

课程编号：3182121321

无线通信安全



第一讲 课程介绍及概述

李晖

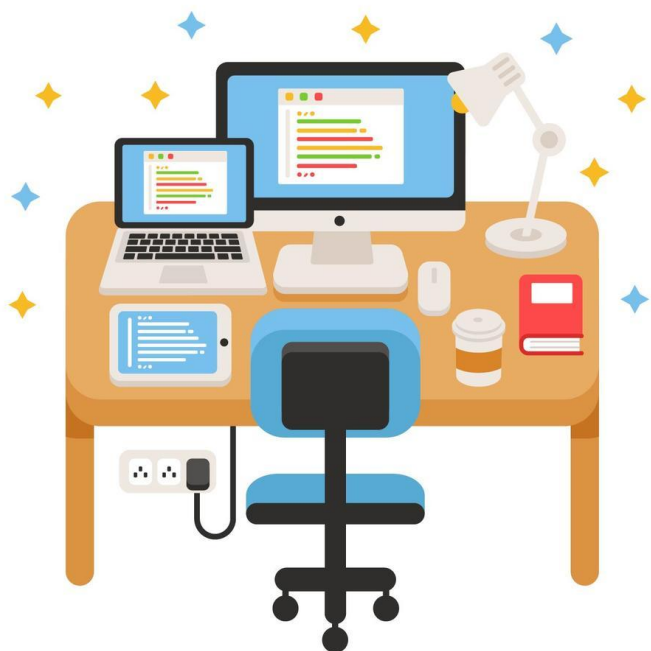
lihuill@bupt.edu.cn

面对面建群



在学习完本讲后，大家能够：

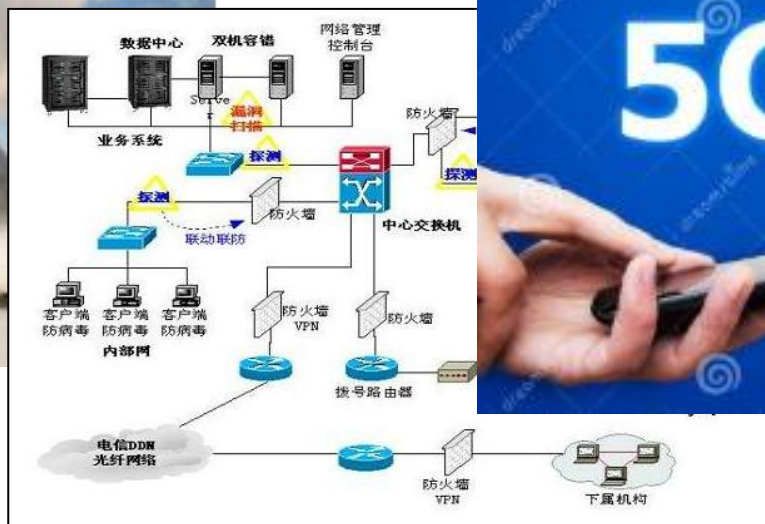
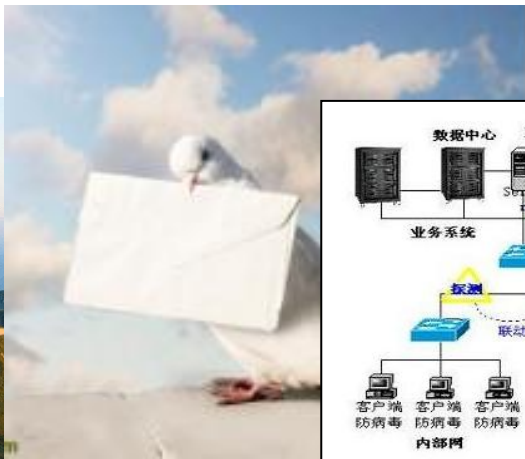
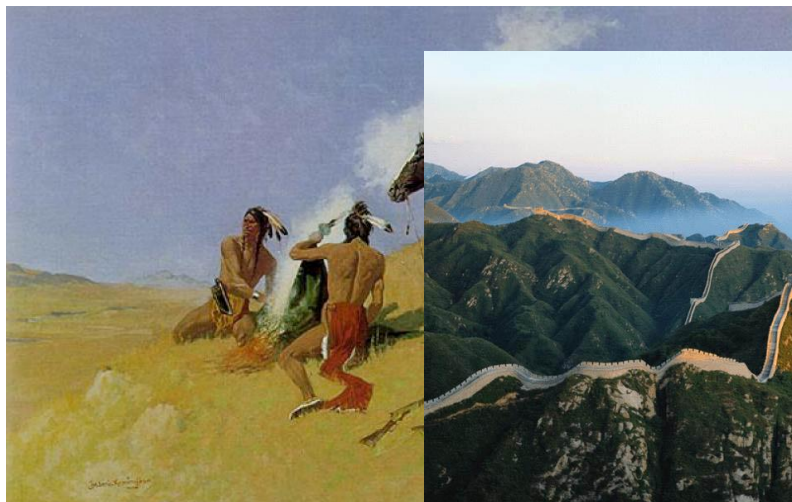
- 了解课程内容
- 了解无线技术的发展历史
- 了解无线技术的分类
- 了解无线安全的发展历史



1. 课程简介
2. 无线技术的发展历史
3. 无线技术的分类
4. 无线安全的发展历史
5. 无线安全事件

1. 课程简介

什么是通信？



- 通信(Communication)，指人与人或人与自然之间通过某种行为或媒介进行的信息交流与传递；
- 特指电信(Telecommunication)，利用“光、电、微波等”来传递消息的通信方法，具有迅速、准确、可靠等特点，且几乎不受时间、地点、空间、距离的限制。

1. 课程简介

- 无线通信(Wireless communication): 利用电磁波信号可以在自由空间中传播的特性进行信息交换的一种通信方式。

无线通信系统

- 集群通信—警察、出租车调度
- 蜂窝移动电话—车载、便携、手持机
- 无线寻呼
- 无绳电话—家用、公共无线接入点
- 卫星移动通信—“铱”、全球星等
- 无线局域网(WLAN)
- 数字微波
- 电视广播、电台广播
- 空间通信
- 物联网、车联网。。。

1. 课程简介

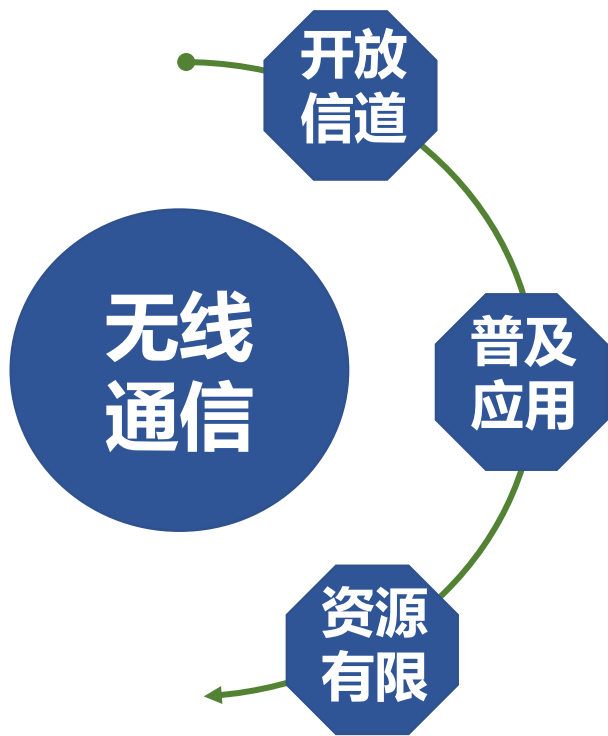
无线通信安全

研究由于使用**无线**传输技术，通信所面临的安全威胁、采用的安全技术及措施。



1. 课程简介

无线通信安全为什么重要？



1. 安全难以保障

导致窃听、假冒身份等多种攻击易于实施

2. 安全攻击增加

移动支付、社交媒体等新应用不断涌现

移动终端/基站/系统成为了新的攻击目

标

3. 安全设计困难

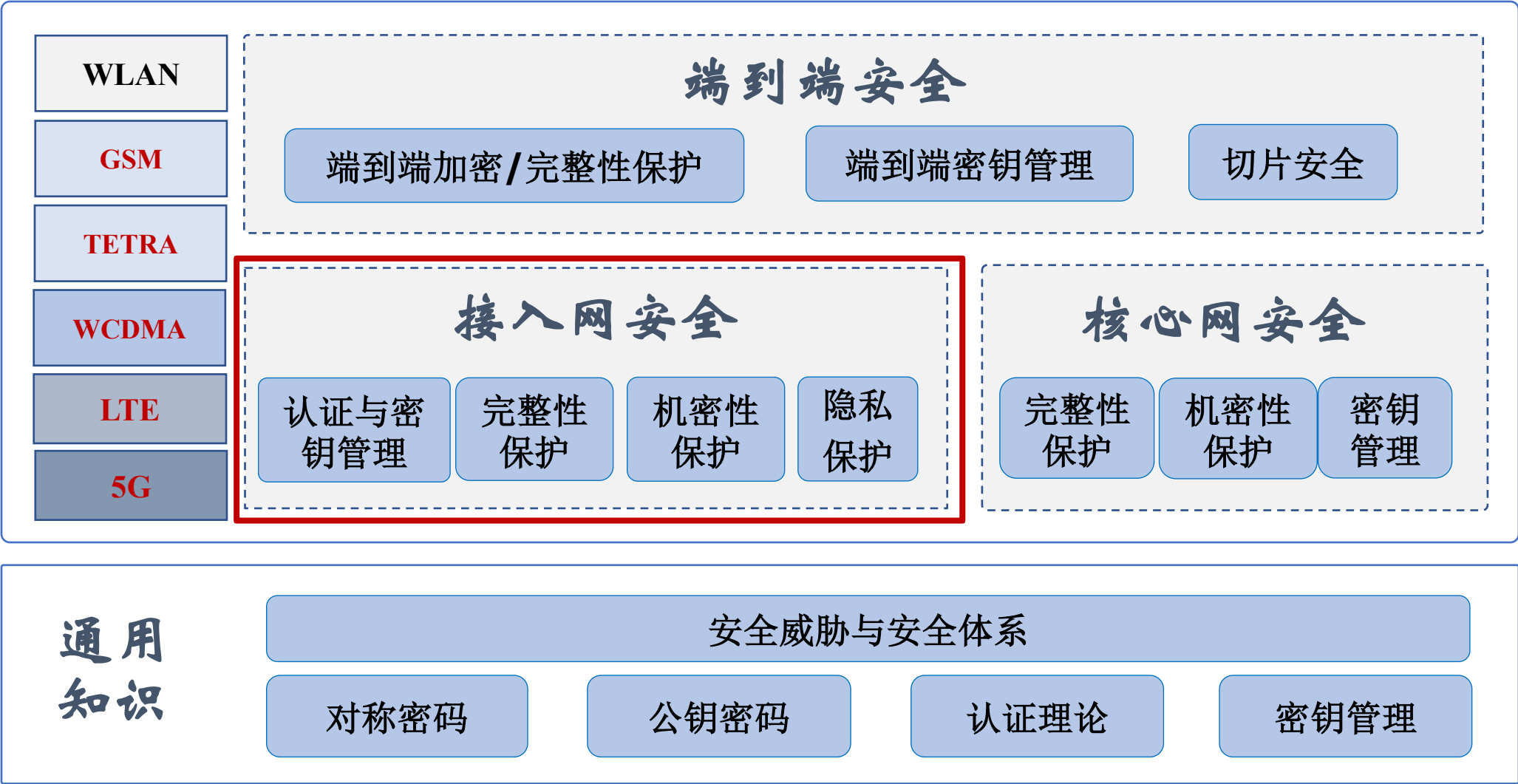
无线终端计算、存储、电池资源有限

空口带宽资源有限

1. 课程简介—课程目标

- **了解无线通信的安全威胁和安全要求**
- **掌握无线通信安全的密码学基础**
- **通过分系统的讲解，掌握构建无线通信网安全的基本措施和技术**
- **注重基本安全技术的讲解的同时，将把学科的最新技术反映到教学中**
- **在论述知识的同时，侧重方法和思路**

1. 课程简介—课程内容



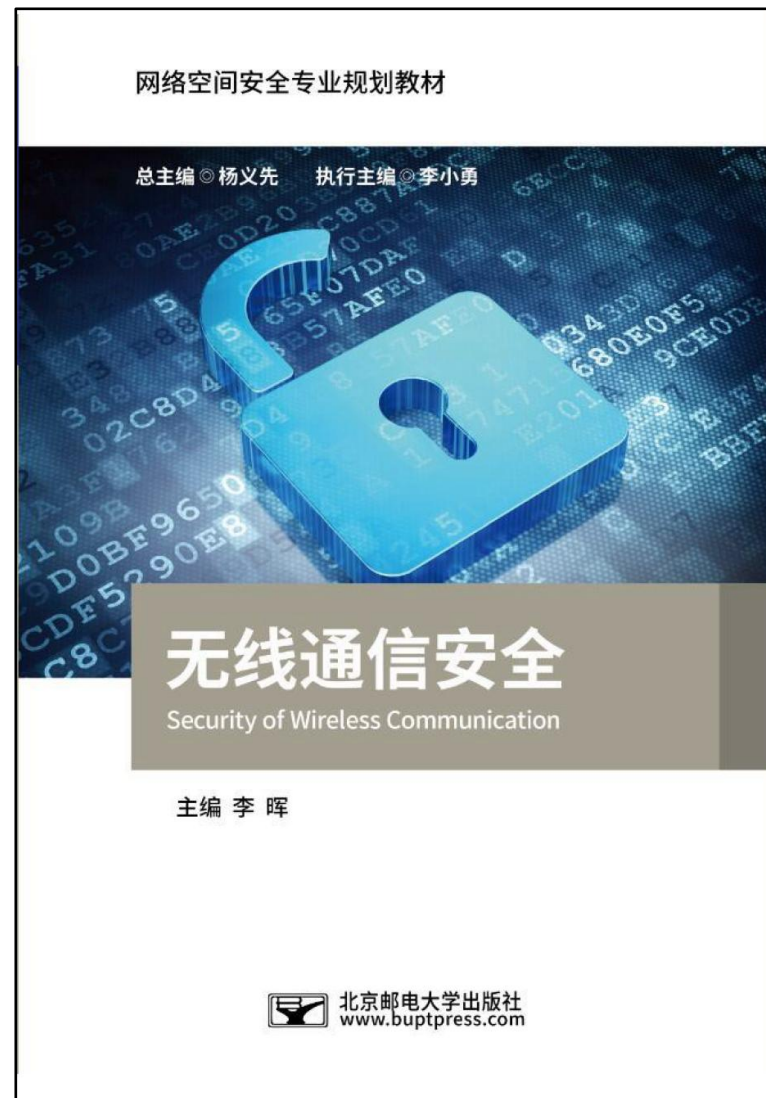
1. 课程简介—课程安排

序号	课时	课程内容
第1讲	2	课程介绍及概述
第2讲	3	密码学基础、认证理论基础
第3讲	1	通信网的安全威胁和安全体系
第4讲	4	WLAN 安全(WEP,WPA2.0)
第5讲	2	GSM 安全 (鉴权、空口加密、匿名)
第6讲	2	数字集群通信 (TETRA)安全
期中总结&考试(预计第8教学周: 4月24日)		

序号	课时	课程内容
第7讲	4	3G 安全(WCDMA 的认证、空口安全等)
第8讲	2	LTE 安全(空口安全、切换密钥管理等)
第9讲 5/29	2	5G 安全概述(安全架构、空口安全、切片安全、安全保障体系等) *华为专家主讲
第10讲	2	5G 安全2: 5G-AKA 协议的分析与改进
第11讲	2	6G 安全愿景+课程总结
第12讲	2	作业讲解+答疑
期末考试(由学校统一安排, 预计第17-18教学周)		

1. 课程简介—教材信息

- 教材：李晖，北京邮电大学出版社，2018年
- 补充资料：5G安全（电子讲义）
- 课件：教学云平台



1. 课程简介

主要参考书

- 《现代密码学》，谷利泽等编著
- 《对称密码学及其应用》，李晖等编著
- 《无线网络安全 —— 技术与策略》，金纯等编著
- 《通信网的安全 - - 理论与技术》，王育民等编著
- 《UMTS安全》，Valtteri Niemi, Kaisa Nyberg著，宋美娜等译
- 《无线局域网安全实务----WPA与802.11i》，Jon Edney, William Arbaugh著
- 《无线局域网安全----方法与技术》，马建明、朱建明等编著
- 相关标准
 - 包括**GSM**、**3GPP**、**TETRA**等国际标准

1.课程简介

课程要求

• 总成绩构成:

- 平时成绩 20%
- 期中成绩 30%
- 期末成绩 50%

• 考核方式:

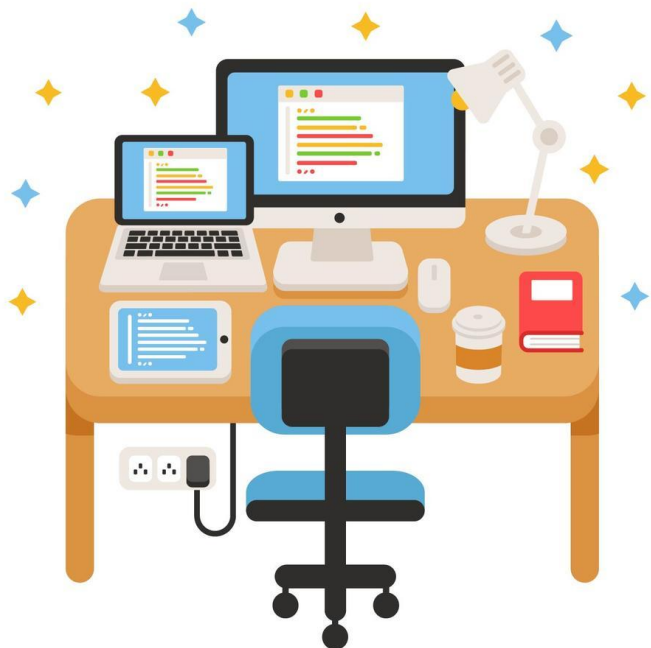
- 平时成绩: 出席情况+作业
- 期中成绩: 开卷考试
- 期末成绩: 开卷考试

• 作业要求:

- 本次留的作业请下次上课之前提交
- 晚提交作业扣分

• 助教:

- 邱国清
- 焦月双
- 黄达威



1. 课程简介
- 2. 无线技术的发展历史**
3. 无线技术的分类
4. 无线安全的发展历史
5. 无线安全事件

无线技术的发展历史

1895年

无线技术起源: Marconi实现无线电报通信, 开启无线通信时代

1978年

出现无线网络: 美国贝尔试验室研制成功高级移动电话系统(AMPS)

1983年

无线网络商用: AMPS (1G) 蜂窝移动通信系统首次商用 (芝加哥)

1991年

成熟无线网络: 1991年商业GSM(芬兰), 1992年实现国际漫游

90年代中期

其他无线网络的出现: 单一数据网络(寻呼/无线局域网/蓝牙等)

90年代后期

无线因特网的兴起: 移动互联网萌芽(成本/体验/安全)

21世纪

多种无线技术并存

21世纪----多种无线技术并存

■ 蜂窝移动通信

- 3G: UMTS/WCDMA、cdma2000、TD-SCDMA
- 4G: LTE(LTE FDD、TD-LTE)
- 5G: 5G NR

■ 宽带无线接入

- WiMAX (IEEE 802.16)

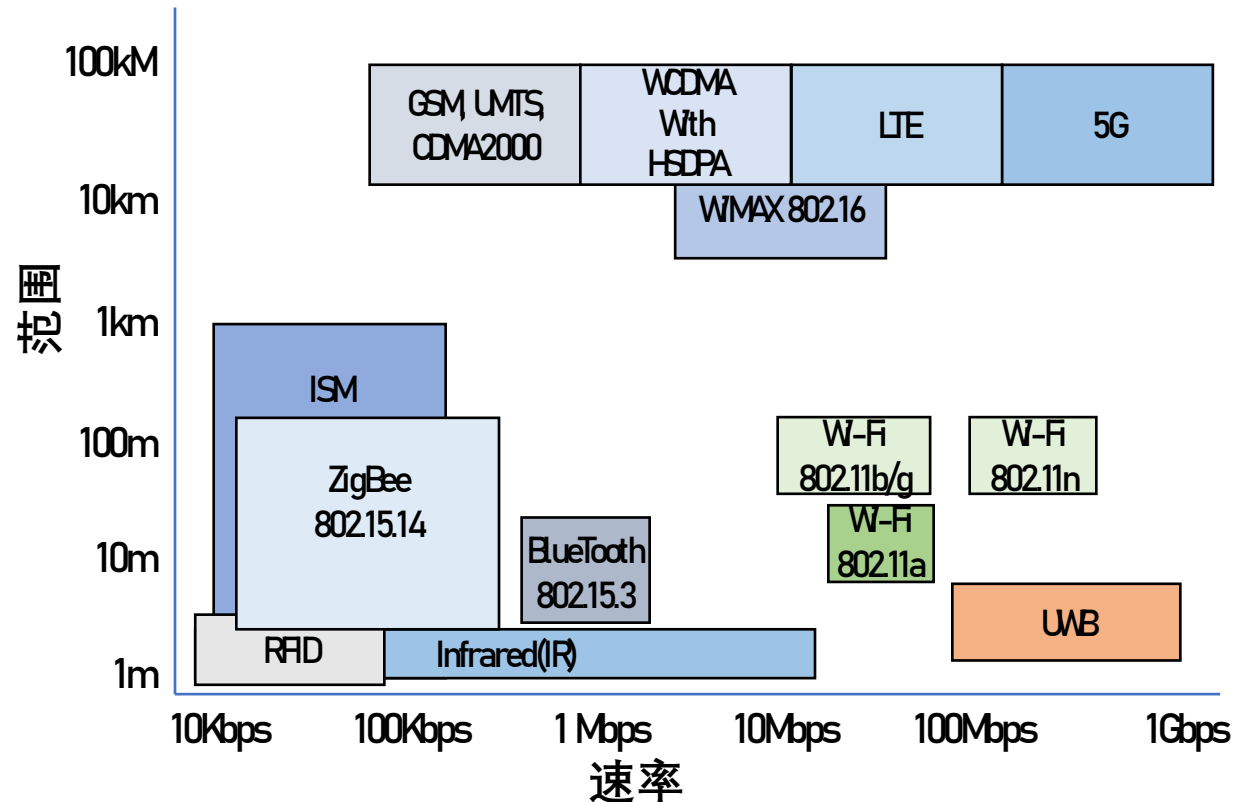
■ 局域无线网络

- WiFi (IEEE 802.11)

■ 短距离无线通信

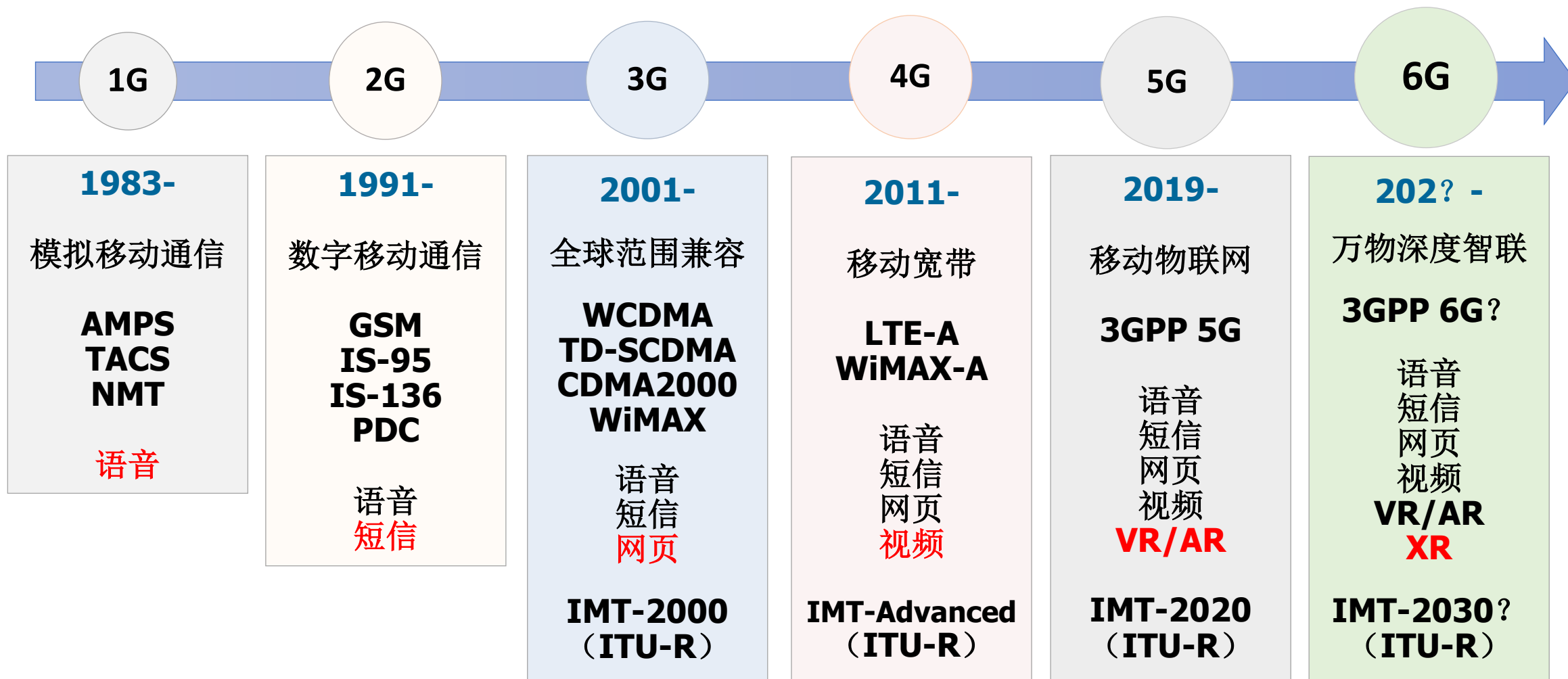
- 超宽带无线接入技术UWB
- Bluetooth
- ZigBee

常用无线通信技术通信范围与速率比较



无线技术的发展历史

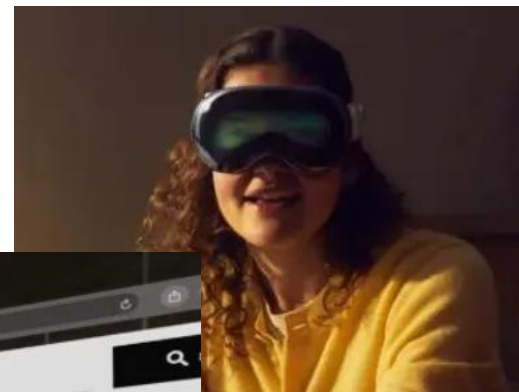
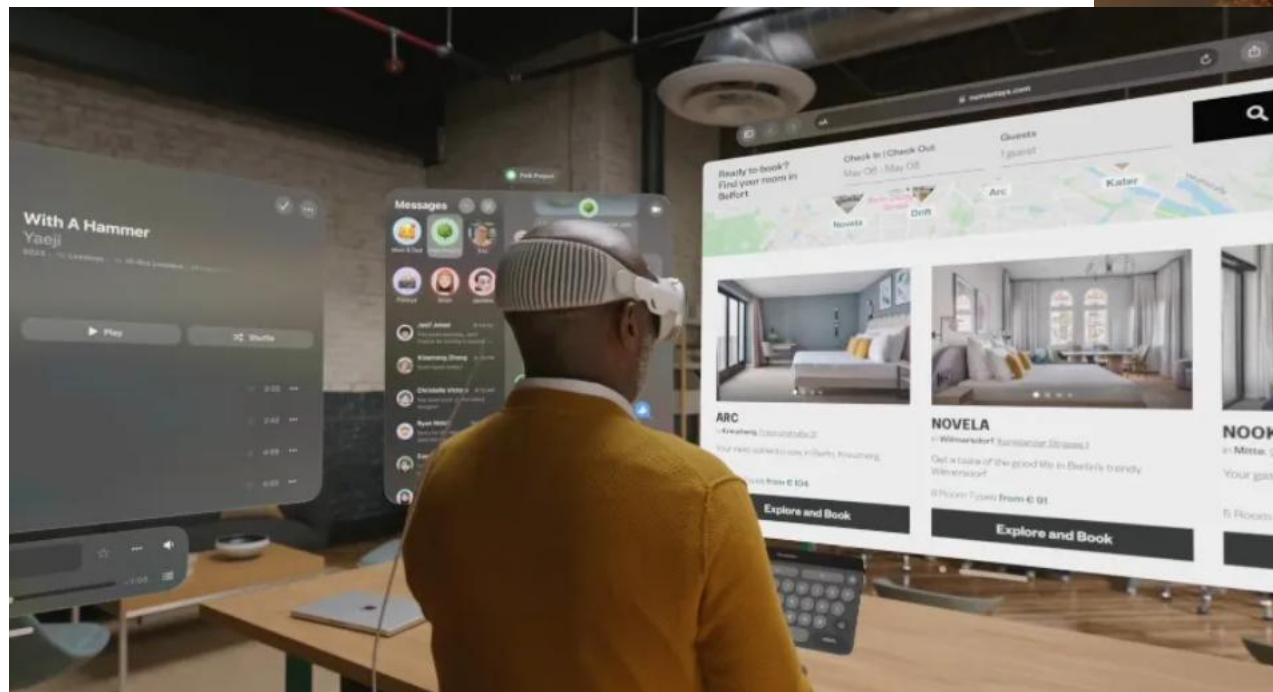
移动无线技术的演进路径

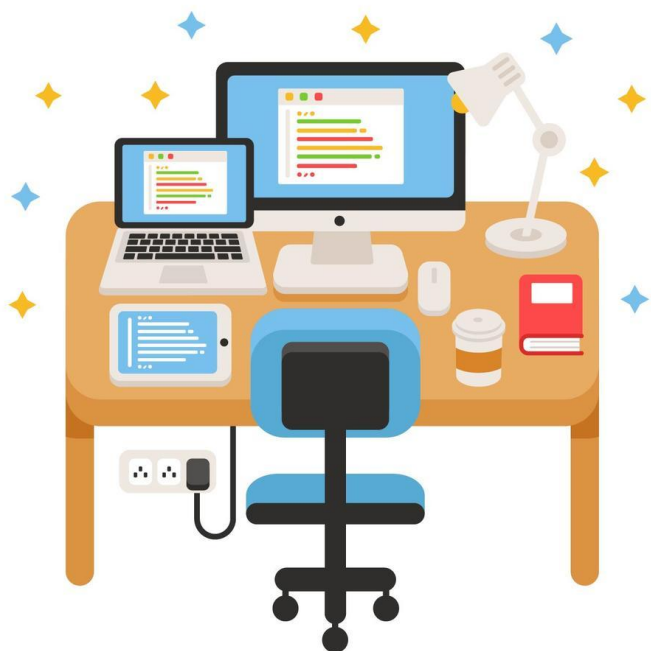


无线技术的发展历史

手机进化史

变的不仅是屏幕





1. 课程简介
2. 无线技术的发展历史
- 3. 无线技术的分类**
4. 无线安全的发展历史
5. 无线安全事件

3. 无线技术的分类

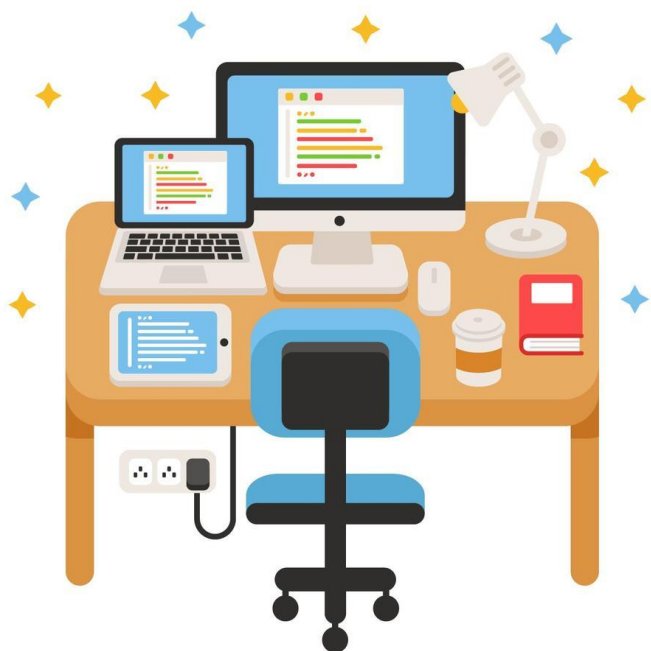
按可移动性分为

■ 无线通信网络

- 无线个域网
- 无线局域网
- WiMAX

■ 移动通信网络（按照使用性质分）

- 公用移动通信
 - GSM, GPRS, 3G
- 专业移动通信
 - TETRA, IDEN
- 特种移动通信



1. 课程简介
2. 无线技术的发展历史
3. 无线技术的分类
- 4. 无线安全的发展历史**
5. 无线安全事件

4. 无线安全的发展历史

无线安全的发展历史

■ 在无线通信发展的最初阶段

- 没有重视无线安全
- 主要事件
 - 军事窃听
 - 模拟移动通信网络中的手机克隆
 - 利用无线电扫描器窃听通话内容
 - 政府机构或运营商滥用特权

4. 无线安全的发展历史

无线威胁

■ 无线威胁

- 窃听无线移动无线信道上的信令或语言信息
- 窃听无线网络上的信用卡授权
- 偷窃蜂窝发射时间
- 窃听无线因特网连接上的电子邮件信箱
- 破坏无人职守基站或其他通信中心的物理安全

■ 无线安全的发展随着人们对于无线安全威胁的认识而发展

4. 无线安全的发展历史

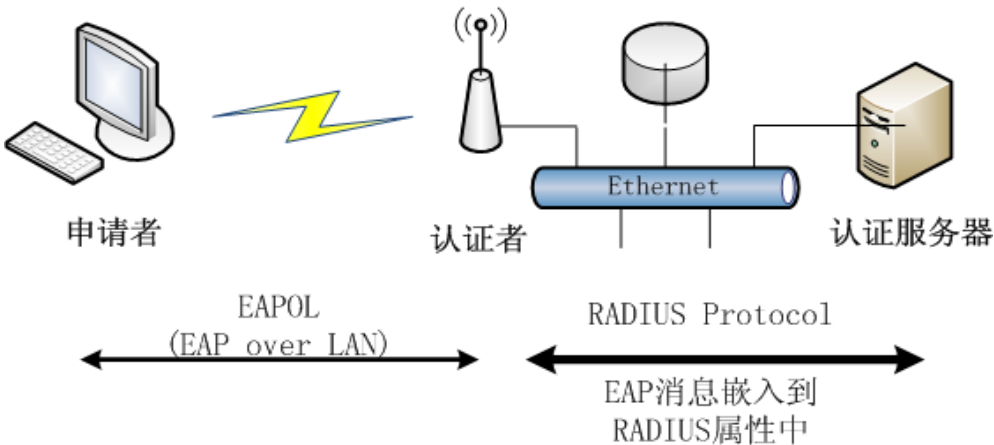
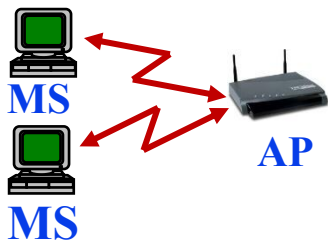
移动通信网络的空口安全历史

- 安全从无到有
- 安全从弱到强
- 安全从简单到复杂



4. 无线安全的发展历史

无线局域网—安全成为关键



802.11

802.1x

WPA

802.11i/WPA2

WPA3

- WEP协议
- 基于共享密钥认证
- 基于RC4算法的机密性保护
- 基于CRC校验码的完整性保护

- EAP协议
- 动态密钥（四步握手协商）

- 预共享密钥认证(WPA 个人)
- 802.1X 服务器认证(WPA 企业)
- 基于128比特RC4流密码
- TKIP（临时密钥完整性协议）
- 使用802.1x中的认证
- TKIP
- CCMP(AES的CCM模式)
- WRAP(AES的OCB模式)

- SAE认证
- 前向安全
- 192位的CNFA算法

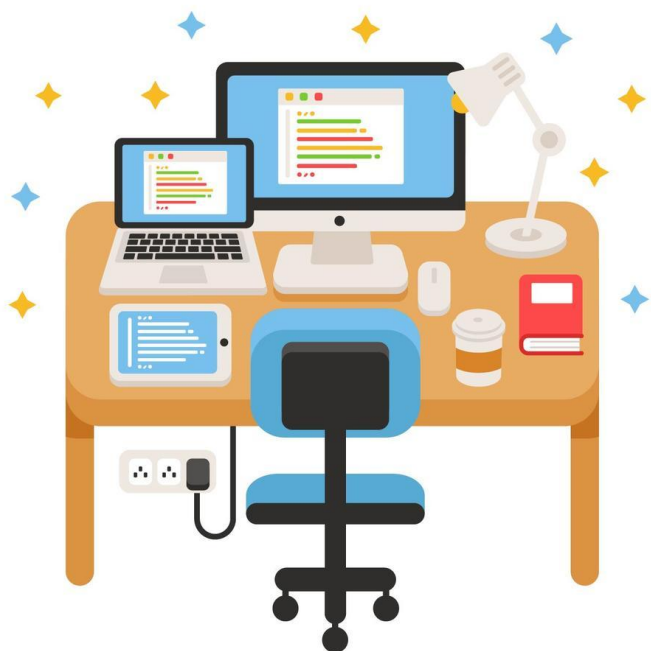
WAPI

- 基于公钥证书的认证与密钥协商协议（身份认证、单播密钥更新、组播密钥更新）
- 密钥管理、完整性保护、机密性保护

4. 无线安全的发展历史

无线安全现状

- 保护移动终端设备上的数据会变得越来越困难，并会引起更多关注
- 随着更多客户使用移动设备进行交易，银行在保护客户的数据和金融资产方面将面临着重大的挑战。
- 更多人对移动环境发起攻击。



1. 课程简介
2. 无线技术的发展历史
3. 无线技术的分类
4. 无线安全的发展历史
- 5. 无线安全事件**

5. 无线安全事件

实例1

《世界新闻报》窃听丑闻曝光



默多克酝酿拆分新闻集团

时间：2011年7月4日 地点：英国伦敦

2011年7月4日，英国《卫报》头条报道称，默多克新闻集团旗下的《世界新闻报》在2002年非法窃听失踪少女米莉·道勒及其家人的电话，干扰警方破案。这篇报道在英国媒体、政界、警方引起巨大反响，继而带出更多窃听丑闻。新闻集团因此遭受重创：多名高管辞职甚至被捕；拥有168年历史的《世界新闻报》停刊；放弃收购英国天空广播公司等。【[详细](#)】

- http://special.caixin.com/event_0704_2/
- 其中包括固定电话及手机被窃听
- 高手根本不需要触碰到你的手机，就可以入侵窥视你的隐私。
- 其中包括语音信箱被窃听，许多运营商的密码都是手机的最后四位

5. 无线安全事件

实例2

■ “棱镜门” 事件

- 2013年6月初，外媒接连披露美国国家安全局和联邦调查局的“棱镜”项目
- 美国政府秘密监听全球民众电话的通话记录，监视民众网络活动，引起世界舆论大哗。
- 9日，曾为中情局和国安局工作的揭秘者爱德华·斯诺登，主动曝光自己的身份及藏身地——中国香港，震动美国政界和情报界



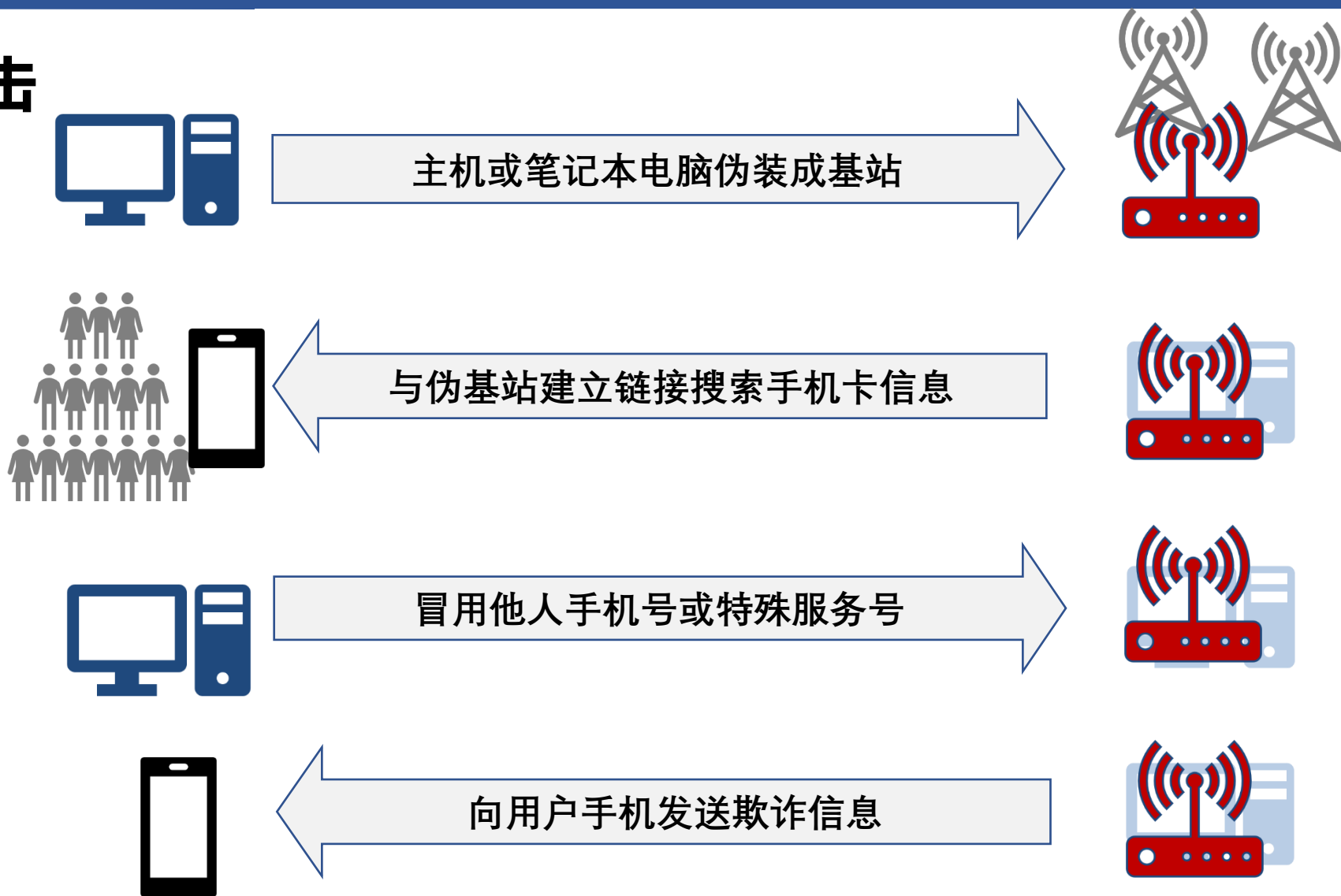
实例2（续）

■ “棱镜门” 中暴露出的信息安全问题

- 利用美国驻各国的大使馆、领事馆内的无线监听系统来实施；
- 从技术的角度，要对功率小、传输距离短的手机进行监听需将监听设备设置在很近位置
- 从法律角度上，使馆/领事馆具有法律豁免权，等同于一国海外领土。即便对方知道使馆、领事馆安装有监听装置也无可奈何
- 斯诺登披露的德国、波兰等国的遭遇也证实了美国确实是利用驻别国使、领馆搞监听。

5. 无线安全事件

实例3：伪基站攻击



5. 无线安全事件

实例3：伪基站攻击

■ 伪基站攻击的原因

- 无线接口是开放信道
- GSM中的鉴权是单向的，缺乏MS对网络侧的认证
- 伪基站还具有很强流动性，很难检测
- 伪基站设备主要由主机、笔记本电脑组成，犯罪成本低

5. 无线安全事件

其他重大无线安全事件汇总

时间	安全事件	类型	影响
1997	WEP破解	Wi-Fi加密漏洞	促使 WPA / WPA2 的出现
2008	GSM A5/1被破解	2G加密缺陷	推动运营商升级到3G
2008	SS7攻击，导致可拦截通信或跟踪用户	核心网漏洞	推动3G加强核心网安全
2010	IMSI Catcher导致IMSI泄露	假基站攻击	推动3G引入双向认证
2017	KRACK (握手协议存在漏洞)	WPA2漏洞	推动WPA3 标准推出
2021	LTE定位攻击	隐私攻击	加强隐私保护，提升攻击难度

安全成为无线技术进一步发展的问題或障碍

- 上网查一则与**无线通信安全**相关的最新安全事件，用AI帮助梳理分析里面提到的安全问题，给出造成安全事件的原因、导致的后果及规避措施。
- 阅读教材第一章

Any Questions?

