**第一章 网络安全概论**

1、计算机网络安全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、网络服务可用性和可审查性受到保护。

A．机密性　 B．抗攻击性

C．网络服务管理性　 D．控制安全性

2、网络安全的实质和关键是保护网络的 安全。

A．系统　 B．软件

C．信息　 D．网站

3、下面不属于TCSEC标准定义的系统安全等级的4个方面是。

A．安全政策　　　 B．可说明性

C．安全保障　　 D．安全特征

4、在短时间内向网络中的某台服务器发送大量无效连接请求，导致合法用户暂时无法访问服务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，则该访问者对网络设备及资源进行非正常使用属于 。

A．破环数据完整性 B．非授权访问

C．信息泄漏 D．拒绝服务攻击

答案: (1) A (2) C (3) D (4) C (5) B

2. 填空题

(1) 计算机网络安全是一门涉及 、 、 、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 、信息安全技术

(2) 网络安全的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) 计算机网络安全所涉及的内容包括是 、 、 、 、

等五个方面。

答案: 实体安全、运行安全 、系统安全、应用安全、 管理安全

(4) 网络信息安全保障包括 、 、 和 四个方面。

(4) 信息安全策略、信息安全管理、信息安全运作和信息安全技术

(5) 网络安全关键技术分为 、 、 、 、 、 、 和 八大类。

(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) 网络安全技术的发展具有 、 、 、 的特点。

(6) 多维主动、综合性、智能化、全方位防御

(7) TCSEC是可信计算系统评价准则的缩写，又称网络安全橙皮书，将安全分为 、 、 和文档四个方面。

(7) 安全政策、可说明性、安全保障

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

(8) 网络安全隐患、安全漏洞、网络系统的抗攻击能力

**第二章 网络安全技术基础**

1. 选择题

（1）SSL协议是（ ）之间实现加密传输的协议。

A.物理层和网络层 B.网络层和系统层

C.传输层和应用层 D.物理层和数据层

（2）加密安全机制提供了数据的（ ）。

A.可靠性和安全性 B.保密性和可控性

C.完整性和安全性 D.保密性和完整性

（3）抗抵赖性服务对证明信息的管理与具体服务项目和公证机制密切相关，通常都建立在（ ）层之上。

A.物理层 B.网络层

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安全服务的是（ ）。

A.认证服务 B.数据保密性服务

C.数据完整性服务 D.访问控制服务

（5）传输层由于可以提供真正的端到端的连接，最适宜提供（ ）安全服务。

A.数据保密性 B.数据完整性

C.访问控制服务 D.认证服务

解答:（1）C （2）D （3）D （4）B （5）B

2. 填空题

（1）应用层安全分解成 、 、 的安全，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）安全套层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。

（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 、 、 、 、

、 、 。

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 、 、 、 、 五种级别的安全服务。

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 三部分组成。一个高效、成功的VPN具有 、 、 、 四个特点。

客户机、隧道、服务器、安全保障、服务质量保证、可扩充和灵活性、可管理性

3、简答题

（1）简述网络安全检测与管理信息中常用的网络命令及其各自的功能？(简述ping命令、ipconfig命令、netstat命令、net命令和at命令的功能和用途。)

1）ping 命令

ping命令功能是通过发送ICMP包来检验与另一台TCP/IP主机的IP级连接情况。网管员常用这个命令检测网络的连通性和可到达性。同时，应答消息的接收情况将和往返过程的次数一起显示出来。

* 如果只使用不带参数的ping命令，窗口将会显示命令及其各种参数使用的帮助信息。
* 使用ping命令的语法格式是：ping 对方计算机名或者IP地址

**第三章 网络安全管理技术**

1、网络安全管理技术涉及网络安全技术和管理的很多方面，从广义的范围来看（ ）是安全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安全设备

C.监控和审计 D. 防火墙及杀毒软件

2、与安全有关的事件，如企业猜测密码、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安全实施的（ ）。

A.信息和软件的安全存储 B.安装入侵检测系统并监视

C.对网络系统及时安装最新补丁软件 D.启动系统事件日志

**3、网络管理的解决方案有哪些？它们的工作原理是什么？**

1.进行全面补丁管理

由于一些最敏感的数据经常放在非微软系统上，如Linux、UNIX或者Macintosh系统。因此，要采用全面的补丁管理解决方案，提供网络的全面的可见性并且覆盖所有的操作系统和所有厂商的产品，不要仅限于微软的产品。

2.实施员工安全培训

通过强制性培训提高员工熟悉安全的程度。每个月通过在线课程进行培训是提醒员工安全是每一个人的责任的好方法。选择能够提供最新课程的培训计划，保证用户了解政策和程序并且向管理层提供报告。

3.采用基于主机的入侵防御系统

威胁现在使用加密、数据包分割、数据包重叠和编码等方法绕过网络入侵检测系统。应考虑使用基于主机的入侵防御系统，因为它能够检测你的系统查找异常行为、安装应用程序的企图、用户权限升级和其它异常事件。

4.进行网络、操作系统和应用层测试

大多数机构都进行基本的外部网络和操作系统安全漏洞测试。这种测试能够发现许多暴露给互联网的安全漏洞。在应用程序级别上进行测试是非常重要的，因为这些攻击正在日益流行，如果能够早期发现，就能够减少安全漏洞的大暴露。

5.应用URL过滤

仍然允许员工自由浏览网络的机构应该了解和面对允许这样做的风险。除了潜在的法律和声誉的担心之外，自由的网络浏览为恶意攻击敞开了一个大窗口。更好的替代方法是预先管理允许员工访问的网站，把这些网站限制在安全的范围内，允许访问声誉好的网络出版商的网站。

6.集中进行台式电脑保护

台式电脑杀毒软件已经成为大多数计算机的一个标准。这是个好消息。然而，如果你分别管理这些系统，你也许就会有没有保护的系统和暴露安全漏洞。确保进行集中的管理和报告。

7.强制执行政策管理系统

对于某些机构来说，政策管理意味着强制执行定期改变的复杂口令。对于其它机构来说，政策管理就是让“管理员”在工作站控制限制的访问。还有一些机构认为，政策管理是报告杀毒更新、补丁水平和操作系统服务包水平的一种方法。要执行一个至少包含上述全部内容的强大的政策管理系统。

8.采用信息发送管理解决方案

由于企事业单位的员工经常接触敏感的数据及发送电子邮件等，所以，机构每天都可能会泄漏敏感的数据。信息发送管理解决方案应当将敏感的数据限制在内部网络，采取的第一个步措施应当就是电子邮件内网的过滤解决方案，这个解决方案可以监控和过滤所有通过简单邮件传输协议发送的敏感数据。

**4、网络安全管理的技术有哪些？**

**1. 网络安全管理技术概念**

网络安全管理技术是实现网络安全管理和维护的技术，需要利用多种网络安全技术和设备，对网络系统进行安全、合理、有效和高效的管理和维护。

网络安全管理技术一般需要实施一个基于多层次安全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安全技术应用于内网，进行统一的管理和控制，各种安全技术彼此补充、相互配合，对网络行为进行检测和控制，形成一个安全策略集中管理、安全检查机制分散布置的分布式安全防护体系结构，实现对内网进行安全保护和管理。

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达到提高网络整体安全性的目的。

**5、网络信息安全政策是什么？包括的具体内容有哪些？**

**1. 信息安全管理政策**

信息安全管理政策是企事业单位信息安全从管理层面对信息安全的一整套包含规定和常规的最高指导原则，是在信息安全战略下为组织管理、保护、和信息资源分派制定的原则。

信息安全管理政策是信息安全政策与标准体系中最高层级的声明，提供较广泛的领导方向以及说明管理阶层的目标和目的。

信息安全管理政策通常以信息安全管理政策总则的形式发布，在信息安全战略的基础上确定单位信息安全管理的结构、各项目标和细化原则。

**2. 信息安全功能性政策**

信息安全功能性政策是比较特定事项的声明，是在信息安全管理政策下针对某特定管理需求建立的政策。

针对管理的特定需求给出明确的规定，具体内容包括：

(1) 信息安全风险管理

(2) 信息安全认知

(3) 信息安全组织

(4) 信息安全审计

(5) 信息安全法律法规符合性

**6、网络安全策略有哪些？如何实现主机网络安全防护功能？**

**网络安全策略有:**

1) 重要的商务信息和软件的安全存储。

2) 对网络系统及时安装最新补丁软件。

3) 安装入侵检测系统并实施监视。

4) 启动系统事件日志。

**如何实现主机网络安全防护功能？**

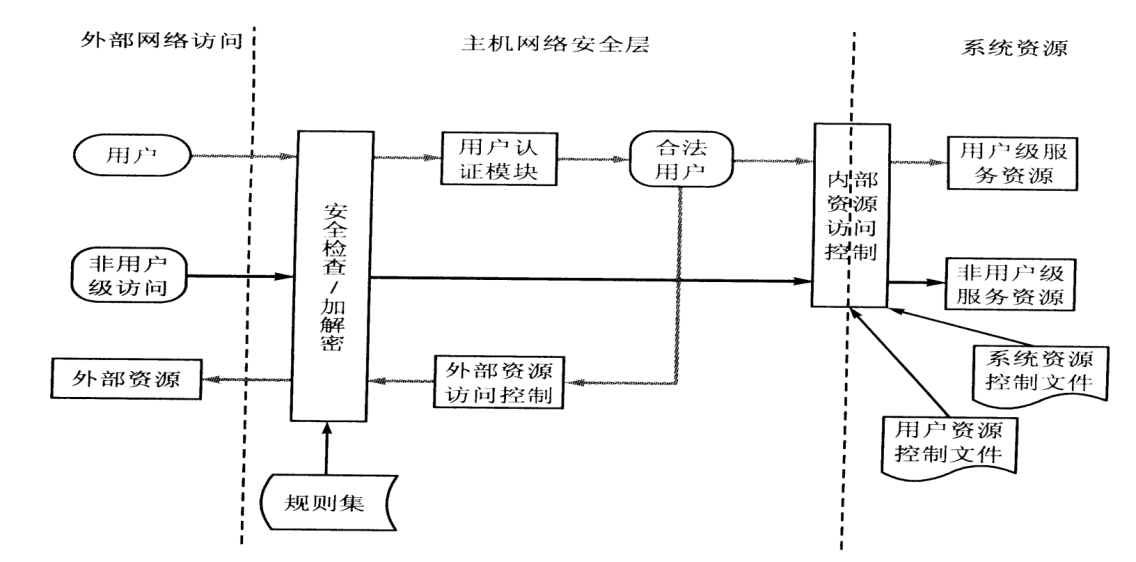
采用主机网络安全技术，主机网络安全技术是一种主动防御的安全技术，它结合网络访问的网络特性和操作系统特性来设置安全策略，用户可以根据网络访问的访问者及访问发生的时间、地点和行为来决定是否允许访问继续进行，以使同一用户在不同场所拥有不同的权限，从而保证合法用户的权限不被非法侵占。主机网络安全技术考虑的元素有IP地址、端口号、协议、MAC地址等网络特性和用户、资源权限以及访问时间等操作系统特性，并通过对这些特性的综合考虑，来达到用户网络访问的细粒度控制。

与网络安全采用安全防火墙、安全路由器等在被保护主机之外的技术手段不同，主机网络安全所采用的技术手段通常在被保护的主机内实现，并且一般为软件形式。因为只有在被保护主机之上运行的软件，才能同时获得外部访问的网络特性以及所访问资源的操作系统特性。

应用最为广泛的此类产品有Wietse Venema 开发的共享软件TCP Wrapper。TCP Wrapper 是一种对进入的网络服务请求进行监视与过滤的工具，可以截获Systat、Finger、FTP、Telnet、Rlogin、RSH、Exec、TFTP、Talk 等网络服务请求，并根据系统管理员设置的服务的访问策略来禁止或允许服务请求。

主机网络安全系统是为了解决主机安全性与访问方便性之间的矛盾，将用户访问时表现的网络特性和操作系统特性进行综合考虑，因此，这样的系统必须建立在被保护的主机上，并且贯穿于网络体系结构中的应用层、传输层、网络层之中。在不同的层次中，可以实现不同的安全策略。

更复杂的设计可以在更多的层实现更多的安全功能，下面就前面的设想提出一个可行的主机网络安全系统的结构模型，如图所示。

****

**第四章 黑客攻防与入侵检测**

1、在黑客攻击技术中，（ ）黑客发现获得主机信息的一种最佳途径。

A.网络监听 B.缓冲区溢出

C.端口扫描 D.口令破解

2、（ ）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，在服务端被执行后，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。

A.冰河 B.网络公牛

C.网络神偷 D.广外女生

**3、密码破解攻防**

1)密码攻防的方法

一般密码攻击有3种方法：

(1) 通过网络监听非法得到用户密码

(2) 密码破解

(3) 放置木马程序

2) 密码攻防对策

通常保持密码安全的要点：

(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。

**4、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

**5、以SYN FlooD攻击为例，分析分布式拒绝服务攻击运行的原理是什么？**

1) 攻击运行原理

如图所示，一个比较完善的DDoS 攻击体系分成4 大部分，最重要的第2 和第3 部分，它们分别用做控制和实际发起攻击;对第4 部分的受害者来说，DDoS的实际攻击包是从第3部分攻击傀儡机上发出的，第2部分的控制机只发布命令而不参与实际的攻击。



2) DDoS 攻击实例——目前最流行的DDoS 攻击手段SYN Flood 攻击

1) Syn Flood 原理与三次握手

Syn Flood 利用了TCP/IP协议的固有漏洞。面向连接的TCP 三次握手是Syn Flood 存在的基础。TCP 连接的三次握手过程，如图所示。



TCP三次握手过程中，在第一步，客户端向服务端提出连接请求。服务端收到该TCP 分段后，在第二步以自己的ISN 回应(SYN 标志置位)，同时确认收到客户端的第一个TCP 分段(ACK 标志置位)。在第三步中，客户端确认收到服务端的ISN(ACK标志置位)。到此为止建立完整的TCP 连接，开始全双工模式的数据传输过程。

2) Syn Flood 攻击者不会完成三次握手。如图所示。



**第五章**

1、访问控制模式有三种模式，即 、 和 。

自主访问控制DAC、强制访问控制MAC、基本角色的访问控制RBAC

2、计算机网络安全审计是通过一定的 ，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。

安全策略、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 提供的服务首先是认证，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。

****

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。

**2. 数字签名与对签名的验证实现过程**

数字签名的全过程分两大部分，即签名与验证。

**数字签名过程**分两部分：左侧为签名过程，右侧为验证过程。即发方将原文用哈希算法求得数字摘要，用签名私钥对数字摘要加密求得数字签名，然后将原文与数字签名一起发送给收方；收方验证签名，即用发方公钥解密数字签名，得出数字摘要；收方将原文采用同样哈希算法又得一新的数字摘要，将两个数字摘要进行比较，如果两者匹配，说明经数字签名的电子文件传输成功。如图5-5 所示。



图5-5 数字签名原理

**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，但数字签名的基本原理仍是相同的，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**基本原理**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PVA，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PBA 采用对称算法加密，得加密信息E。

(4) 发方用收方B 的公钥PBB，采用RSA 算法对对称密钥SK 加密，形成数字信封DE，就好像将对称密钥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PVB 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，还原出原文信息、数字签名DS 及发方A 证书的公钥PBA。

(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′进行比较，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，否则拒绝该签名。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、安全的、数字签名的技术实现原理和全部过程。

**4、试述访问控制的安全策略以及实施原则？**

**1. 基于身份的规则的安全策略**

建立基于身份安全策略和基于规则安全策略的基础是授权行为。

(1) 基于身份的安全策略是过滤对数据或资源的访问，只有能通过认证的那些主体才有可能正常使用客体的资源。基于身份的安全策略包括基于个人的策略和基于组的策略，主要有两种基本的实现方法，分别为能力表和访问控制表。

基于个人的策略。基于个人的策略是指以用户个人为中心建立的一种策略，由一些列表组成。这些列表针对特定的客体，限定了哪些用户可以实现何种安全策略的操作行为。

基于组的策略。基于组的策略是基于个人的策略的扩充，指一些用户被允许使用同样的访问控制规则访问同样的客体。

(2) 基于规则的安全策略

基于规则的安全策略中的授权通常依赖于敏感性。在一个安全系统中，数据或资源应该标注安全标记。代表用户进行活动的进程可以得到与其原发者相应的安全标记。在实现上，由系统通过比较用户的安全级别和客体资源的安全级别来判断是否允许用户进行访问。

**2. 综合访问控制策略**

访问控制技术的目标是防止对任何资源的非法访问。从应用方面的访问控制策略包括以下几个方面。

(1) 入网访问控制

(2) 网络的权限控制

(3) 目录级安全控制

(4) 属性安全控制

(5) 网络服务器安全控制

(6) 网络监测和锁定控制

(7) 网络端口和节点的安全控制

(8) 防火墙控制

**3. 安全策略实施原则**

安全策略实施原则：访问控制安全策略的实施原则围绕主体、客体和安全控制规则集三者之间的关系展开。

(1) 最小特权原则。是指主体执行操作时，按照主体所需权利的最小化原则分配给主体权力。最小特权原则的优点是最大限度地限制了主体实施授权行为，可以避免来自突发事件、错误和未授权主体的危险。也就是说，为了达到一定目的，主体必须执行一定操作，但他只能做他所被允许做的，其他除外。

(2) 最小泄漏原则。是指主体执行任务时，按照主体所需要知道的信息最小化的原则分配给主体权力。

(3) 多级安全策略。是指主体和客体间的数据流向和权限控制按照安全级别的绝密（TS）、秘密（S）、机密（C）、限制（RS）和无级别（U）5级来划分。多级安全策略的优点是避免敏感信息的扩散。具有安全级别的信息资源，只有安全级别比它高的主体才能够访问。

**5、简述安全审计的目的和类型？**

**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，保证与既定安全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、安全策略与规程中特定的改变作出评价和反馈，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。

**第六章**

（1）（ ）密码体制，不但具有保密功能，并且具有鉴别的功能。

A. 对称 B. 私钥

C. 非对称 D. 混合加密体制

（2）网络加密方式的（ ）是把网络上传输的数据报文的每一位进行加密，而且把路由信息、校验和等控制信息全部加密。

A. 链路加密 B. 节点对节点加密

C. 端对端加密 D.混合加密

（3）恺撒密码是（ ）方法，被称为循环移位密码，优点是密钥简单易记，缺点是安全性较差。

A.代码加密 B.替换加密

C.变位加密 D.一次性加密

（4）数据加密标准DES是 加密技术，专为 编码数据设计的，典型的按 方式工作的 密码算法。

（4）代码加密、替换加密、变位加密、一次性加密

**5、网络的加密方式有哪些？优缺点及适合范围是什么？**

计算机网络加密方式有3种：链路加密、节点对节点加密和端对端加密。

**1) 链路加密方式**

链路加密方式是指把网络上传输的数据报文的每一位进行加密，链路两端都用加密设备进行加密，使整个通信链路传输安全。

在链路加密方式下，只对传输链路中的数据加密，而不对网络节点内的数据加密，中间节点上的数据报文是以明文出现的。目前，一般网络传输安全主要采这种方式。

缺点：需要公共网络提供者配合，修改其交换节点，增加安全单元或保护装置；同时，节点加密要求报头和路由信息以明文形式传输，以便中间节点能得到如何处理消息的信息，也容易受到攻击。

**2) 节点对节点加密**

为了解决在节点中数据是明文的缺陷，在中间节点内装有用于加、解密的保护装置，即由这个装置来完成一个密钥向另一个密钥的变换（报文先解密再用另一个不同的密钥重新加密）。

缺点：需要公共网络提供者配合，修改其交换节点，增加安全单元或保护装置；同时，节点加密要求报头和路由信息以明文形式传输，以便中间节点能得到如何处理消息的信息，也容易受到攻击。

**3) 端对端加密**

对端加密也称面向协议加密方式，是指只在用户双方通信线路的两端进行加密，数据是以加密的形式由源节点通过网络到达目的节点，目的节点用于源节点共享的密钥对数据解密。这种方式提供了一定程度的认证功能，同时也防止网络上链路和交换机的攻击。

优点是网络上的每个用户可以有不同的加密关键词，而且网络本身不需增添任何专门的加密设备。

缺点是每个系统必须有一个加密设备和相应的管理加密关键词软件，或者每个系统自行完成加密工作，当数据传输率是按兆位/秒的单位计算时，加密任务的计算量是很大的。

链路加密方式和端对端加密方式的**区别**是：链路加密方式是对整个链路的传输采取保护措施，而端对端方式则是对整个网络系统采取保护措施，端对端加密方式是未来发展主要方向。对于重要的特殊机密信息，可以采用将二者结合的加密方式。

**6、试述DES算法的加密过程？**

DES是一种专为二进制编码数据设计的、典型的按分组方式工作的单钥密码算法。**基本原理**是将二进制序列的明文分组，然后用密钥对这些明文进行替代和置换，最后形成密文。DES算法是对称的，既可用于加密又可用于解密。密钥输入顺序和加解密步骤完全相同，从而在制作DES芯片时很容易达到标准化和通用化，很适合现代通信。

DES采用64位长的密钥，包括8个校验位，密钥长度为56位，可将原文的多个64位块变换成加密的多个64位代码块。**原理**是将原文经过一系列的排列与置换所产生的结果再与原文异或合并。该加密过程重复16次，每次所用的密钥位排列不同。即使按照目前的标准，采用该方法的加密结果也相当安全。然而, 任何安全都是相对的。

**7、2．密码分析**

密码分析就是在不知道密钥的情况下，利用数学方法破译密文或找到秘密密钥。

(1) 已知明文的破译方法：密码分析员可以通过一段明文和密文的对应关系，经过分析发现加密的密钥。所以，过时或常用加密的明文、密文和密钥，仍然具有被利用的危险性。

(2) 选定明文的破译方法：密码分析员可以设法让对手加密一段选定的明文，并获得加密后的结果，经过分析也可以确定加密的密钥。

**8、如何进行简单的变位加密？已知明文是“来宾已出现住在人民路”， 密钥是：4168257390，则加密后，密文是什么？**

简单的变位加密：首先选择一个用数字表示的密钥，写成一行，然后把明文逐行写在数字下。按密钥中数字指示的顺序，逐列将原文抄写下来，即为加密后的密文 。

密钥： 4 1 6 8 2 5 7 3 9 0

明文：来 宾 已 出 现 住 在 人 民 路

0 1 2 3 4 5 6 7 8 9

密文：路 宾 现 人 来 住 已 在 出 民

**9、已知明文是“One World One Dream”，按行排在矩阵中，置换f=，用矩阵变位加密方法后，密文是什么？**

矩阵变位密码是把明文中的字母按给定的顺序排列在一个矩阵中，然后用另一种顺序选出矩阵的字母来产生密文。

按照置换f中第1行的顺序将明文安排在一矩阵中：

**O n e W**

**o r l d**

**O n e D**

**r e a m**

按照置换f中第2行的顺序2413将上述矩阵中的各行重新排列：

**n W O e**

**r d o l**

**n D O e**

**e m** r a

则密文是：**nWOerdolnDOeem**ra

（答案错误，按照老师讲的来）

书上P127 加密5-10

**第七章**

1、数据库安全可分为两类：系统安全性和 。

A. 数据安全性 B. 应用安全性

C. 网络安全性 D. 数据库安全性

2、下载数据库数据文件，然后攻击者就可以打开这个数据文件得到内部的用户和帐号以及其它有用的信息，这种攻击称为 。

A. 对SQL的突破 B. 突破script的限制

C. 数据库的利用 D. 对本地数据库的攻击

3、由非预期的、不正常的程序结束所造成的故障是 。

A. 系统故障 B. 网络故障

C. 事务故障 D. 介质故障

4、权限管理属于下面哪种安全性策略： 。

A. 系统安全性策略 B. 用户安全性策略

C. 数据库管理者安全性策略 D. 应用程序开发者的安全性策略

5、数据库系统的完整性主要包括 和 。

物理完整性、 逻辑完整性

6、数据库安全可分为二类： 和 。

系统安全性、 数据安全性

**第九章**

1、驻留在多个网络设备上的程序在短时间内产生大量的请求信息冲击某web服务器，导致该服务器不堪重负，无法正常相应其他合法用户的请求，这属于（ ）

1. 上网冲浪 B中间人攻击 C．DDoS攻击 D．MAC攻击

2、防火墙隔离了内部、外部网络，是内、外部网络通信的 途径，能够根据制定的访问规则对流经它的信息进行监控和审查，从而保护内部网络不受外界的非法访问和攻击。

唯一

3、防火墙是一种 设备，即对于新的未知攻击或者策略配置有误，防火墙就无能为力了。

被动安全策略执行

4、从防火墙的软、硬件形式来分的话，防火墙可以分为 防火墙和硬件防火墙以及 防火墙。

软件、芯片级

5、第一代应用网关型防火墙的核心技术是 。

代理服务器技术

6、单一主机防火墙独立于其它网络设备，它位于 。

网络边界

7、 是位于外围网络中的服务器，向内部和外部用户提供服务。

堡垒主机

8、 利用TCP协议的设计上的缺陷，通过特定方式发送大量的TCP请求从而导致受攻击方CPU超负荷或内存不足的一种攻击方式。

SYN Flood

**9、防火墙是什么？**

防火墙是一种位于两个（或多个）网络之间，通过执行访问控制策略来保护网络安全的设备。它隔离了内部、外部网络，是内、外部网络通信的唯一途径，能够根据制定的访问规则对流经它的信息进行监控和审查，从而保护内部网络不受外界的非法访问和攻击。

**2、简述防火墙的分类及主要技术**

**1 以防火墙的软硬件形式分类**

可以分为**软件防火墙**和**硬件防火墙**以及**芯片级防火墙**。

（1）软件防火墙需要客户预先安装好的计算机操作系统的支持，俗称个“人防火墙”。

（2）硬件防火墙一般至少应具备三个端口，分别接内网，外网和DMZ区。

（3）芯片级防火墙基于专门的硬件平台，没有操作系统。专有的ASIC芯片促使它们比其他种类的防火墙速度更快，处理能力更强，性能更高。

**2 按照防火墙的技术分类**

**可以分为包过滤型和应用代理型两大类。**

1. 包过滤型防火墙

工作在OSI网络参考模型的网络层和传输层，它根据数据包头源地址，目的地址、端口号和协议类型等标志确定是否允许通过。只有满足过滤条件的数据包才被转发到相应的目的地，其余数据包则被从数据流中丢弃。

在整个防火墙技术的发展过程中，包过滤技术出现了两种不同版本，称为“第一代静态包过滤”和“第二代动态包过滤”。

1）第一代，静态包过滤类型防火墙

这类防火墙几乎是与路由器同时产生的，它是根据定义好的过滤规则审查每个数据包，以便确定其是否与某一条包过滤规则匹配。过滤规则基于数据包的报头信息进行制订。报头信息中包括IP源地址、IP目标地址、传输协议(TCP、UDP、ICMP等等)、TCP/UDP目标端口、ICMP消息类型等。

2）第二代，动态包过滤类型防火墙

这类防火墙采用动态设置包过滤规则的方法，避免了静态包过滤所具有的问题。这种技术后来发展成为包状态监测(Stateful Inspection)技术。采用这种技术的防火墙对通过其建立的每一个连接都进行跟踪，并且根据需要可动态地在过滤规则中增加或更新条目。

1. 应用代理(Application Proxy)型

应用代理型防火墙是工作在OSI的最高层，即应用层。其特点是完全“阻隔”了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。

在代理型防火墙技术的发展过程中，它也经历了两个不同的版本，即：第一代应用网关型代理防火和第二代自适应代理防火墙。

1）第一代应用网关(Application Gateway)型防火墙

这类防火墙是通过一种代理(Proxy)技术参与到一个TCP连接的全过程。从内部发出的数据包经过这样的防火墙处理后，就好像是源于防火墙外部网卡一样，从而可以达到隐藏内部网结构的作用。这种类型的防火墙被网络安全专家和媒体公认为是最安全的防火墙。它的核心技术就是代理服务器技术。

2）第二代自适应代理(Adaptive proxy)型防火墙

它可以结合代理类型防火墙的安全性和包过滤防火墙的高速度等优点，在毫不损失安全性的基础之上将代理型防火墙的性能提高10倍以上。组成这种类型防火墙的基本要素有两个：自适应代理服务器(Adaptive Proxy Server)与动态包过滤器(Dynamic Packet filter)。

**3 以防火墙体系结构分类**

主要有：**单一主机防火墙**、**路由器集成式防火墙**和**分布式防火墙**三种。

（1）单一主机防火墙是最为传统的防火墙，独立于其它网络设备，它位于**网络边界**。

（2）路由器集成式防火墙是将防火墙功能集成在中、高档路由器中，大大降低了网络设备购买成本。

（3）分布式防火墙不是只是位于网络边界，而是渗透于网络的每一台主机，对整个内部网络的主机实施保护。

**4 以防火墙在性能等级上的分类**

如果按防火墙的性能来分可以分为**百兆级防火墙**和**千兆级防火墙**两类。

**第十一章**

1、电子商务对安全的基本要求不包括（ ）

A.存储信息的安全性和不可抵赖性 B. 信息的保密性和信息的完整性

C.交易者身份的真实性和授权的合法性 D.信息的安全性和授权的完整性

2、在Internet上的电子商务交易过程中，最核心和最关键的问题是（ ）

A. 信息的准确性 B. 交易的不可抵赖性

C. 交易的安全性 D. 系统的可靠性

3、电子商务以电子形式取代了纸张，在它的安全要素中（ ）是进行电子商务的前提条件。

A. 交易数据的完整性 B. 交易数据的有效性

C. 交易的不可否认性 D. 商务系统的可靠性

4、应用在电子商务过程中的各类安全协议，（ ）提供了加密、认证服务，并可以实现报文的完整性，以完成需要的安全交易操作。

A. 安全超文本传输协议（S-HTTP）） B. 安全交易技术协议（STT）

C. 安全套接层协议（SSL） D. 安全电子交易协议（SET）

5、电子商务按应用服务的领域范围分类，分为 和 两种模式。

企业对终端客户（或B2C） 企业对企业（或B2B）

6、电子商务的安全性主要包括五个方面，它们是 、 、

、 、 。

系统的可靠性、交易的真实性、数据的安全性、数据的完整性、交易的不可抵赖性

**7、什么是电子商务安全？ （了解）**

电子商务安全性是一个系统的概念，不仅与计算机系统结构有关，还与电子商务应用的环境、人员素质和社会因素有关。

电子商务对安全的基本要求：  
 ● 授权的合法性  
 ● 不可抵赖性  
 ● 信息的保密性  
 ● 交易者身份的真实性  
 ● 信息的完整性  
 ● 存储信息的安全性。

电子商务安全从整体上可分为两大部分：计算机网络安全和商务交易安全。计算机网络安全与商务交易安全实际上是密不可分的，两者相辅相成，缺一不可。

电子商务安全具体涉及以下五个方面：

（1）电子商务系统硬件(物理)安全

（2）电子商务系统软件安全

（3）电子商务系统运行安全

（4）电子商务交易安全

（5）电子商务安全立法

**第十二章**

**1、网络安全方案的主要内容有哪些？**

安全解决方案的框架(内容)主要可以概括为6个方面，在实际应用中可以根据企事业用户的实际需求进行适当优化选取和调整。

1. 安全风险概要分析

2. 实际安全风险分析

通常可以从4个方面进行实际安全风险的分析：

(1) 网络风险分析

(2)系统风险分析

(3)应用安全分析

(4)对系统和应用的安全分析

3. 网络系统的安全原则

网络系统的安全原则主要体现在5个方面：动态性、唯一性、整体性、专业性和严密性。

4. 主要安全技术

常用的安全产品和安全技术有5种：防火墙、防病毒、身份认证、传输加密和入侵检测。

5. 风险评估

6.安全管理与服务

(1) 网络拓扑安全

(2) 系统安全加固

(3) 应用安全

(4) 灾难恢复

(5) 紧急响应

(6) 安全管理规范

(7)服务体系和培训体系

**2、网络安全的目标及设计原则是什么？**

**1. 安全方案的目标**

应用网络安全技术设计网络安全方案的目标：

　　(1) 各部门、各单位局域网的安全保护

　　(2) 与Internet相连的安全保护

　　(3) 关键信息的加密传输与存储

　　(4) 应用业务系统的安全

(5) 安全网的监控与审计

(6) 最终目标：机密性、完整性、可用性、可控性与可审查性

具体地主要包括以下3个方面：访问控制、数据加密、安全审计

**2. 网络安全方案设计原则**

(1) 努力提高系统的安全性和保密性；

(2) 保持网络原有的性能特点，对网络的协议和传输具有很好的透明性；

(3) 易于操作、维护，并便于自动化管理，而不增加或少增加附加操作；

(4) 尽量不影响原网络拓扑结构，同时便于系统及系统功能的扩展；

(5) 安全保密系统具有较好的性能价格比，一次性投资，可以长期使用；

(6) 安全与密码产品具有合法性，及经过国家有关管理部门的认可或认证；

(7) 分步实施。对于网络安全综合解决方案，需要采取几个阶段进行分步实施、分段验收、确保总体质量。

**3、评价网络安全方案的质量标准有哪些？**

(1) 确切唯一性是评估安全解决方案最重要的标准之一，对每一项具体指标的要求都应当是确切唯一的不能模棱两可，以便根据实际情况需要来进行具体实现。 (2) 综合把握和理解现实中的安全技术和安全风险，并具有一定的预见性。

(3) 对用户的网络系统可能遇到的安全风险和安全威胁，结合现有的安全技术和安全隐患，应当给出一个具体、合适、实际准确的评估结果和建议。

(4) 针对企事业用户系统安全问题，利用先进的安全产品、安全技术和管理手段，降低用户的网络系统可能遇到的风险和威胁，消除风险和隐患，增强防范安全风险和威胁的能力。

(5) 切实体现对用户的服务支持。

(6) 在整个设计方案过程中，应当清楚网络系统安全是一个动态的、整体的、专业的工程，需要分步实施不能一步到位彻底解决用户所有的安全问题。

(7) 以网络安全工程的思想和方式组织实施。

(8) 具体方案中所采用的安全产品、安全技术和具体安全措施，都应当经得起验证、推敲和论证实施，应当有实际的理论依据和基础。

4、**网络安全的具体解决方案包括哪些内容？**

具体的安全解决方案主要包括：

(1) 物理安全解决方案

主要包括3个方面：

1) 环境安全 2) 设备安全 3) 媒体安全

在物理安全方面应采取4个方面措施：

　　 1) 产品保障方面 2) 运行安全方面

　　 3) 防电磁辐射方面 4) 保安方面

(2) 链路安全解决方案

(3) 网络安全解决方案

(4) 信息安全解决方案