第1章 网络平安概论

1. 选择题

(1) 计算机网络平安是指利用计算机网络管理控制和技术措施，保证在网络环境中数据的 _____ 、完整性、网络效劳可用性和可审查性受到保护。

A．机密性　　B．抗攻击性

C．网络效劳管理性　D．控制平安性

(2) 网络平安的实质和关键是保护网络的 _____ 平安。

A．系统　　B．软件

C．信息　　D．网站

(3) 下面不属于 TCSEC 标准定义的系统平安等级的 4 个方面是。

A．平安政策　　B．可说明性

C．平安保障　　D．平安特征

(4) 在短时间内向网络中的某台效劳器发送大量无效连接请求，导致合法用户暂时无法访问效劳器的攻击行为是破坏了 _____ 。

A．机密性　　B．完整性

C．可用性　　D．可控性

(5)如果访问者有意避开系统的访问控制机制，那么该访问者对网络设备及资源进行非正常使用属于 _____ 。

A．破坏数据完整性　B．非授权访问

C．信息泄漏　　D．拒绝效劳攻击

答案: (1) A　　(2) C　　(3) D　　(4) C　　(5) B

2. 填空题

(1) 计算机网络平安是一门涉及 _____、_____、_____、通信技术、应用数学、密码技术、信息论等多学科的综合性学科。

答案: 计算机科学 、网络技术 、信息平安技术

(2) 网络平安的 5 大要素和技术特征，分别是 _____、_____、_____、_____、_____。

答案: 机密性、完整性、可用性、可控性、不可否认性

(3) 计算机网络平安所涉及的内容包括是_____、_____、_____、_____、_____ 等五个方面。

答案:　实体平安、运行平安 、系统平安、应用平安、 管理平安

(4) 网络信息平安保障包括_____、_____、_____和_____四个方面。

(5) 网络平安关键技术分为_____、_____、_____、_____、_____、_____、_____和_____ 八大类。

(6) 网络平安技术的开展具有_____、_____、_____、_____ 的特点。

(7) TCSEC 是可信计算系统评价准那么的缩写，又称网络平安橙皮书，将平安分为_____、_____、

和文档四个方面。

(8) 通过对计算机网络系统进行全面、充分、有效的平安评测，能够快速查出_____、_____、_____。

答案:

(4) 信息平安策略、信息平安管理、信息平安运作和信息平安技术

(5) 身份认证、访问管理、加密、防恶意代码、加固、监控、审核跟踪和备份恢复

(6) 多维主动、综合性、智能化、全方位防御

(7) 平安政策、可说明性、平安保障

(8) 网络平安隐患、平安漏洞、网络系统的抗攻击能力

3. 简答题

(1) 简述网络平安关键技术的内容？

网络平安关键技术主要包括：

(1) 身份认证〔Identity and Authentication Management〕

(2) 访问管理〔Access Management〕

(3) 加密〔Cryptograghy〕

(4) 防恶意代码〔Anti-Malicode〕

(5) 加固〔Hardening〕

(6) 监控〔Monitoring〕

(7) 审核跟踪〔Audit Trail〕

(8) 备份恢复〔Backup and Recovery〕

(3) 网络平安框架由哪几局部组成？

(1)信息平安战略

(2)信息平安政策和标准

(3)信息平安管理

(4)信息平安运作

(5)信息平安技术

(6) 网络平安设计的原那么有哪些？

在进行网络系统平安方案设计、规划时，应遵循以下 7 项根本原那么：

(1) 综合性、整体性原那么

(2) 需求、风险、代价平衡的原那么

(3)一致性原那么

(4)易操作性原那么

(5) 分步实施原那么

(6) 多重保护原那么

(7) 可评价性原那么

(7) 网络平安的设计步骤是什么？

根据信息平安标准和网络平安设计的原那么,可以确定网络平安设计的 5 个步骤:

(1) 明确平安需求，进行风险分析

(2) 选择并确定网络平安措施
(3) 方案实施
(4) 网络试验及运行
(5) 优化及改良

第 2 章 网络平安技术根底

1. 选择题

〔1〕SSL 协议是〔　〕之间实现加密传输的协议。

〔2〕加密平安机制提供了数据的〔　〕。

〔3〕抗抵赖性效劳对证明信息的管理与具体效劳工程和公证机制密切相关，通常都建立在〔　〕层之上。

C.传输层　　D.应用层

〔4〕能在物理层、链路层、网络层、传输层和应用层提供的网络平安效劳的是〔　〕。

〔5〕传输层由于可以提供真正的端到端的连接，最适宜提供〔　〕平安效劳。

解答:〔1〕C　〔2〕D　〔3〕D　〔4〕B　〔5〕B

2. 填空题

〔1〕应用层平安分解成_____、_____、_____ 的平安，利用_____各种协议运行和管理。

解答: 〔1〕网络层、操作系统、数据库、TCP/IP

〔2〕平安套层 SSL 协议是在网络传输过程中，提供通信双方网络信息的_____性__和_____性，由_____和_____两层组成。

解答:〔2〕保密性、可靠性、SSL 记录协议、SSL 握手协议

〔3〕OSI/RM 开放式系统互连参考模型七层协议是_____、_____、_____、_____、_____、_____、_____。

解答:物理层、数据链路层、网络层、传输层、会话层、表示层、应用层

〔4〕ISO 对 OSI 规定了_____、_____、_____、_____、_____五种级别的平安效劳。

解答: 对象认证、访问控制、数据保密性、数据完整性、防抵赖

〔5〕一个 VPN 连接由 _____、_____和_____ 三局部组成。一个高效、成功的 VPN 具有 _____、_____、_____、_____ 四个特点。

解答: 客户机、隧道、效劳器、平安保障、效劳质量保证、可扩充和灵活性、可管理性

〔2〕简述 IPV6 协议的根本特征及与 IPV4 的 IP 报头格式的区别？

TCP/IP的所有协议的数据都以IP数据报的形式传输，TCP/IP协议簇有两种IP版本： IPv4和IPv6。

IPv4的IP地址是TCP/IP网络中唯一指定主机的32位地址,一个IP包头占20字节包括IP版本号、长度、效劳类型和其他配置信息及控制字段。IPv4在设计之初没有考虑平安性，IP包本身并不具有任何平安特性。

IPv6 简化了 IP 头，其数据报更加灵活，同时 IPv6 还增加了对平安性的设计。 IPv6 协议相对于 IPv4 协议有许多重要的改良，具有以下**根本特征**：

(1)扩展地址空间：IPv6 将 IPv4 的 IP 地址从 32 位扩充到 128 位，这使得网络的规模可以得到充分扩展，连接所有可能的装置和设备，并使用唯一的全局网络地址。

(2)简化报头：IPv4 有许多域和选项，由于报头长度不固定，不利于高效地处理，也不便于扩展。I Pv6 针对这种实际情况，对报头进行了重新设计，由一个简化的长度固定的根本报头和多个可选的扩展报头组成。这样既加快了路由速度，又能灵活地支持多种应用，还便于以后扩展新的应用。IPv4 及 IPV6 根本报头如图 2-8 和图 2-9 所示。

版本（4位）	头长度（4位）	服务类型（8位）	封包总长度（16位）
封包标识（16位）		标志（3位）	片断偏移地址（13位）
存活时间（8位）	协议（8位）	校验和（16位）	
来源IP地址（32位）			
目的IP地址（32位）			
选项（可选）		填充（可选）	
数据			

图 2-8 IPV4 的 IP 报头

版本号	业务流类别	流标签
净荷长度	下一头	跳数限制
源地址		
目的地址		

图 2-9 IPV6 根本报头

(3)更好支持效劳质量 QoS (Quality of Service):为上层特殊应用的传送信息流可以用流标签来识别，便于专门的处理。

(4)改善路由性能：层次化的地址分配便于实现路由聚合，进而减少路由表的表项，而简化的 IP 分组头部也减少了路由器的处理负载。

(5)内嵌的平安机制：要求强制实现 IPSec，提供了支持数据源发认证、完整性和保密性的能力，同时可以抗重放攻击。IPv6 内嵌的平安机制主要由以下两个扩展报头来实现：**认证头 AH**(Authentication Header)和**封装平安载荷 ESP**(Encapsulation Security Payload)。

◆ 其中认证头 AH 可以实现以下三个功能：保护数据完整性(即不被非法篡改)；数据源发认证(即防止源地址假冒)和抗重放(Replay)攻击。

◆ 封装平安载荷 ESP 那么在 AH 所实现的平安功能根底上，还增加了对数据保密性的支持。

◆ AH 和 ESP 都有两种使用方式：传输模式和隧道模式。传输模式只应用于主机实现，并只提供对上层协议的保护，而不保护 IP 报头。隧道模式〔一种以隐含形式把数据包封装到隧道协议中传输数据的方法，将在介绍〕可用于主机或平安网关。在隧道模式中，内部的 IP 报头带有最终的源和目的地址，而外面的 IP 报头可能包含性质不同的 IP 地址，如平安网关地址。

〔6〕简述无线网络的平安问题及保证平安的根本技术？

1. 无线网络的平安问题

无线网络的数据传输是利用微波进行辐射传播，因此，只要在 Access Point (AP)覆盖的范围内，所有的无线终端都可以接收到无线信号，AP 无法将无线信号定向到一个特定的接收设备，因此，无线的平安保密问题就显得尤为突出。

2. 无线平安根本技术

(1) 访问控制-利用 ESSID、MAC 限制，可以防止非法无线设备入侵

(2) 数据加密-基于 WEP 的平安解决方案

(3) 新一代无线平安技术

(4) TKIP-新一代的加密技术 TKIP 与 WEP 一样基于 RC4 加密算法

(5) AES- 是一种对称的块加密技术，提供比 WEP/TKIP 中 RC4 算法更高的加密性能

(6) 端口访问控制技术〔〕和可扩展认证协议〔EAP〕

(7) WPA〔WiFi Protected Access〕标准- WPA 是一种可替代 WEP 的无线平安技术

第 3 章　网络平安管理技术

1. 选择题

〔1〕计算机网络平安管理主要功能不包括〔　〕。

〔2〕网络平安管理技术涉及网络平安技术和管理的很多方面，从广义的范围来看〔　〕是平安网络管理的一种手段。

A.扫描和评估　　B. 防火墙和入侵检测系统平安设备

C.监控和审计　　D. 防火墙及杀毒软件

〔3〕名字效劳、事务效劳、时间效劳和平安性效劳是〔　〕提供的效劳。

A. 远程 IT 管理的整合式应用管理技术　B. APM 网络平安管理技术

C. CORBA 网络平安管理技术　　D. 基于 WeB 的网络管理模式

〔4〕与平安有关的事件，如企业猜想密码、使用未经授权的权限访问、修改应用软件以及系统软件等属于平安实施的〔　〕。

A.信息和软件的平安存储　　B.安装入侵检测系统并监视

〔5〕〔　〕功能是使用户能够能过轮询、设置关键字和监视网络事件来到达网络管理目的，并且已经开展成为各种网络及网络设备的网络管理协议标准。

C.简单网络管理协议 SNMP　　D.用户数据报文协议 UDP

解答: 〔1〕D　〔2〕B　〔3〕C　〔4〕D　〔5〕C

2. 填空题

〔1〕OSI/RM 平安管理包括_____、_____和_____，其处理的管理信息存储在_____ 或 _____ 中。

解答: 〔1〕系统平安管理、平安效劳管理、平安机制管理、数据表、文件

〔2〕网络平安管理功能包括计算机网络的_____、_____、_____、_____等所需要的各种活动。ISO 定义的开放系统的计算机网络管理的功能包括_____、_____、_____、_____、_____。

〔2〕运行、处理、维护、效劳提供、故障管理功能、配置管理功能、性能管理功能、平安管理功能、计费管理功能

〔3〕_____是信息平安保障体系的一个重要组成局部，按照_____的思想，为实现信息平安战略而搭建。一般来说防护体系包括_____、_____和_____三层防护结构。

〔3〕信息平安管理体系、多层防护、认知宣传教育、组织管理控制、审计监督

〔4〕网络管理是通过_____来实现的，根本模型由_____、_____ 和_____三局部构成。

〔4〕构建网络管理系统 NMS、网络管理工作站、代理、管理数据库

〔5〕在网络管理系统的组成局部中，_____最重要，最有影响的是_____和_____代表了两大网络管理解决方案。

〔5〕网络管理协议、SNMP、CMIS/CMIP

〔3〕网络平安管理的技术有哪些？

1. 网络平安管理技术概念

网络平安管理技术是实现网络平安管理和维护的技术，需要利用多种网络平安技术和设备，对网络系统进行平安、合理、有效和高效的管理和维护。

网络平安管理技术一般需要实施一个基于多层次平安防护的策略和管理协议，将网络访问控制、入侵检测、病毒检测和网络流量管理等平安技术应用于内网，进行统一的管理和控制，各种平安技术彼此补充、相互配合，对网络行为进行检测和控制，形成一个平安策略集中管理、平安检查机制分散布置的分布式平安防护体系结构，实现对内网进行平安保护和管理。

监控和审计是与网络管理密切相关的技术。监控和审计是通过对网络通信过程中可疑、有害信息或行为进行记录为事后处理提供依据，从而对黑客形成一个强有力的威慑和最终到达提高网络整体平安

性的目的。

〔4〕网络管理系统的逻辑模型的构成及各组成局部的内容是什么？

现代计算机**网络管理系统**〔Network Management System, 简称 NMS〕主要由如下局部**组成**：

- 多个被管代理〔Managed Agents〕及被管理对象〔Managed Object〕
- 用于执行具体管理工作的网络管理器〔Network Management〕
- 公共网络管理协议〔Network Manager Protocol，简 NMP〕
- 系统管理应用进程(System Management Application Programme，简称管理进程 SMAP)
- 管理信息库〔Management Information Base，简称 MIB〕。

第4 章 黑客攻防与入侵检测

1. 选择题

〔1〕在黑客攻击技术中，〔 〕黑客发现获得主机信息的一种最正确途径。

A.网络监听　　B.缓冲区溢出

〔2〕一般情况下，大多数监听工具不能够分析的协议是〔 〕。

A. 标准以太网　　B. TCP/IP

C. SNMP 和 CMIS　　D. IPX 和 DECNet

〔3〕改变路由信息、修改 WinDows NT 注册表等行为属于拒绝效劳攻击的〔 〕方式。

A.资源消耗型　　B.配置修改型

C.效劳利用型　　D. 物理破坏型

〔4〕〔 〕是建立完善的访问控制策略，及时发现网络遭受攻击情况并加以追踪和防范，防止对网络造成更大损失。

A. 动态站点监控　　B.实施存取控制

C. 平安管理检测　　D.完善效劳器系统平安性能

〔5〕〔 〕是一种新出现的远程监控工具，可以远程上传、修改注册表等，集聚危险性还在于，在效劳端被执行后，如果发现防火墙就会终止该进程，使安装的防火墙完全失去控制。

C.网络神偷　　D.广外女生

解答：〔1〕C　〔2〕C　〔3〕B　〔4〕A　〔5〕D

2. 填空题

〔1〕黑客的“攻击五部曲”是_____、_____、_____、_____、_____。

解答：隐藏 IP、 踩点扫描、获得特权、种植后门、隐身退出

〔2〕端口扫描的防范也称为_____，主要有_____和_____两种方法。

解答：系统加固、关闭闲置及危险端口、屏蔽出现扫描病症的端口

〔3〕密码攻击一般有_____、_____和_____三种方法。其中_____有蛮力攻击和字典攻击两种方式。

解答：网络监听非法得到用户密码、密码破解、放置特洛伊木马程序、密码破解

〔4〕网络平安防范技术也称为_____，主要包括访问控制、_____、_____、_____、补丁平安、_____、数据平安等。

解答：加固技术、平安漏洞扫描、入侵检测、攻击渗透性测试、关闭不必要的端口与效劳等

〔5〕入侵检测系统模型由_____、_____、_____、_____以及_____五个主要局部组成。

解答：信息收集器、分析器、响应、数据库、目录效劳器

〔1〕常用的黑客攻击技术有哪些？对每一种攻击技术的防范对策是什么？

1) 端口扫描攻防

1) 端口扫描作用

网络端口为一组16位号码，其范围为0~65535，效劳器在预设得端口等待客户端的连接。如WWW效劳使用TCP的80号端口、FTP端口21、Telnet端口23。一般各种网络效劳和管理都是通过端口进行的，同时也为黑客提供了一个隐蔽的入侵通道。对目标计算机进行端口扫描能得到许多有用的信息。通过端口扫描，可以得到许多需要的信息，从而发现系统的平安漏洞防患于未然。端口扫描往往成为黑客发现获得主机信息的一种最正确途径。

2)端口扫描的防范对策

端口扫描的防范也称为系统“加固”，主要有两种方法。

(1) 关闭闲置及危险端口

(2) 屏蔽出现扫描病症的端口

2)网络监听攻防

网络嗅探就是使网络接口接收不属于本主机的数据。通常账户和密码等信息都以明文的形式在以太网上传输，一旦被黑客在杂错节点上嗅探到，用户就可能会遭到损害。

对于网络嗅探攻击，可以采取以下一些措施进行防范。

(1) 网络分段

(2) 加密

(3) 一次性密码技术

5) 缓冲区溢出攻防

(1) 编写正确的代码

(2) 非执行的缓冲区

(3) 数组边界检查

(4) 程序指针完整性检查

6) 拒绝效劳攻防

到目前为止，进行 DDoS 攻击的防御还是比拟困难的。首先，这种攻击的特点是它利用了 TCP/IP 协议的漏洞。

检测 DDoS 攻击的主要方法有以下几种：

(1)根据异常情况分析

(2)使用 DDoS 检测工具

对 DDoS 攻击的主要防范策略包括：

(1)尽早发现系统存在的攻击漏洞，及时安装系统补丁程序。

(2)在网络管理方面，要经常检查系统的物理环境，禁止那些不必要的网络效劳。

(3)利用网络平安设备如防火墙等来加固网络的平安性。

(4)比拟好的防御措施就是和你的网络效劳提供商协调工作，让他们帮助你实现路由的访问控制和对带宽总量的限制。

(5)当发现自己正在遭受 DDoS 攻击时，应当启动应付策略，尽快追踪攻击包，并及时联系 ISP 和有关应急组织，分析受影响的系统，确定涉及的其他节点，从而阻挡攻击节点的流量。

(6)对于潜在的 DDoS 攻击，应当及时去除，以免留下后患。

〔2〕说明特洛伊木马攻击的步骤及原理？

1〕 使用木马工具进行网络入侵，根本过程可以分为 6 个步骤。

(1) 配置木马

(2) 传播木马

(3) 运行木马

(4) 泄露信息。收集一些效劳端的软硬件信息，并通过 E-mail 或 ICQ 等告知控制端用户。

(5) 建立连接。效劳端安装木马程序，且控制端及效劳端都要在线。控制端可以通过木马端口与效劳端建立连接。

(6) 远程控制。通过木马程序对效劳端进行远程控制。

控制端口可以享有的控制权限： 窃取密码、文件操作、修改注册表和系统操作。

2)特洛伊木马攻击原理

特洛伊木马是指隐藏在正常程序中的一段具有特殊功能的恶意代码，是具备破坏和删除文件、发送密码、记录键盘和攻击 Dos 等特殊功能的后门程序。

一个完整的木马系统由硬件局部、软件局部和具体连接局部组成。

〔6〕入侵检测系统的主要功能有哪些？其特点是什么？

入侵检测系统主要功能包括 6 个方面：

(1) 监视、分析用户及系统活动；

(2) 系统构造和弱点的审计；

(3) 识别反映进攻的活动模式并向相关人员报警；

(4) 异常行为模式的统计分析；

(5) 评估重要系统和数据文件的完整性；

(6) 操作系统的审计跟踪管理，并识别用户违反平安策略的行为。

入侵检测系统的特点：

入侵检测技术是动态平安技术的最核心技术之一，通过对入侵行为的过程与特征的研究，使平安系统对入侵事件和入侵过程能做出实时响应，是对防火墙技术的合理补充。

IDS 帮助系统防范网络攻击，扩展了系统管理员的平安管理功能，提高了信息平安根底结构的完整性。

入侵检测被认为是防火墙之后的第二道平安闸门，提供对内部攻击、外部攻击和误操作的实时保护。

入侵检测和平安防护有根本性的**区别**

：平安防护和黑客的关系是“防护在明，黑客在暗”，入侵检测和黑客的关系那么是“黑客在明，检测在暗”。平安防护主要修补系统和网络的缺陷，增加系统的平安性能，从而消除攻击和入侵的条件；入侵检测并不是根据网络和系统的缺陷，而是根据入侵事件的特征一般与系统缺陷有逻辑关系，对入侵事件的特征进行检测，所以入侵检测系统是黑客的克星。

〔7〕简述网络平安防范攻击的根本措施有哪些？

1. 提高防范意识
2. 设置平安口令
3. 实施存取控制
4. 加密及认证
5. 定期分析系统日志
6. 完善效劳器系统平安性能
7. 进行动态站点监控
8. 平安管理检测
9. 做好数据备份
10. 使用防火墙和防毒软件

〔8〕简述端口扫描的原理。

最简单的端口扫描程序仅仅是检查目标主机在哪些端口可以建立 TCP 连接，如果可以建立连接，那么说明主机在那个端口被监听。

对于非法入侵者而言，要想知道端口上具体提供的效劳，必须用相应的协议来验证才能确定，因为一个效劳进程总是为了完成某种具体的工作而设计的。

〔9〕从网络平安角度分析为什么在实际应用中要开放尽量少的端口？

网络端口为一组16位号码，其范围为0~65535，效劳器在预设得端口等待客户端的连接。如WWW效劳使用TCP的80号端口、FTP端口21、Telnet端口23。一般各种网络效劳和管理都是通过端口进行的，同时也为黑客提供了一个隐蔽的入侵通道。对目标计算机进行端口扫描能得到许多有用的信息。通过端口扫描，可以得到许多需要的信息，往往成为黑客发现获得主机信息的一种最正确途径, 所以从网络平安角度在实际应用中要开放尽量少的端口。

〔10〕在实际应用中应怎样防范口令破译？

通常保持密码平安的要点：

(1) 要将密码写下来，以免遗失；
(2) 不要将密码保存在电脑文件中；
(3) 不要选取显而易见的信息做密码；
(4) 不要让他人知道；
(5) 不要在不同系统中使用同一密码；
(6) 在输入密码时应确认身边无人或其他人在 1 米线外看不到输入密码的地方；
(7) 定期改变密码，至少 2—5 个月改变一次。

〔11〕简述出现DDoS 时可能发生的现象。

被攻击主机上出现大量等待的 TCP 连接，网络中充满着大量的无用数据包，源地址为假的，制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通讯，利用受害主机提供的效劳或传输协议上的缺陷，反复高速地发出特定的效劳请求，使受害主机无法及时处理所有正常请求，严重时会造成系统死机。

〔12〕简述电子邮件炸弹的原理及防范技术。

原理：是用伪造的 IP 地址和电子邮件地址向同一信箱发送数以千计、万计甚至无穷屡次的内容相同的垃圾邮件，致使受害人邮箱被“炸”，严重者可能会给电子邮件效劳器操作系统带来危险，甚至瘫痪。

防范技术：其防范方法与防范其他密码破解、拒收垃圾邮件和防范病毒方法类似。

第 5 章 身份认证与访问控制

1. 选择题

〔1〕在常用的身份认证方式中，〔 〕是采用软硬件相结合、一次一密的强双因子认证模式，具有平安性、移动性和使用的方便性。

A. 智能卡认证　　B. 动态令牌认证

C. USB Key　　D. 用户名及密码方式认证

〔2〕以下〔 〕属于生物识别中的次级生物识别技术。

A. 网膜识别　　B. DNA

C. 语音识别　　D. 指纹识别

〔3〕数据签名的〔 〕功能是指签名可以证明是签字者而不是其他人在文件上签字。

A. 签名不可伪造　　B. 签名不可变更

C. 签名不可抵赖　　D. 签名是可信的

〔4〕在综合访问控制策略中，系统管理员权限、读/写权限、修改权限属于〔 〕。

A. 网络的权限控制　　B. 属性平安控制

C. 网络效劳平安控制　　D. 目录级平安控制

〔5〕以下〔 〕不属于 AAA 系统提供的效劳类型。

A. 认证　　B. 鉴权

C. 访问　　D. 审计

解答：〔1〕B　〔2〕C　〔3〕A　〔4〕D　〔5〕C

2. 填空题

〔1〕身份认证是计算机网络系统的用户在进入系统或访问不同_____的系统资源时，系统确认该用户的身份是否_____、_____和_____的过程。

解答：保护级别、真实、合法、唯一

〔2〕数字签名是指用户用自己的_____对原始数据进行_____所得到_____，专门用于保证信息来源的_____、数据传输的_____和_____。

解答：私钥 加密、特殊数字串、真实性、完整性、防抵赖性

〔3〕访问控制包括三个要素，即_____、_____和_____。访问控制的主要内容包括_____、和_____ 三个方面。

解答：主体 客体、控制策略、认证、控制策略实现、审计

〔4〕访问控制模式有三种模式，即 _____、_____ 和 _____。

解答：自主访问控制 DAC、强制访问控制 MAC、根本角色的访问控制 RBAC

〔5〕计算机网络平安审计是通过一定的_____，利用_____系统活动和用户活动的历史操作事件，按照顺序_____、_____和_____每个事件的环境及活动，是对和的要补充和完善。

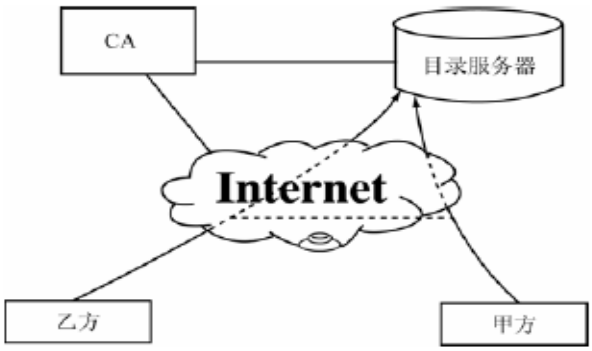
解答：平安策略、记录及分析、检查、审查、检验、防火墙技术、入侵检测技术

3. 简答题

〔1〕简述数字签名技术的实现过程？

对一个电子文件进行数字签名并在网上传输，通常需要的**技术实现过程**包括：网上身份认证、进行签名和对签名的验证。

1. 身份认证的实现过程



PKI 提供的效劳首先是认证，即身份识别与鉴别，就是确认实体即为自己所声明的实体。认证的前提是甲、乙双方都具有第三方 CA 所签发的证书。认证分单向认证和双向认证。

1) 单向认证 ，单向认证是甲、乙双方在网上通信时，甲只需要认证乙的身份。这时甲需要获取乙的证书，获取的方式有两种，一种是在通信时乙直接将证书传送给甲，另一种是甲向CA 的目录效劳器查询索取。甲获得乙的证书后，首先用CA 的根证书公钥验证该证书的签名，验证通过说明该证书是第三方CA 签发的有效证书。然后检查证书的有效期及检查该证书是否已被作废(LRC 检查)而进入黑名单。

2)双向认证。甲乙双方在网上查询对方证书的有效性及黑名单时，采用 LDAP 协议(Light Directory Access Protocol)，它是一种轻型目录访问协议，过程如下图。

网上通信的双方，在互相认证身份之后，即可发送签名的数据电文。

3.原文保密的数据签名的实现方法

上述数字签名中定义的对原文做数字摘要及签名并传输原文，实际上在很多场合传输的原文要求保密，不许别人接触。要求对原文进行加密的数字签名方法的实现涉及到“数字信封”的问题，这个处理过程稍微复杂一些，但数字签名的根本原理仍是相同的，其签名过程如图5-8 所示。

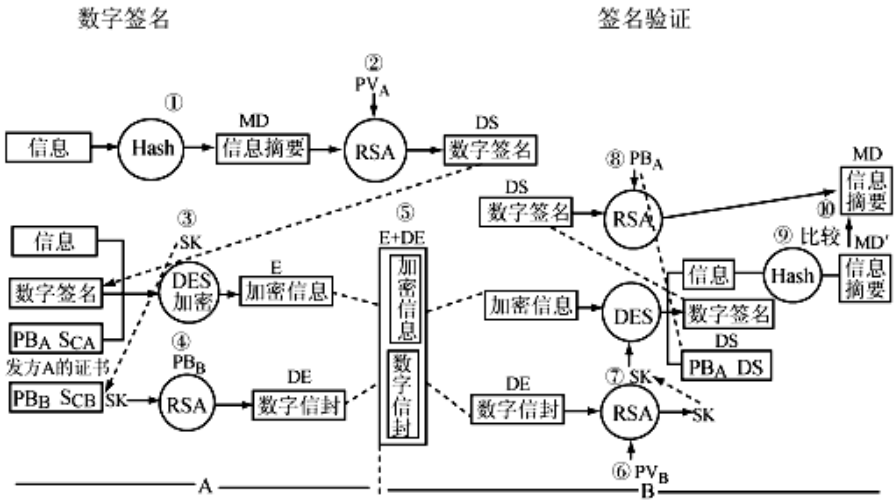


图5-8 原文加密的数字签名实现方法

这是一个典型的“数字信封”处理过程。其**根本原理**是将原文用对称密钥加密传输，而将对称密钥用收方公钥加密发送给对方。如同将对称密钥放在同一个数字信封，收方收到数字信封，用自己的私钥解密信封，取出对称密钥解密得原文。

原文加密的数字签名的过程：

(1) 发方A 将原文信息进行哈希(Hash)运算，得到一哈希值，即数字摘要MD。

(2) 发方A 用自己的私钥PV_A，采用非对称RSA 算法对数字摘要MD 进行加密，即得数字签名DS。

(3) 发方A 用对称算法DES 的对称密钥SK 对原文信息、数字签名DS 及发方A 证书的公钥PB_A 采用对称算法加密，得加密信息E。

(4) 发方用收方B 的公钥PB_B，采用RSA 算法对对称密钥SK 加密，形成数字信封DE，就好似将对称密钥SK 装到了一个用收方公钥加密的信封里。

(5) 发方A 将加密信息E 和数字信封DE 一起发送给收方B。

(6) 收方B 接收到数字信封DE 后，首先用自己的私钥PV_B 解密数字信封，取出对称密钥SK。

(7) 收方B 用对称密钥SK 通过DES 算法解密加密信息E，复原出原文信息、数字签名DS 及发方A 证书的公钥PB_A。

(8) 收方B 验证数字签名，先用发方A 的公钥解密数字签名得数字摘要MD。

(9) 收方B 同时将原文信息用同样的哈希运算，求得一个新的数字摘要MD′。

(10)将两个数字摘要MD 和MD′进行比拟，验证原文是否被修改，如果二者相等，说明数据没有被篡改，是保密传输的，签名是真实的，否那么拒绝该签名。这样就做到了敏感信息在数字签名的传输中不被篡改，其他没经认证和授权的人看不见或读不懂原数据，起到了在数字签名传输中对敏感数据的保密作用。以上就是现行电子签名中普遍被使用而又具有可操作性的、平安的、数字签名的技术实现原理和全部过程。

〔3〕简述平安审计的目的和类型？

目的和意义在于：

(1) 对潜在的攻击者起到重大震慑和警告的作用；

(2) 测试系统的控制是否恰当，以便于进行调整，保证与既定平安策略和操作能够协调一致。

(3) 对于已经发生的系统破坏行为，作出损害评估并提供有效的灾难恢复依据和追究责任的证据；

(4) 对系统控制、平安策略与规程中特定的改变作出评价和反应，便于修订决策和部署。

(5) 为系统管理员提供有价值的系统使用日志，帮助系统管理员及时发现系统入侵行为或潜在的系统漏洞。

平安审计有三种类型：

(1) 系统级审计

(2) 应用级审计

(3) 用户级审计