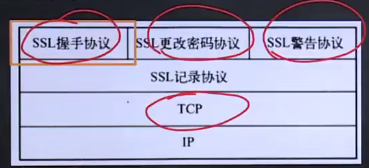
网络安全协议

1. 安全电子邮件
2. 电子邮件安全需求
   1. 机密性
   2. 完整性
   3. 身份认证性
   4. 抗抵赖性
3. 安全电子邮件标准：PGP（加密、公钥、数字签名技术）
4. 安全套接字SSL
5. SSL是介于应用层和传输层之间的安全协议
6. SSL协议栈
7. SSL握手过程：协商密码组，生成密钥，服务器/客户认证与界鉴别
8. 虚拟专用网VPN和IP安全协议IPSec
9. VPN：建立在公共网络上的安全通道，实现远程用户、分支机构、业务伙伴等与机构总部网络的安全连接，从而构建针对特定组织机构的专用网络。关键技术：隧道技术（加密你的信息），如IPSec
10. 典型的网络层安全协议——IPSec：提供机密性、身份鉴别、数据完整性和防重放攻击服务。

体系结构：认证头AH协议、封装安全载荷ESP协议（两个可选择）。

运行模式：传输模式（AH传输模式、ESP传输模式）

隧道模式（AH隧道模式、ESP隧道模式）

本章小结

1. 本章介绍了网络安全基本概念、数据加密算法、消息完整性与数字签名、身份认证、密钥分发中心与证书认证机构、防火墙与入侵检测以及网络安全协议等内容
2. 本章重难点回顾：
   1. 网络安全基本属性
   2. 典型数据加密算法
   3. 消息完整性、数字签名以及身份认证原理