移动互联网安全

第四章 移动通信与物联网安全综述

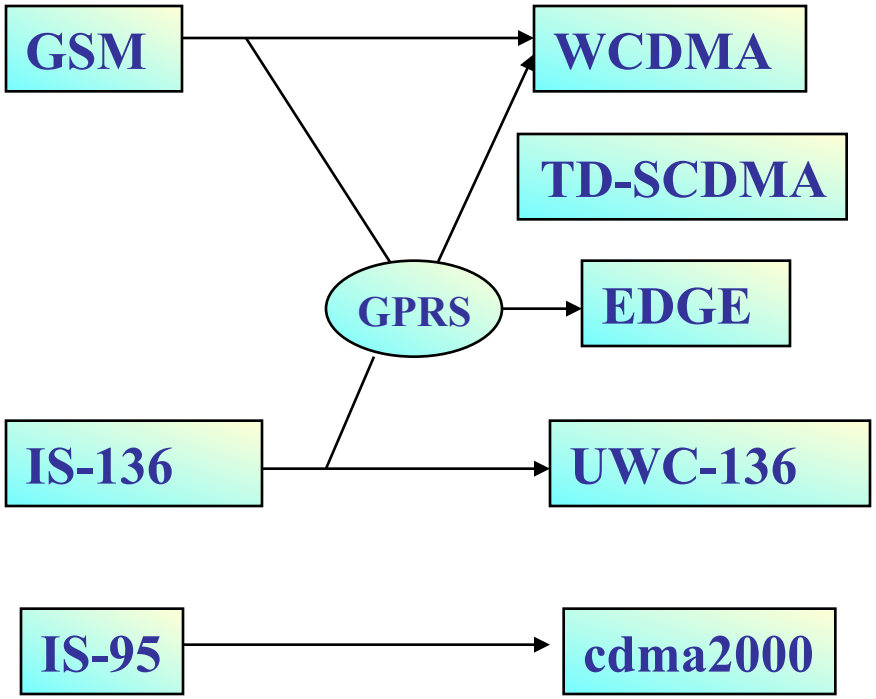
黄 玮

内容提纲

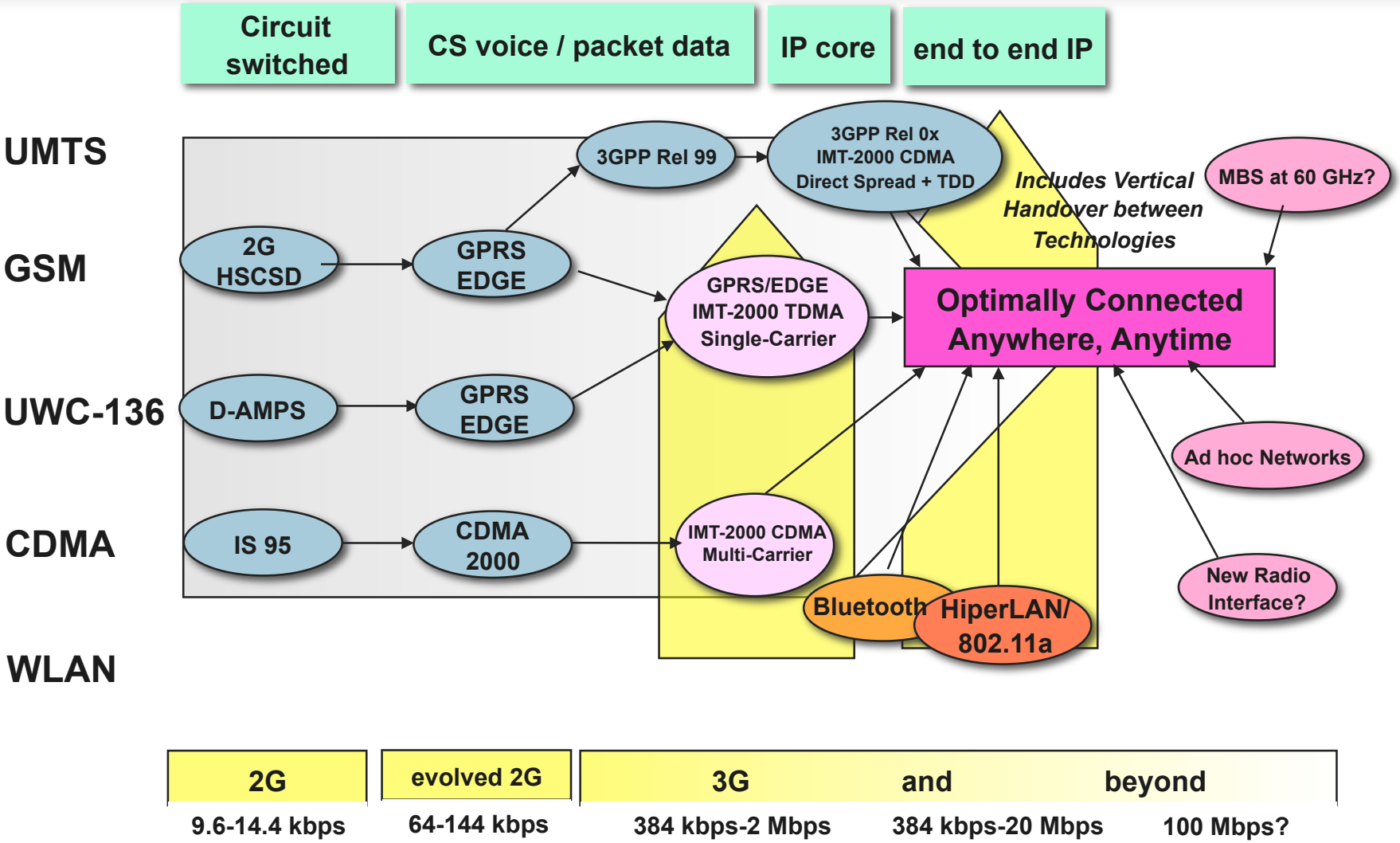
- 2G / 2.5G
- 3G / 4G / 5G
- 物联网安全
- “智能”硬件

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


Circuit switched
CS voice / packet data
IP core
end to end IP
UMTS
GSM
UWC-136
CDMA
WLAN
3GPP Rel 99
3GPP Rel 0x
IMT-2000 CDMA
Direct Spread + TDD
Includes Vertical Handover between Technologies
MBS at 60 GHz?
2G HSCSD
GPRS EDGE
GPRS/EDGE
IMT-2000 TDMA
Single-Carrier
Optimally Connected Anywhere, Anytime
D-AMPS
GPRS EDGE
Ad hoc Networks
IS 95
CDMA 2000
IMT-2000 CDMA
Multi-Carrier
New Radio Interface?
Bluetooth
HiperLAN/ 802.11a
2G
evolved 2G
3G
and
beyond
9.6-14.4 kbps
64-144 kbps
384 kbps-2 Mbps
384 kbps-20 Mbps
100 Mbps?

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

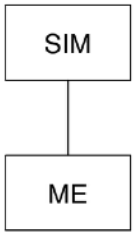
- MS (Mobile Station) 移动终端，例如手机
- MSC (Mobile Switching Center) 移动交换中心，移动网络完成呼叫连接、过区切换控制、无线信道管理等功能的设备，同时也是移动网与公用电话交换网(PSTN)、综合业务数字网(ISDN)等固定网的接口设备
- IMSI (International Mobile Subscriber Identity) 跨国移动用户标识，是TD系统分给用户的唯一标识号，它存储在SIM卡、HLR/VLR中，最多由15个数字组成
- IMEI (International Mobile Equipment Identity) 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

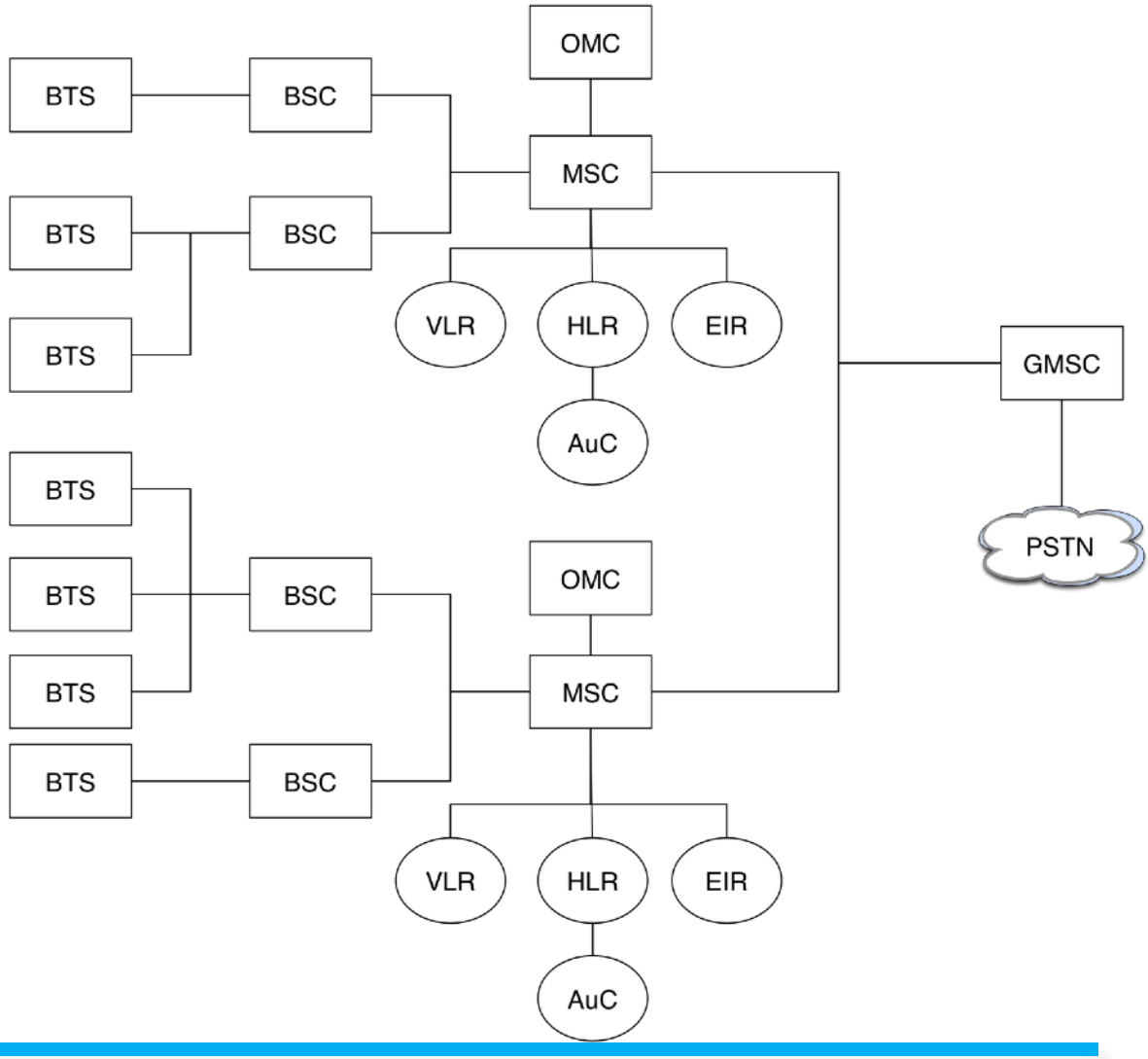
GSM网络概述

- 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

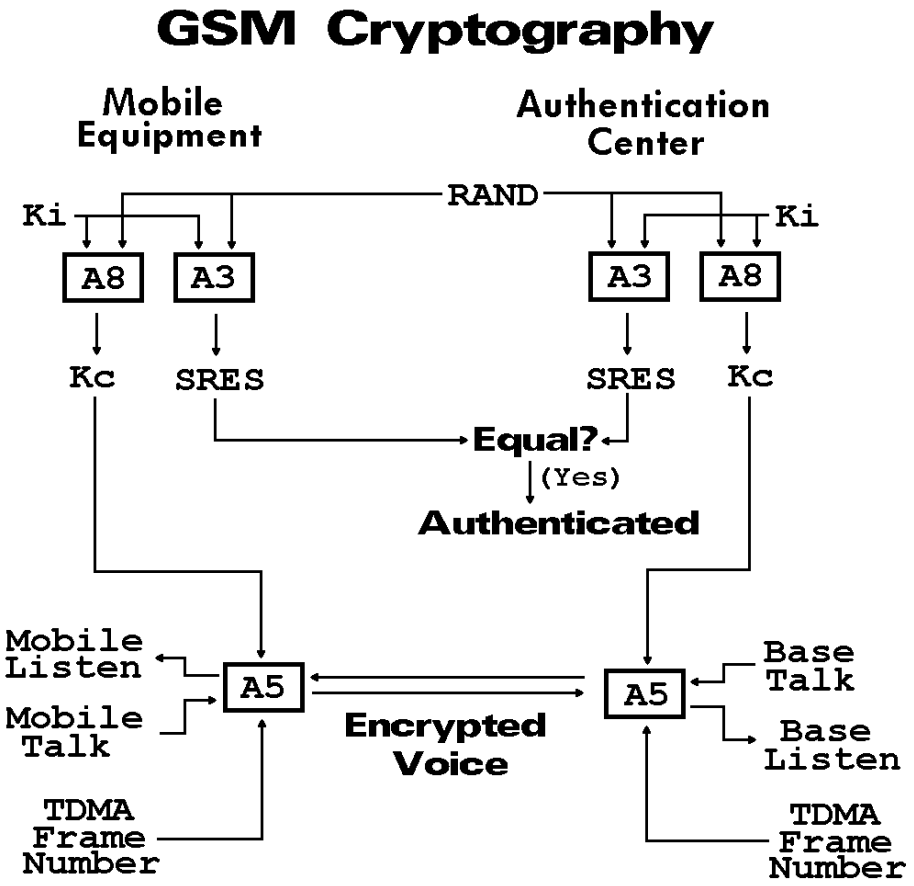
- Ki用于A3、A8的用户认证密钥
  - 与HLR共享，128bit的秘密数据
- A3为认证算法，单向散列函数
  - 对于HLR的询问产生32bit响应SRES
  - SRES=A3(Ki, RAND)
- A5是分组加密算法，会话秘钥Kc的长度为64bit
- A8为生成Kc的单向散列函数
  - Kc=A8(Ki, RAND)

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

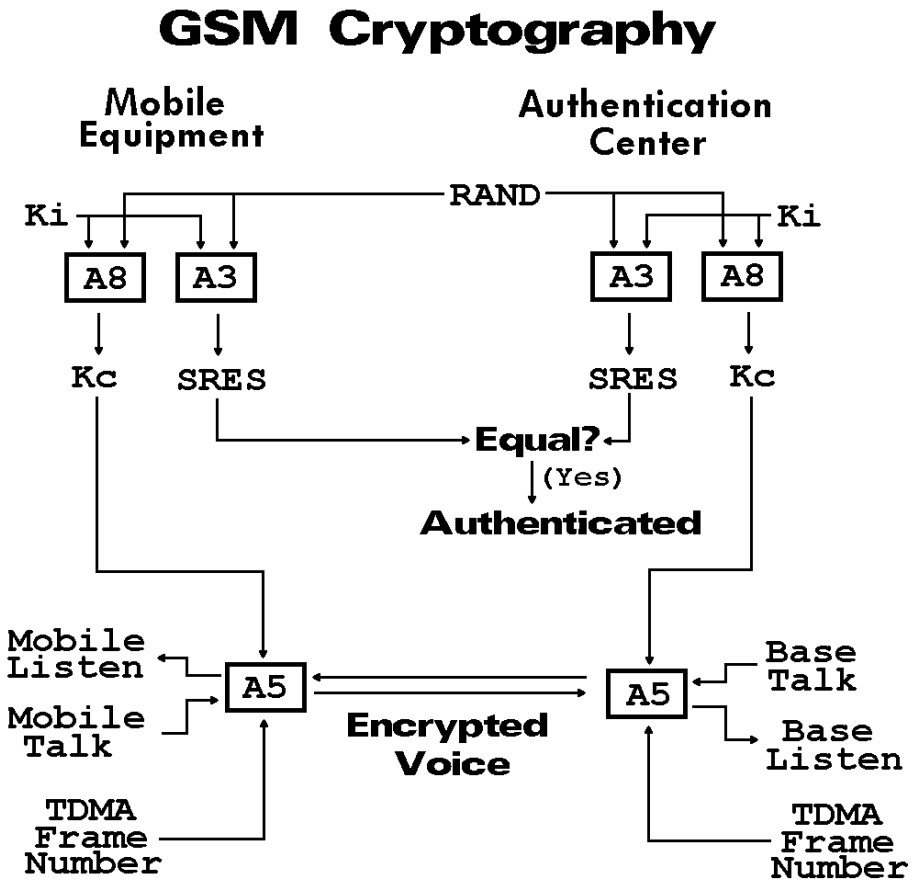
GSM安全机制——认证

- 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

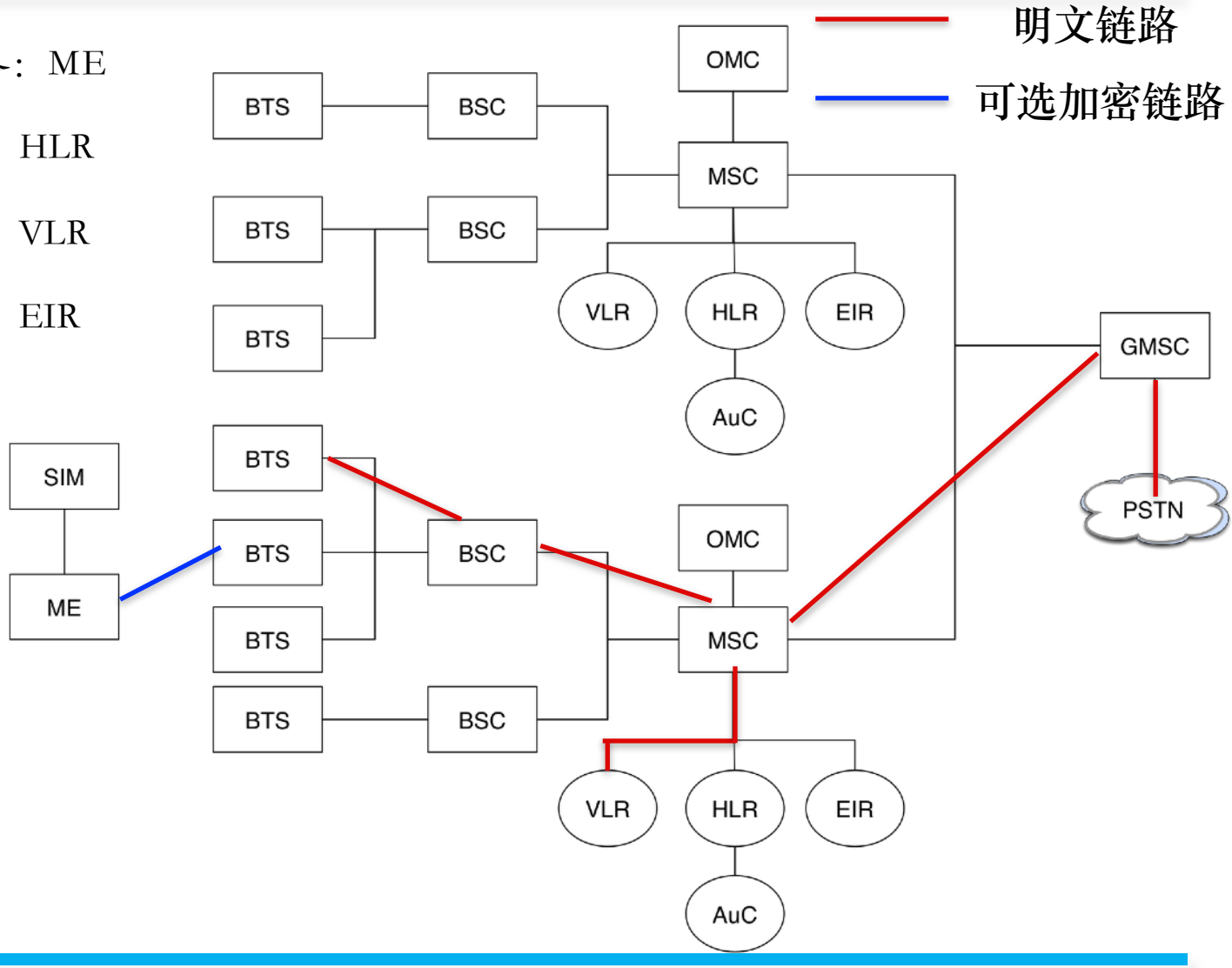
- COMP-128 算法会泄漏 Ki (1998.4)
- A8的有效密钥长度只有54 bits（最后10位全0)
- A5
  - 缺乏数据完整性验证机制
  - A5/1 (欧洲标准)
  - A5/2 (北美标准)
  - A5/0 (不加密，比如我国)

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

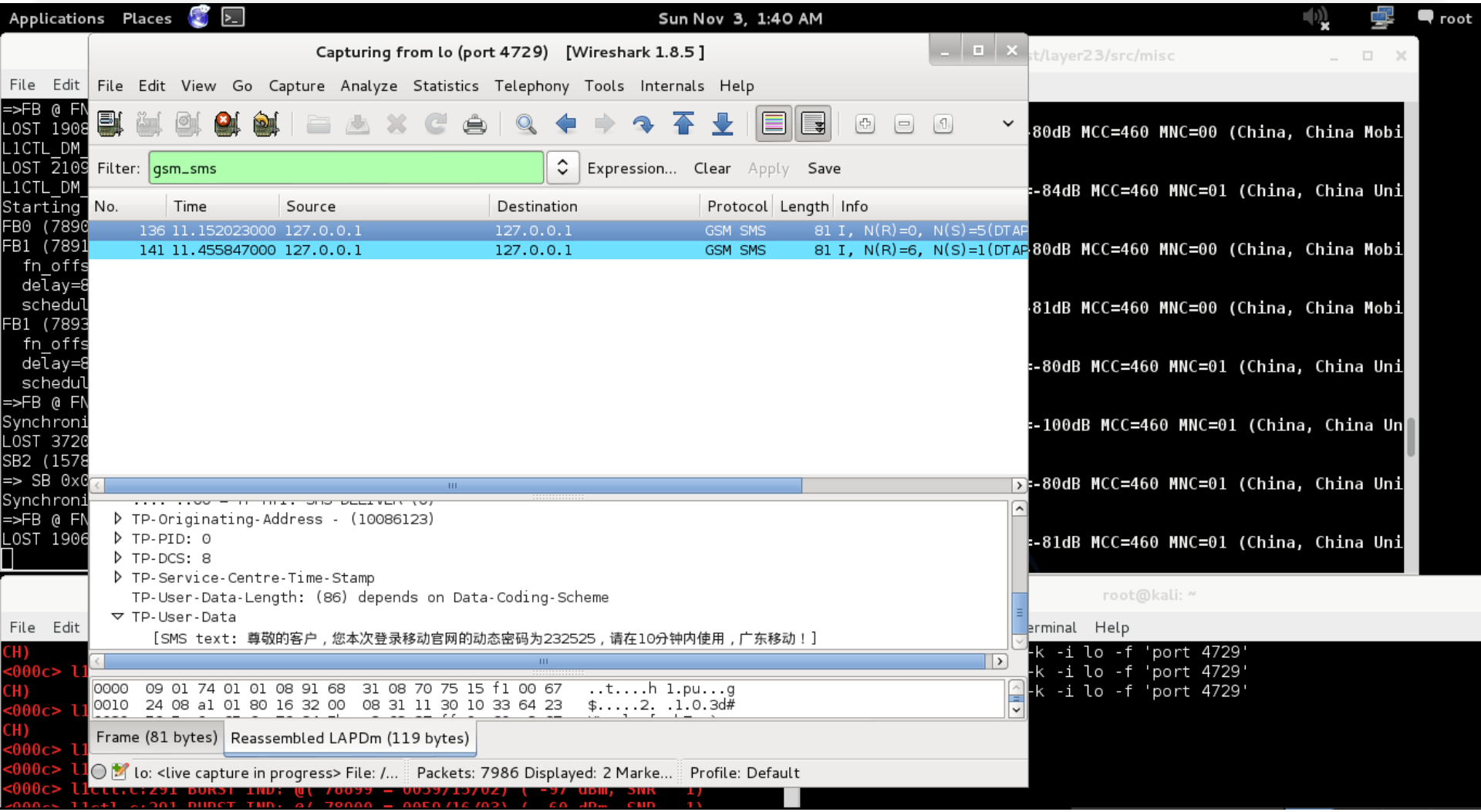
- 带有SIM卡的移动设备：ME
- 归属位置登记数据库：HLR
- 访问位置登记数据库：VLR
- 设备标识注册数据库：EIR
- 基站收发信台：BTS
- 基站控制器：BSC
- 移动交换中心：MSC
- 认证中心：AuC
- 运营管理中心：OMC
- 有线固话网络：PSTN



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



真实世界中的GSM威胁——伪基站

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

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

ref: http://www.zhihu.com/question/19821864

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）

https://zh.wikipedia.org/wiki/物联网

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

https://zh.wikipedia.org/wiki/物联网

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
- 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

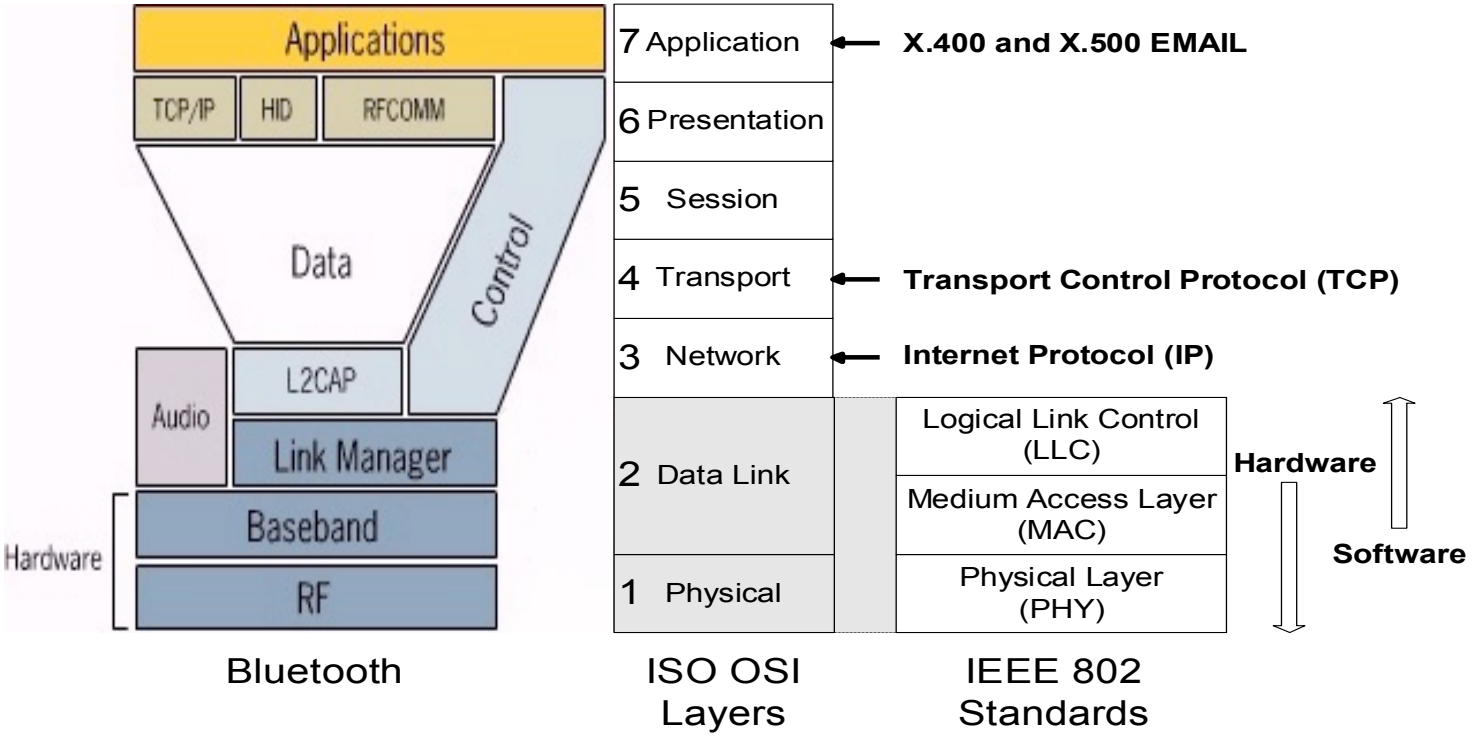
蓝牙概述

- 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

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

Bluetooth and IEEE Structure



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	*1～100*米	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
- 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

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
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 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)

ref: http://en.wikipedia.org/wiki/Near_field_communication

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

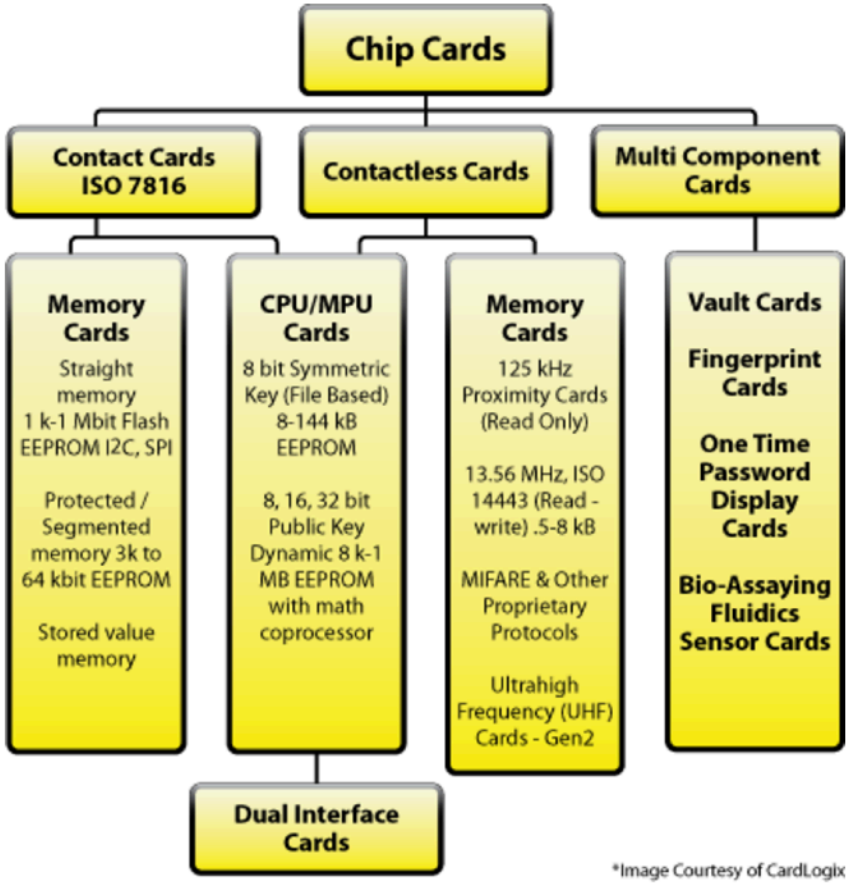
- CRT显示器行场信息还原
  - 一个抛物面天线,一台电视机
  - 数百米到数公里
- 普通键盘和鼠标的电磁泄露问题

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



http://www.smartcardbasics.com/smart-card-types.html

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

  —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

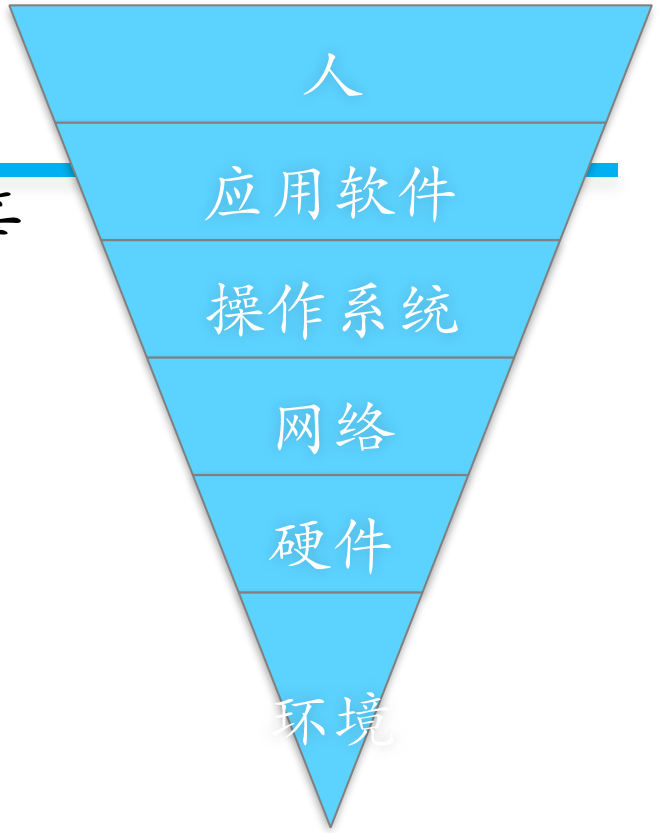
- 多功能卡
  - 内置操作系统
    - Windows for Smart Cards, MULTOS, Java Card
  - 支持灵活丰富的应用场景

智能卡风险

- 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

https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf

智能卡威胁建模



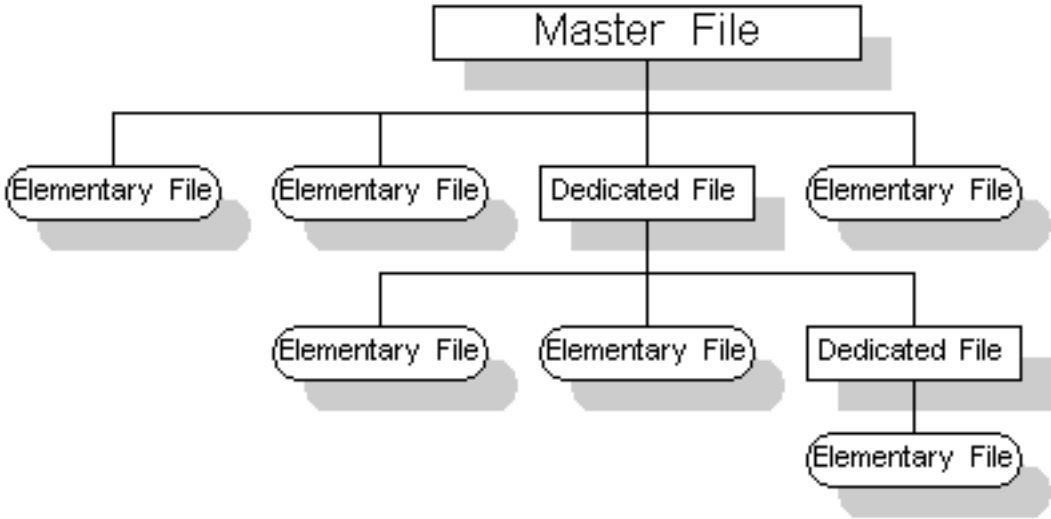
- 人：遗失、外借、设置PIN码等
- 软件：软件设计与实现漏洞
- 操作系统
  - 固定文件系统
  - 动态文件系统
- 网络：明文传输风险，MITM，嗅探器调试
- 硬件：直接读取或破坏（改变电压/温度/酸碱度/电路板重新焊接搭线等）EEPROM
- 环境: 钓鱼风险

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

https://zh.wikipedia.org/wiki/MIFARE

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	Crypot-1	Crypo-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

https://zh.wikipedia.org/wiki/MIFARE

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）
- 奇偶校验位信息混淆
- 仅硬件实现（依赖于硬件化“提升”防逆向能力）

MIFARE的黑历史

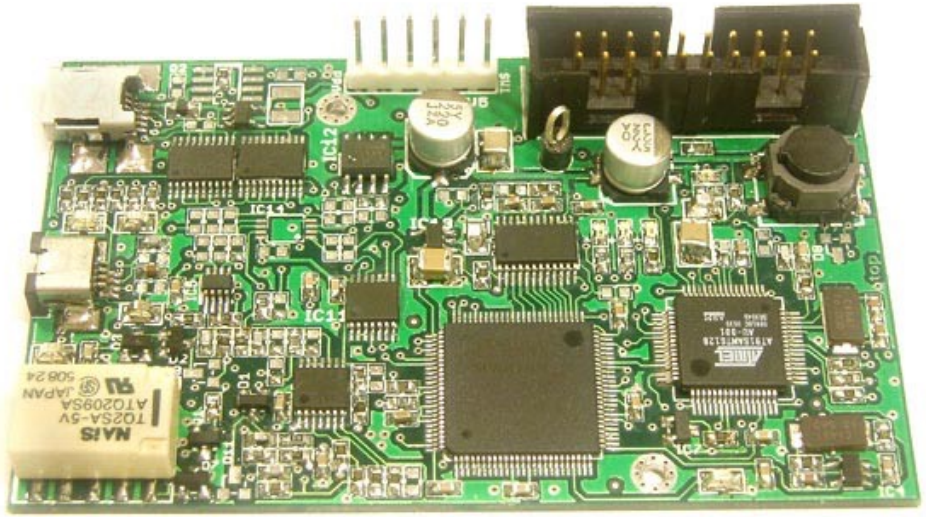
- 2007年12月两个德国人Nohl 和 Plötz在 Chaos Communication Congress上展示了通过Crypto-1的一些缺陷部分逆向了其算法
- 2008年3月来自荷兰Radbond大学的研究者完全逆向了Crypto-1算法并予以公开
  - NXP试图通过法律途径禁止上述公开行为，但在2008年7月被当地法庭以言论自由原因驳回了申诉
- 2008年10月Radbond大学以GNU GPL v2协议开源了Crypto-1算法代码
- 大量针对MIFARE Classic卡的黑客工具被公开

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



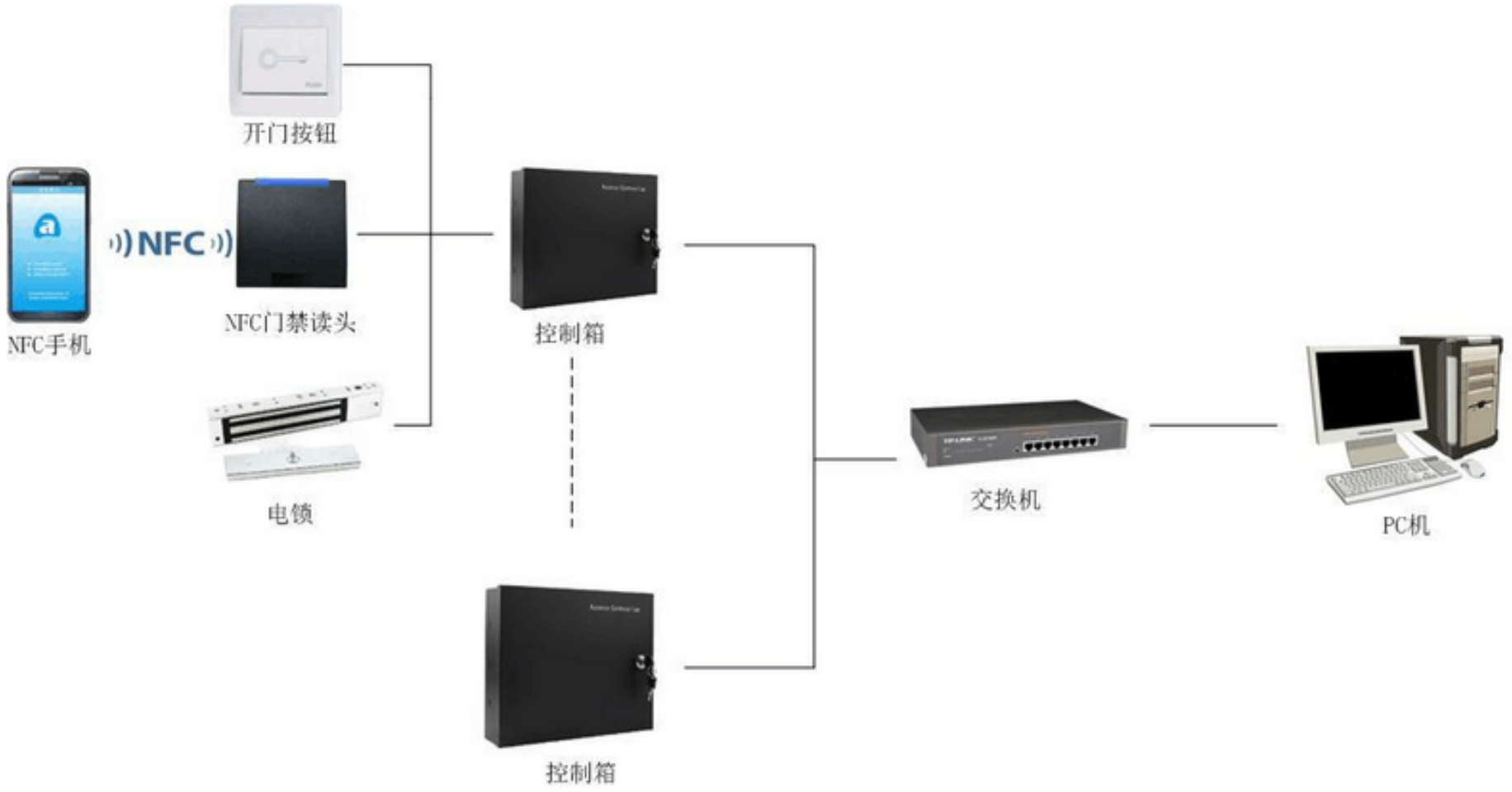
开放式讨论

- 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	• （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	• 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



http://www.freebuf.com/news/topnews/80786.html

“智能”硬件

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

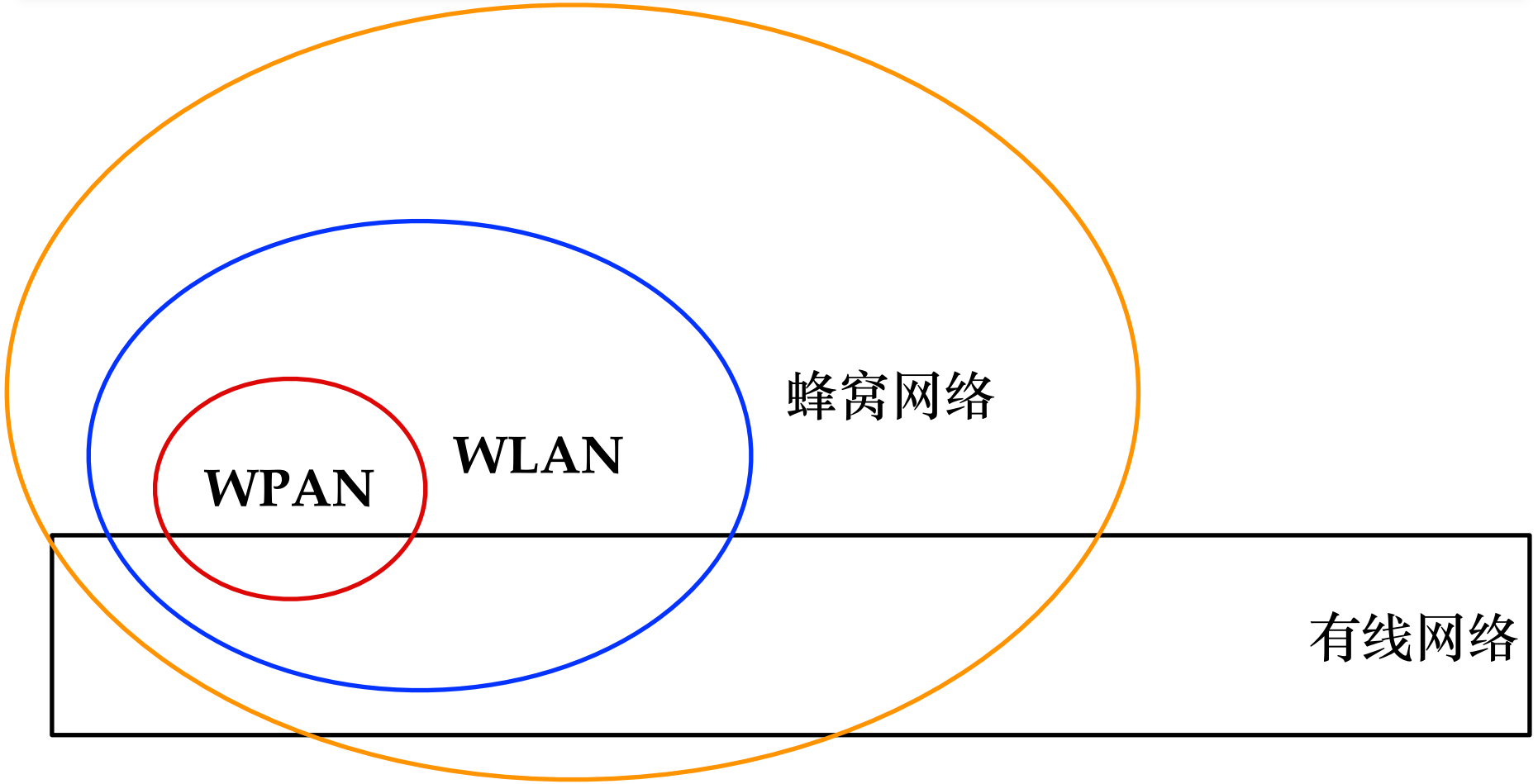
智能路由器安全特性分析 from 腾讯安全应急响应中心 2015

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

无线网络安全小结

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

ref: http//security.tencent.com/index.php/blog/msg/52

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 Sm artcard 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