教学课题：计算机网络安全体系

教学目的要求：1、明确网络安全的含义。

2、掌握网络安全的五大特征

3、掌握网络安全的五大机制

4、明确常用的网络安全技术

教学重点：1、网络安全五大特征

2、网络安全机制

3、网络安全技术

课时：2 课时

教学过程：

计算机网络安全体系

一、网络安全概述

（一）网络安全的概念：网络安全是指网络系统中的硬件、软件及数据受到保护，不受偶然的或恶意的原因而遭到破坏、更改、泄露，确保系统能连续、正常的运行，网络服务不中断。

（二）网络安全应具有以下五个特征：可靠性、可用性、保密性、完整性、不可抵赖性。

保密性：信息不泄露给非授权用户。

完整性：数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

可用性：可被授权实体访问并按需求使用的特性。例如网络环境下的拒绝服务、破坏网络和有关系统的正常运行都属于对可用性的攻击。

可靠性（可控性）：对信息的传播及内容具有控制能力

不可抵赖性：信息发送方不能否认信息是由自己发出去的。

（三）网络安全面临的威胁

包括对网络中信息的威胁和对网络中设备的威胁。

计算机网络面临的最大威胁是人为的恶意攻击。人为的恶意攻击分为主动攻击和被动攻击。以各种方式有选择地破坏信息的有效性和完整性，这是主动攻击；被动攻击，是指在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要的机密信息。

二、计算机网络安全体系

为了维护网络的安全，保证计算机网络正常运行，应该建立完善的网络完全机制，并对其进行合理的分类，形成网络安全体系。

（一）常用的网络安全机制有哪些

1、加密机制。加密是提供信息保密的核心方法。后面要详细介绍。

2、访问控制机制。访问控制可以防止未经授权的用户非法使用系统资源。访问控制是通过对访问者的有关信息进行检查来限制或禁止访问者使用资源的技术。

3、数据完整性机制。数据的完整性是指数据在存储或传输过程中保持不被修改、不被破坏和丢失的特性，即保证数据的完整，数据被破坏、被修改，甚至丢失，那就不完整了。如何保证数据的完整性，后面还要展开讲解。

4、数字签名机制。数字签名机制的目的是保证数据的完整性和发送方的不可抵赖性。后面要展开讲解。这里的抵赖是指甲方向乙方发送了信息，却又不承认是自己发出的，是谁发的就是谁发的，无法栽赃别人。（类似于我们平时的签字，有了你的签字，你就不能不承认了，但签字可能会被别人模仿你的笔迹签了你的名，但数字签名绝对完全）

5、公证机制。可以找一个大家都信任的公证机构，各方交换的信息都通过公证机构来中转，公证机构从中转的信息中提取必要的证据，日后一旦发生纠纷，就可以据此做出仲裁。最常见的就是数字证书技术。

（二）网络安全分类。

网络安全的内容包括：网络实体安全、软件安全、网络数据安全、网络安全管理。

（三）为保障网络的安全问题，可采用以下措施：1 物理措施、2 访问控制（应用防火墙属于访问控制）、3 数据加密、4 网络隔离（VPN 和 VLAN 都属于网络隔离技术）。

(四)网络安全策略主要有：1 先进的网络安全技术；2 严格的安全管理；3 严格的法律法规。

(五)常用的网络安全技术：

1、防火墙技术。（安装防火墙, 可预防可用性攻击，采用的是访问控制机制。）

2、数据的加密技术与数字签名技术（可实现数据的保密性，数据的完整性及不可抵赖性）

3、虚拟局域网技术。（用于局域网，属于网络隔离技术）

4、虚拟专用网技术。（可用于远程网络，也属于网络隔离技术）

(六)网络安全法律法规。

1、网络安全法。2、网络安全等级保护条例。

三、习题分析：

举例：

1. 计算机网络安全体系中,网络安全体制不包括以下哪一项()

A). 数字签名机制　　B). 端口扫描机制

C). 访问控制机制　　D). 加密机制

标准答案:b

解析：

数字签名机制、访问控制机制、加密机制都是网络安全，也是我们常说的。

端口扫描，好象是破坏别人安全的。

2. 隔离是操作系统安全保障的措施之一，物理隔离是属于安全隔离措施中的一种。（）

A). 正确　　B). 错误

标准答案:a

解析:应该是正确的，记住吧。

3. 以下关于 VPN 说法正确的是（）

A). VPN 只能提供身份认证，不能提供加密数据的功能。

B). VPN 指的是用户自己租用线路，和公共网络物理上完全隔离的、安全的线路。

C). VPN 不能做到信息认证和身份认证

D). VPN 指的是用户通过公用网络建立的临时的、安全的连接

标准答案:d

解析:VPN 虚拟属于隔离技术，但不是物理隔离，而是逻辑隔离。

VPN 虚拟专用网络

（一）、VPN 的英文全称是"Virtual Private Network"，即"虚拟专用网络"。可以把它理解成虚拟的企业内部专线。它可以通过特殊的加密的通讯协议在连接在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条专有的通讯线路。

（二）、虚拟专用网络：指的是在公用网络上建立专用网络的技术。其之所以称为虚拟网，主要是因为整个 VPN 网络的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，而是架构在公用网络服务商所提供的网络平台。

（ 三）、VPN 主要采用了隧道技术、加解密技术、密钥管理技术和使用者与设备身份认证技术。（使用者与设备身份认证技术不同于用户登录技术）

（ 四）、VPN 有多种分类方式，主要是按协议进行分类。VPN 可通过服务器、硬件、软件等多种方式实现。VPN 具有成本低，易于使用的特点。