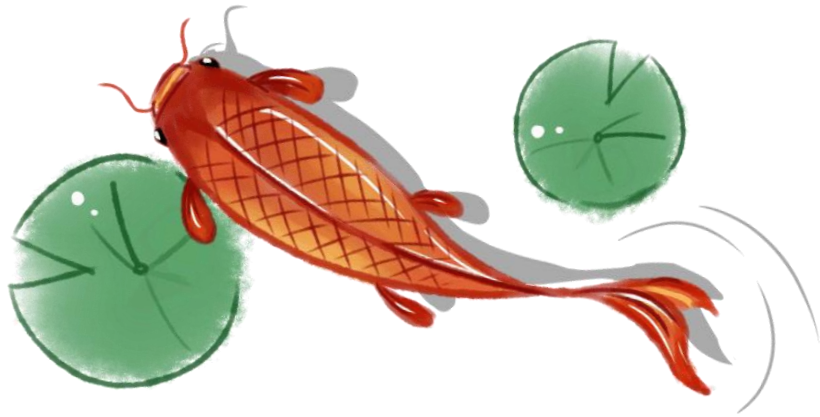
计算机网络安全技术

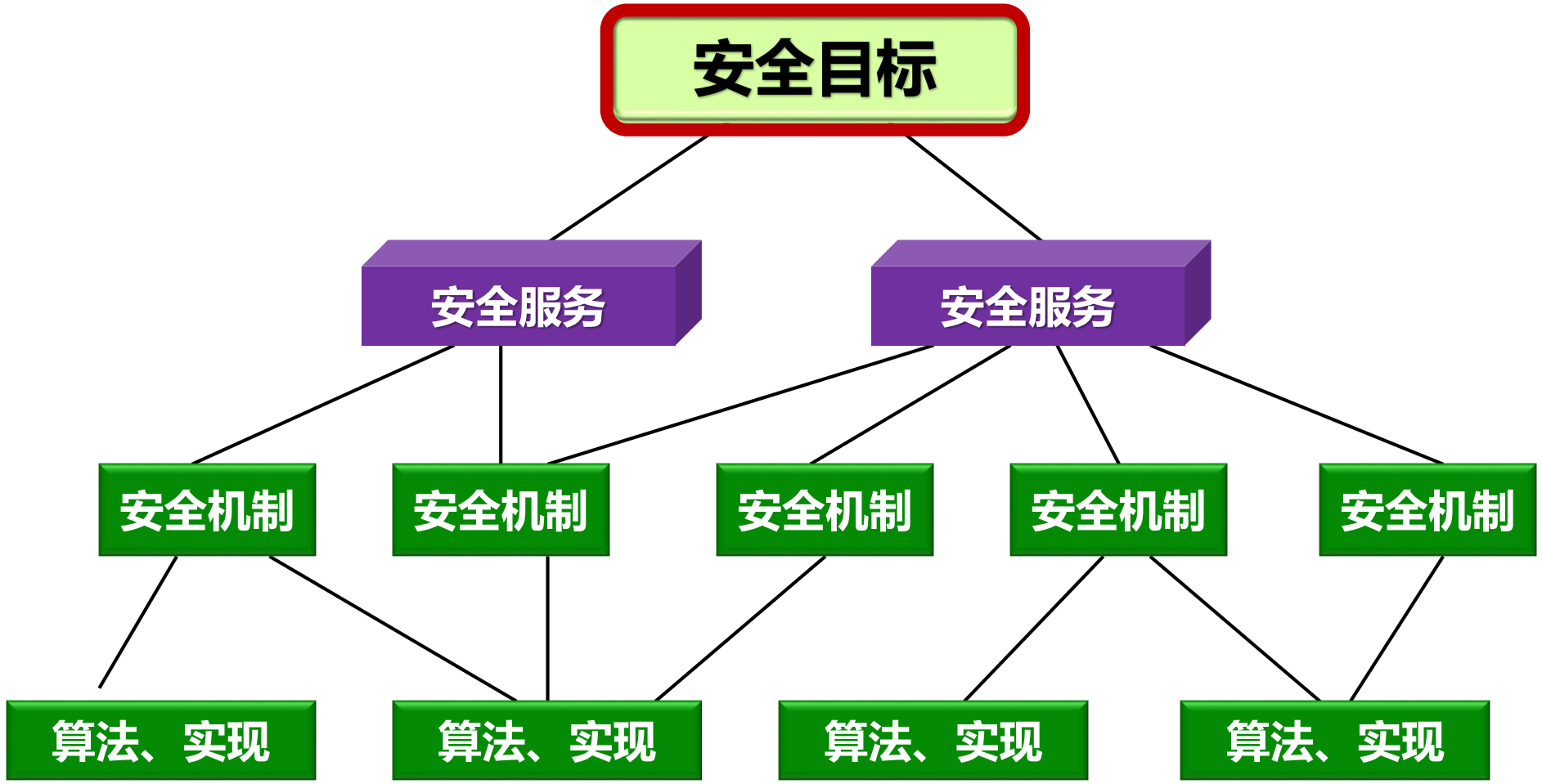
- 课程代号：*40240572*
- 课程对象：本科生
- 授课教师：尹　霞
- 开课单位：计算机系网络所

计算机网络安全体系结构

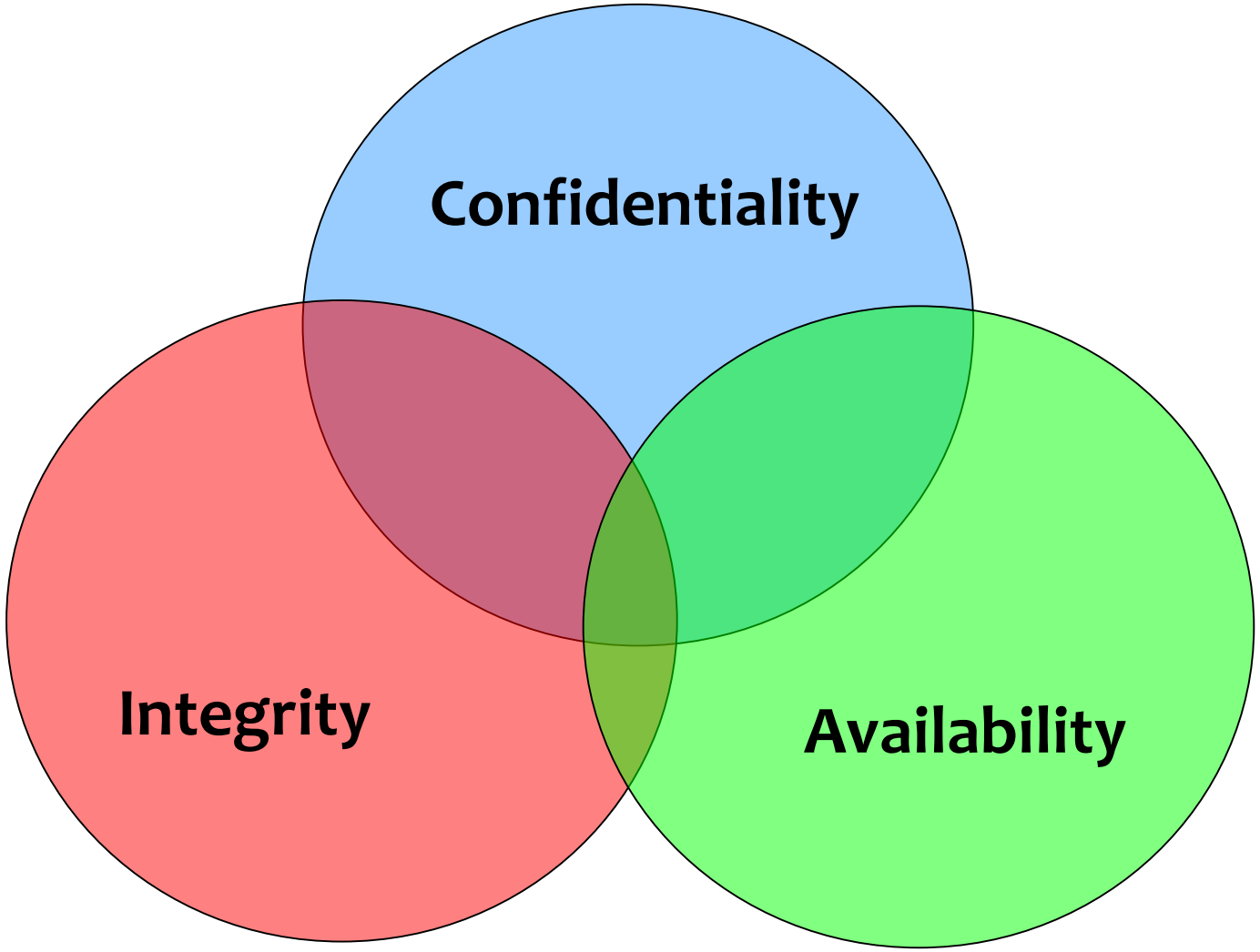
- 安全目标/安全服务/安全机制



安全目标、服务、机制的关系



安全目标： CIA



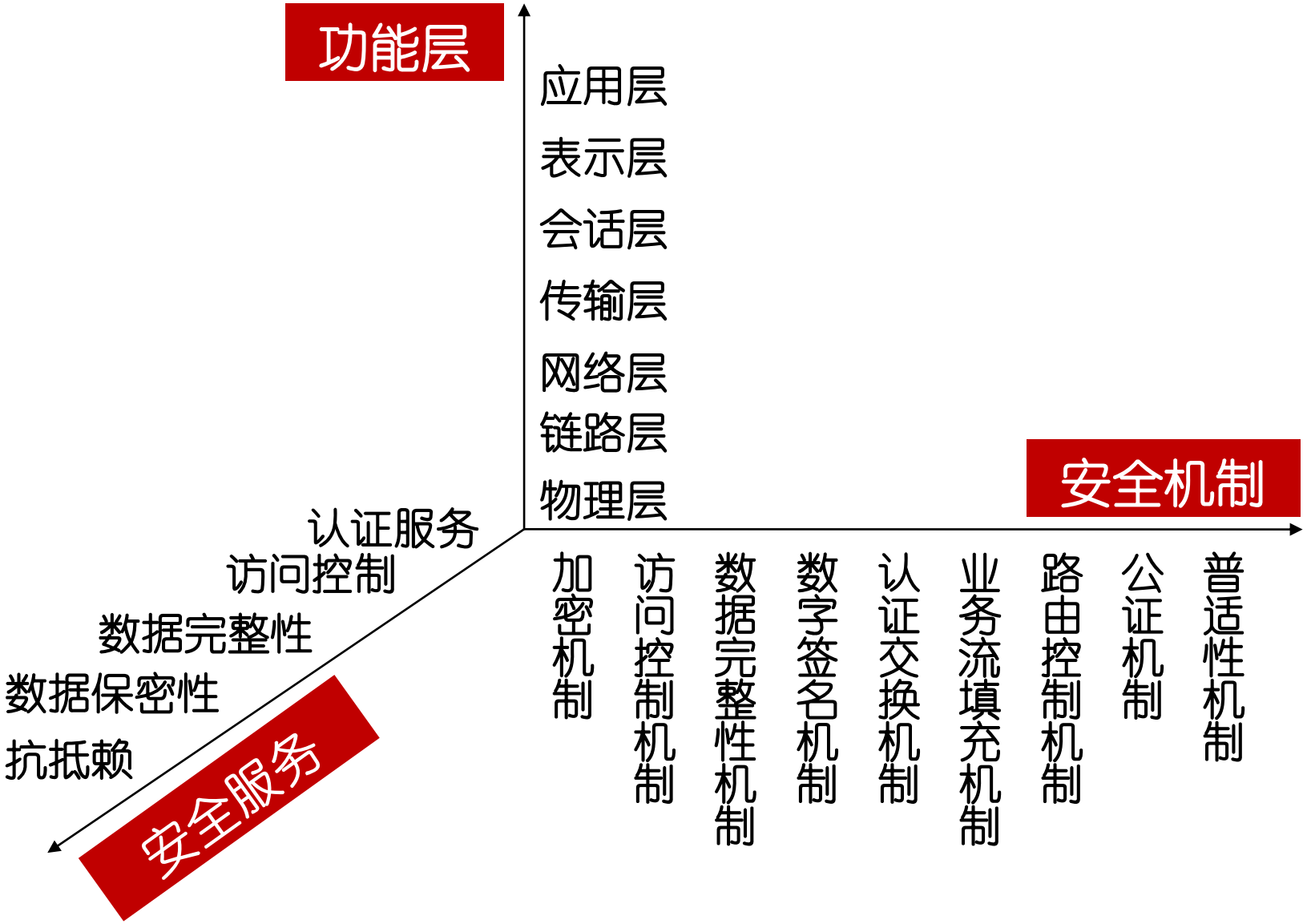
安全目标： CIA

- Confidentiality：保密性、机密性
  - 保护信息内容不会被泄露给未授权的实体
  - 业务数据、网络拓扑、流量都可能有保密性要求；防止被动攻击
- Integrity：完整性
  - 保证信息不被未授权地修改，或者如果被修改可以检测出来
  - 防止主动攻击，比如篡改、插入、重放
- Availability：可用性
  - 保证资源的授权用户能够访问到应得的资源或服务，防止拒绝服务攻击
  - 对信息系统可用性的攻击
  - 对路由设备的处理能力、缓冲区、链路带宽等的攻击

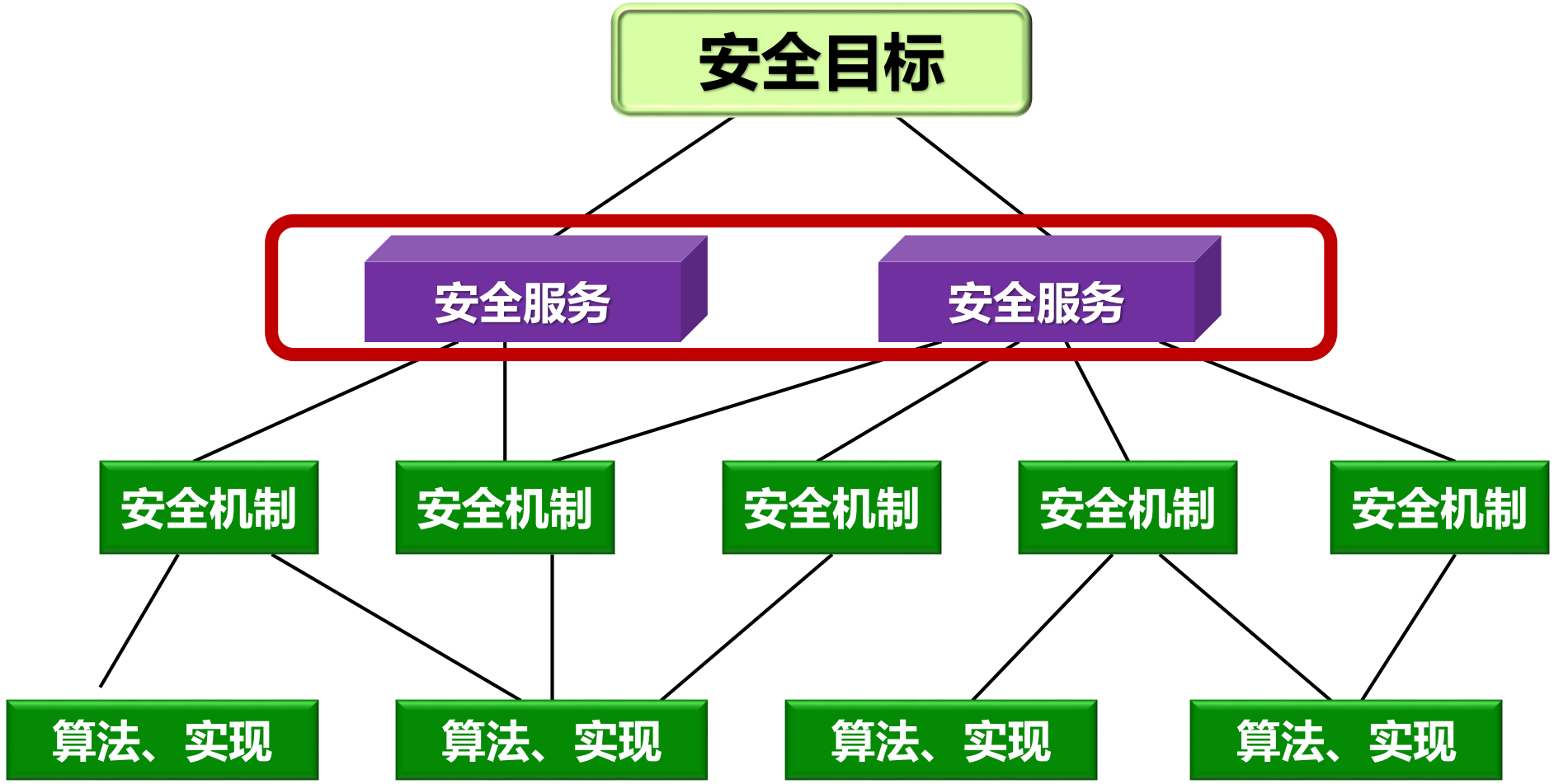
OSI安全框架

- ITU-T推荐方案X.800，即OSI安全框架，定义了一种系统方法，为网络管理员提供了一种安全的组织方法
- OSI安全框架主要关注安全服务、安全机制和安全攻击
  - 安全服务：
    - 一种由系统提供的对系统自愿进行特殊的处理或通信服务，安全服务通过安全机制来实现安全策略 (RFC 2828)
  - 安全机制：
    - 用来保护系统免受监听、阻止安全攻击及恢复系统的机制
  - 安全攻击：
    - 主动攻击、被动攻击

OSI安全体系结构


功能层
应用层
表示层
会话层
传输层
网络层
链路层
物理层
安全机制
普适性机制
公证机制
路由控制机制
业务流填充机制
认证交换机制
数字签名机制
数据完整性机制
访问控制机制
加密机制
安全服务
认证服务
访问控制
数据完整性
数据保密性
抗抵赖

安全目标、服务、机制的关系



安全服务

- X.800提供了下面一些的安全服务：
  - Authentication：　　认证服务
  - Confidentiality：　　保密服务
  - Integrity：　　数据完整性保护
  - Access Control：　　访问控制服务
  - Non-repudiation：　　抗抵赖服务
  - Availability：　　可用性服务

Authentication

- 认证服务Authentication与保证通信的真实性有关
- 在单条消息的情况下：
  - 认证服务向接受方保证发送方的真实性
- 在双方通信的时候：
  - 在连接的初始化阶段，认证服务保证双方的真实性
  - 认证服务还需要保证该连接不受第三方非法干扰：第三方能够伪装成两个实体中一个进行非授权的传输或者接收数据

Authentication

- 两个特殊的认证服务：
  - 对等实体认证（Peer Authentication）
    - 参与通信的实体的身份是真实的
    - 一个实体不能试图进行伪装或者对以前连接进行非授权的重放
    - 面向连接的应用
  - 数据源认证（Data original authentication）
    - 对数据的来源提供确认，但是对数据的复制和修改不提供保护
    - 保证接收到的信息的确来自它所宣称的来源
    - 面向无连接的应用

Confidentiality

- 保密服务Confidentiality是防止传输数据遭到被动攻击
  - 连接保密服务与无连接保密服务
  - 保密力度：流(stream)、消息(message)、选择字段(field)

- 保密服务的另一方面是防止流量分析
  - 防止攻击者观察到消息的源、目的、频率、长度或者其它流量特征

Integrity & Access Control

- 数据完整性服务Integrity：可对消息流、单条消息或消息的选定部分进行保护
  - 面向连接的完整性服务保证收到的消息和发出的消息一致
  - 面向无连接的完整性服务仅保证单条消息不被修改
  - 完整性服务与主动攻击有关，我们更关心的是检测而不是阻止攻击

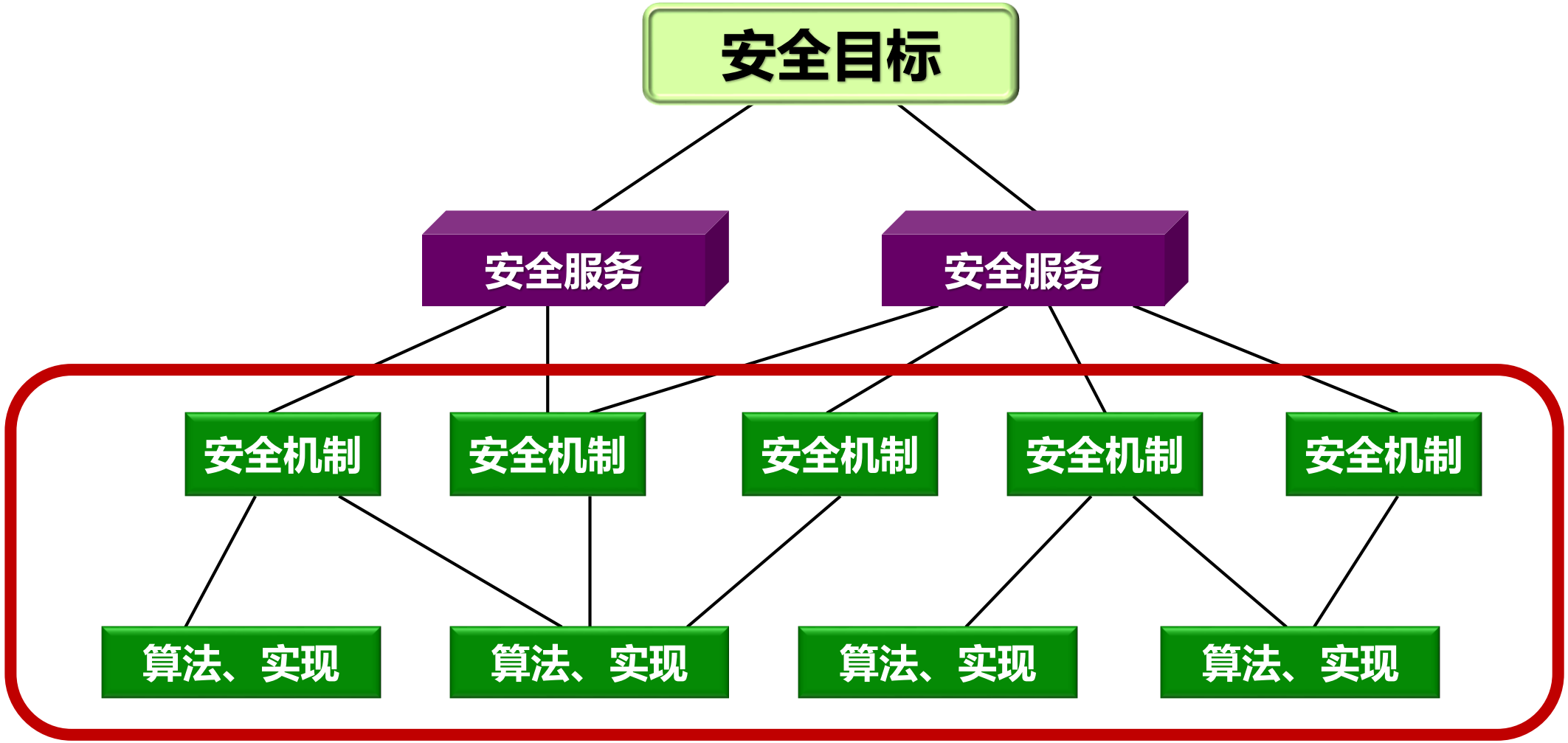
- 访问控制服务Access Control：是指限制实体的访问权限，通常是经过认证的合法的实体才可以访问；标识与认证是访问控制的前提

Non-repudiation & Availability

- 抗抵赖服务Non-repudiation：防止发送方或者接收方否认传输或者接收过某条消息
  - 源发抗抵赖：
    消息发出后，接收方能够证明消息是由声称的发送方发出的
  - 交付抗抵赖：
    消息接收后，发送方能够证明消息确实已经被接收方收到

- 可用性服务Availability：根据系统的性能说明，能够按照授权的系统实体的要求存取或使用系统或系统资源的性质

安全目标、服务、机制的关系



安全机制

- 安全机制分成两类：普通安全机制和特定安全机制
- 普通安全机制：
  - 不属于任何协议层或者安全服务的安全机制
- 特定安全机制：在特定的协议层实现的安全机制
  - 加密机制、通信业务流量填充机制
  - 访问控制机制、数据完整性机制
  - 认证交换机制、数字签名机制
  - 路由控制机制、公证机制

普通的安全机制

- 可信功能(trusted functions)
  - 根据某些标准被认为是正确的
- 安全标签(security Labels)
  - 资源的标志，指明该资源的安全属性
- 事件检测 (Event Detection)
  - 检测与安全相关的事件
- 审计跟踪 (security audit Trail)
  - 收集用于安全审计的数据，对系统记录和行为的独立回顾和检查
- 安全恢复 (security recovery)
  - 处理来自安全机制的请求，如事件处理、管理功能和采取恢复行为

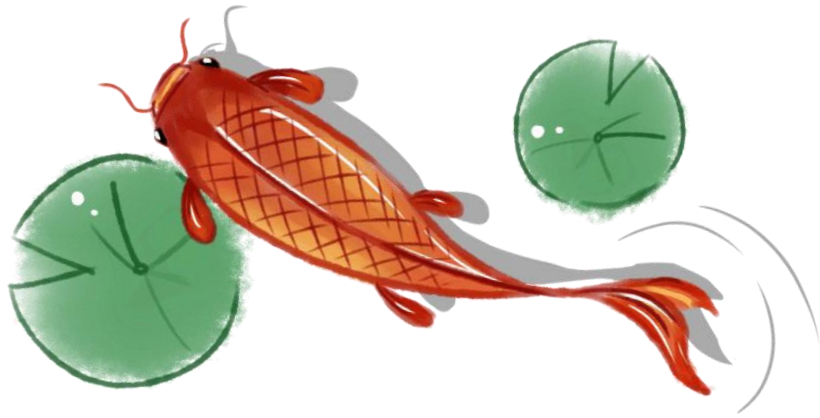
八种特定的安全机制

- 八种特定的安全机制包括
  - ① 加密机制
  - ② 数字签名机制
  - ③ 访问控制机制
  - ④ 数据完整性机制
  - ⑤ 认证机制
  - ⑥ 业务流填充机制
  - ⑦ 路由控制机制
  - ⑧ 公证机制

安全性攻击

- 安全性攻击分成两类。
  - 主动攻击：试图改变系统资源或者影响系统运行。
  - 被动攻击：试图了解或者利用系统的信息但不影响系统资源。
- 被动攻击对传输进行窃听和监测。
  - 窃听：Sniffer/ wiretapping/ Interception
  - 流量分析(Traffic analysis)：
    通过对通信业务流的观察
    (出现、消失、总量、方向与频度)，
    而推断出有用的信息，
    比如主机的位置，业务的变化等

虚拟专用网VPN



了解VPN，学习互联网安全协议

清华大学

登录服务

您现在使用的是校外IP，需通过VPN服务访问信息门户和校内资源，详细操作请参看VPN相关说明。

WebVPN登录入口

SSL VPN登录入口

VPN相关说明：

清华大学WebVPN使用说明
SSL VPN客户端安装使用说明（Win10及以上版本）
SSL VPN服务使用说明（WEB使用、Win8.1及以下版本客户端安装）
SSL VPN客户端安装演示视频（Windows 10及以上版本）
SSL VPN客户端安装演示视频（for MAC）
SSL VPN客户端安装配置使用说明（for MAC）

SSL VPN客户端程序：

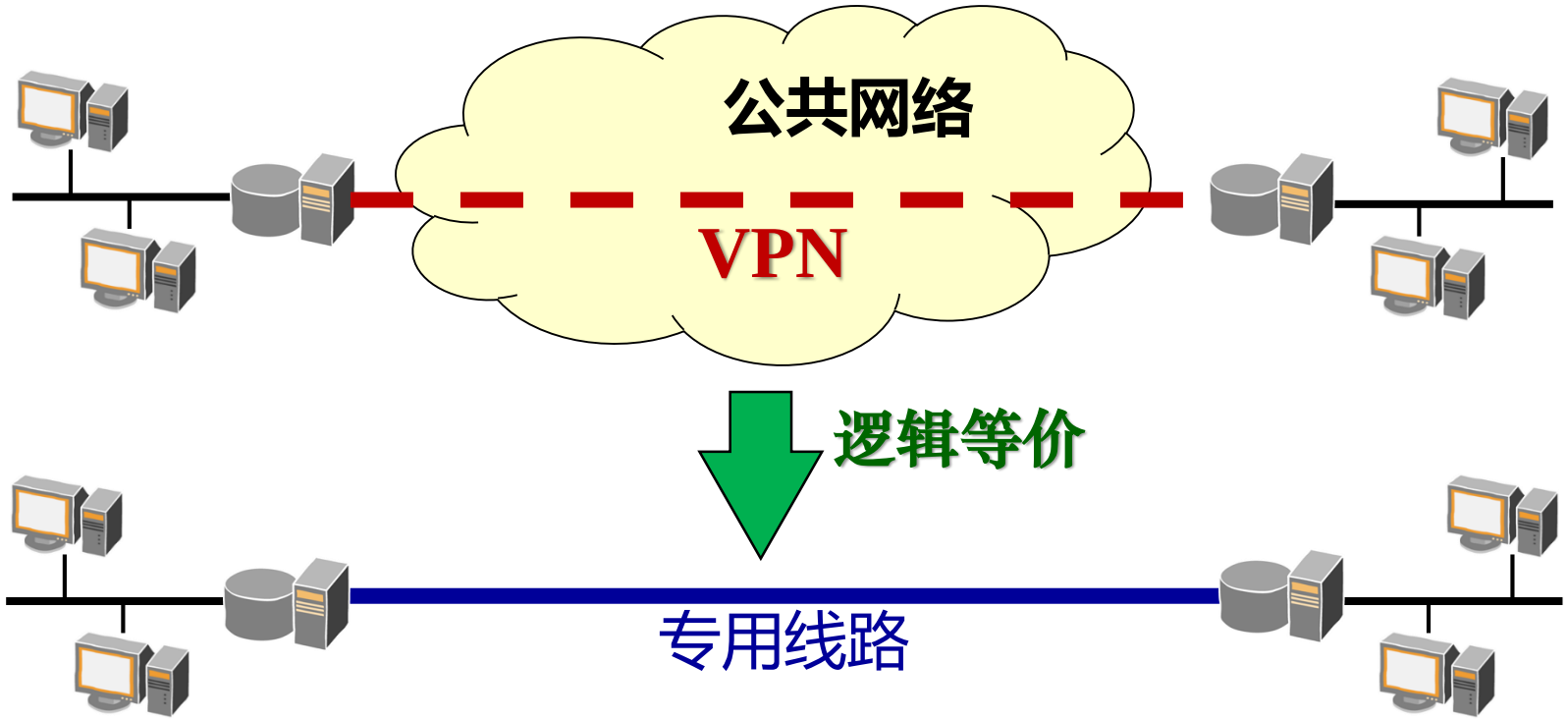
for Windows 10及以上版本
for MAC
for Linux
版本及对应文件说明

VPN的需求背景

- TCP/IP协议在设计之初是基于可信环境的，根本没有考虑安全问题，所以TCP/IP协议簇本身存在许多固有的安全缺陷
  - 攻击者可以方便地通过软件设置IP地址、监听数据包并篡改内容、同一数据包重放攻击
  - IP协议支持源路由方式，即源发方可以通过制定信息包传到目的节点的中间路由，为源路由攻击埋下隐患
  - TCP/IP协议实现中也存在一些安全缺陷和漏洞，如序列号容易被猜测，参数不检查导致缓冲区溢出等
- 租用专线或拨号网络等传统方式的物理专用网价格高昂、架设实施难度大；同时，企业/组织/商家等对高性能、高速度和高安全的专用网需求越来越强烈，VPN成为最佳解决方案

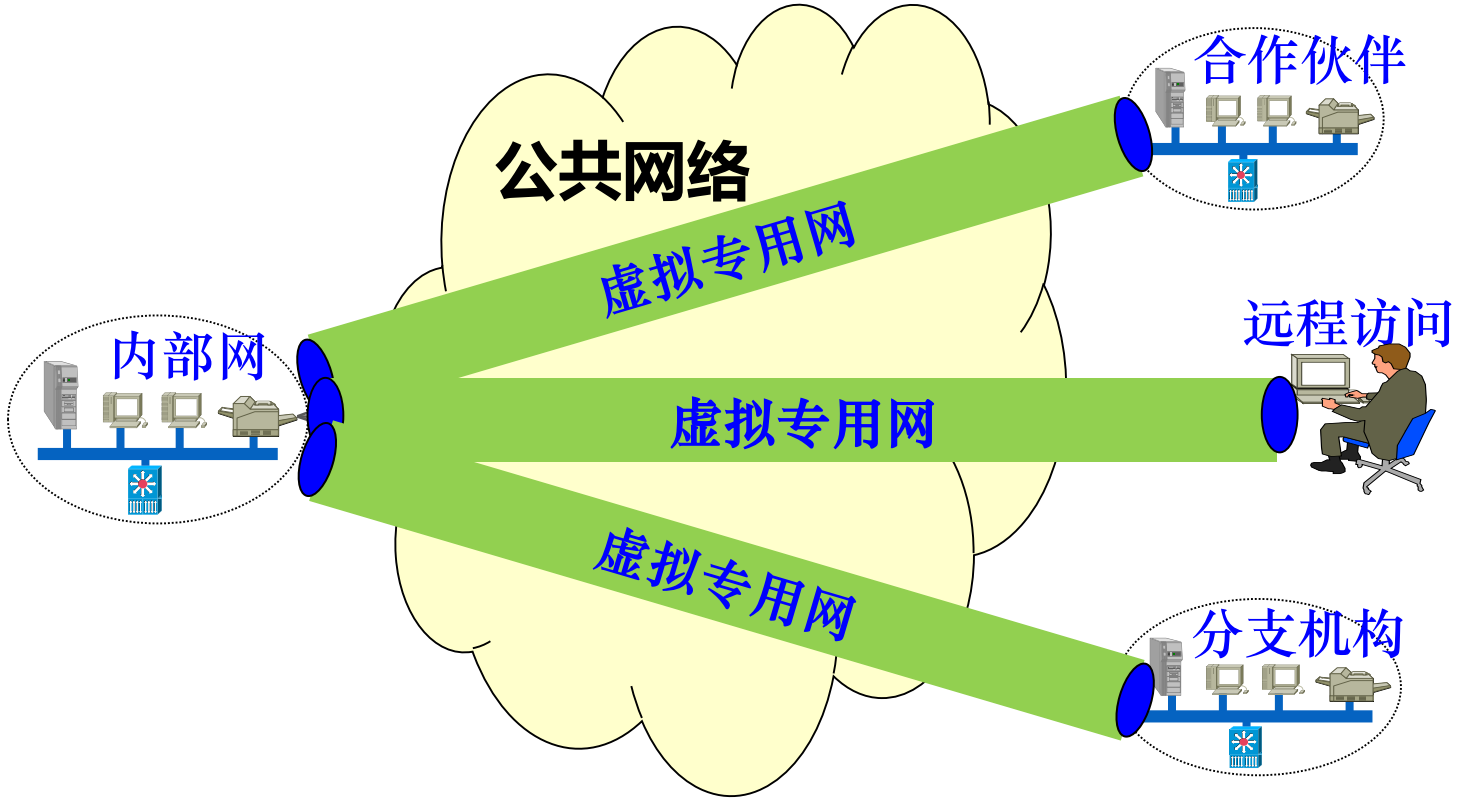
VPN的定义

- VPN - - Virtual Private Network，虚拟专用网
  - 所谓“虚拟”是指用户不再需要拥有实际的长途数据线路，而是使用公众网络的长途数据线路
  - 所谓“专用”是指用户可以为自己制定一个最符合自己需求的网络



VPN是企业网在互联网等公共网络上的延伸

- VPN通过一个私有的通道在公共网络上仿真一条点到点的私有连接，将远程用户、公司分支机构、公司的业务伙伴等跟企业网连接起来，形成一个扩展的公司企业网



- 在虚拟专用网中，任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是利用某种公众网的资源动态组成

VPN提供的安全功能

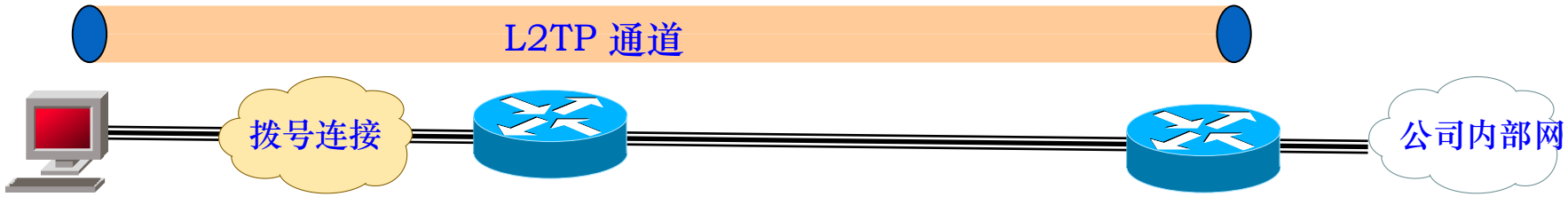
- 数据机密性保护
- 数据完整性保护
- 数据源身份认证
- 重放攻击保护

VPN的解决方案

- 基于数据链路层的VPN解决方案
  - L2TP：Lay 2 Tunneling Protocol
  - PPTP：Point-to-Point Tunneling Protocol
  - L2F：Lay 2 Forwarding
- 基于网络层的VPN解决方案
  - IPsec/IKE
- 基于传输层的VPN解决方案
  - SSL

基于数据链路层的VPN解决方案

- 由于数据链路层的VPN技术在认证、数据完整性以及密钥管理等方面的不足，现在已经很少应用

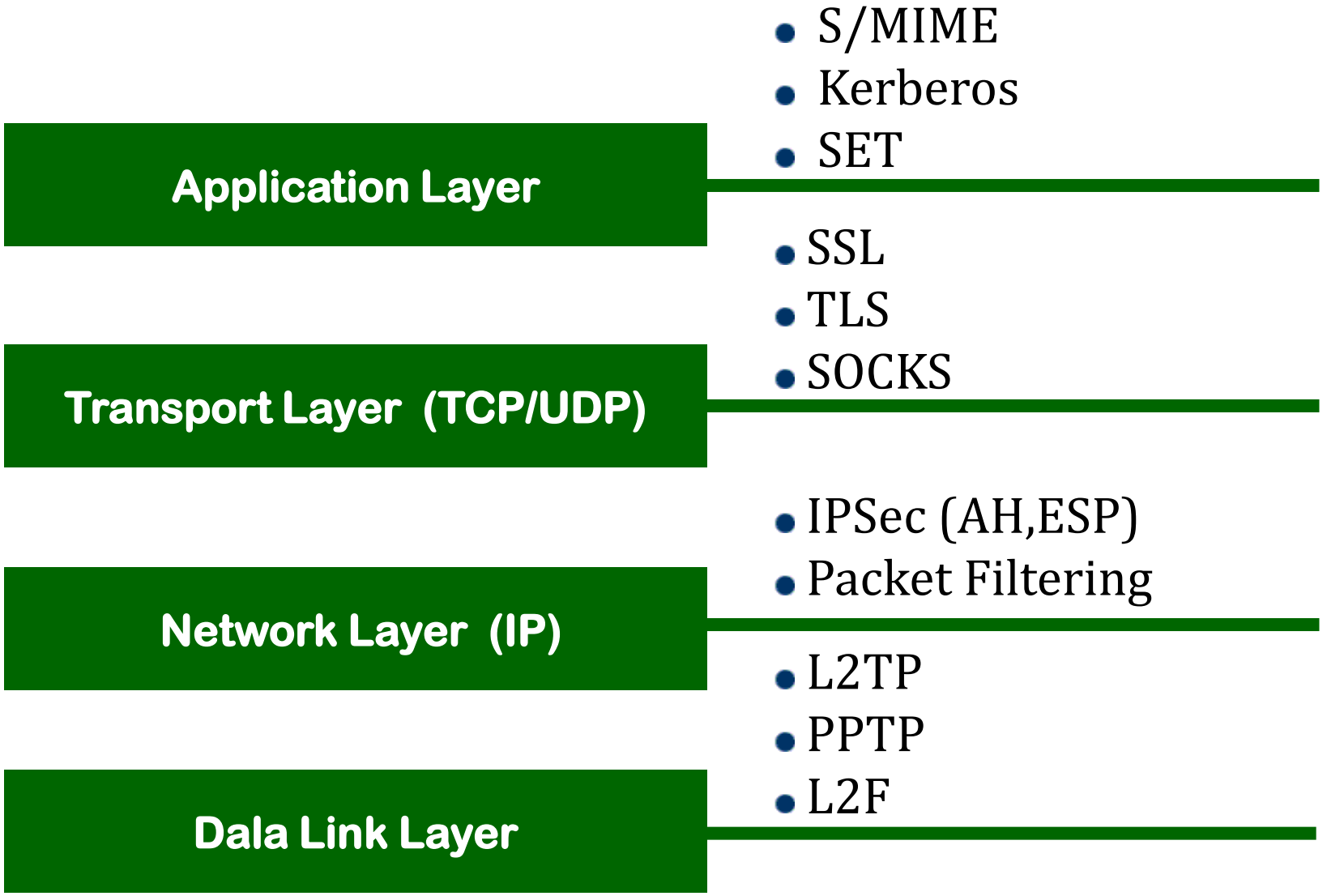


- L2TP的缺陷：
  - 仅对通道的终端实体进行身份认证，而不认证通道中流过的每一个数据报文，无法抵抗插入攻击、地址欺骗攻击
  - 没有针对每个数据报文的完整性校验，就有可能进行拒绝服务攻击：发送假冒的控制信息，导致L2TP通道或者底层PPP连接的关闭
  - 虽然PPP报文可以加密，但PPP不支持密钥的自动产生和自动刷新，因此攻击者就可能最终破解密钥，从而得到明文

基于传输层的VPN解决方案

- 基于传输层SSL协议的VPN解决方案，零客户端是其最大优势；SSL VPN可以适用于任何基于B/S结构的应用
- 在实际应用中，SSL VPN和IPsec VPN两种方案往往结合实行，SSL VPN网关和IPSEC网关有时也被集成到一个设备内
- SSL的低成本优势使得它迅速的得到了应用，但象视频会议这样的非B/S结构的业务是无法通过SSL VPN建立和开展的

TCP/IP 协议栈与对应的VPN协议



互联网安全协议

网络层安全协议

- **IPsec**：IP+安全
- **IKE**：IPsec管理密钥

传输层安全协议

- **SSL**：为应用层服务

应用层安全协议

- **HTTPS**：HTTP+SSL
- **S/MIME**：安全电子邮件
- **SET**：安全电子交易

Thanks a lot !

Activity is the only road to knowledge!

Computer Network Security @ 2022Fall