

课程编号：3182121321

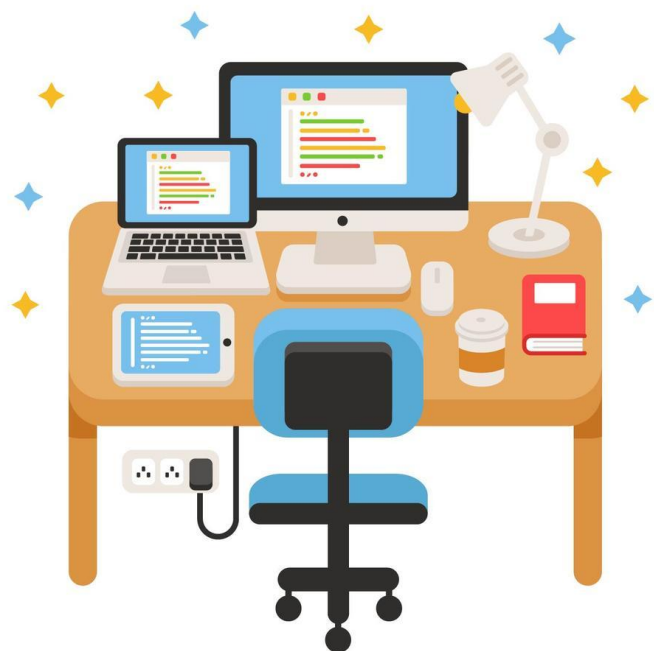
无线通信安全



第三讲 无线通信的安全威胁和安全体系

李晖

lihuill@bupt.edu.cn



1. 威胁分析的重要性
2. 无线威胁
3. 无线安全的基本要求
4. 无线通信中的安全策略
5. 无线通信中的安全体系

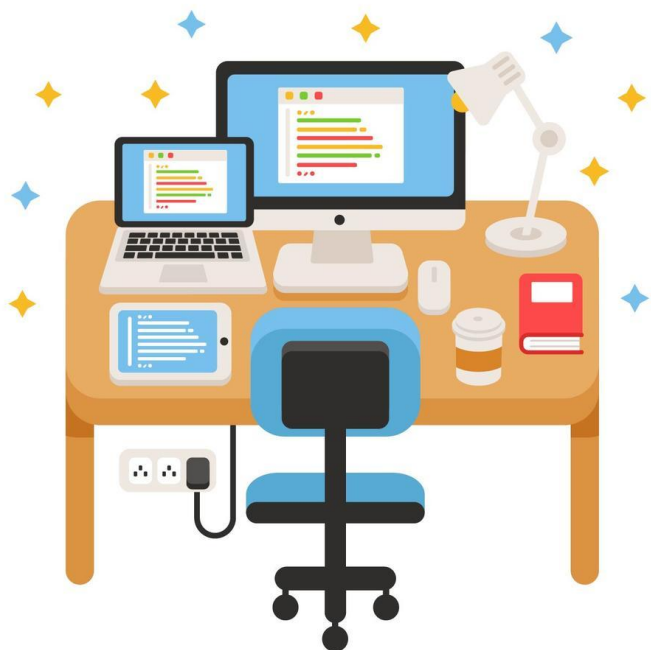
1. 本讲目标

- 了解移动通信网络的基本架构
- 了解安全威胁分析的内容
- 能够列出主要的无线通信系统的安全威胁

1. 威胁分析的重要性

威胁分析是安全设计的基础

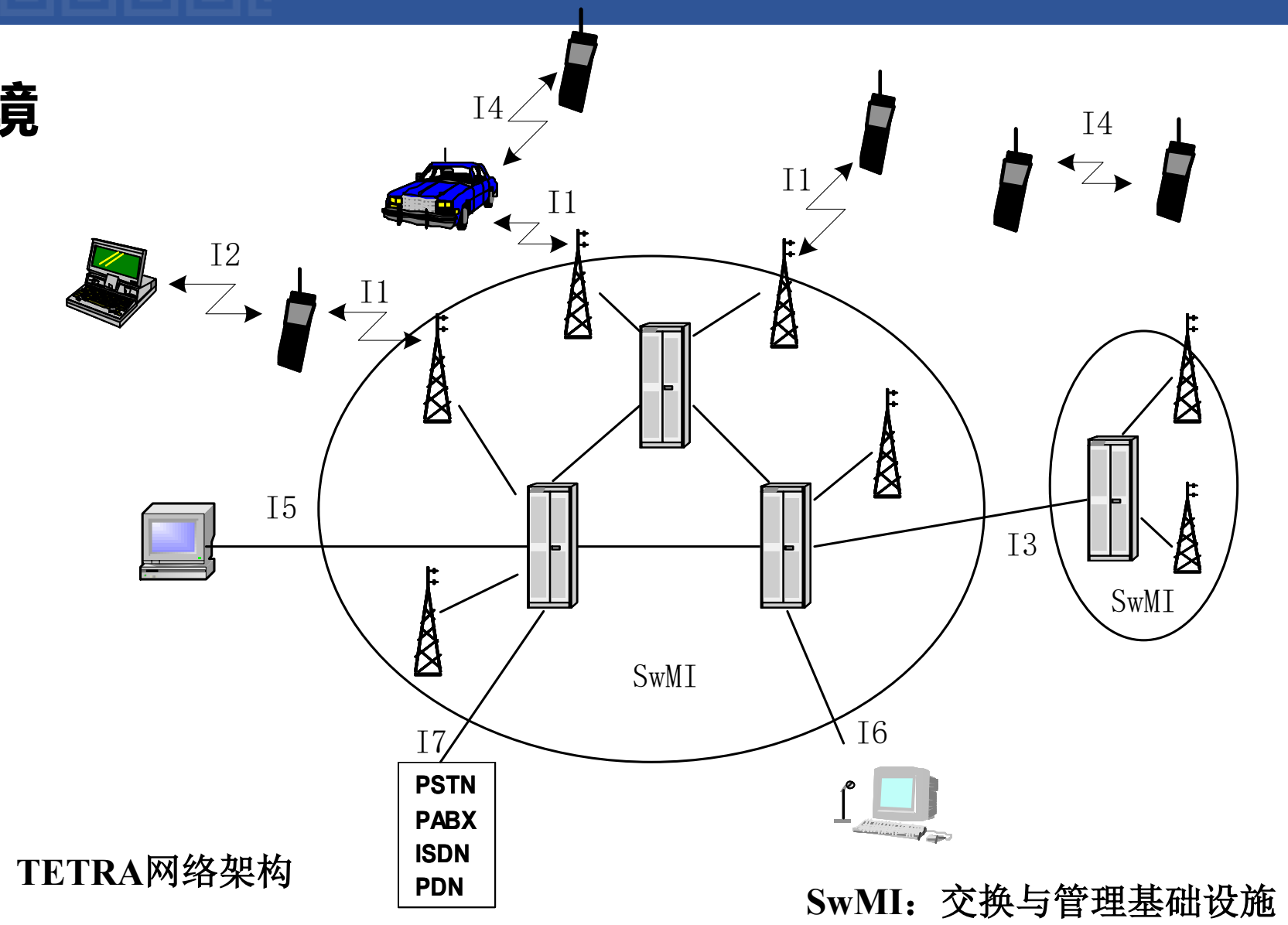
- **威胁分析**：列出所有对系统可能的威胁
- **风险分析**：定量的测评攻击的复杂性和后果
- **确定安全需求/目标**
 - 确定系统需要哪些安全功能；
 - 在一定的安全假设条件下来确定安全需求和安全目标
- **设计安全机制**：设计适当的安全机制
- **安全分析**：对安全机制进行分析和评估
 - 尽早发现系统的安全漏洞；
- **反应阶段**：发现漏洞或攻击后，系统的应对过程
 - 原始设计足够灵活，则能够及时增加防范新攻击的方法。



1. 威胁分析的重要性
2. **无线威胁**
3. 无线安全的基本要求
4. 无线通信中的安全策略
5. 无线通信中的安全体系

2. 无线威胁

无线通信网络环境



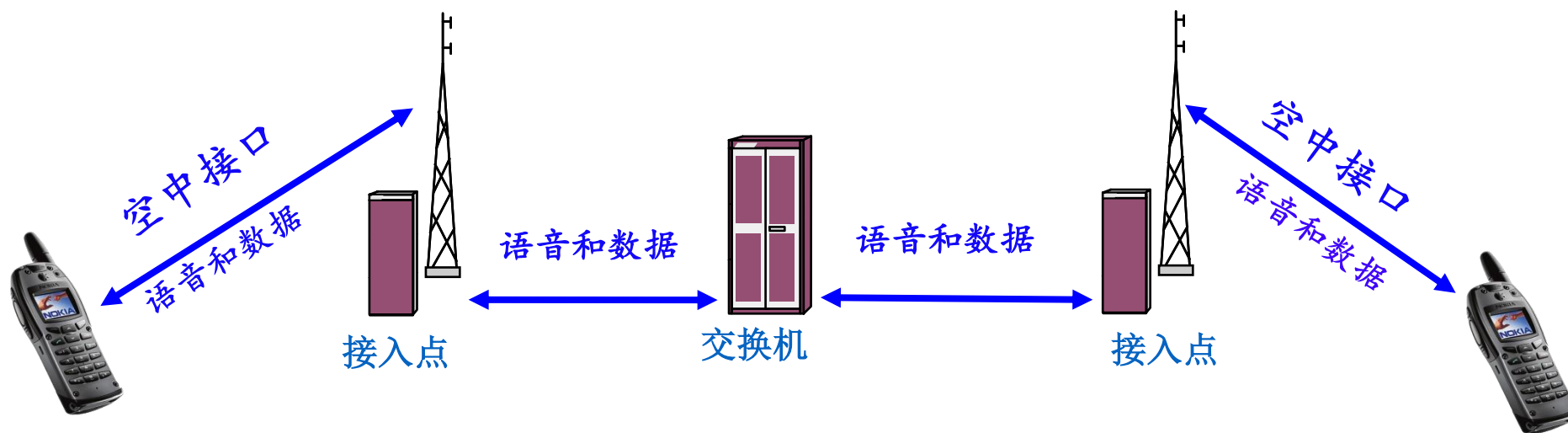
TETRA网络架构

SwMI: 交换与管理基础设施

2. 无线威胁

无线通信面临的安全威胁

- 根据攻击的位置可分为
 - 无线链路威胁
 - 服务网络威胁
 - 终端威胁等



2. 无线威胁

无线通信面临的安全威胁

- 根据威胁的对象可分为：

- 对传递信息的威胁：

- 针对在系统中传输的个人消息，例如系统中两个用户之间、网络运行商之间、用户和服务提供商之间的消息等。

- 对用户的威胁：

- 针对系统中用户的一般行为，例如试图找出用户在什么时间、什么地点在做什么等。

- 对通信系统的威胁：

- 破坏整个系统的完整或为得到系统的访问权而破坏局部系统或损坏系统的功能等。

分析内容

- 攻击类型
- 攻击点
- 可能的攻击者
- 攻击的动机
- 可能的利益
- 攻击的复杂程度
- 阻止攻击的机制

2. 无线威胁

无线通信面临的安全威胁

■ 侦听

- 非授权方获悉传输或存储在移动通信系统中的信息

■ 篡改

- 非授权方更改系统中的各种信息
- 主要是指信息的非法修改和重放，其中信息非法修改包括简单更改（例如，数据位的颠倒）、删除或插入部分消息或文件、删除整个消息或文件、插入新数据或语音信号、调整信息顺序。

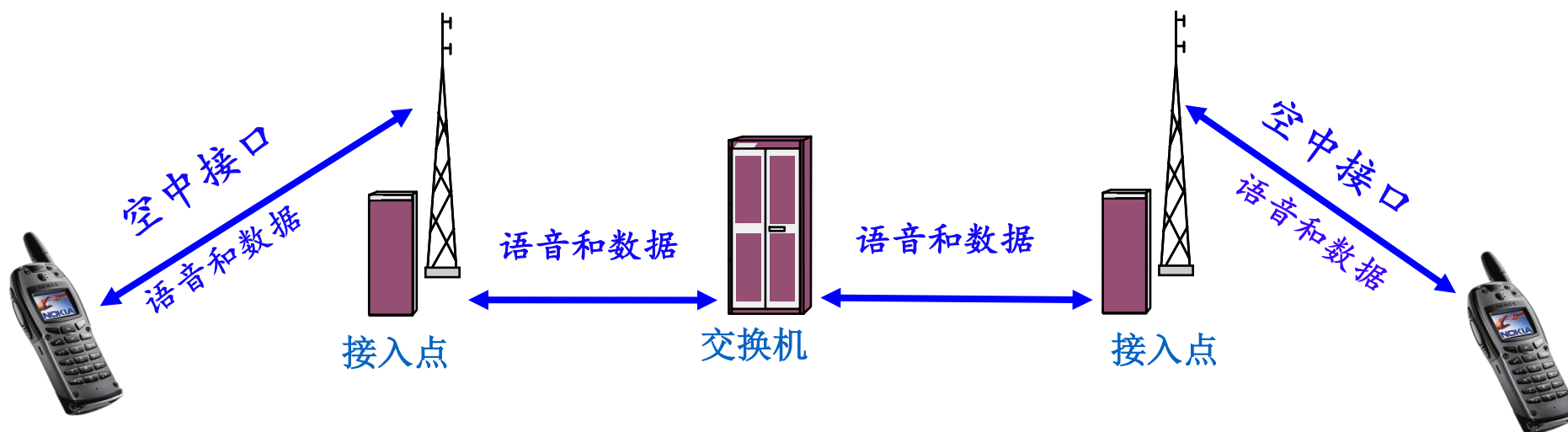
■ 抵赖

- 参与通信的一方否认或部分否认他的行为
 - 接收抵赖
 - 源发抵赖

2. 无线威胁

侦听

- 在空中接口实施：相对简单
 - 伪装成终端
 - 伪装成基站
- 在固定网络实施：需要和移动通信系统、网络实体或线缆进行物理连接
- 所截取的信息类型：语音或用户数据、控制数据、管理数据



2. 无线威胁

篡改

- 在空中接口实施：相对简单
 - 攻击者需要配备能够与某个移动台使用同一信道发送数据的发射器
 - 消息不能被重新排序；
 - 数据或语音信号只能被间接删除：消息可以被修改，从而使接收者（例如语音编码器）由于有太多的错误而丢弃该数据；
 - 只能在传送间隔实现插入。
- 在固定网络实施：
 - 所有类型的篡改都可能发生
 - 这种攻击需要能够物理访问某个网络节点，例如基站等
- 篡改的信息类型：语音或用户数据、控制数据、管理数据

1. 无线威胁

抵赖

- 接收抵赖
 - 指接收到信息的用户否认他接收到了信息；
- 源发抵赖
 - 指发送信息的用户否认发送了信息。
- 潜在的攻击者是系统中发送或接收消息的正常用户。
- 在公共网络和私有网络，如果用户之间无法相互信任，则存在这种威胁。
- 这种攻击可以采用密码安全机制来防止。

对用户的威胁

- 欺诈
 - 模仿或克隆客户身份从而试图获得对网络 and 业务的访问
- 流量分析
 - 指分析网络中的通信流量
 - 包括信息速率、消息长度、接收者和发送者的标识等
- 监视
 - 监视一个特殊用户的行为

2. 无线威胁

对通信系统的威胁1

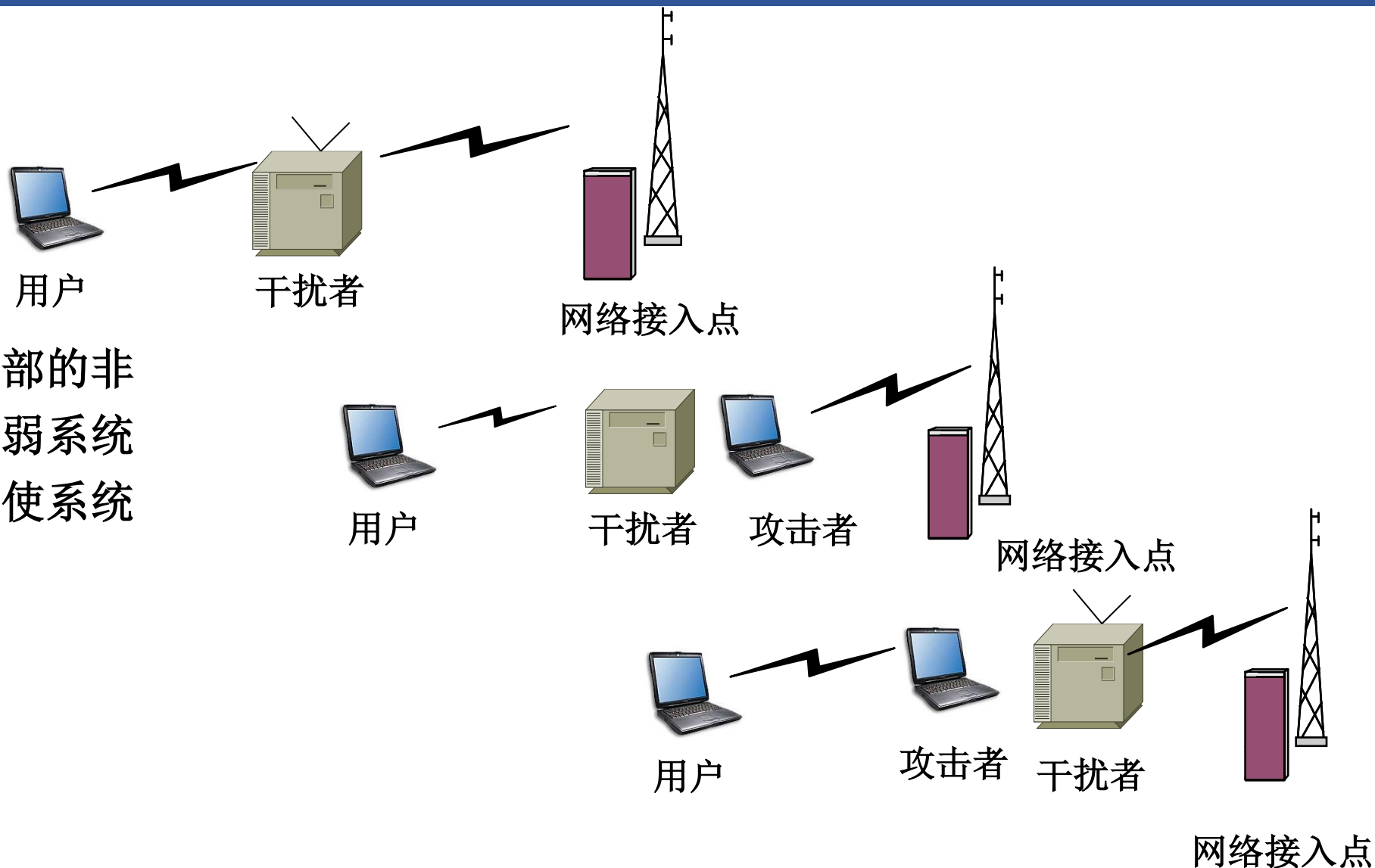
■ 干扰

■ 拒绝服务

- 指系统内部或外部的非法攻击者故意削弱系统的服务能力，或使系统无法提供服务。

■ 客户台干扰

■ 基站干扰



2. 无线威胁

对通信系统的威胁2

- 资源的非授权访问

- 资源的非授权访问是指使用禁用资源或越权使用无线信道、设备、服务或系统数据库等系统资源

- 禁用资源：

- 用户根本不允许使用的资源

- 越权使用资源

- 该用户允许使用一些资源，但是该用户所访问的资源超过了其权限范围

2. 无线威胁

移动安全威胁日益严重

■ 2025年，SK Telecom 数据泄露

- SK Telecom 在 2025 年 4 月披露因网络攻击发生客户数据泄露，消息公布后其股价一度下跌 8.5%。随后韩国政府认定其在保护 USIM 数据方面存在疏忽，并要求整改。
- 到 2025 年 7 月，SK Telecom 宣布未来五年投入 7000 亿韩元加强数据保护，同时为全部 2300 万用户提供免费更换 USIM。

■ 2025 年发生，2026 年公开，新加坡四大电信运营商遭 UNC3886 渗透

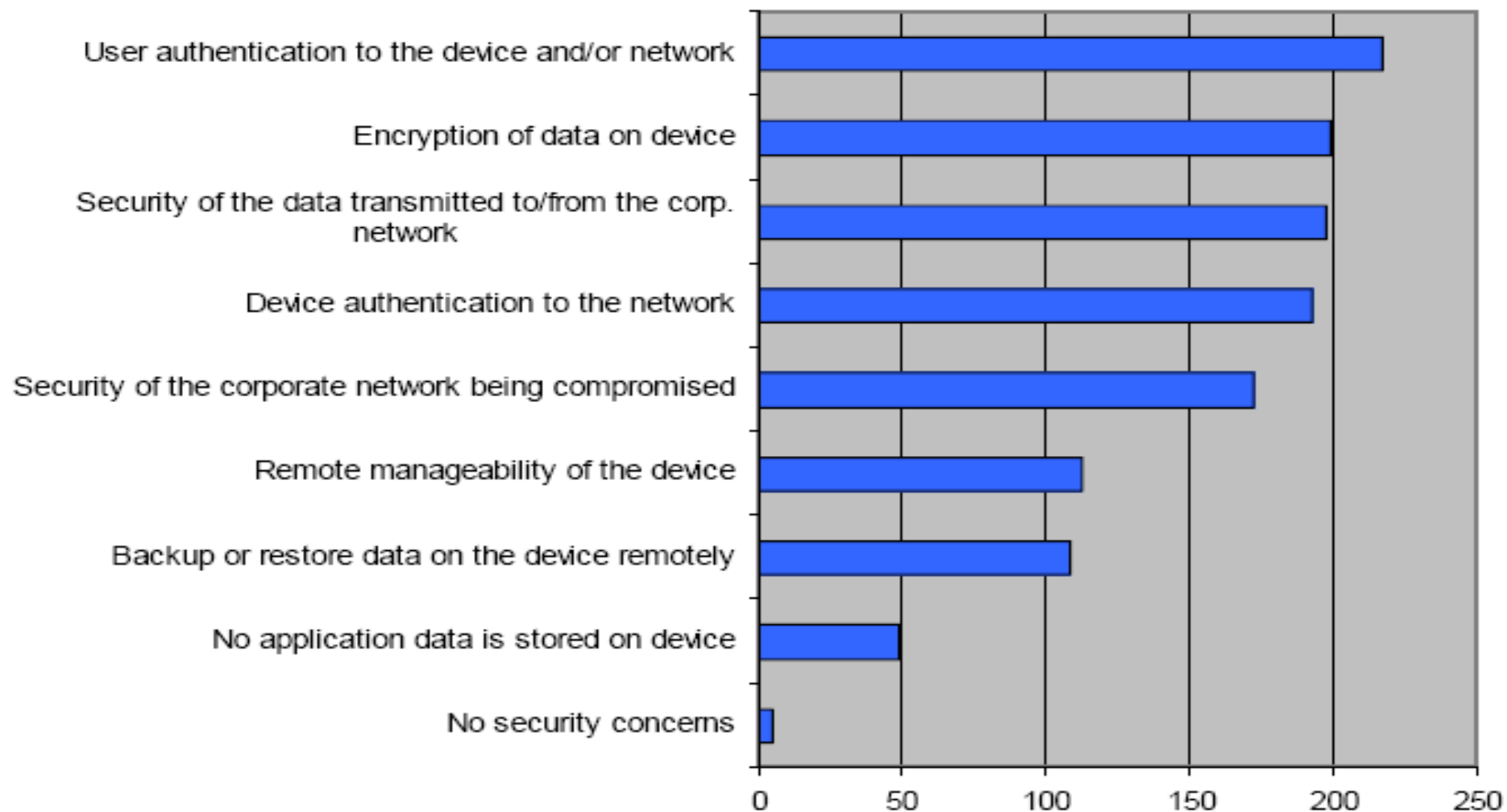
- 攻击者曾进入电信行业的系统，并且这次事件涉及新加坡电信行业。

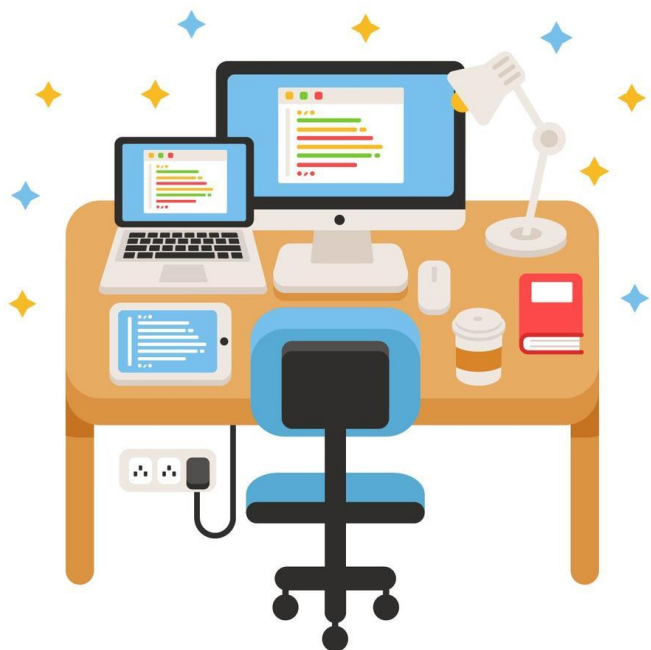
■ 2022年2月，葡萄牙最大电信公司遭攻击导致全国性断网

- 沃达丰的葡萄牙公司表示，遭受了“以损害与破坏为目的的蓄意网络攻击”，其大部分客户数据服务被迫下线。攻击迅速摧毁了该公司的4G和5G网络，并使固定语音、电视、短信、语音等服务瘫痪。

2. 无线威胁

Figure: Wireless Security Concerns Among Enterprise IT Managers





1. 威胁分析的重要性
2. 无线威胁
3. **无线安全的基本要求**
4. 无线通信中的安全策略
5. 无线通信中的安全体系

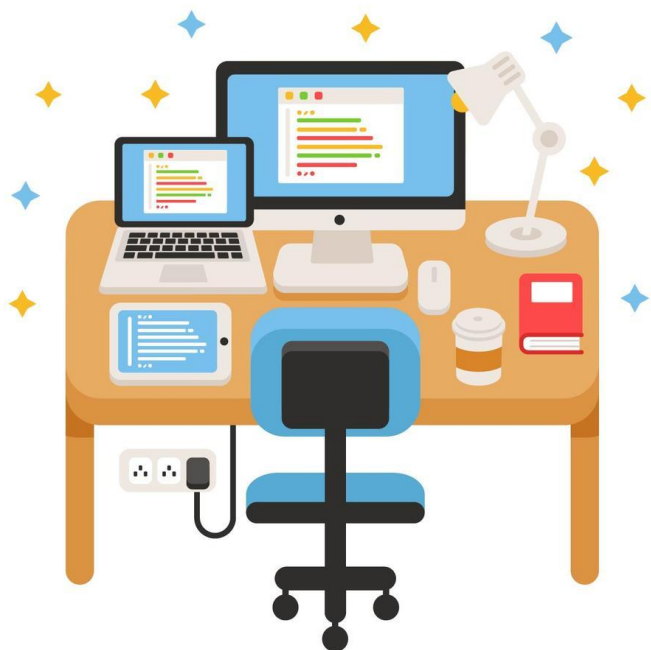
3. 无线安全的基本要求

无线移动网络的安全缺陷

- 使用无线介质
 - 没有有线网络可靠，丢包率大
 - 易于实现窃听
- 有限的带宽
 - 要求设计高效的通信和安全协议
- 移动网络中的有限的终端资源
 - 限制了加密算法的类型
 - 限制了协议的开销

无线安全的基本要求

- 能应用和整合已存在的解决方案和基础设施；
- 促进各种不同移动设备和无线设备的一致性和兼容性
- 提供高级安全但不对用户访问产生不利影响



1. 威胁分析的重要性
2. 无线威胁
3. 无线安全的基本要求
- 4. 无线通信中的安全策略**
5. 无线通信中的安全体系

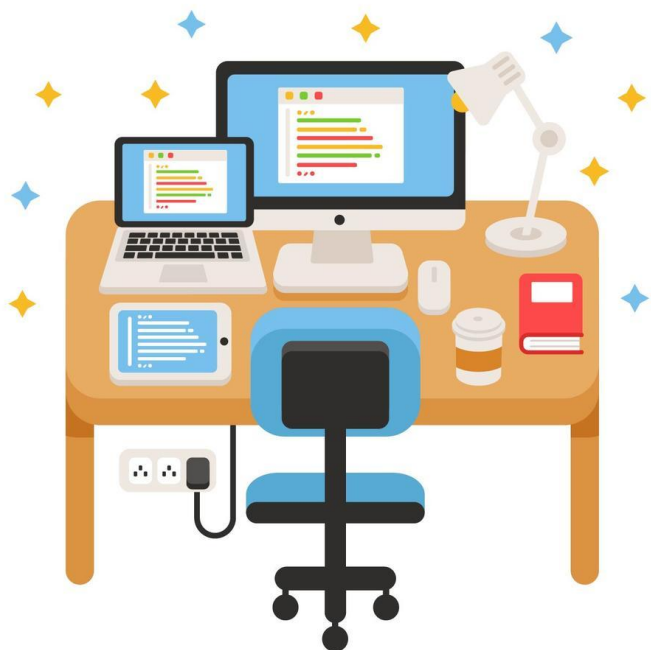
4. 无线安全的安全策略

技术策略

- 鉴权
- 访问控制
- 加密
 - 链路加密
 - 节点加密
 - 端到端加密
- 数据完整性检验
- 数字签名与反否认

管理策略

- 集成无线和有线网络安全策略
- 有效管理无线网络的网络标识
- 防范内部人员的破坏



1. 威胁分析的重要性
2. 无线威胁
3. 无线安全的基本要求
4. 无线通信中的安全策略
5. 无线通信中的安全体系

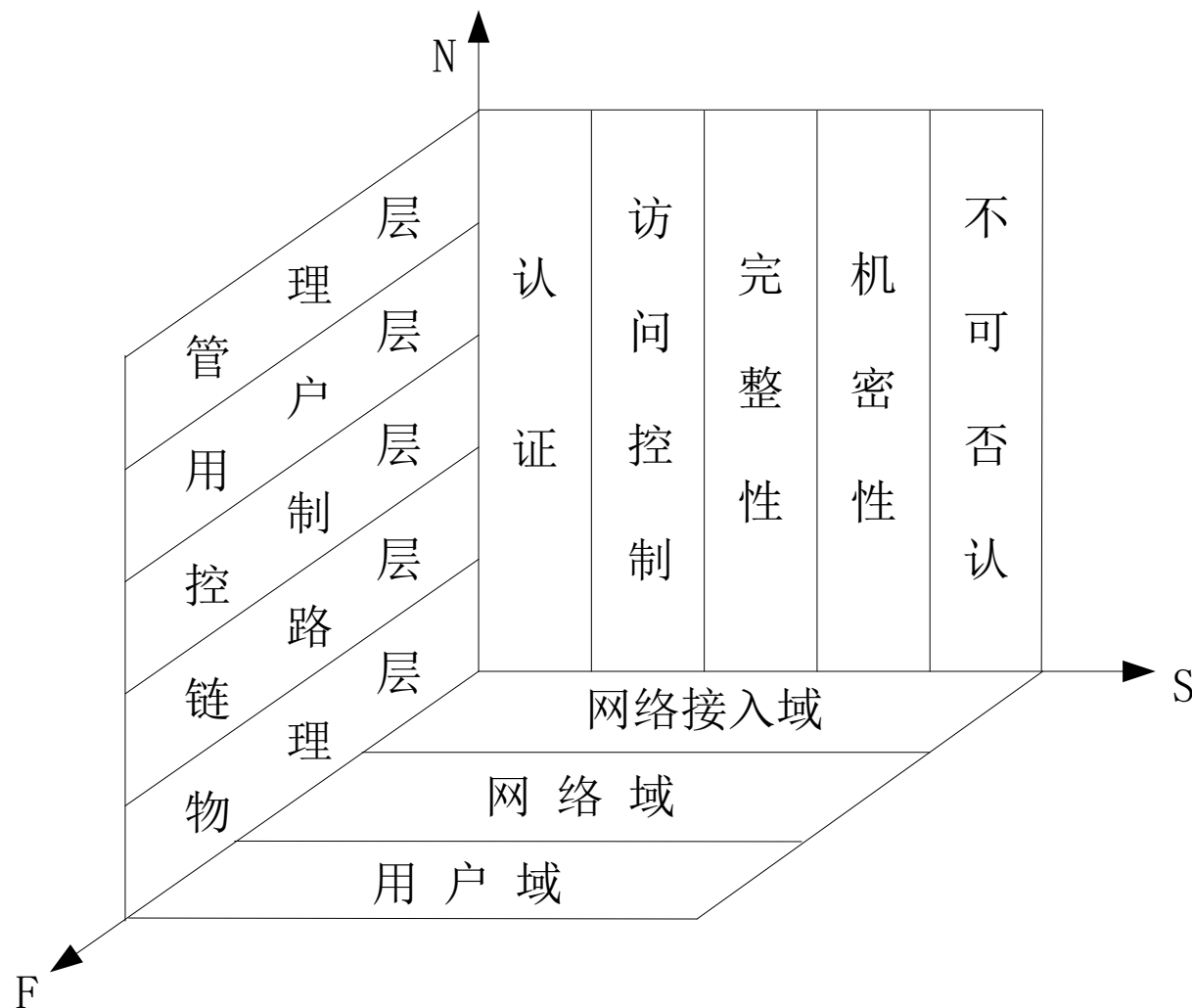
5. 无线安全的安全体系

- 安全服务轴 S

- 安全需求 N

- 安全域 F

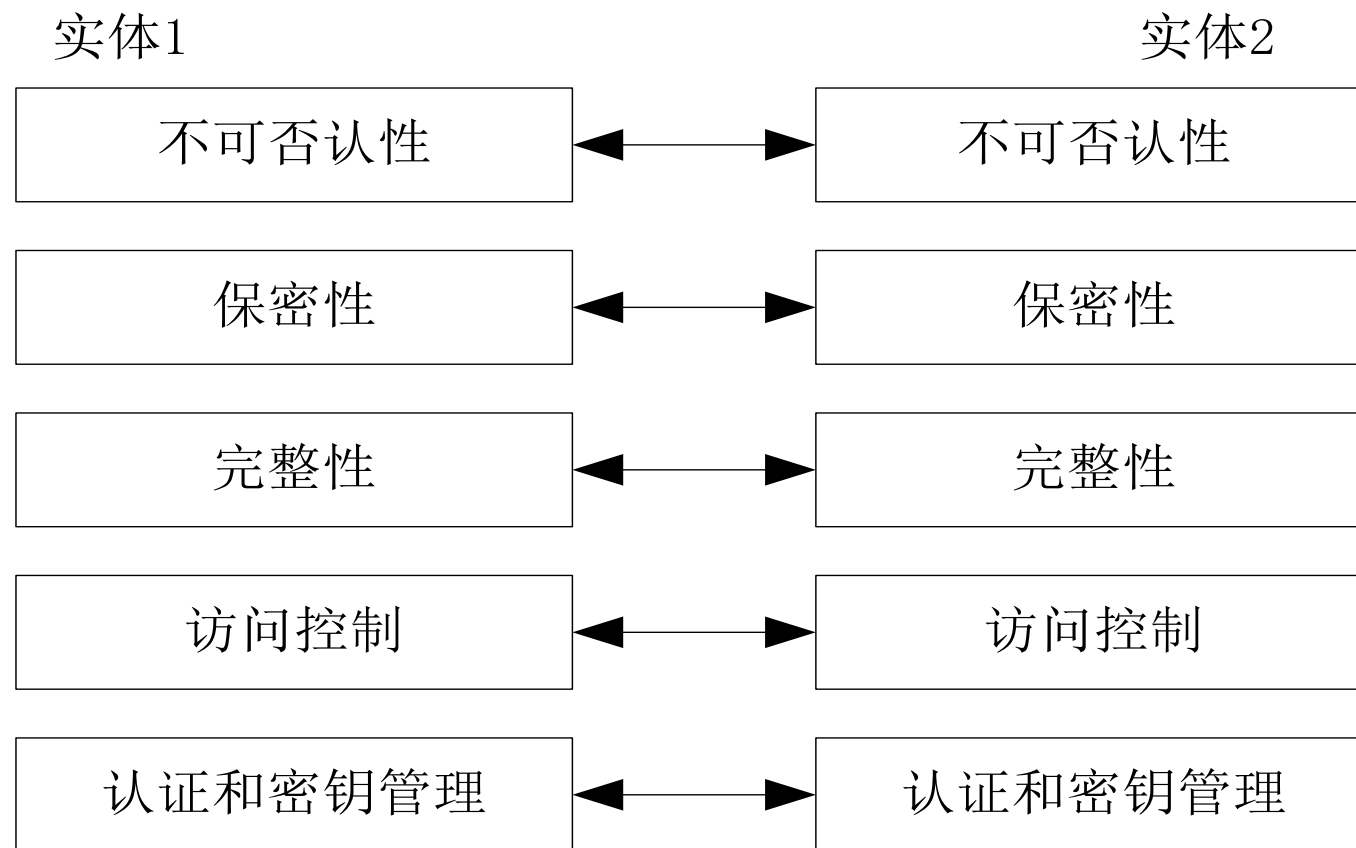
- **安全域**：是由一组具有相同安全保护需求、并相互信任的系统组成的**逻辑区域**。



- 参考开发系统互连参考模型（**OSI/RM**）中提出的安全体系结构框架

5. 无线安全的安全体系

安全服务



安全服务层次模型

5. 无线安全的安全体系

安全需求

- 管理层：制定安全策略，包括对安全威胁的管理、确定被保护的资源和使用的安全技术；
- 用户层：提供事务处理的端到端安全；
- 控制层：负责网络过程，实现鉴权和用户管理等安全服务；
- 链路层：主要保证数据在无线电线路上传输的正确性和安全性；
- 物理层：主要是防止物理通路的损坏、对物理通路的窃听和干扰等。

5. 无线安全的安全体系

安全域

■ 接入域/网络接入域

- 主要提供安全接入服务，包括用户身份机密性、用户认证、在网络接入信道和设备间传输数据的机密性和完整性、移动设备的鉴定。

■ 网络域

- 主要提供网络实体间的认证、数据传输机密性和完整性、攻击信息的监视等安全机制。

■ 用户域

- 主要提供终端安全服务模块与用户间的认证以及终端安全服务模块与移动终端间的认证。

总结



思考题

- 什么是安全域？
- 列出移动通信系统在接入域、网络域和用户域的主要安全威胁。



Thank You !