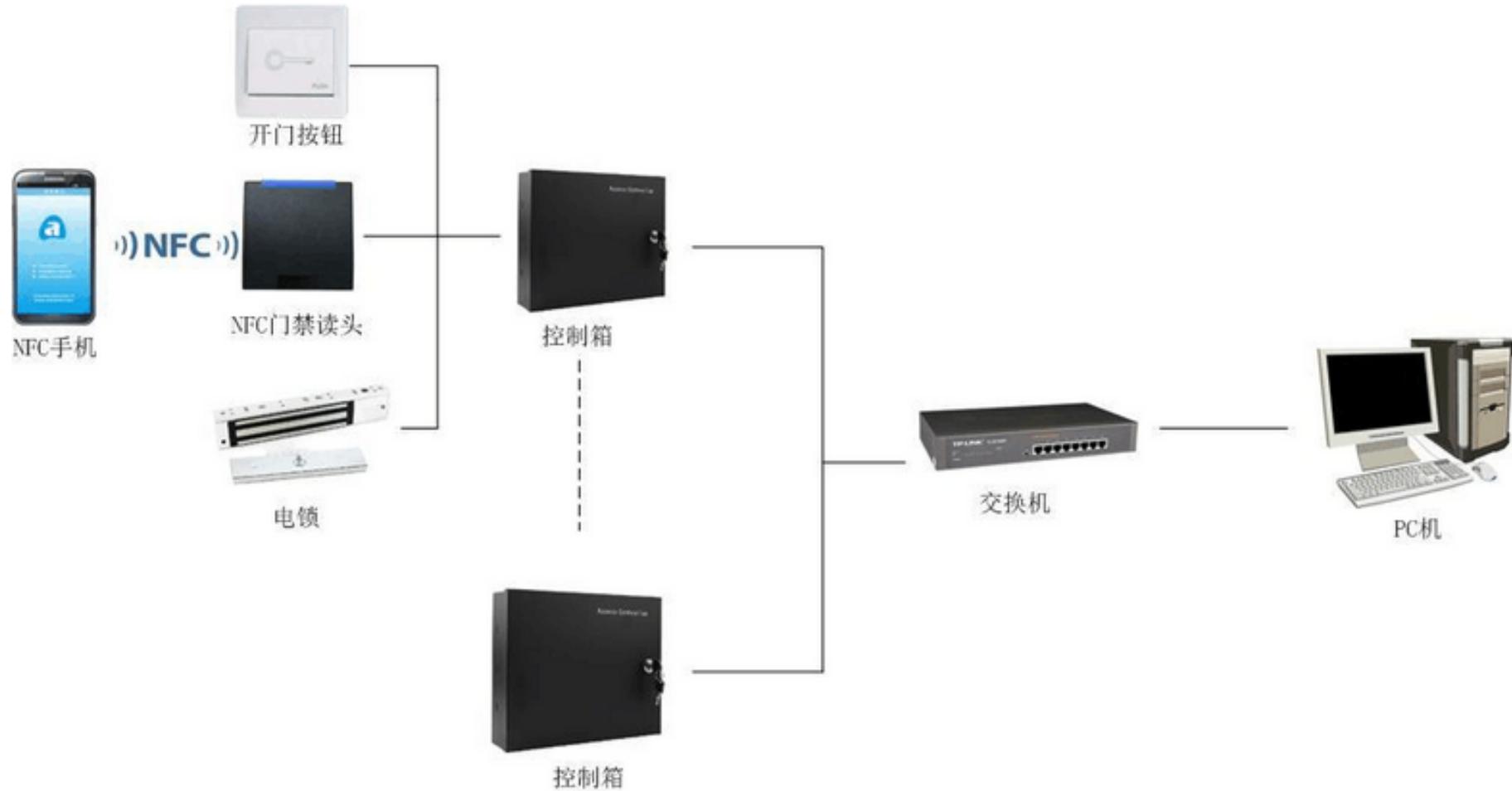


非接触式智能卡与RFID标签的比较

	非接触式智能卡	RFID标签
身份认证	<ul style="list-style-type: none">（读卡器与卡片之间）双向认证支持PIN或生物特征识别数据传输加密软硬件双重加密防止伪造身份	<ul style="list-style-type: none">单向认证（不认证读卡器）存储空间小（不支持生物特征信息存储）无板载芯片用于计算预共享静态秘钥
功能场景	公民身份标识、金融交易、物理访问控制等	物品标识（例如：库存管理、物流管理）为主
可读写能力	内置可读写持久存储器	内存小（92字节） 通常只读
通信距离	近距离为主	取决于射频的工作频率
价格	较贵	便宜



案例：基于智能卡的应用系统风险





“智能”硬件

中国传媒大学



概念与定义

- 没有一个公认的统一定义
- 本课程接下来要介绍的“智能”硬件其“智能”主要体现在至少具备其一特性
 - 具备通用或专用计算能力
 - 具有可编程性，支持软件定义硬件
 - 具备感知外界的能力
 - 低功耗或节能型



代表性产品

- DIY硬件
- 机器人、无人机
- 智能家电
 - 豆浆机，热水器，空调，净水器，电源开关，电源插座，电视，摄像机等等
- 智能家居
- 可穿戴设备（健康医疗、VR/AR等等）



DIY硬件

- Raspberry Pi
 - 微尺寸、全功能Linux主机
 - 英国剑桥大学出品，原设计用于教学计算机硬件维修
实验对象：满足物美价廉、可定制的全功能计算机硬件特性
- Arduino
 - 微控制器
 - 意大利一所交互设计专业教师出品，原设计同样用于教学：快速硬件产品原型构建



• Raspberry Pi VS. Arduino

	Arduino Uno	Raspberry Pi Model B
Price	\$30	\$35
Size	7.6 x 1.9 x 6.4 cm	8.6cm x 5.4cm x 1.7cm
Memory	0.002MB	512MB
Clock Speed	16 MHz	700 MHz
On Board Network	None	10/100 wired Ethernet RJ45
Multitasking	No	Yes
Input voltage	7 to 12 V	5 V
Flash	32KB	SD Card (2 to 16G)
USB	One, input only	Two, peripherals OK
Operating System	None	Linux distributions
Integrated Development Environment	Arduino	Scratch, IDLE, anything with Linux support



DIY硬件

- Raspberry Pi + Arduino
 - 全功能计算平台+丰富传感器和控制器
- 智能手机+USB OTG+配件（网卡、键盘等）
- 创新创业产品
 - MODI
 - Robotics of Things
 - Modular Kit for Robots





PoisonTap on Raspberry Pi

- <https://github.com/samyk/poisonTap>

- 基于USB接口通过物理连接Hack掉一台电脑

- 流量嗅探和劫持

- Cookie毒化

- RAT: Remote Access Toolkit



Rogue Access Point

- 通过物理联入的一个无线热点实现远程接入一个安全隔离的有线网络
 - 有线网络的安全性可以通过物理安全保障，但恶意AP的接入打破了原有的物理隔离和限制措施
 - 一个可编程的恶意AP可以实现自动化的局域网攻击
 - 智能手机、使用开源路由器固件（OpenWrt/DD-Wrt等等）的无线路由器/AP/Raspberry Pi



智能路由器

- 路由器厂商预留的“调试”后门
 - 关于多款路由器设备存在预置后门漏洞的情况通报
2014.02.10 from CNCERT
- 固件更新设计与实现缺陷
 - 仅使用简单的Hash算法校验下载文件完整性，未使用数字签名算法鉴别文件真实性
- 配置信息保存不当（明文）
- WPS功能未默认关闭
- 固件防逆向能力的高低



智能路由器

- 不安全的默认设置
 - 默认SSID
 - 默认WEB管理界面的缺省管理员密码
- WEB管理系统安全性



蓝牙安全

中国传媒大学



蓝牙概述

- WPAN技术之一
- 支持服务能力描述/声明配置文件
 - 声明蓝牙设备所具备的应用能力
 - 输入（键盘、鼠标）、输出（音频、文件传送、打印机）
 - 设备和能力发现
- 越来越多的物联网应用采用蓝牙（特别是蓝牙低功耗）作为底层通信协议
 - 例如各种智能锁、智能家居产品等

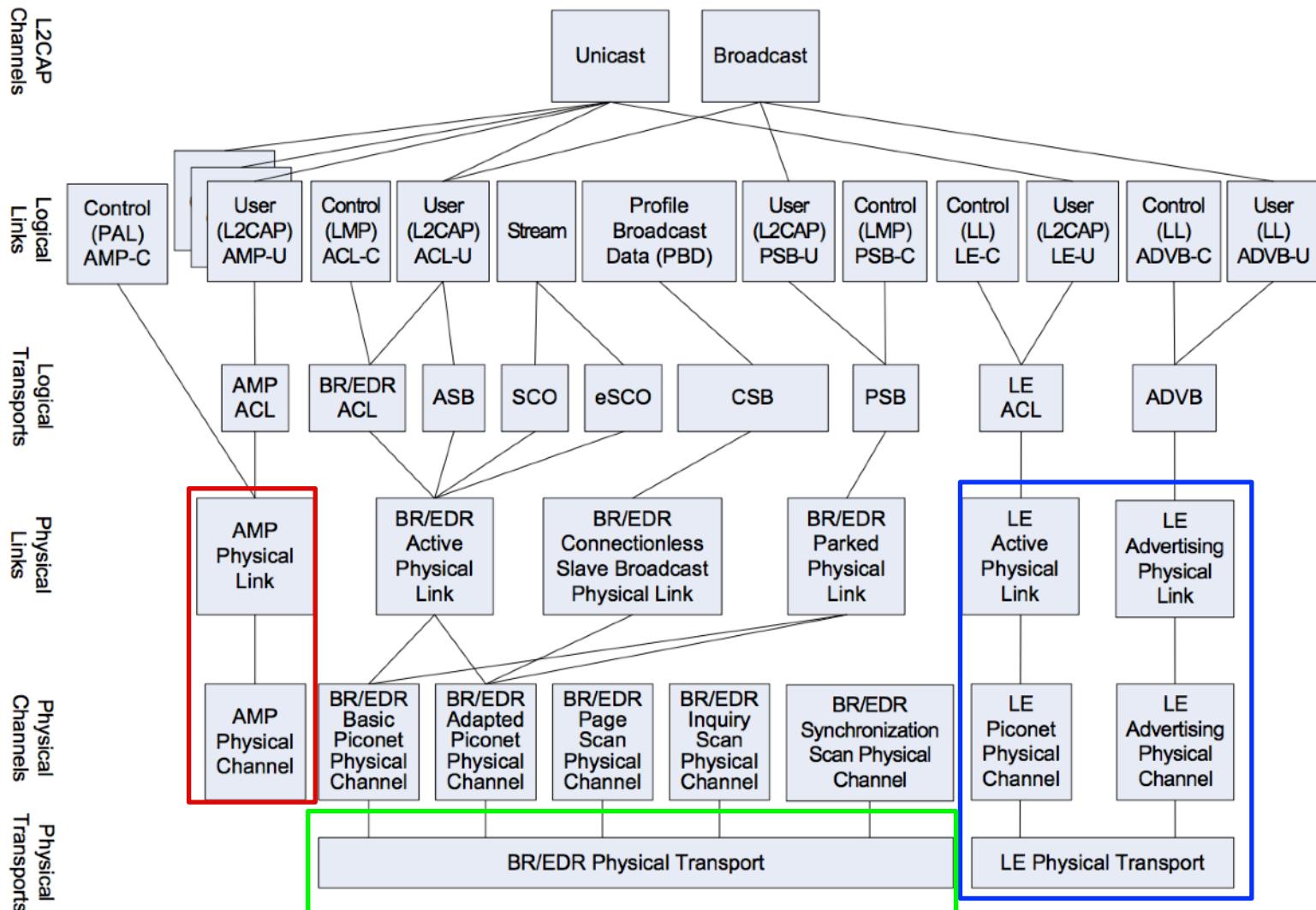


蓝牙设备（功耗）等级分类

设备类型	功耗	最大功耗等级	设计通信距离	典型设备
Class 1	高	100 mW (20 dBm)	< 100米	USB适配器、接入点
Class 2	中	2.5 mW (4 dBm)	< 10米	移动设备、蓝牙适配器、智能卡读卡器
Class 3	低	1 mW (0 dBm)	< 1米	蓝牙适配器



蓝牙协议栈



中国传媒大学



蓝牙技术基础

- 使用2.4 GHz ISM频段的2400~2483.5 MHz
 - Industrial Scientific Medical Band
- Basic Rate(BR) 721.2Kbps
 - optional EDR (Enhanced Data Rate) 2.1Mbps
 - AMP (Alternate MAC and PHY layer extension) 54Mbps
 - “借用”802.11协议的物理层和MAC层规范
 - BR/EDR和AMP必须二选一
- Low Energy(LE)



蓝牙与IEEE 802.11

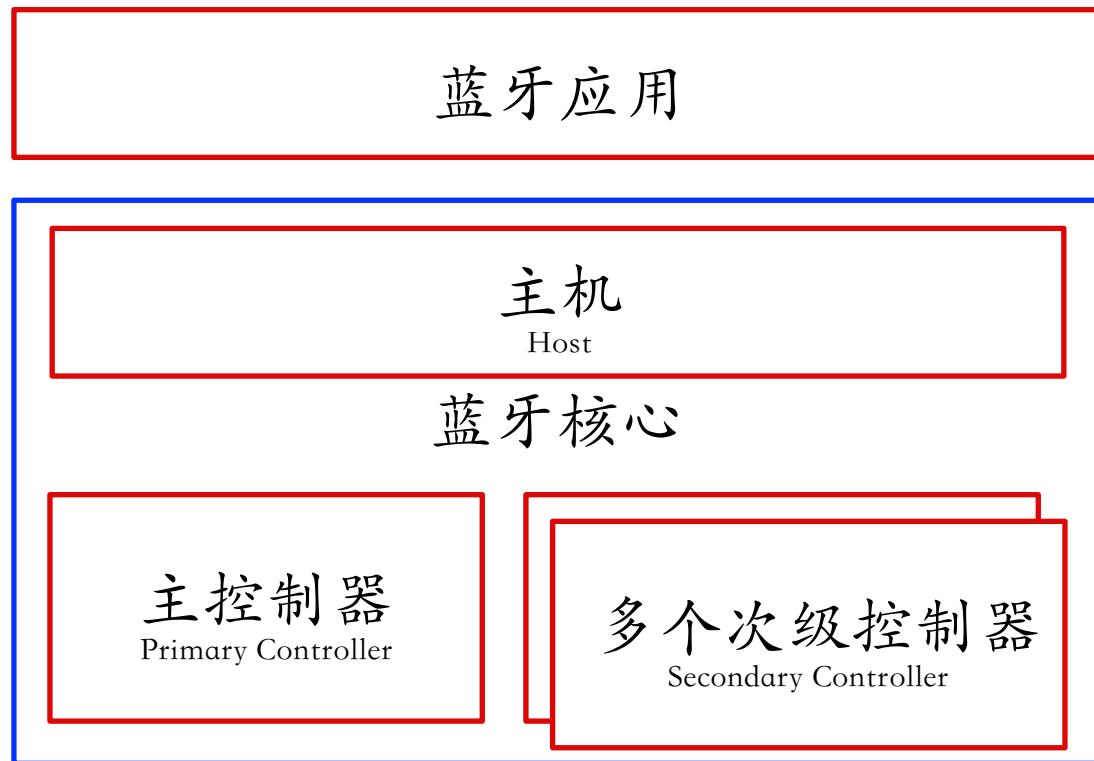
特性	蓝牙	IEEE 802.11
网络拓扑	对称（点对点）	非对称 (以AP为中心)
工作频段	2.4 GHz	2.4 GHz / 5 GHz
传输速率	1~24 Mbps	5.5~1000 Mbps
传输距离	1~300米 ^{蓝牙5.0}	室外最大250米左右
协议兼容性	3.0+版本兼容802.11n (物理层使用802.11协议)	-



蓝牙系统逻辑组成

Host在负责逻辑链路的基础上
为上层蓝牙应用提供
更易使用的封装

Controller负责定义RF、
Baseband等偏硬件的规范
在此基础之上抽象出
用于通信的逻辑链路





蓝牙ISM频段划分方法

- BR/EDR控制器，分成79个频率，每个为1 MHz
 - 跳频(Frequency Hopping)，1秒至多改变1600次
 - 物理信道 (Physical Channel) 是由跳频图谱 (Hopping Pattern) 决定的
 - 跳频图谱是一种规则，规定了蓝牙RF在某一时刻需要跳到79个频率中的哪个频率上通信
- LE控制器，分成40个频率，每个为2 MHz
 - 3个频率为广播信道 (Advertising Channel)
 - 37个频率为数据信道 (Data Channel)



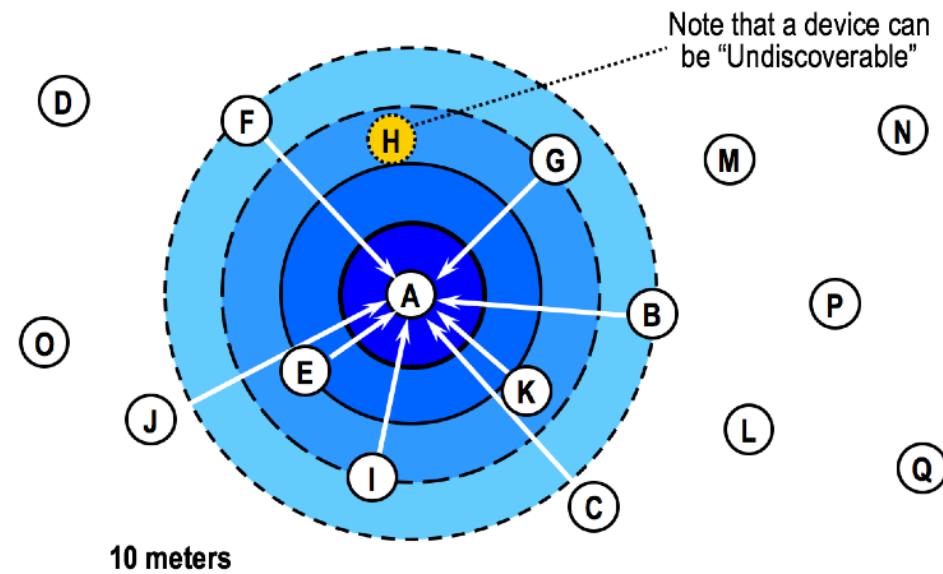
BR/EDR Controller

- 物理信道有三类：
 - 搜索用的信道 (Inquiry scan channel)
 - 连接用的信道 (Page scan channel)
 - 连接后设备之间通信的信道
- 连接建立后，多个设备共享同一个物理信道，决定跳频图的那个设备称作Master，其他设备称作Slave
 - Master只有一个，Slave可以有多个
- 连接建立后，双方根据已建立的、基于BR/EDR控制器的L2CAP(**Logical Link Control and Adaptation Protocol**)，可以协商各自是否具备可以使用的AMP信道，如果具备，是否愿意将后续的数据输出转移到这些控制器上（可以提高蓝牙传输速率）



BR/EDR Controller物理层控制

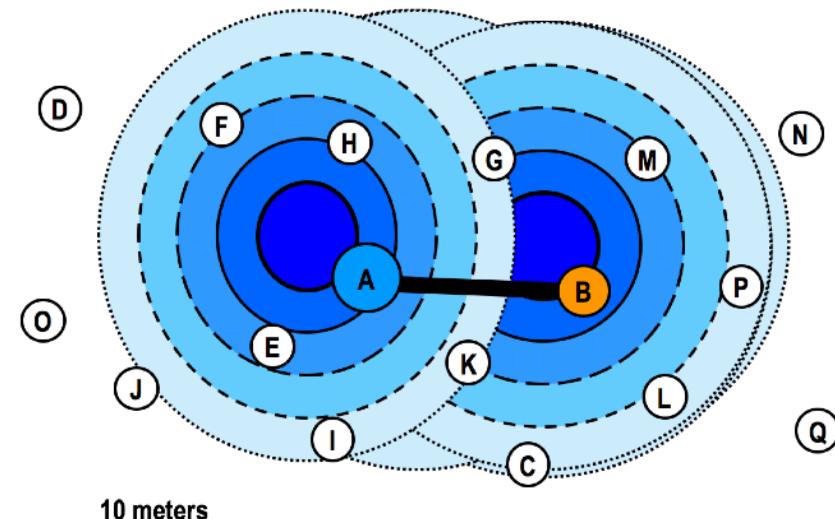
- 蓝牙设备之间进行数据通信前需要：
 - 找到对方
 - 搜索和可被搜索，处于搜索状态的一方以较快的速度跳频，被搜索设备以较慢的速度跳频并广播自身信息





BR/EDR Controller物理层控制

- 蓝牙设备之间进行数据通信前需要：
 - 和对方建立连接
 - 连接和可被连接
 - 连接是两个蓝牙设备同步到同一个跳频图谱（即物理信道）的过程，发起连接的一方作为Master，接受连接的一方为Slave





BR/EDR Controller链路层控制

- 在同一个物理信道上，只有Master和Slave之间可以通信，Slave和Slave之间不能通信
- 多个设备共享一个物理信道，Master和不同Slave之间可以时分复用信道，看起来就像独占了一个信道，称为：物理链路(Physical Link)
- 在物理链路之上抽象出逻辑链路，用于传输不同类型的数据，如异步数据、同步数据、单向(unidirectional)数据、广播数据等。逻辑链路时分复用物理链路。
- 链路管理协议(Link Management Protocol, LMP)用于管理抽象出来的逻辑链路
- LMP之上提供L2CAP层，从应用的角度复用逻辑链路。
 - 负责不同应用类型数据的封包和解包，类似TCP/IP里的端口



LE Controller

- 广播信道为预先设定的物理信道，其个数和占用的频率，都可以设定
 - 这些信道被划为时间单元，在这些时间单元上传输的数据包也称作事件(event)
 - 有广播和连接两种事件
- 37个数据信道用于连接建立后的数据通信，采用跳频技术



LE Controller广播通信

- 在广播信道发送广播数据的一方称作广播者(Advertiser)，接收广播数据但不打算连接的一方称作扫描者(Scanner)
 - 该特性主要用于那些没必要建立点对点连接的数据通信，如多播或广播
- Advertiser发送的广播数据中有一种称为“可连接广播数据包”，表示它可以被其他设备连接。接收到该包的设备可以在广播信道上回应“连接请求”，这样可以建立起来点对点连接，同时该设备被称作发起者(Initiator)
- 类似BR/EDR技术，Initiator为Master，Advertiser为Slave。点对点连接建立后的数据通信物理信道是由Master生成的跳频图谱决定的。



蓝牙4.0安全机制（协议规范）

- 配对(Pairing), 一次性过程
 - JustWorks(R), 如果设备没有显示屏
 - 6位PIN, 如果设备有显示屏
 - 带外(Out of band)
- 秘钥产生(Key Generation)
- 加密
 - 应用层 (GATT) 加密
- 数字签名



BLE

中国传媒大学



BLE - Bluetooth Low Energy

- 别名：Bluetooth Smart
- 经典蓝牙协议的一个轻量级子集（另一个是 Basic Rate），但不能与经典蓝牙协议互通
- 蓝牙4.0核心规范的组成部分
- 面向现代移动终端平台设计
 - iOS5+ (iOS7+ preferred)
 - Android 4.3+ (numerous bug fixes in 4.4+)
 - Apple OS X 10.6+
 - Windows 8 (XP, Vista and 7 only support Bluetooth 2.1)
 - GNU/Linux Vanilla BlueZ 4.93+



使用场景

- 广播通信

—单一方向的、无连接的数据通信，数据发送者在广播信道上广播数据，数据接收者扫描、接收数据

GAP

负责从应用程序的角度，抽象并封装LL提供的功能，以便让应用以比较傻瓜的方式进行广播通信。非必须选项，没有GAP也可以进行广播通信。

HCI(Host Controller Interface)

负责将LL提供的所有功能，以Command/Event的形式抽象出来，供Host使用

LL(Link Layer)

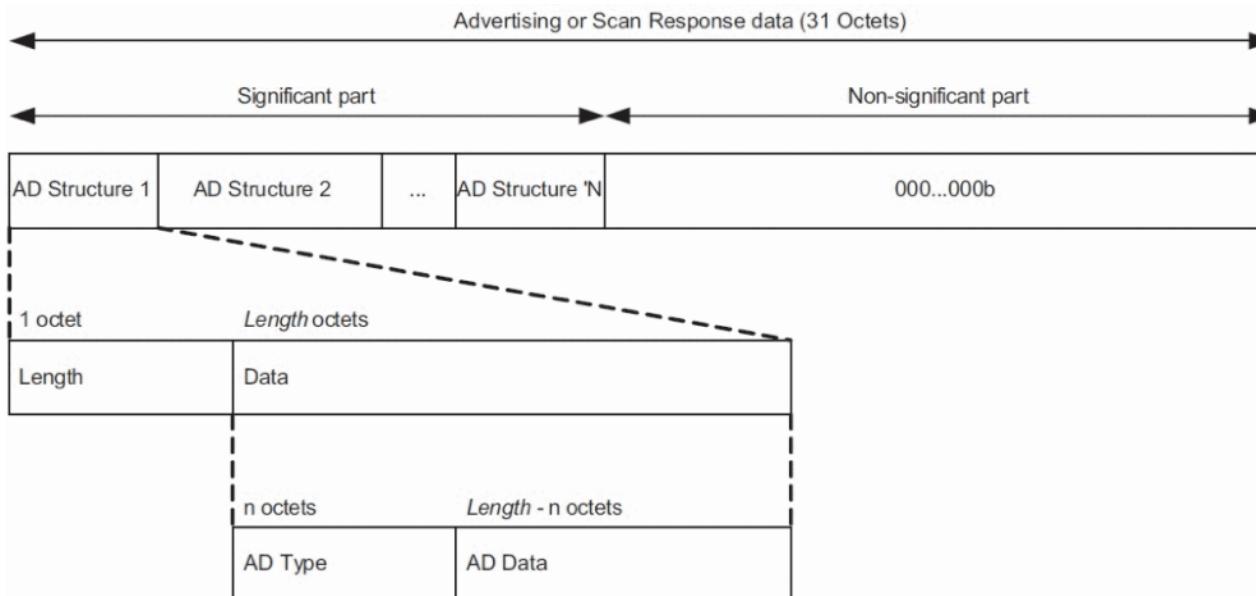
负责广播通信有关功能的定义和实现，包括物理通道的选择、相关的链路状态的定义、PDU的定义、设备过滤（Device Filtering）机制的实现等

- 连接建立



广播通信和扫描响应数据

- Advertising Data / Scan Response (可选)

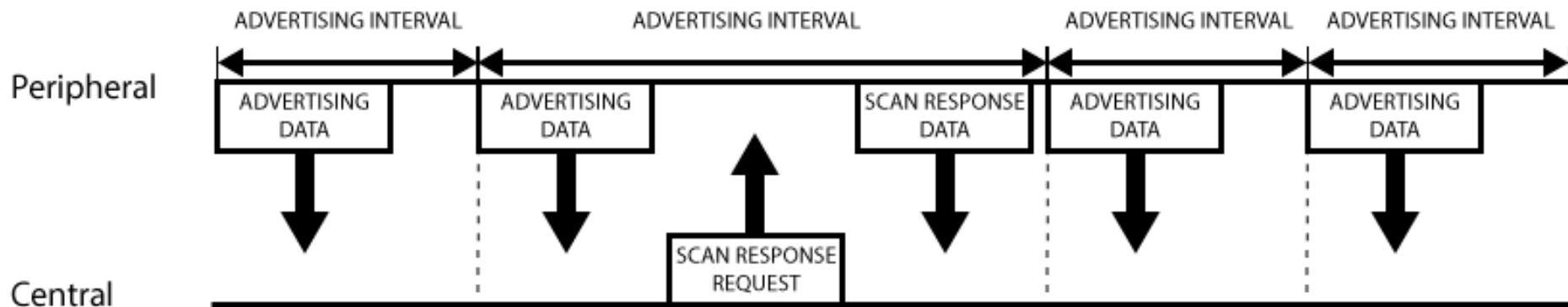


- 广播数据（或者扫描应答数据）由一个一个的AD Structure组成，对于未满31bytes的其它数据，则填充为0
- 每个AD Structure由两部分组成：1byte的长度信息（Data的长度），和剩余的Data信息
- Data信息又由两部分组成：AD Type（长度不定）指示该AD Structure的类型，以及具体的AD Data



广播通信过程

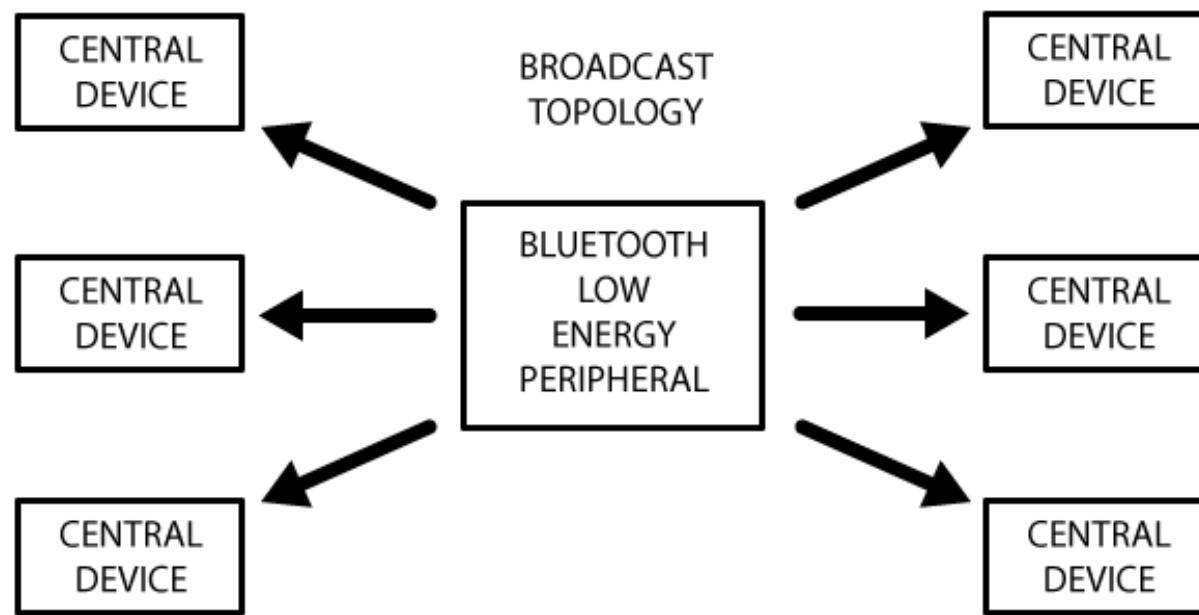
- 周边设备会设置一个广播间隔并周期性的重新传送它的主广播数据报文
一间隔设置的长短会影响到设备的耗电和响应延迟
- 监听设备通过发送SR请求来获得周边设备的SR数据





广播通信网络拓扑

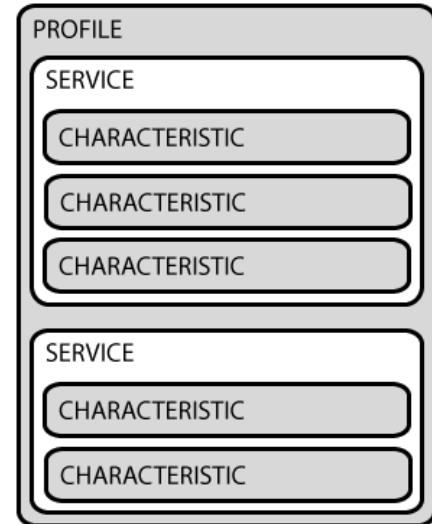
- 周边设备一旦和中心设备建立连接，则广播通信过程终止，改用GATT服务来进行双向通信





GATT - Generic Attribute Profile

- 定义了2个BLE设备数据交换的方式
 - 服务 Services
 - 特性 Characteristics
- ATT - Attribute Profile
 - 存储服务、特性和相关数据于一个简单的查找表，使用16-bit 唯一编号在表中查找匹配
- 一个BLE周边设备一次只能连接一个中心设备
 - 连接一旦建立，广播通信立刻停止，其他设备就无法发现它所以无法再建立新连接了





GATT - 服务和特性

- Profile

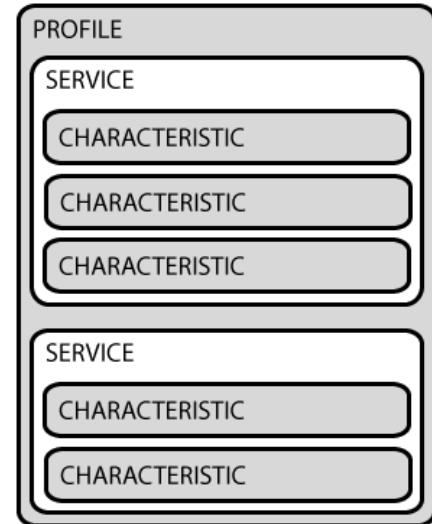
- 由蓝牙标准委员会或周边设备生产商预定义的一个服务集合

- Service

- BLE标准委员会官方采纳的服务采用16-bit UUID进行标识，最多允许包含3个特性，私有自定义服务采用128-bit唯一标识

- Characteristic

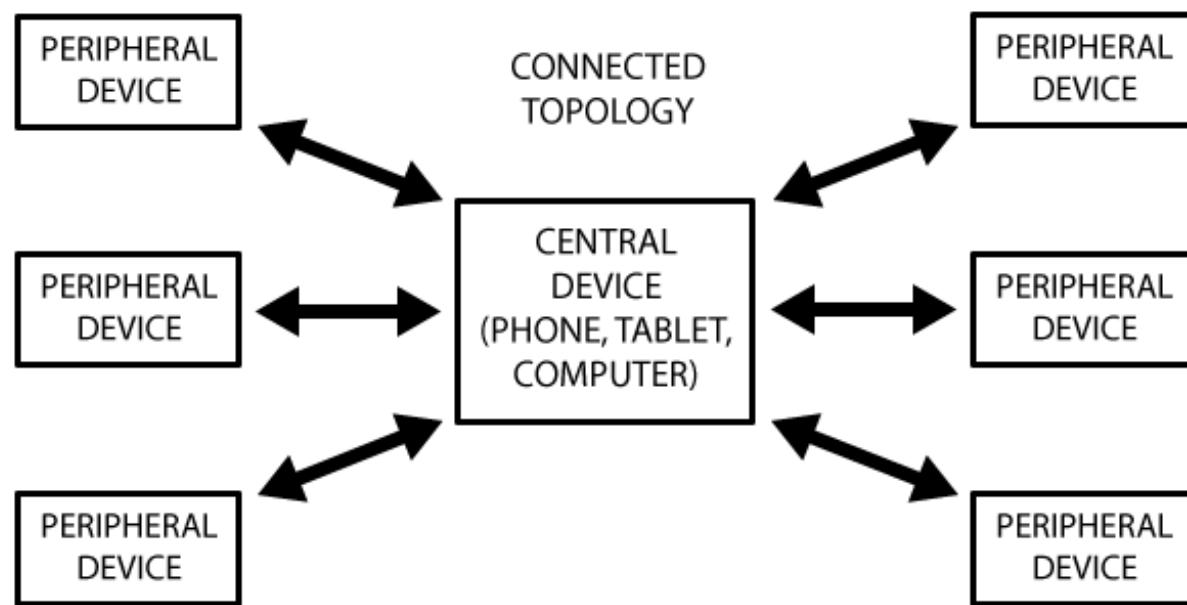
- BLE标准委员会官方采纳的特性采用16-bit UUID进行标识，私有自定义特性采用128-bit唯一标识
 - 一个特性字段存一个独立数据（可以是复合数据结构）





已建立连接时的网络拓扑

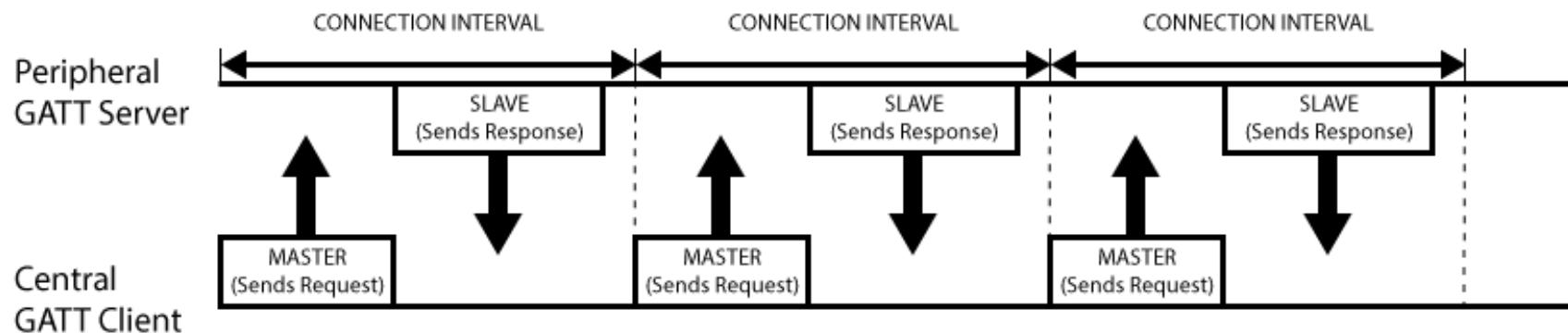
- 一个中心设备可以被多个周边设备连接
- 连接一旦建立就是一个双向通信的信道





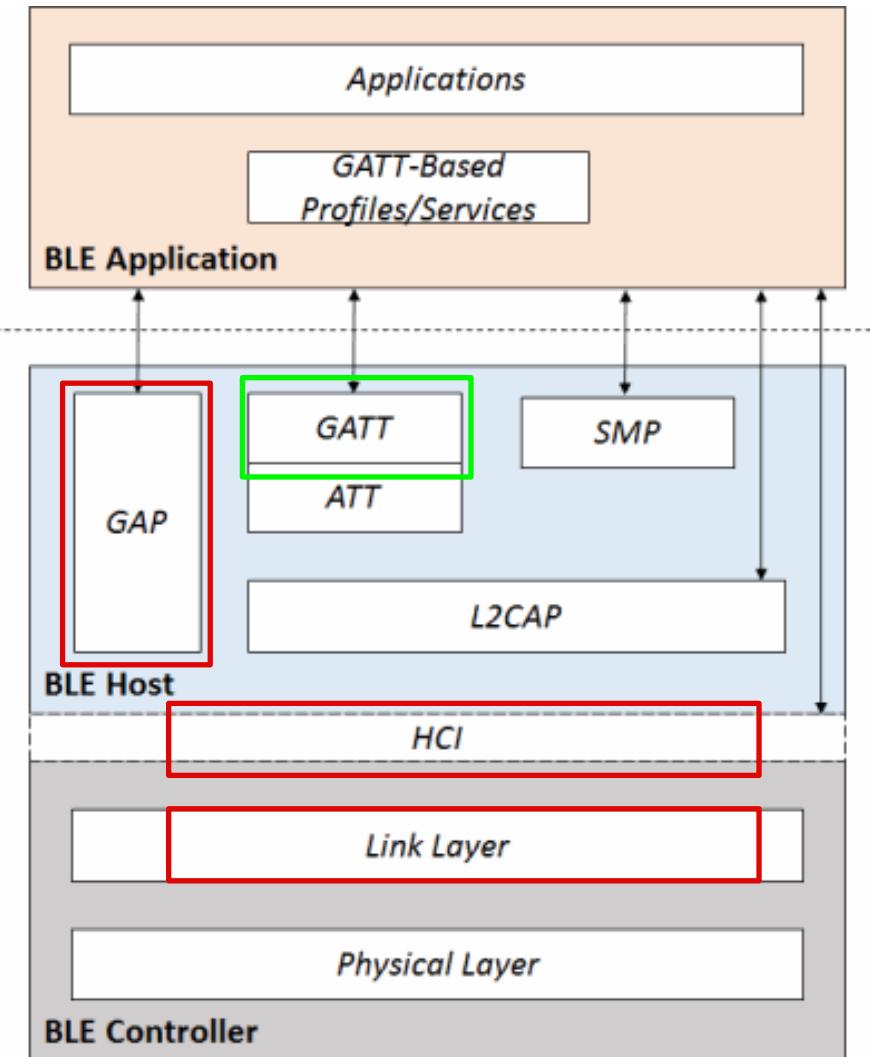
GATT会话

- 周边设备：GATT Server
 - 持有ATT查找数据、服务和特性定义
- 中心设备：GATT Client
 - 向Server发起请求
- 连接间隔
 - Server设置建议值，Client不一定照办（并发处理多个会话带来的可能延迟）





典型协议栈结构



GATT提供多种认证机制

- 静态口令/秘钥
- 挑战-响应（最常见）
- PKI

SMP (Security Manager Protocol) :点对点的协议，基于专用的L2CAP channel, 用于生成加密和识别 (identity) 用的密匙
SM控制包括配对 (pairing,) 、认证 (authentication) 和加密 (encryption) 等过程

L2CAP包括两个子模块：

- Channel Manager主要负责创建、管理、释放L2CAP channel
- L2CAP Resource Manager负责统一管理、调度 L2CAP channel上传递的PDU (Packet Data Unit) , 以确保那些高QoS的packet可以获得对物理信道的控制权



GAP - Generic Access Profile

- 一个基础的蓝牙profile，用于提供蓝牙设备的通用访问功能，包括设备发现、连接、鉴权、服务发现等等
- 通过定义设备角色来控制蓝牙连接和广播通信，实现不同设备的互操作
 - 中心设备(Central Device)，主动发现的设备
 - 计算能力更强，耗电量更大，例如手机、平板电脑等
 - 周边设备(Peripheral Device)，被发现的设备
 - 体积小、功耗低，通常需要连入中心设备。例如心率监控设备



链路层状态定义

- Advertising, 数据发送方, 周期性的发送广播数据
- Scanning, 数据接收方, 扫描、接收广播数据
- Initiating, 连接发起方, 扫描带有“可连接”标志的广播数据, 一旦发现, 则发起连接请求 (都是由Link Layer自动完成, 不需要Host软件参与)



蓝牙安全概述

• 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，重放和中间人攻击

— 隐私问题：标识追踪

• 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

- 配对验证码PIN是默认值或弱PIN码

- 蓝牙直接绑定应用相对复杂

 - BlueSnarf

 - OverFlow



蓝牙标识伪造

```
root@KaliRolling:~# hciconfig --all
hci0:  Type: Primary  Bus: USB
BD Address: B8:E8:56 [REDACTED]  ACL MTU: 1021:8  SCO MTU: 64:1
UP RUNNING PSCAN INQUIRY AUTH
RX bytes:12278 acl:46 sco:0 events:514 errors:0
TX bytes:4099 acl:48 sco:0 commands:266 errors:0
Features: 0xbf 0xfe 0xcf 0xfe 0xdb 0xff 0x7b 0x87
Packet type: DM1 DM3 DM5 DH1 DH3 DH5 HV1 HV2 HV3
Link policy: RSWITCH SNIFF
Link mode: SLAVE ACCEPT
Name: 'c4pr1c3_rmbp'
Class: 0x000000
Service Classes: Unspecified
Device Class: Miscellaneous,
HCI Version: 4.0 (0x6) Revision: 0x242c
LMP Version: 4.0 (0x6) Subversion: 0x4189
Manufacturer: Broadcom Corporation (15)
```

原始设备信息

新设备信息

```
root@KaliRolling:~# hciconfig hci0 class 0x800404
root@KaliRolling:~# hciconfig -a
hci0:  Type: Primary  Bus: USB
BD Address: B8:E8:56 [REDACTED]  ACL MTU: 1021:8  SCO MTU: 64:1
UP RUNNING PSCAN INQUIRY AUTH
RX bytes:12669 acl:46 sco:0 events:542 errors:0
TX bytes:4210 acl:48 sco:0 commands:282 errors:0
Features: 0xbf 0xfe 0xcf 0xfe 0xdb 0xff 0x7b 0x87
Packet type: DM1 DM3 DM5 DH1 DH3 DH5 HV1 HV2 HV3
Link policy: RSWITCH SNIFF
Link mode: SLAVE ACCEPT
Name: 'c4pr1c3_rmbp'
Class: 0x800404
Service Classes: Information
Device Class: Audio/Video, Device conforms to the Headset profile
HCI Version: 4.0 (0x6) Revision: 0x242c
LMP Version: 4.0 (0x6) Subversion: 0x4189
Manufacturer: Broadcom Corporation (15)
```

中国传媒大学



蓝牙设备存活性探测

```
root@KaliRolling:~# hcitool scan
```

Scanning ...

2C:20:0B: [REDACTED] poc

```
root@KaliRolling:~# l2ping 2C:20:0B:[REDACTED]
```

Ping: 2C:20:0B:[REDACTED] from B8:E8:56:[REDACTED] (data size 44) ...

44 bytes from 2C:20:0B:[REDACTED] id 0 time 117.84ms

44 bytes from 2C:20:0B:[REDACTED] id 1 time 166.33ms

44 bytes from 2C:20:0B:[REDACTED] id 2 time 138.81ms

^C3 sent, 3 received, 0% loss

```
root@KaliRolling:~# hcitool lescan
```

LE Scan ...

44:29:AE:[REDACTED] (unknown)

44:29:AE:[REDACTED] (unknown)

44:29:AE:[REDACTED] (unknown)

40:52:15:[REDACTED] (unknown)

40:52:15:[REDACTED] (unknown)

在[蓝牙](#)(Bluetooth®)4.2核心规范当中，支持一项新的特性，可以通过周期性地改变蓝牙设备的随机地址帮助蓝牙设备的使用者来保护自身的隐私，避免其设备被黑客或者是窃听者通过射频侦听以及对数据分析的方式得以窃取。



蓝牙设备信息探测

```
root@KaliRolling:~# hcitool -i hci0 inq
Inquiring ...
 2C:20:0B: [REDACTED]          clock offset: 0x2314      class: 0x7a020c
root@KaliRolling:~# hcitool -i hci0 scan --info --class
Scanning ...
Username: [REDACTED]
BD Address: 2C:20:0B: [REDACTED] [mode 1, clkoffset 0x2314]
Device class: Phone, Smart phone (0x7a020c)
Manufacturer: Broadcom Corporation (15)
LMP version: 4.2 (0x8) [subver 0x6103]
LMP features: 0xbf 0xfe 0xcf 0xfe 0xdb 0xff 0x7b 0x87
               <3-slot packets> <5-slot packets> <encryption> <slot offset>
               <timing accuracy> <role switch> <sniff mode> <RSSI>
               <channel quality> <SCO link> <HV2 packets> <HV3 packets>
               <u-law log> <A-law log> <CVSD> <paging scheme> <power control>
               <transparent SCO> <broadcast encrypt> <EDR ACL 2 Mbps>
               <EDR ACL 3 Mbps> <enhanced iscan> <interlaced iscan>
               <interlaced pscan> <inquiry with RSSI> <extended SCO>
               <EV4 packets> <EV5 packets> <AFH cap. slave>
               <AFH class. slave> <LE support> <3-slot EDR ACL>
               <5-slot EDR ACL> <sniff subrating> <pause encryption>
               <AFH cap. master> <AFH class. master> <EDR eSCO 2 Mbps>
               <EDR eSCO 3 Mbps> <3-slot EDR eSCO> <extended inquiry>
               <LE and BR/EDR> <simple pairing> <encapsulated PDU>
               <err. data report> <non-flush flag> <LST0> <inquiry TX power>
               <EPC> <extended features>
```



蓝牙通信数据嗅探

- 工具软件
 - btmon / hcidump / wireshark
 - nRF Connect for Mobile (Android App)
- 数据存储格式
 - BTsnoop
- 注意事项!
 - 没有专用硬件支持则只能嗅探到本机收发的蓝牙数据，无法捕获其他设备之间的蓝牙通信数据
 - 类比802.11网络的“监听”模式与有线网卡的“混杂”模式的区别



数据构造和发送

- Linux上的蓝牙协议栈——BlueZ



蓝牙通信协议逆向

- 重放攻击
 - 智能灯泡逆向与控制实例
 - Blue picking - hacking Bluetooth Smart Locks



NFC - Near Field Communication

- 短距离高频无线通信技术，由RFID演变而来
- NFC仅限13.56MHz高频段，RFID有较多频段选择
- NFC的有效通信距离大多在10厘米以内，RFID的通信距离范围从几厘米到几十米都有
- NFC是一种“集成”RFID技术，单芯片内置非接触读卡器、非接触卡和点对点功能，RFID通常使用独立的阅读器和标签
- RFID多用于生产、物流、资产管理等，NFC则更多用于公交、门禁、手机支付等



NFC与蓝牙的关系

特性	NFC	蓝牙	低功耗蓝牙(BLE)
标签是否耗能	否	是	是
标签成本	10美分	5美元	5美元
RFID兼容性	ISO 18000-3	有源（主动）	有源（主动）
标准化组织	ISO/IEC	Bluetooth SIG	Bluetooth SIG
网络协议标准	ISO 13157 etc.	IEEE 802.15.1	IEEE 802.15.1
网络拓扑类型	点对点	WPAN	WPAN
加密	基于RFID技术的没有	可选	可选
通信距离	< 0.2m	~ 100m (class 1)	~ 50m
频段	13.56 MHz	2.4-2.5GHz	2.4-2.5GHz
传输(比特)速率	424 kbps	2.1/24 Mbps	1 Mbps
(网络)建立时间	< 0.1s	< 6s	< 0.006s
功耗	< 15 mA(读)	不同级别有差异	< 15 mA (读和传输)



蓝牙协议安全实战

中国传媒大学



蓝牙通信嗅探的难点

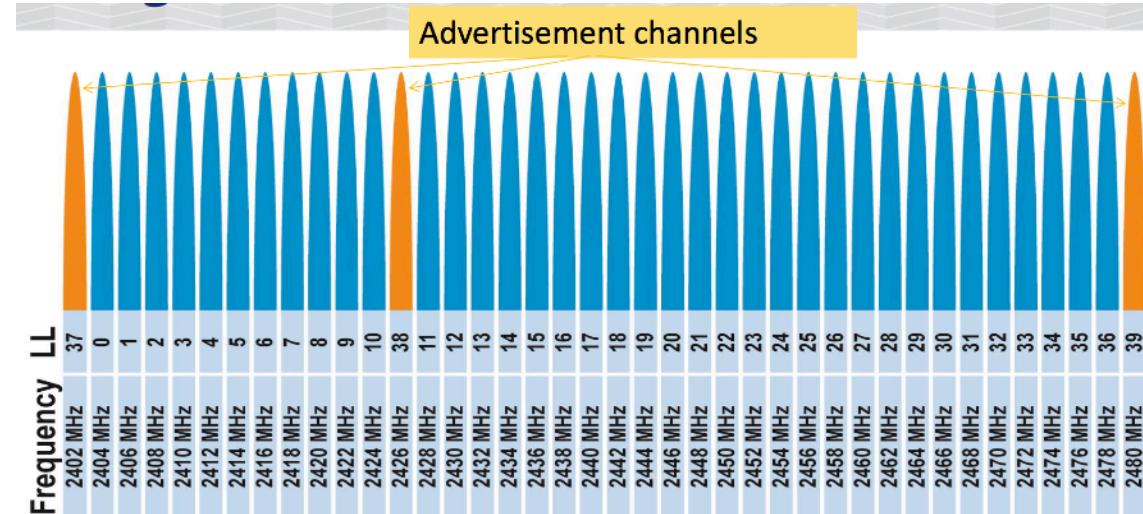
- 两种模式：经典（BR/EDR）和LE（不兼容）
- 复杂的软件（2000多页的蓝牙核心协议规范）
- 一直在演进的协议规范（蓝牙5.0于2016年6月发布）
- 不同设备厂商生产设备的互操作性问题（利用蓝牙扩展协议）



蓝牙通信嗅探的难点

- 以BLE为例

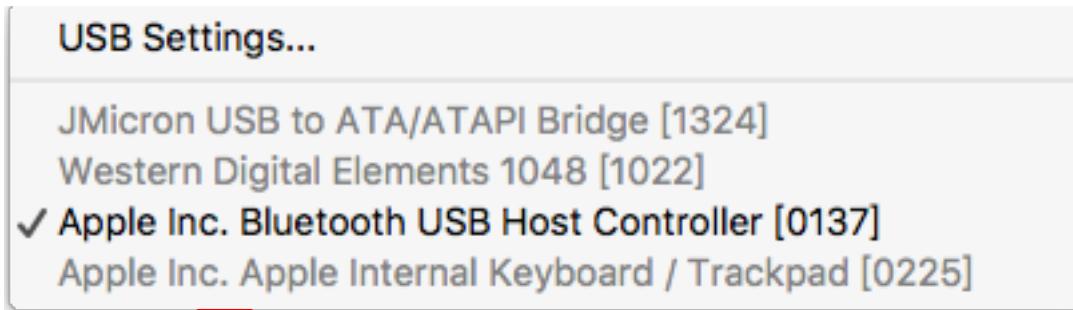
- 数据传送在37个频点上跳频通信，1秒至多1600次跳频
- 每个数据帧只在一个频点上传输
- 跳频图谱动态产生：需要实时抓包并按照会话实时计算
 - 设备内部时钟频率决定跳频周期间隔
- 2.4 GHz频段拥挤
- 蓝牙并发连接





免费硬件方案

- 笔记本电脑内置蓝牙模块（USB接口）

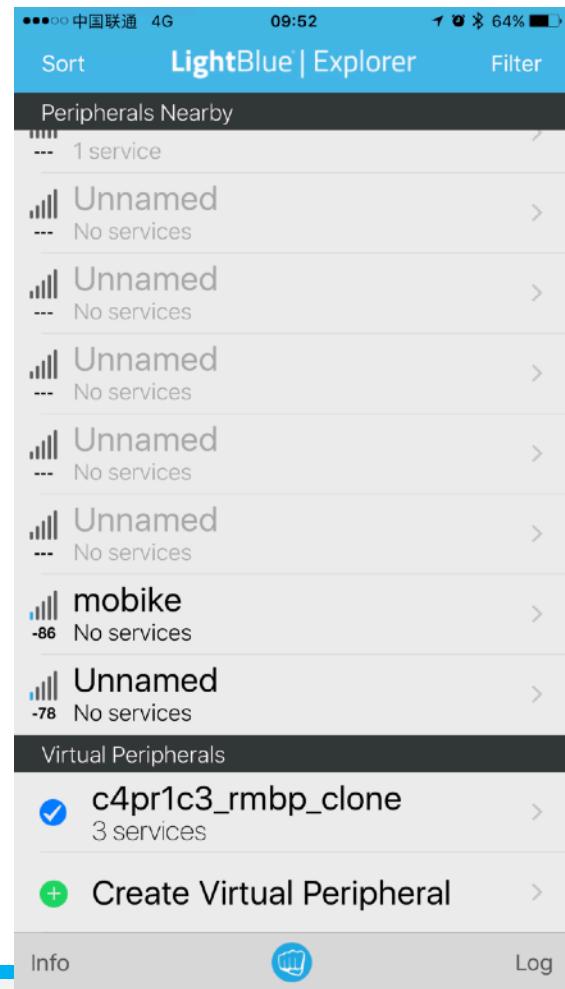
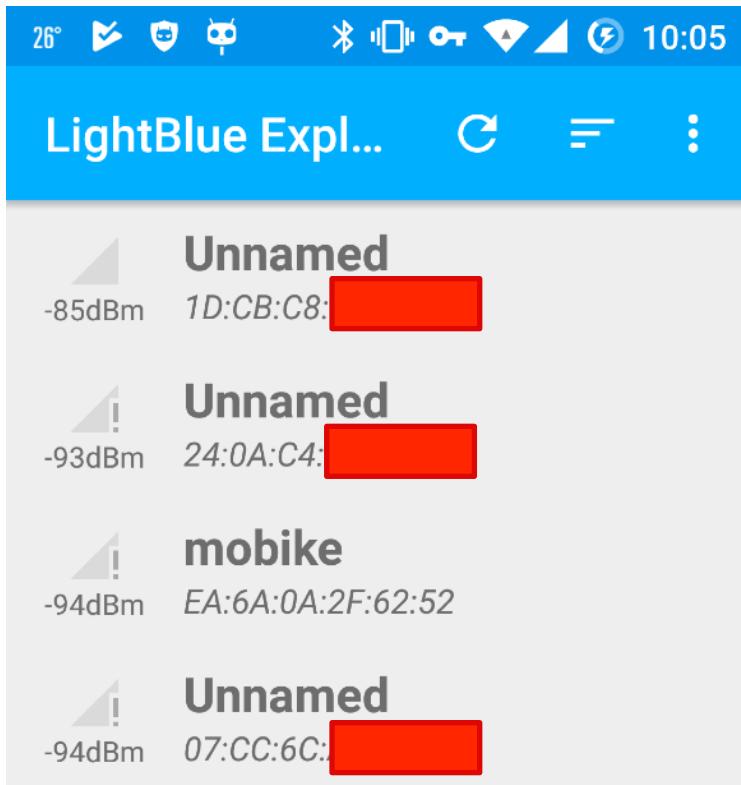


```
root@KaliRolling:~# hciconfig hci0 features
hci0:  Type: Primary  Bus: USB
BD Address: B8:E8:56 [REDACTED]  ACL MTU: 1021:8  SCO MTU: 64:1
Features page 0: 0xbf 0xfe 0xcf 0xfe 0xdb 0xff 0x7b 0x87
  <3-slot packets> <5-slot packets> <encryption> <slot offset>
  <timing accuracy> <role switch> <sniff mode> <RSSI>
  <channel quality> <SCO link> <HV2 packets> <HV3 packets>
  <u-law log> <A-law log> <CVSD> <paging scheme> <power control>
  <transparent SCO> <broadcast encrypt> <EDR ACL 2 Mbps>
  <EDR ACL 3 Mbps> <enhanced iscan> <interlaced iscan>
  <interlaced pscan> <inquiry with RSSI> <extended SCO>
  <EV4 packets> <EV5 packets> <AFH cap. slave>
  <AFH class. slave> <LE support> <3-slot EDR ACL>
  <5-slot EDR ACL> <sniff subrating> <pause encryption>
  <AFH cap. master> <AFH class. master> <EDR eSCO 2 Mbps>
  <EDR eSCO 3 Mbps> <3-slot EDR eSCO> <extended inquiry>
  <LE and BR/EDR> <simple pairing> <encapsulated PDU>
  <err. data report> <non-flush flag> <LST0> <inquiry TX power>
  <EPC> <extended features>
Features page 1: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
```



免费硬件方案

- 使用智能手机，具体操作参见本课程第7章课件相关内容





前述两种“免费”硬件方案的局限性

- 标准蓝牙设备不支持“混杂”模式
 - 无法嗅探其他设备之间的蓝牙通信数据
 - 目的地址不是自己的蓝牙数据在硬件底层就被“丢弃”
 - 需要专门定制的硬件，例如SDR
- 所有通过蓝牙协议发送的数据都是“混淆”的
 - 抓包的同时需要实时的“解混淆”这些数据
- 跳频图谱需要动态实时计算出来才能完整捕获连接建立后的通信数据
 - 基于Master的MAC地址实时计算



付费硬件方案

• SmartRF Protocol Packet Sniffer from TI

适用于蓝牙低功耗网络的数据包监听器。

适用于 ZigBee 和 IEEE 802.15.4 网络的数据包监听器。

适用于 RF4CE 网络的数据包监听器。

适用于 SimpliciTI™ 网络的数据包监听器。

适用于通用协议（原始数据包数据）的数据包监听器。

保存/打开含有捕获的数据包的文件。

选择要显示和隐藏的字段。

过滤要显示的数据包。

通过显示由无线电设备接收的原始数据来显示数据包详细信息。

收到的数据包有准确的时间戳。

具有网络中所有已知节点的地址簿。

按照接收顺序显示所有数据包的简单时间线。

可以将捕获的数据转发至 UDP 套接字，用于通过自定义工具来实时监控数据包



付费硬件方案

- Nordic

- BLE: nRF51822
- Bluetooth 5: nRF52xxx

	nRF52840	nRF52832	nRF52810
支持协议	蓝牙5/BLE/ANT/ 802.15.4/2.4GHz RF SoC	蓝牙5/BLE/ANT/ 2.4GHz RF SoC	蓝牙5/BLE/ANT/ 2.4GHz RF SoC
长距离(x4)	✓		
高吞吐(x2)	✓	✓	✓
广播容量增加(x8)	✓	✓	✓
增强信道共存算法	✓	✓	✓

中国传媒大学



付费硬件方案

- Adafruit Bluefruit LE Sniffer - Bluetooth Low Energy (BLE 4.0) - nRF51822 - v3.0

- Adafruit 公司是一家致力于创造最好的在线学习电子和做出最好的设计产品的制造商，公司成立于2005年，由麻省理工学院的工程师利莫Ladyada创立
- 基于Nordic公司的nRF51822解决方案



付费硬件方案

- ellisys

—专业蓝牙协议分析仪（价格昂贵）

- Ellisys Bluetooth Explorer All-in-One Bluetooth® Protocol Analysis System
- Ellisys Bluetooth Tracker Ultra-Portable BLE and Wi-Fi Protocol Analyzer





付费硬件方案

- Ubertooth

- 软硬件均开源的2.4 GHz无线开发平台，可以用于蓝牙相关实验
- 硬件：可以通过开源的电子器件原理图DIY也可以直接购买现成设备
- 固件：运行在Ubertooth One上的ARM处理器
- 主机代码：运行在通过USB连接了Ubertooth One设备的普通电脑上



不同硬件方案比较

	价格	优点	缺点
<u>Ellisys Bluetooth Tracker</u>	> \$10,000	高度集成和便携，支持蓝牙5(包括BLE) 和Wi-Fi	贵
<u>TI BLE Sniffer (CC2540EMK-USB dongle)</u>	~\$50	相对简单易用，价格便宜	仅能支持单广播信道监听（硬件限制），使用私有分析软件，抓包结果难以导出，偶尔丢包和崩溃
<u>Nordic nRF Sniffer (nRF51 PCA10031 USB dongle)</u>	~\$50	价格便宜，使用Nordic nRFSniffer软件和Wireshark集成（仅Win平台）	仅能支持单广播信道监听（硬件限制），偶尔丢包，配置步骤较复杂
<u>Adafruit Bluefruit LE Sniffer</u>	~\$30	价格便宜，使用Nordic nRFSniffer软件和Wireshark集成（仅Win平台）	仅能支持单广播信道监听（硬件限制），偶尔丢包，配置步骤较复杂
<u>Ubertooth One</u>	~\$120	开源软硬件	仅能支持单广播信道监听（硬件限制），仅Linux支持完善
<u>Ellisys Bluetooth Explorer 400-STD-LE</u>	~\$30,000	基于SDR，设备固件可升级以支持新版本蓝牙协议	太贵

以上表格数据最后更新：2017.3



不同硬件方案比较

	Ubertooth	HackRF	BladeRF	nRF51822
工作频率	2.4G	10 MHz - 6GHz	300 MHz - 3.8GHz	BLE 2.4G
工作方式	半双工	半双工	全双工	半双工
接口	USB 2.0	USB 2.0	USB 3.0	USB 2.0
应用范围	蓝牙	SDR	SDR	蓝牙BLE
开源资源	全开源	全开源	部分	部分
价格	1000	2000	2800	100



广义无线网络安全实战——软件 定义无线电 (SDR)

中国传媒大学



知法守法

• 中华人民共和国无线电管理条例

第十四条 使用无线电频率应当取得许可，但下列频率除外：

- (一) 业余无线电台、公众对讲机、制式无线电台使用的频率；
- (二) 国际安全与遇险系统，用于航空、水上移动业务和无线电导航业务的国际固定频率；
- (三) 国家无线电管理机构规定的微功率短距离无线电发射设备使用的频率。

第十五条 取得无线电频率使用许可，应当符合下列条件：

- (一) 所申请的无线电频率符合无线电频率划分和使用规定，有明确具体的用途；
- (二) 使用无线电频率的技术方案可行；
- (三) 有相应的专业技术人员；
- (四) 对依法使用的其他无线电频率不会产生有害干扰。



软件定义无线电

- Software Defined Radio
 - 基于通用的硬件平台上用软件来实现各种通信模块
- 推荐阅读 《HackRF与GnuRadio入门指南》



低价硬件解决方案

- RTL2832U
- HackRF
- bladeRF
- USRP
- LimeSDR



HackRF vs. bladeRF vs. USRP

2013年数据所制表格

	HackRF	bladeRF		USRP		
		x40	x115	B100 Starter	B200	B210
Radio Spectrum	30 MHz – 6 GHz	300 MHz – 3.8 GHz		50 MHz – 2.2 GHz [1]	50MHz – 6 GHz	
Bandwidth	20 MHz	28 MHz		16 MHz [2]	61.44 MHz [3]	
Duplex	Half	Full		Full	Full	2x2 MIMO
Sample Size (ADC/DAC)	8 bit	12 bit		12 bit / 14 bit	12 bit	
Sample Rate (ADC/DAC)	20 Msps	40 Msps		64 Msps / 128 Msps	61.44 Msps	
Interface (Speed)	USB 2 HS (480 megabit)	USB 3 (5 gigabit)		USB 2 HS (480 megabit)	USB 3 (5 gigabit)	
FPGA Logic Elements	[4]	40k	115k	25k	75k	150k
Microcontroller	LPC43XX	Cypress FX3		Cypress FX2	Cypress FX3	
Open Source	Everything	HDL + Code Schematics		HDL + Code Schematics	Host Code [5]	
Availability	January 2014	Now		Now	Now	
Cost	\$300 [6]	\$420	\$650	\$675	\$675	\$1100

[1] – Separate daughterboards are required to receive/transmit. The WBX transceiver is included in this kit

[2] – Half this if 16 bit samples are used

[3] – 56 MHz for single half duplex channel, 30.72 MHz per channel full duplex

[4] – There is a CPLD on the board, but no FPGA

[5] – Ettus confirmed that the HDL + Code + Schematics will be released for the B210/B200

[6] - Estimated retail price, cheaper though Kickstarter



RTL 电视棒、 HackRF、 BladeRF、 USRP、 LimeSDR 参数对比表

	HackRF One	Ettus B200	Ettus B210	BladeRF x40	RTL-SDR	LimeSDR
Frequency Range	1MHz-6GHz	70MHz-6GHz	70MHz-6GHz	300MHz-3.8GHz	22MHz-2.2GHz	100kHz-3.8GHz
RF Bandwidth	20MHz	61.44MHz	61.44MHz	40MHz	3.2MHz	61.44MHz
Sample Depth	8 bits	12 bits	12 bits	12 bits	8 bits	12 bits
Sample Rate	20MSPS	61.44MSPS	61.44MSPS	40MSPS	3.2MSPS	61.44MSPS (Limited by USB 3.0 data rate)
Transmitter Channels	1	1	2	1	0	2
Receivers	1	1	2	1	1	2
Duplex	Half	Full	Full	Full	N/A	Full
Interface	USB 2.0	USB 3.0	USB 3.0	USB 3.0	USB 2.0	USB 3.0
Programmable Logic Gates	64 macrocell CPLD	75k	100k	40k (115k avail)	N/A	40k
Chipset	MAX5864, MAX2837, RFFC5072	AD9364	AD9361	LMS6002M	RTL2832U	LMS7002M
Open Source	Full	Schematic, Firmware	Schematic, Firmware	Schematic, Firmware	No	Full
Oscillator Precision	+/-20ppm	+/-2ppm	+/-2ppm	+/-1ppm	?	+/-1ppm initial, +/-4ppm stable
Transmit Power	-10dBm+ (15dBm @ 2.4GHz)	10dBm+	10dBm+	6dBm	N/A	0 to 10dBm (depending on frequency)
Price	\$299	\$686	\$1,119	\$420 (\$650)	~\$10	\$299 (\$199 early bird)



一些实战案例

- K. Wang, S. Chen, and A. Pan, “Time and position spoofing with open source projects,” Black Hat Europe, vol. 148, 2015. [ppt white paper](#)

hackrf unlock

大约 484 条结果

Unlocking cars with hackrf
Osama Eshmili · 4.5万次观看 · 1年前
Unlocking cars using Hackrf + GNURadio...

HackRF Replay Attack on Jeep Patriot
Caleb Madrigal · 1.8万次观看 · 1年前
This is me demoing a replay attack on my Jeep Patriot's keyless entry system. Here's a little tutorial: ...

SDR Unlocking cars with HackRF One
Nosferatu Hacking · 4,000次观看 · 10 个月前
Apertura y desactivacion de sistemas de alarmas vehiculares usando el HackRF ONE.

Unlocking car with RF sniffer
Radoslav Gerganov · 2,800次观看 · 7 个月前

Hacking car remote control with hackRF

hackrf tesla

HackRF vs. Tesla Model S
CFSworks · 1.6万次观看 · 2年前
As it turns out, Tesla's "open charge port" signal (as used by their various charge cables) can be replayed quite easily. :)

HackRF As a Spectrum Analyzer | Finding My Cellphone Signal
Corrosive · 1,500次观看 · 1 个月前
Using HackRF Sweep to find my cellphone transmission. Driver Installation Tutorial ...

HackRF + PortaPack OOK transmit (PT2262, HK526E, HT12E encoders...)
furrtrek · 6,000次观看 · 11 个月前
New module for HAVOC :) <https://github.com/furrtrek/portapack-havoc>.

HackRF One optional RF shield Installation
Cameron Conover · 1.2万次观看 · 2年前
I bought the HackRF One shield and component kit from NooElec here: ...

Controlling an RC car using GNU Radio and HackRF
Orinoco Labs · 1,900次观看 · 6 个月前

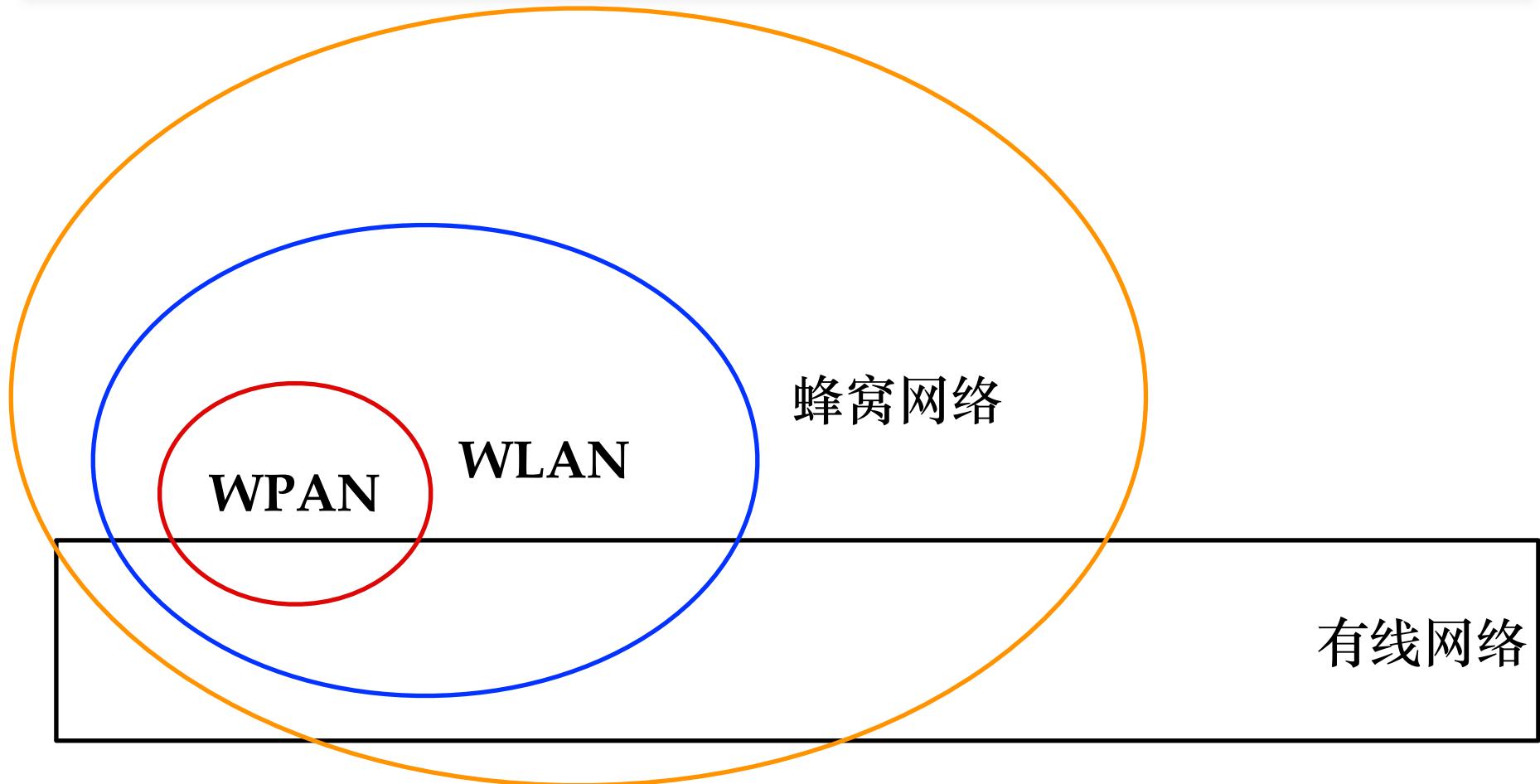


无线网络安全小结

中国传媒大学



可移动的数据网络





无线网络主要威胁与风险

- Data Interception
- DoS
- Rogue APs
- Wireless Intruders
- Misconfigured APs
- Ad Hoc and soft APs
- Evil Twin APs
- Wireless Phishing
- Endpoint Attacks
- Misbehaving Clients



无线网络安全加固——蜂窝通信

- 尽快升级你的移动通信网络制式到4G
- 不要依赖2G网络的短信传送机密信息
- 服务提供商要正确的实现验证码短信功能
 - 不要在短信中同时出现完整帐号和验证码
 - 验证码有效周期尽可能短，建议重要验证码1分钟过期
- 遇到疑似伪造来源号码的电话和短信，回拨可验证真伪
 - 更换另一个手机号、固定电话，逐个号码输入方式回拨



无线网络安全加固——蓝牙

- 默认不启用设备的蓝牙功能，除非需要用到
- 尽可能使用最低等级的蓝牙默认功耗，限制蓝牙传输距离
- 关闭蓝牙的“可被发现”能力
- 使用动态、健壮的PIN码
- 尽可能使用高版本的蓝牙协议支持设备
- 关闭不需要的蓝牙功能
- 建议开启蓝牙配对设备的双向认证功能



无线网络安全加固——RFID

- 给你口袋/钱包里的RFID卡增加一个RFID屏蔽卡套，防止近距离复制
- 避免使用Mfiare Classic芯片卡，而采用更强加密算法的芯片卡，比如CPU卡
- 涉及金额等敏感数据应进行加密处理，禁止明文存储
- 读卡器与后端主机数据库实行线上作业，采用即时连线的方式进行系统核查
- 结合uid进行加密，并设置uid白名单，提高攻击者破解成本，但可能被特殊卡绕过
- 对全扇区采用非默认密码加密，提高破解成本，但可能通过DarkSide方式暴力破解



参考资料

- Dan Veeneman, Vulnerabilities of Cellular and Satellite-based Voice and Data Networks, Blackhat 2002 USA.
- <http://seclists.org/fulldisclosure/2011/Aug/76>
- <http://wulujia.com/2013/11/10/OsmocomBB-Guide/>
- [Cloning 3G/4G SIM Cards with a PC and an Oscilloscope: Lessons Learned in Physical Security presented on Blackhat USA 2015](#)
- [THE NSA HAS HACKED YOUR PHONE: WHAT YOU NEED TO KNOW, AND HOW TO PROTECT YOURSELF](#)
2015.02.25
- [SIM 卡制造商金雅拓遭黑 嫌疑人是美英情报机构](#) 2015.02.27



参考资料

- Smart Card Basics
- Smart Card Technology and Security
- Smart Cards: How Secure Are They? 2002.3.1 from SANS Institute
- A Review of Smartcard Security Issues 2011.
- 如何通过劫持的无线鼠标或键盘入侵100米内的一台计算机 2016.2 from 传媒信安
- Proxmark/proxmark3 on GitHub



参考资料

- <http://www.cellcrypt.com/gsm-cracking>
- 创见WiFi SD卡破解之路 2014-03-17 from FreeBuf
- 中国教授在BlackHat现场演示破解SIM卡AES-128加密 2015-08-07 from FreeBuf
- <https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf>
- 用临时身份证补卡成电信诈骗新招 2016.5.18 from 京华时报
- [极客有意思]人人都爱免费洗衣 2013.08.23 from FreeBuf



参考资料

- 逆向路由器固件之动态调试 2016.9.20
- 详细的路由器漏洞分析环境搭建教程
2016.08.24 from 看雪学院