石家莊鐵道大學
SHIJIAZHUANG TIEDAO UNIVERSITY

网络精品课程

大学计算机应用基础

第7章 计算机网络基础

计算机网络安全基础

主讲 ： 王书海

目录

计算机网络安全概述

- 网络的发展日新月异，网络技术更新速度惊人，针对网络漏洞的攻击和威胁花样翻新层出不穷，网络入侵的方式和手段也越来越多。
- 什么是网络安全
  - 是指网络系统的硬件、软件及其系统中的数据处于安全状态，不会由于偶然或者恶意的原因而遭到破坏、更改或者泄漏，系统能够连续稳定地提供网络服务。
  - 网络安全的本质就是在信息的安全期内保证数据在网络上传输时或者存储时不被非法访问和修改。
- 网络安全主要分为：
  - 系统安全、信息安全、传输安全

计算机网络安全概述

- 系统安全
  - 系统安全侧重于研究如何保证系统正常地运行，怎样避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏。
  - 主要包括：
    - 保护存放计算机硬件系统的机房稳定牢固；
    - 保障计算机的软、硬件体系结构不被破坏；
    - 保障硬件系统的可靠安全运行，维护计算机操作系统和应用软件的完整；
    - 保证数据库系统的安全，同时控制各种电磁辐射防止信息泄露的防护等。

计算机网络安全概述

- 信息安全
  - 主要侧重于研究如何保证信息的机密性、真实性和完整性。
  - 目标是：
    - 即使攻击者利用系统的安全漏洞通过窃取、监听、诈骗等手段获得了信息，也无法破解其中的内容并加以利用。

计算机网络安全概述

- 传输安全
  - 研究如何建立安全的信息传输路径，怎样保证传输过程中的数据不被窃取或监听，同时考虑如何防止和控制非法、有害的信息的传播。
  - 传输安全实质就是协议安全（如Ipsec、VPN、SSL等）。

信息加密技术

- 加密技术是最常用的安全保密手段，也是实现信息安全的基础。
- 利用技术手段把重要的数据变为乱码（加密）传送，到达目的地后再用相同或不同的手段还原（解密）。

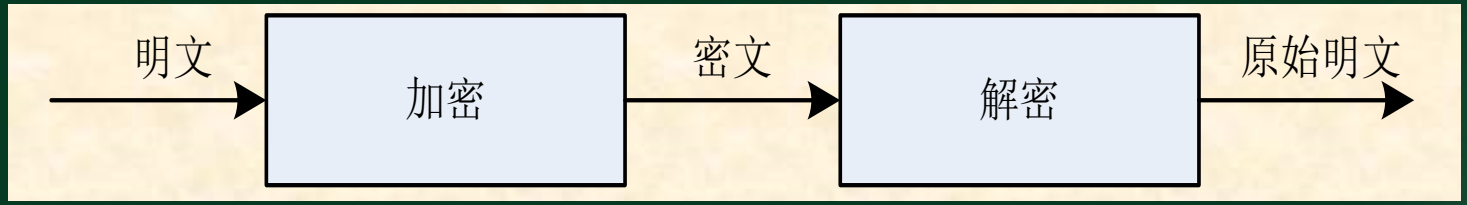
信息加密技术

- 基本概念：
  - 明文：具有明确含义且不用解密便可理解的文本或信号。
  - 密文：经过加密算法把明文变换得到的不可懂的符号。
  - 加密：将明文经过加密密钥和加密算法转换，变成不可理解的密文的过程。
  - 解密：用适当密钥，将密文转换为明文的过程。
  - 密钥：密码学中，一系列控制加密、解密操作的字符。
  - 加密算法：将明文与密钥结合，产生不可理解的密文的步骤

信息加密技术

- 明文用M（消息）或P（明文）表示，密文用C表示。
- 加密函数E（M）=C；
- 解密函数D（C）=M；D（E（M））=M。

- 加解密过程



信息加密技术

- 根据加密时采用的算法不同，可将加密技术分为对称加密和非对称加密。
- 对称加密算法：
  - 加密和解密使用相同密钥的加密算法。
  - 其特点是：速度快，但密钥管理复杂，不适用于大用户量的应用，常用于快速的加密/解密。
  - 常用的对称加密算法有：DES、3-DES、SSF33、IDEA、AES等

信息加密技术

- 非对称加密算法：
  - 非对称加密算法也称公开密钥算法，
  - 加解密思想是：
    - 用户A拥有两个对应的密钥，其中一个用于加密，另一个用于解密，两者一一对应。用户A将其中一个私下保存（私钥），另一个公开发布（公钥）。
    - 如果B想送秘密信息给A，B获得A的公钥，并使用该公钥加密信息发送给A，A使用自己的私钥便可解密信息。
  - 非对称加密的特点是：效率较慢，不适用于大量的数据加密，但公钥可以公开、分布式存放，便于管理。常用于数据加密、数字签名、密钥交换等。
  - 常用的非对称加密算法有：RSA、ECC、Diffie-Hellman、DSA

信息加密技术

- 组合密码技术
  - 由于对称加密算法和非对称加密算法都有自身的优缺点，在实际应用中，常将这两种算法结合使用，形成组合密码技术。
  - 其主体思想是：使用非对称加密算法加密并传递对称加密时需要的密钥，使用对称加密算法进行大批量的数据加密。
  - 这样既解决了对称加密的密钥管理问题，又解决了非对称加密的效率问题。

身份认证技术

- 在网络上如何证明“我是谁？” 如何知道“你是谁？”这些就是身份认证技术要解决的问题。
- 目前，计算机及网络系统中常用的身份认证方式主要有以下几种：
  - 用户名/密码方式、智能卡认证、USB Key认证、生物识别技术

用户名/密码方式

- 用户名/密码是最简单也是最常用的身份认证方法。
- 存在问题：
  - 密码太简单，容易被猜
  - 密码传输时容易被截获
- 方便但不安全、仍广泛采用

智能卡认证

- 智能卡是一种内置集成电路的芯片，芯片中存有与用户身份相关的数据。
- 登录时将智能卡插入专用的读卡器读取其中的信息，以验证用户的身份。
- 通过智能卡硬件不可复制来保证用户身份不会被仿冒。
- 由于每次从智能卡中读取的数据是静态的，通过内存扫描或网络监听等技术还是很容易截取到用户的身份验证信息，因此还是存在安全隐患。

动态口令

- 动态口令技术是一种让用户密码按照时间或使用次数不断变化，每个密码只能使用一次的技术。
- 用户每次使用的密码都不相同，即使黑客截获了一次密码，也无法利用这个密码来仿冒合法用户的身份

USB Key认证

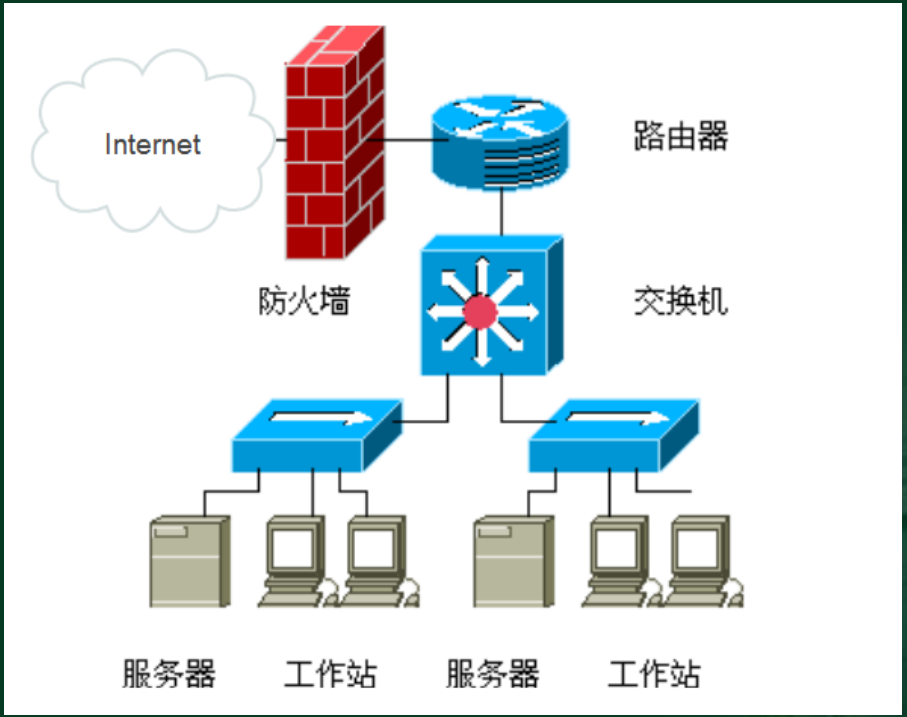
- 基于USB Key的身份认证方式是近几年发展起来的一种方便、安全的身份认证技术。
- 它采用软硬件相结合、一次一密的强双因子认证模式，很好地解决了安全性与易用性之间的矛盾。
- USB Key是一种USB接口的硬件设备，它内置单片机或智能卡芯片，可以存储用户的密钥或数字证书，利用USB Key内置的密码算法实现对用户身份的认证。

生物特征识别技术

- 生物特征识别技术主要是指通过可测量的身体或行为等生物特征进行身份认证的一种技术。
- 生物特征分为身体特征和行为特征两类。
  - 身体特征包括：指纹、掌型、视网膜、虹膜、人体气味、脸型、手的血管和DNA等；
  - 行为特征包括：签名、语音、行走步态等。
- 采用生物识别技术，可不必再记忆和设置密码，使用更加方便。

防火墙技术

- 在网络连接之间建立一个安全的控制点，实现对进、出内部网络的服务和访问的审计和控制。



防火墙技术

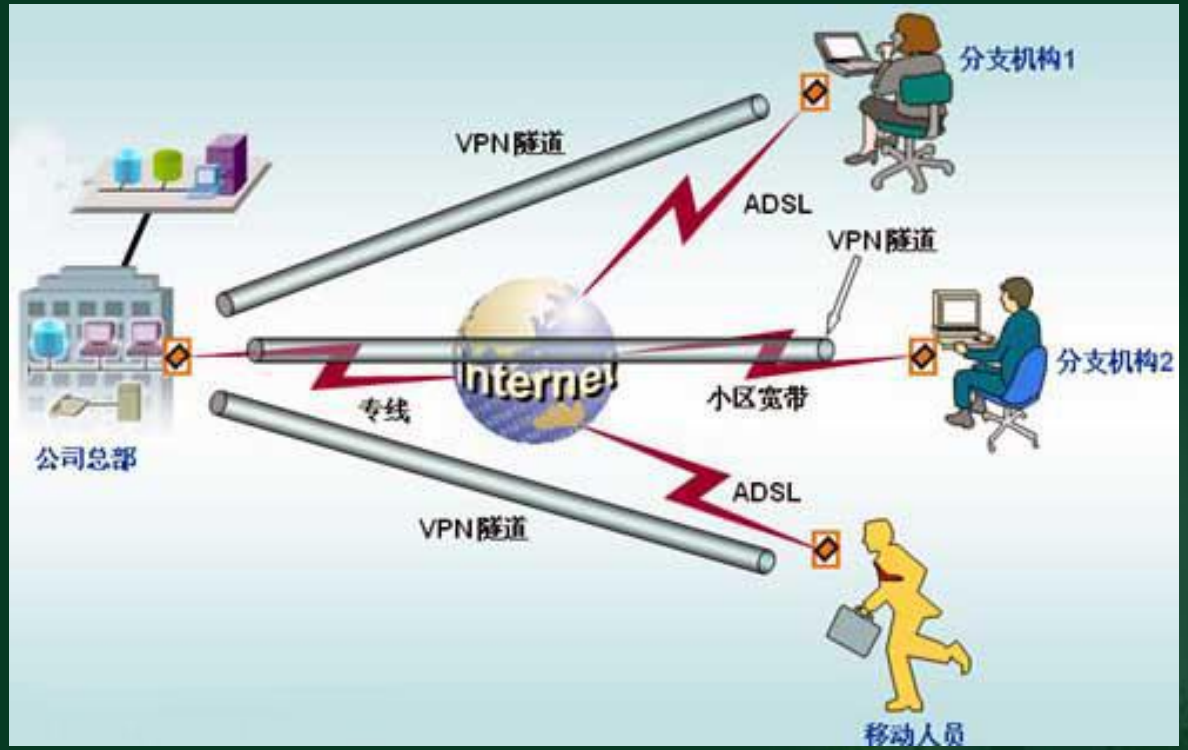
- 防火墙的主要功能
  - 实现了网段之间的隔离或控制；
  - 记录与 Internet 之间的通信活动；
  - 强化了安全访问策略；
  - 提供一个安全策略的检查站；
  - 实现了数据包的过滤；
  - 网络地址翻译。

防火墙技术

- 网络防火墙功能的局限
  - 不能防备全部威胁；
  - 一般没有配置防病毒的功能；
  - 不能防范不通过它的连接；
  - 不能完全防范内外部恶意的知情者；

VPN技术

- 虚拟专用网(VPN, Virtual Private Network)
  - 就是通过一个公用网络建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。



VPN技术

- 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Internet公众数据网络的长途数据线路。
- 所谓专用网络，是指用户可以为自己制定一个最符合自己需求的网络。
- 针对不同的用户要求，VPN有三种解决方案：
  - 远程访问虚拟网（Access VPN）、
  - 企业内部虚拟网（Intranet VPN）
  - 企业扩展虚拟网（Extranet VPN）

VPN技术

- VPN的核心技术是隧道技术。
- 隧道是利用一种协议传输另一种协议的技术
- 封装是构建隧道的基本手段，它使得IP隧道实现了信息隐蔽和抽象。
- 隧道技术包括数据封装、传输和解包在内的全过程。
- 实现VPN的隧道协议有：PPTP、L2F、L2TP、IPSec、SSL、MPLS等。

网络黑客

- 网络黑客(Hacker)一般指的是计算机网络的非法入侵者。
- 一般黑客的攻击分为：信息收集、探测分析系统的安全弱点、实施攻击三个步骤。
- 黑客一般会实施以下的攻击：
  - 毁掉入侵痕迹、建立新的安全漏洞或后门
  - 安装探测器软件，继续收集信息
  - 发现目标系统的信任等级，以展开对整个系统攻击。

网络黑客

- 黑客的攻击方式
  - 密码破解
  - IP嗅探与欺骗
  - 系统漏洞
  - 端口扫描

网络黑客

- 防止黑客攻击的策略主要有：数据加密、身份认证、建立完善的访问控制策略、审计等
- 如何预防黑客攻击？
  - 不随便从Internet上下载软件，不运行来历不明的软件，不随便打开陌生人发来的邮件中的附件，经常运行专门的反黑客软件，可以在系统中安装具有实时检测、拦截和查找黑客攻击程序用的工具软件，经常检查用户的系统注册表和系统启动文件中的自启动程序项是否有异常，做好系统的数据备份工作，及时安装系统的补丁程序等等可以提高防止黑客攻击的能力。

习题讲解

- 在计算机及网络系统中，不属于常用的身份认证方式是____。
  - A. 用户名/密码方式
  - B. 智能卡认证
  - C. 生物识别技术
  - D. 电子签名

习题讲解

- 一般防火墙不具备的功能是____。
  - A. 数据包过滤
  - B. 网络地址转换
  - C. 应用级代理
  - D. 防病毒

习题讲解

- 关于入侵检测，不正确的说法是____。
  - A. 入侵检测是对网络入侵行为的检测
  - B. 入侵检测系统可分为误用检测和异常检测两种
  - C. 入侵检测作为一种积极主动的安全防护技术，能提供对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前能拦截和响应所有入侵
  - D. 入侵检测系统（IDS）的发展方向是入侵防御系统（IPS）

习题讲解

- 关于VPN，不正确的说法是____。
  - A. 虚拟专用网(VPN，Virtual Private Network)就是通过一个公用网络建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道
  - B. VPN的核心技术是隧道技术。
  - C. 实现VPN的隧道协议有：PPTP、DNS、FTP、TCP/IP、SSL、MPLS 等
  - D. 针对不同的用户要求，VPN有三种解决方案：远程访问虚拟网（Access VPN）、企业内部虚拟网（Intranet VPN）和企业扩展虚拟网（Extranet VPN）

习题讲解

- 关于黑客的叙述，不正确的是_____。
  - A. 所谓黑客，就是利用计算机技术、网络技术，非法侵入、干扰、破坏他人计算机系统，或擅自操作、使用、窃取他人的计算机信息资源，对电子信息交流和网络实体安全具有程度不同的威胁性和危害性的人
  - B. 黑客分类的方法很多，从黑客的动机和目的，以及对社会造成的危害程度来分类，可以分成技术挑战性黑客、戏谑取趣性黑客和捣乱破坏性黑客三种类型
  - C. 制作、传播计算机病毒等破坏性程序，是黑客危害网络社会和攻击他人计算机信息系统的一种常用手段
  - D. 技术挑战性黑客对社会没有什么危害，应该鼓励

小结

- 网络安全的概念
- 信息加密、身份认证、防火墙、VPN等常见安全技术
- 网络黑客的概念