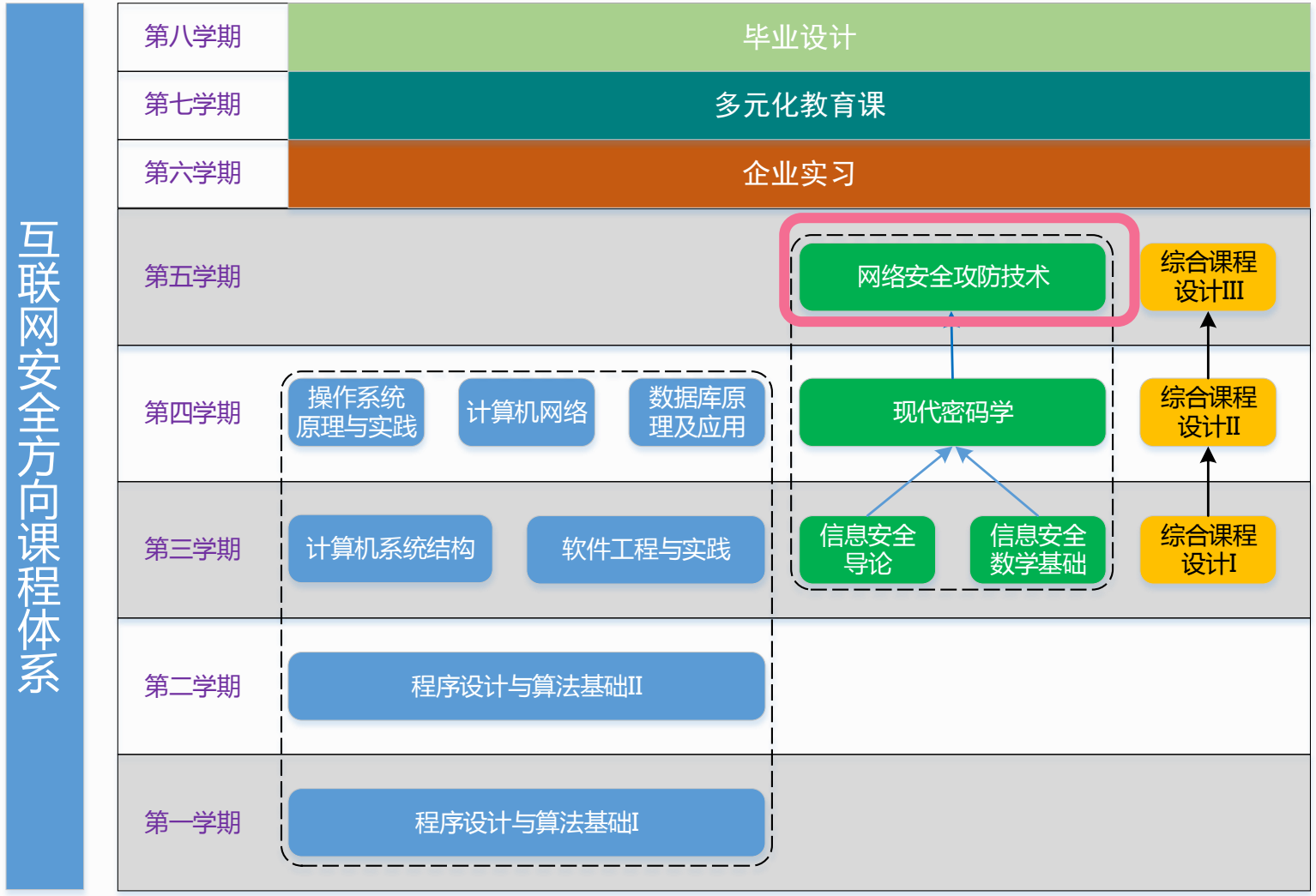
电子科技大学
University of Electronic Science and Technology of China

网络攻防技术

电子科技大学 信息与软件工程学院

2020年9月3日

互联网安全课程体系


互联网安全方向课程体系
第八学期
毕业设计
第七学期
多元化教育课
第六学期
企业实习
第五学期
网络安全攻防技术
综合课程设计III
第四学期
操作系统原理与实践
计算机网络
数据库原理及应用
现代密码学
综合课程设计II
第三学期
计算机系统结构
软件工程与实践
信息安全导论
信息安全数学基础
综合课程设计I
第二学期
程序设计与算法基础II
第一学期
程序设计与算法基础I

网络安全攻防技术——课程目标

- 建立关于网络安全的基本概念，了解网络安全及其相关技术的发展历史、核心技术及最新前沿领域

- 通过分析网络攻击的方法和原理，提出防治网络攻击的安全策略，培养分析网络安全问题的能力。

- 掌握各种协议的应用部署，建立网络安全协议流量分析的能力，培养撰写报告和设计文档，清晰阐述复杂软件工程问题的能力。

目标一

目标二

目标三

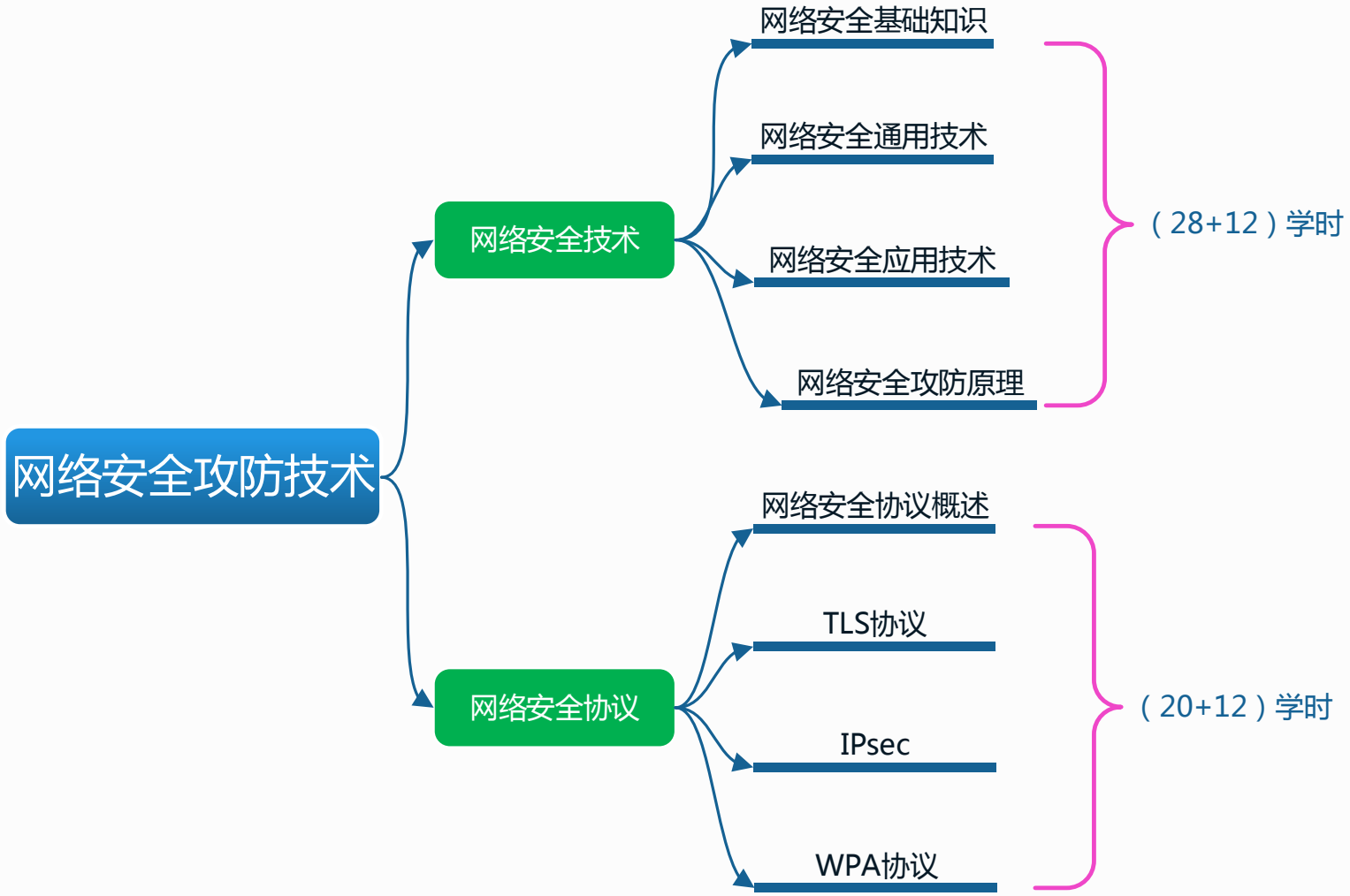
目标四

目标五

- 对网络安全基础知识、技术体系结构等有基本了解，培养分析网络协议存在的安全问题，提出解决安全问题的合理安全策略的能力。

- 掌握现存网络安全技术，选择和使用网络安全技术实现恰当的安全机制，培养学生解决网络安全问题的工程实践能力。

网络安全攻防技术——课程内容



网络安全攻防技术——成绩构成

- 平时成绩（40%）
  - 关于网络安全技术的课程报告一篇（5%）
    - 如：对比分析开源网络扫描器
  - 关于网络安全协议的课程报告一篇（5%）
    - 如：总结分析各网络安全协议的设计思路
  - 6个课程实验，每个占5%（30%）
- 期末成绩（60%）
  - 期末考试（60%）

课程简介—— 教学交流

- 教学交流群

2020网络GF技术-王老师

QQ群：799786789

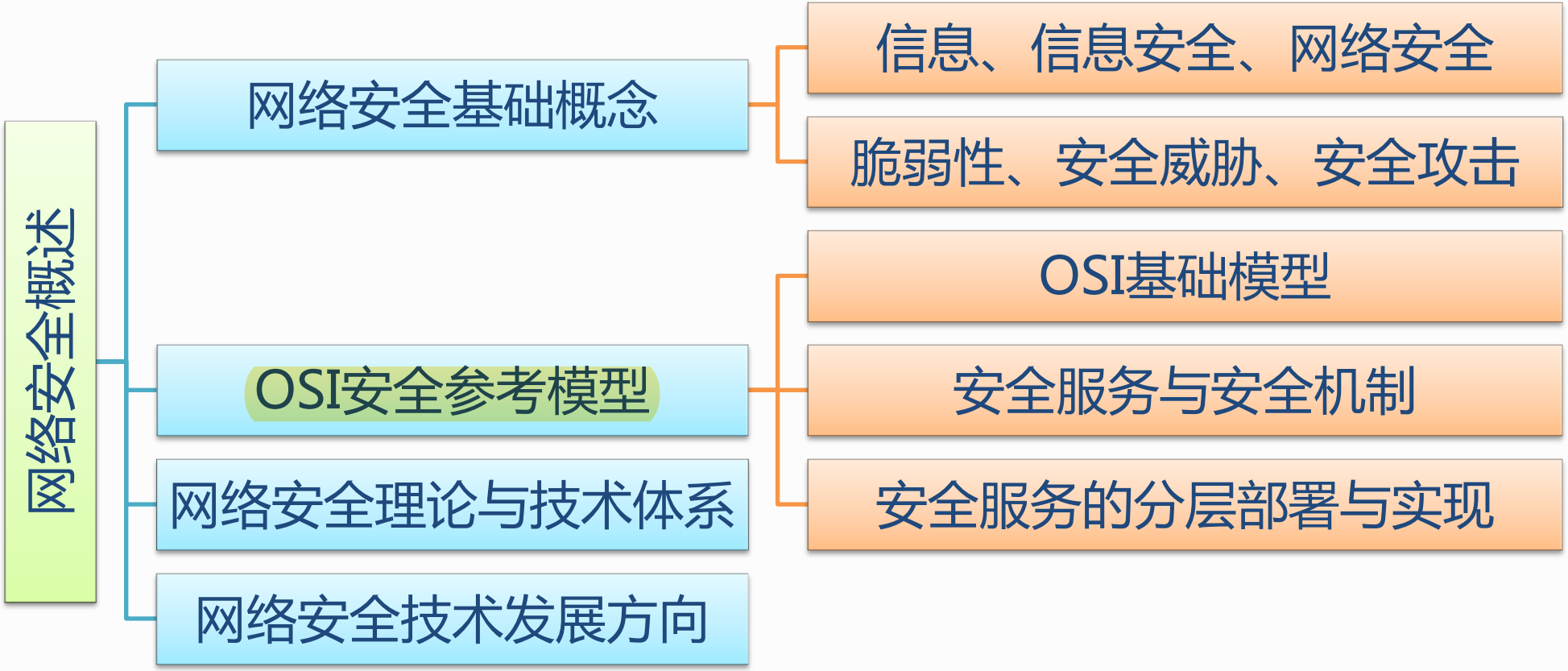
注意事项：加群后请使用实名，群内名称“学号-姓名”，

群内不允许讨论与课程学习无关的话题，谢谢理解！

第一讲 网络安全概述

了解网络安全的基本概念、网络安全技术的发展历史、OSI安全参考模型，网络安全核心技术体系及网络安全前沿技术领域。

内容安排


网络安全概述
网络安全基础概念
信息、信息安全、网络安全
脆弱性、安全威胁、安全攻击
OSI安全参考模型
OSI基础模型
安全服务与安全机制
安全服务的分层部署与实现
网络安全理论与技术体系
网络安全技术发展方向

第一讲 网络安全概述

1、网络安全基础概念 —— 信息

- 什么是信息？
  - “信息就是用来消除随机和不确定性的东西”。—— 香农
  - “信息是区别于物质与能量的第三种资源，是客观事物的基本存在形态之一”。—— 维纳
  - “信息是事物运动的状态与方式”。 —— 钟义信
- 信息的特性
  - 价值性、可传递性、载体依附性、时效性、真伪性、共享性、可处理性……

第一讲 网络安全概述

1、网络安全基础概念 —— 信息安全

- 什么是信息安全？
  - “在技术上和管理上为数据处理系统建立的安全保护，保护信息系统的硬件、软件及相关数据不因偶然或者恶意的原因遭到破坏、更改及泄露”。

    —— ISO国际标准化组织
  - “对信息的保密性、完整性和可用性的保持，也可包括诸如真实性、可核查性、抗抵赖和可靠性等其他特征。”

    —— GB/T 29246-2017 信息技术 安全技术信息安全管理体系 概述和词汇

1、网络安全基础概念 —— 信息安全

- 信息安全基础属性
  - 保密性：信息对未授权的个人、实体或过程不可用或不泄露的特性。
  - 完整性：信息保持准确和完备的特性。
  - 可用性：根据授权实体的要求，可以访问和可以使用的特性。

上述属性被称为信息安全CIA三要素

1、网络安全基础概念 —— 信息安全

- 信息安全其他属性
  - 真实性（authenticity）：一个实体是其所声称实体的这种特性。
  - 抗抵赖（non-repudiation）：证明所声称事态或行为的发生及其源头的能力。
  - 可靠性（reliability）：与预期行为和结果一致的特性。
  - 可控性（controllability）：对信息的传播及内容具有控制能力的特性。

1、网络安全基础概念 —— 网络安全

- 什么是网络安全？
  - 从本质上来讲，网络安全就是网络上的信息安全。
  - 网络的安全是指网络系统的硬件、软件及其系统中的数据受到保护，不会因偶然或者恶意的因素的影响而遭到破坏、更改或泄露，系统能够连续、可靠地正常运行，网络服务不被中断。

网络系统是信息最大的生产、存储和加工和应用空间

根据2018微信数据报告显示，2018年里微信的日活量已经达到了10.1亿人，每天发出去的信息450亿条，每天有4亿次音视频呼叫成功，视频通话用户比三年前多了570%。

1、网络安全基础概念 —— 脆弱性

- 什么是脆弱性？
  - 所谓网络系统的脆弱性，是指系统的硬件资源、通信资源、软件及信息资源等存在的弱点和缺陷。
    - 硬件系统的弱点和缺陷
    - 软件系统的弱点和缺陷
    - 网络和通信协议的弱点和缺陷
    - 使用者的弱点

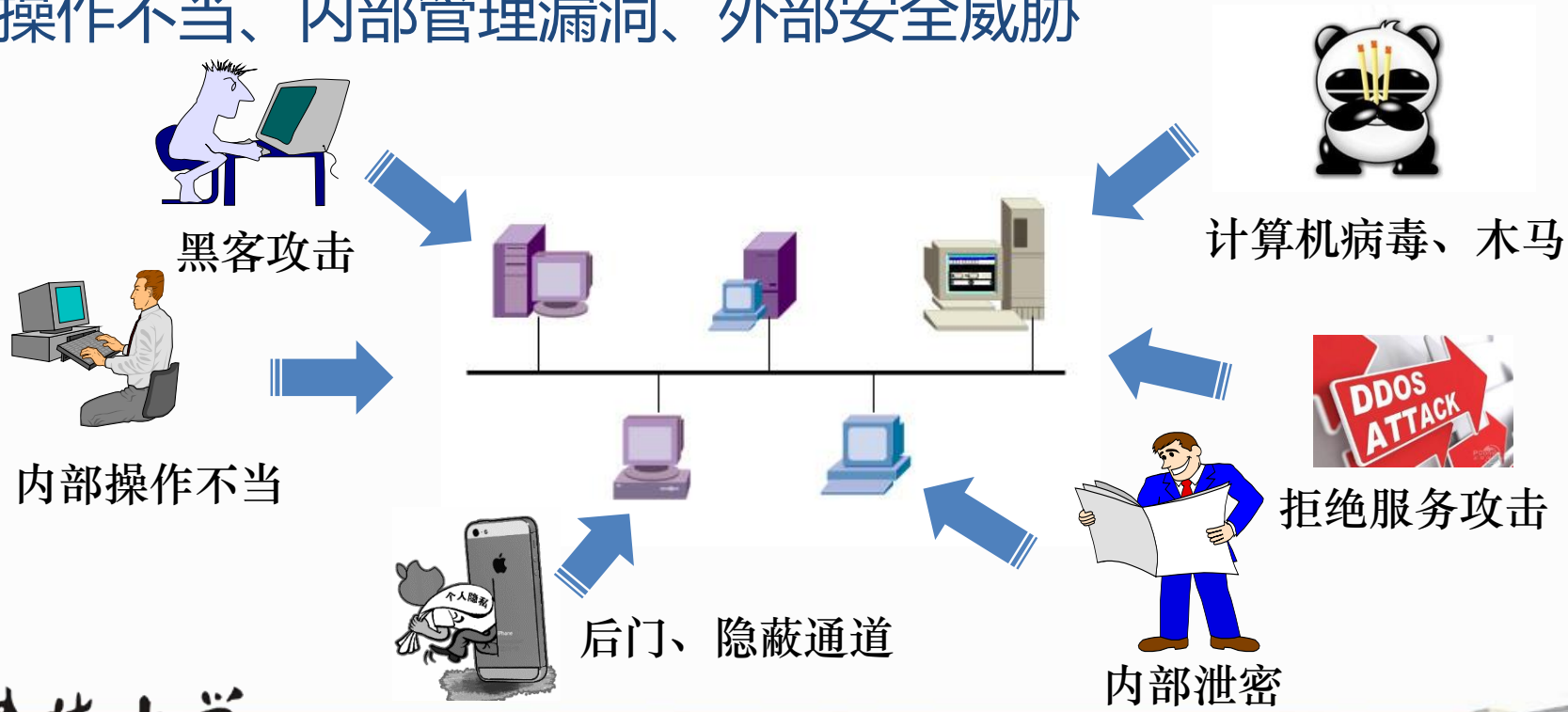
1、网络安全基础概念 —— 安全威胁

- 什么是安全威胁？
  - 可能对系统或组织造成危害的不期望事件的潜在原因。脆弱性的普遍存在是安全威胁产生的根本原因。
- 威胁的主要类型
  - 信息泄露
  - 完整性破坏
  - 服务拒绝
  - 未授权访问

1、网络安全基础概念 —— 安全威胁

◘ 威胁来源

- ➢ 内部操作不当、内部管理漏洞、外部安全威胁



第一讲 网络安全概述

1、网络安全基础概念 —— 安全攻击

- 什么是安全攻击？
  - 任何危及到信息安全的行为，安全攻击往往要利用一个或多个威胁。
- 安全攻击的类型（IATF定义）
  - 被动攻击
  - 主动攻击
  - 物理临近攻击
  - 内部人员攻击
  - 配装分发攻击

1、网络安全基础概念—— 安全攻击

- 什么是被动攻击？
  - 被动监视网络上的信息传递过程或内容，如网络监听、流量分析。
  - 对策：信道加密和流量填充。

1、网络安全发展历程 —— 安全攻击

- 什么是主动攻击？
  - 避开或破坏安全部件， 引入恶意代码，破坏数据或系统完整性。
  - 对策：增强区域边界保护、基于网络管理交互身份认证的访问控制、受保护远程访问、质量安全管理、自动病毒检测工具、审计和入侵检测。

1、网络安全发展历程 —— 安全攻击

- 什么是物理临近攻击？
  - 一个未授权的个人近距离物理接触网络、系统或设备，以修改、收集信息或者拒绝对信息的访问。这种接近可以通过秘密进入、公开访问或者两者结合
  - 对策：配置环境监控体系，提供设备物理安全保护。

1、网络安全基础概念—— 安全攻击

- 什么是内部人员攻击？
  - 由在信息安全处理系统物理边界内的合法人员或者能够直接访问信息安全处理系统的人员发起的攻击。
  - 对策：安全意识和训练；审计和入侵检测；安全策略和增强安全性；关键数据、服务和局域网的特殊的访问控制；加强身份识别与认证能力等。

1、网络安全基础概念—— 安全攻击

- 什么是配装分发攻击？
  - 硬件或软件在生产与安装过程中，或者在运输过程中，被恶意地修改。
  - 对策：可以通过加强处理配置控制将这类威胁降低到最低。通过使用受控分发，或使用由最终用户检验的签名软件和存取控制可以解除分发威胁。

第一讲 网络安全概述

测试点1-1

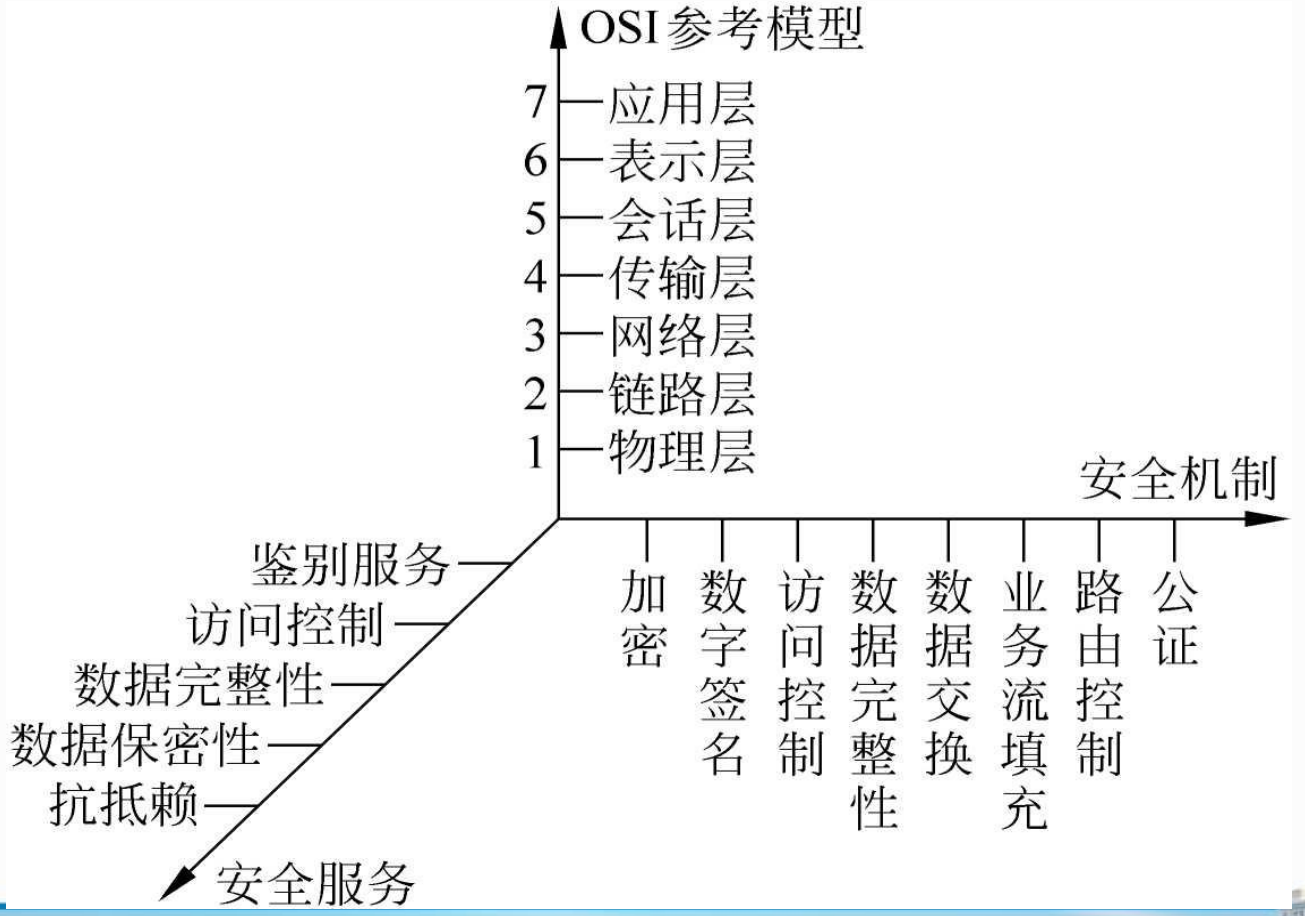
- 什么是网络安全？
- 什么是脆弱性？脆弱性分为哪几类？
- 什么是安全威胁？安全威胁分为哪几类？
- 什么是安全攻击？安全攻击分为哪几类？

2、OSI安全参考模型——OSI模型基础

- 模型概述
  - ISO 7498-2中描述了开放系统互联安全的体系结构，提出了设计安全的信息系统的基础架构应该包含五种安全服务(安全功能)和能够对这五种安全服务提供支持的八种安全机制。
  - 主要作用：一是指导可实现的安全标准的设计；二是提供一个通用的术语平台。

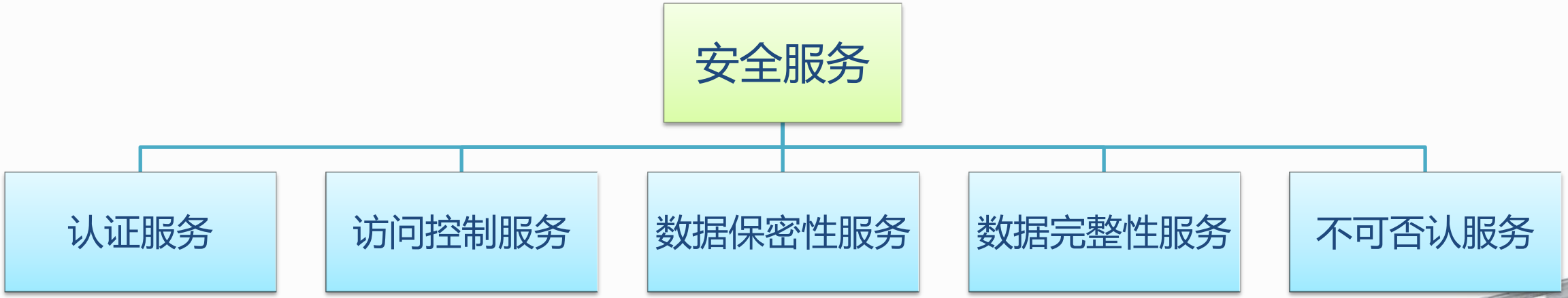
2、OSI安全参考模型——OSI模型基础

- 模型构成



2、OSI安全参考模型——安全服务与安全机制

- 什么是安全服务？
  - 是指提供数据处理和数据传输安全性保护的方法。
- 安全服务分类



2、OSI安全参考模型——安全服务与安全机制

- 什么是认证服务？
  - 认证服务是对通信的双方实体进行身份识别的服务，保证某一个实体所声称的身份是真实有效的，信息确实是由具有真实身份的实体发送的。
- 什么是访问控制服务？
  - 访问控制服务是对使用者确认身份后访问某些资源的限制，允许授权用户访问相应的资源或者接受其通信请求，防止未授权用户非法访问受控的资源，也防止已授权用户超越自己的权限访问资源。

2、OSI安全参考模型——安全服务与安全机制

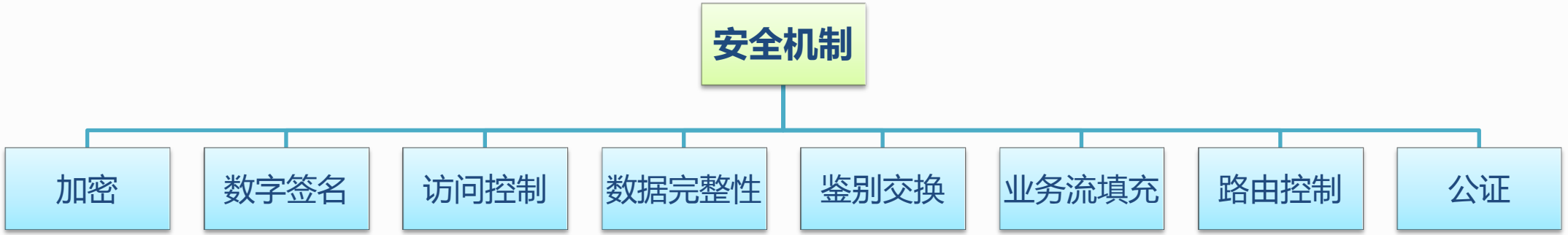
- 什么是数据保密性服务？
  - 数据保密性服务保证信息不泄漏或不暴露给未授权得到信息的实体，即使网络中各通信主体之间交换的数据被拦截和窃取，窃取者也一时难以解读出数据的内容。
- 什么是数据完整性服务？
  - 数据完整性服务就是用来防止非法实体(用户)的主动攻击，如对数据进行修改、插入、使数据延时以及丢失等。

2、OSI安全参考模型——安全服务与安全机制

- 什么是不可否认服务？
  - 不可否认性又称抗抵赖性，实际上就是保证数据的有效性。这种服务用来防止发送数据方发送数据后否认自己发送过数据，或接收方接收数据后否认自己收到过数据。

2、OSI安全参考模型——安全服务与安全机制

- 什么是安全机制？
  - 安全机制是保护信息与信息系统安全技术措施的总称。
- 安全机制分类



2、OSI安全参考模型——安全服务与安全机制

- 什么是加密机制？
  - 加密是提供信息保密的核心方法。加密是靠加密算法来实现的，发送方按照加密算法用加密密钥对信息进行处理，使信息不可直接阅读；接收方用解密密钥对收到的信息进行恢复，得到源信息明文。
- 什么是数字签名机制？
  - 数字签名就是基于加密技术，用来确定用户的身份是否真实，同时提供了不可否认功能的信息保密方法。要求具有可证实性、不可否认性、不可伪造性和不可重用性的特点。

2、OSI安全参考模型——安全服务与安全机制

- 什么是访问控制机制？
  - 访问控制机制允许授权用户合法访问网络和系统资源，拒绝未经授权的访问，并把它记录在审计报告中。
- 什么是完整性机制？
  - 数据完整性机制保证了信息传递过程中不被恶意篡改。常用的数据完整性机制的技术有加密、散列函数和报文认证码MAC三种。

2、OSI安全参考模型——安全服务与安全机制

- 什么是鉴别交换机制？
  - 交换鉴别机制是通过互相交换特有身份信息的方式来确定彼此的身份。如提供口令、智能卡、指纹、声音频谱、虹膜图像等。
- 什么是业务流填充机制？
  - 业务流填充是针对网络流量分析攻击的安全机制，防范攻击者根据流量变化推导出一些有用的信息或线索。如通过在通信空闲时间发送无效数据，使各个通信节点流量保存平衡。

2、OSI安全参考模型——安全服务与安全机制

- 什么是路由控制机制？
  - 在网络通信过程中，消息从源节点到目标节点有多条路径可以选择，路由控制机制的原则就是尽量避免走那些可能存在危险的路径。
- 什么是公证机制？
  - 信息传递过程中有时会因为网络的一些故障和缺陷而导致信息的丢失或延误，或者被篡改。因此，为了避免发生纠纷，事先可以选择一个各方信任的公正机构来对各方要交换的信息进行中转或确认，即公证机制。

2、OSI安全参考模型——安全服务与安全机制

- 安全服务与安全机制的关系
  - 安全服务体现网络信息系统的安全需求
  - 安全机制是实现安全服务采取的具体技术措施
  - 安全服务与安全机制是多对多的关系
    - 安全服务可以用不同的安全机制来实现
    - 安全机制可以用来实现不同的安全服务

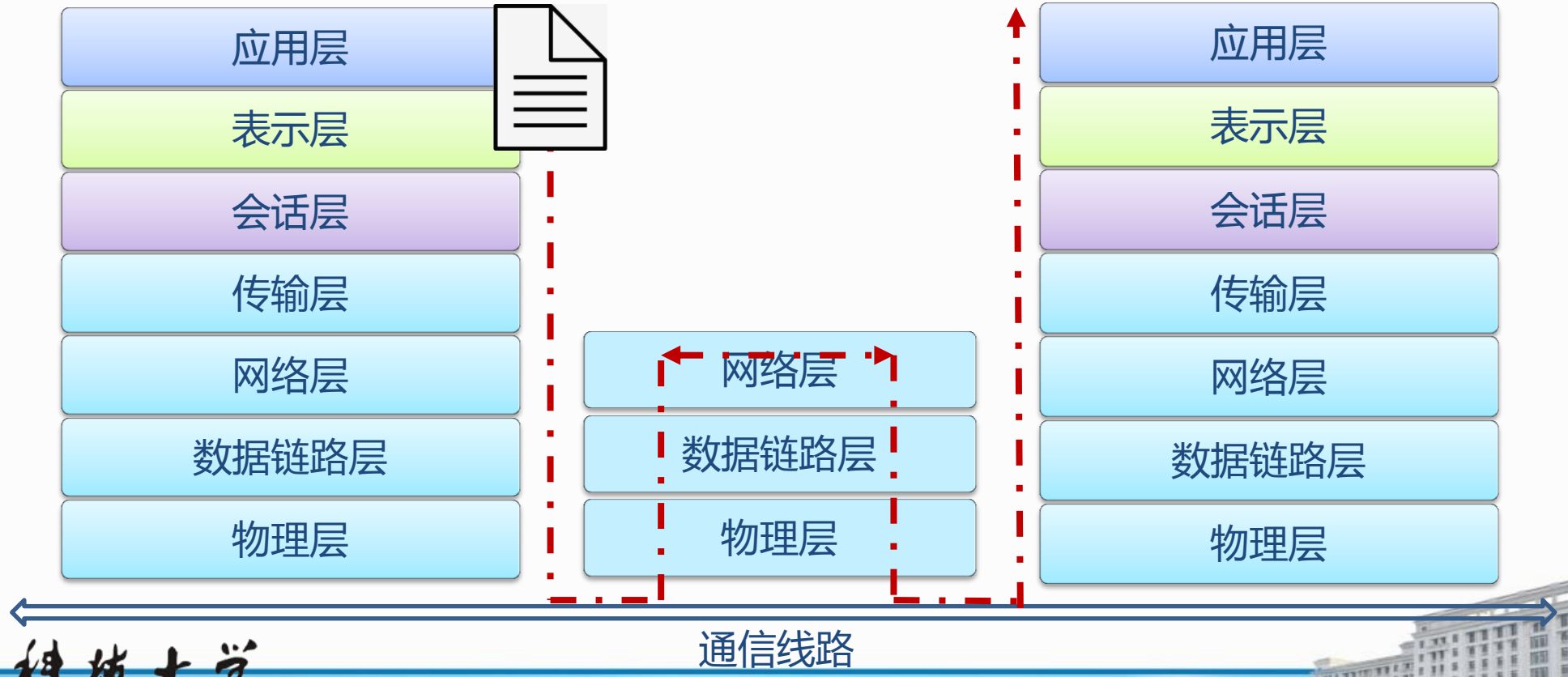
2、OSI安全参考模型——安全服务与安全机制

- 安全服务与安全机制对应表

机制/服务	机密性	完整性	认证	访问控制	不可否认
加密	Y	Y	Y	-	-
数字签名	-	Y	Y	-	Y
访问控制	-	-	-	Y	-
完整性	-	Y	-	-	Y
鉴别交互	-	-	Y	-	-
业务填充	Y	-	-	-	-
路由控制	Y	-	-	-	-
公证	-	-	-	-	Y

2、OSI安全参考模型——安全服务的分层部署与实现

- OSI网络分层模型



2、OSI安全参考模型——安全服务的分层部署与实现

- 物理层安全服务
  - 建立在物理通信介质的基础上，作为系统和通信介质的接口，为设备之间的数据通信提供传输媒体及互连装置，为实现数据链路实体间透明的比特(bit)流传输提供可靠的环境。
  - 物理层安全除了要防止物理通路被损坏外，还应采用加密数据流的方法来防止物理通路遭到窃取和攻击。

2、OSI安全参考模型——安全服务的分层部署与实现

- 链路层安全服务
  - 数据链路层的作用就是负责将由物理层传来的未经处理的bit数据分装成数据帧，检查和改正物理层上可能发生的错误，正确地交给网络层。
  - 数据链路层安全要确保所传送的数据不被窃取或破坏，主要采用划分虚拟局域网(VLAN)、加密等机制。

2、OSI安全参考模型——安全服务的分层部署与实现

- 网络层安全服务
  - 网络层将数据按固定大小分组，在分组头中标识源节点和目的节点的逻辑地址，并能够根据这些地址来选择从源地址到目的地址的路径，保证每个数据包能够成功和有效地从出发点到达目的地。
  - 网络层安全需要保证只给授权的客户使用授权的服务，保证网络路由正确，避免被拦截或监听，主要采用身份验证、访问控制、加密、一致性检验等方法来确保所传送的数据受到应有的保密性和完整性保护，防止其受到非授权的泄露或破坏。

2、OSI安全参考模型——安全服务的分层部署与实现

- 传输层安全服务
  - 传输层提供对上层透明(不依赖于具体网络)的端到端的可靠的数据传输。
  - 传输层信息安全保护是网络系统信息安全保护的重要组成部分，主要应采用身份验证、访问控制、加密等方法来确保所传送的数据受到应有的保密性和完整性保护，防止其受到非授权的泄露或破坏。

2、OSI安全参考模型——安全服务的分层部署与实现

- 会话层安全服务
  - 会话层在应用程序间建立、管理和终止通信应用服务请求和响应等会话。
  - 会话层主要安全保护是采用交换鉴别、访问控制等办法来确保所传送的数据应有的保密性和完整性保护。

2、OSI安全参考模型——安全服务的分层部署与实现

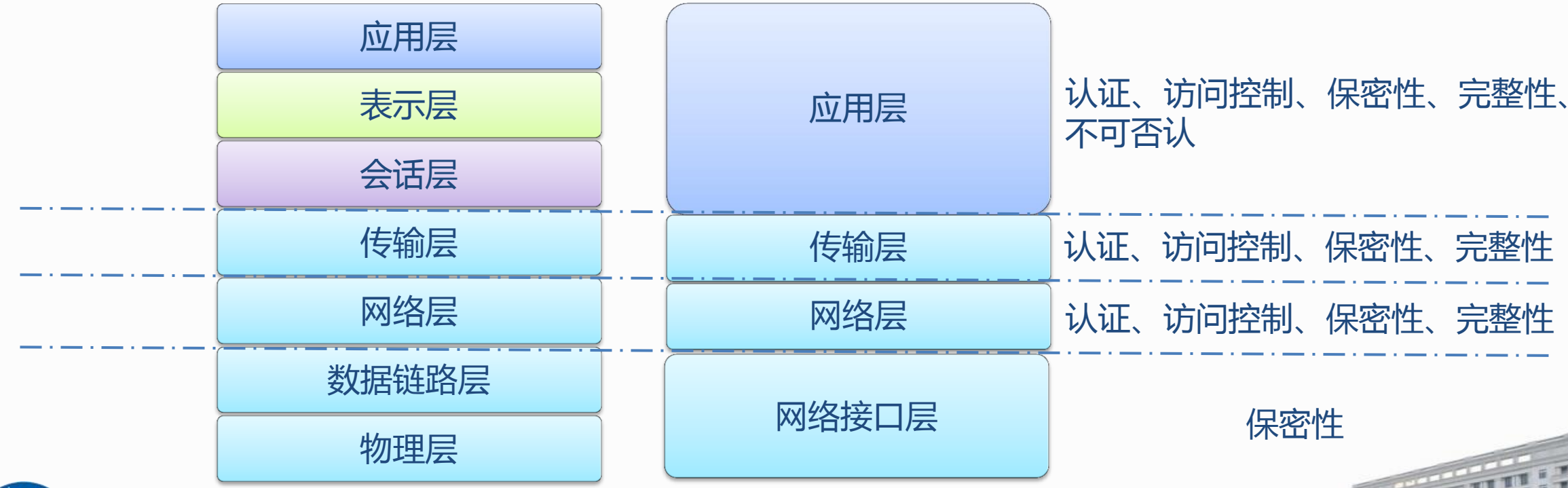
- 表示层安全服务
  - 表示层定义了一系列代码和代码转换功能，以保证源端数据在目的端同样能被识别，如大部分PC机使用的ASCII码，表示图像的GIF或表示动画的MPEG等。
  - 表示层的主要安全保护是交换鉴别、访问控制、保密性、完整性和禁止否认等，可采用多种技术(如SSL等)对来自外部的访问要求进行控制。

2、OSI安全参考模型——安全服务的分层部署与实现

- 应用层安全服务
  - 应用层提供应用进程访问网络服务的窗口，负责应用程序间的通信。这一层直接为网络用户或应用程序提供各种各样的网络服务，如Web服务、文件传送、电子邮件、远程登录等，通过软件应用实现网络与用户的直接对话，是计算机网络与最终用户间的界面。
  - 应用层除了保证主机安全之外，还要采取身份验证、加密等手段增强应用平台的安全。

2、OSI安全参考模型——安全服务的分层部署与实现

- OSI安全模型与TCP/IP安全模型的对应关系



2、OSI安全参考模型——安全服务的分层部署与实现

- 应用层提供安全服务
  - 只能在通信两端的主机系统上实施。

优点：

- 对数据的实际含义有着充分的理解
- 不必依赖操作系统来提供这些服务
- 对用户想要保护的数据具有完整的访问权，因而能很方便地提供一些服务
- 安全策略和措施通常是基于用户制定的

缺点：

- 改动太多，出现错误的概率大增，为系统带来更多的安全漏洞
- 对现有系统的兼容性太差
- 效率太低

2、OSI安全参考模型——安全服务的分层部署与实现

- 传输层提供安全服务
  - 只能在通信两端的主机系统上实施。

优点：

- 现有的和未来的应用可以很方便地得到安全服务
- 提供了更加细化的基于进程对进程的安全服务
- 能为其上的各种应用提供安全服务

缺点：

- 由于传输层很难获取关于每个用户的背景数据，实施时通常假定只有一个用户使用系统，所以很难满足针对每个用户的安全需求

2、OSI安全参考模型——安全服务的分层部署与实现

- 网络层提供安全服务
  - 在端系统和路由器上都可以实现。

优点：

密钥协商的开销小
- 由于多种传送协议和应用程序可共享由网络层提供的密钥管理架构，密钥协商的开销大大降低

网络层支持以子网为基础的安全
- 子网可采用物理分段或逻辑分段，因而可很容易实现VPN和内联网，防止对网络资源的非法访问

主要优点是透明性
- 能提供主机对主机的安全服务，不要求传输层和应用层做改动，也不必为每个应用设计自己的安全机制；

缺点：

无法实现针对用户和用户数据语义上的安全控制

2、OSI安全参考模型——安全服务的分层部署与实现

- 链路层提供安全服务
  - 只能在链路的两端实现。

优点：

整个分组（包括分组头信息）都被加密，保密性强

缺点：

使用范围有限

- 只有在专用链路上才能很好地工作，中间不能有转接点

测试点1-2

- 什么是安全服务？什么是安全机制？常见的安全服务与安全机制有哪些？
- 安全服务和安全机制的关系是什么？
- 简要说明在应用层、网络层、传输层和链路层部署安全服务的优缺点？

3、网络安全理论与技术体系

应用理论层

技术理论层

基础理论层

4、网络安全技术发展方向

- 核心基础理论突破及基于密码学的数据保护技术

  以量子密码、DNA密码、混沌密码等基础研究为代表的新一代理论研究

- 与新技术深度融合
  - 与以人工智能技术为代表的信息技术进行深度融合，如智能化入侵检测。
- 满足先进计算环境的安全需求
  - 物联网、云计算、大数据等先进计算环境下的安全技术研究
- 传统安全技术的增强
  - 如应对APT攻击的网络态势感知技术研究

结束语

感 谢 聆 听!

ruijinwang@uestc.edu.cn