信息安全导论练习题

《信息安全导论》练习题及参考答案

一、选择题

1、保密性表示对信息资源开放范围的控制，不让不应涉密的人涉及秘密信息，实现保密性的一般方法有（ A B C D F ）

A）数据加密

B）访问控制

C）信息流控制

D）推理控制

E）IDS

F）TEMPEST

2、信息安全的概念与技术是随着人们的需求、随着计算机、通信与网络等信息技术的发展而不断发展的。大体可以分为如下几个阶段（ B C D ）

A）Key Agreement阶段

B）网络信息安全阶段

C）信息保障阶段

D）信息保密阶段

E）Hello阶段

F）Finish阶段

3、下列那些密码体制是对称密码系统（ A C ）

A）DES

B）RSA

C）IDEA

D）MD5

E）SHA

4、数字证书的标准有多种，X.509是数字证书的一个重要标准，一个数字证书通常如下的内容（ ＡＣＤＥ ）

A）要被证实的实体的名字

B）这个实体的私钥

C）证书机构（CA）的名字

D）一个数字签名

E）使用的算法

5、散列函数就是一个将任意长度的消息映射为定长的散列值的公共函数，那么MD5最后的输出散列值的长度为（ Ｃ ）bit。

A）512

B）160

C）128

D）256

6、进程p指定一个安全类SC(p)，说明p可以读入的最高类和可写入的最低类。进程p需要从x1,x2,…xm读出而向y1,y2,…yn写入，那么下列那个关系式满足这个访问控制的要求（ Ｂ ）

A）SC(y1)□SC(y2)□…□SC(yn)<=SC(P)<=SC(x1)⊙SC(x2)⊙…⊙SC(xm)

B）SC(x1)□SC(x2)□…□SC(xm)<=SC(P)<=SC(y1)⊙SC(y2)⊙…⊙SC(yn)

C）SC(y1)⊙SC(y2)⊙…⊙SC(yn)<=SC(P)<=SC(x1)□SC(x2)□…□SC(xm)

D）SC(x1)⊙SC(x2)⊙…⊙SC(xm)<=SC(P)<=SC(y1)□SC(y2)□…□SC(yn)

7、在各种访问控制技术中，ACL方式是实现DAC策略的最好方法。下表是客体FILE1

C D ）

A）组prog中只有Joann有REW权，同组其他成员只有R权。

B）任意组中，用户zbs有RE权。

C）无论那个组，任何用户都没有权限。

D）组prog的所有用户都只有R权。

8、为了保证数据的完整性、一致性，DBMS通常提供相关的技术来保证数据库的安全，下面哪些技术是数据库管理系统的提供的安全措施（ A B C ）

A）两阶段提交

B）并发访问控制

C）触发器

D）推理控制

9、下列那些是数字签名的基本要求（ A B C ）

A）签名不能伪造

B）签名不可抵赖

C）签名不可改变

D）签名不易验证

10、DES密码体制：它是应用位密钥，加密___比特明文分组的分组秘钥密码体制。（ C ）

A）56 56

B）64 64

C）56 64

D）64 56

11、IDEA密码体制：它是应用位密钥，加密___比特明文分组的分组秘钥密码体制。（ B ）

A）128 128

B）128 64

C）64 128

D）64 64

12、访问控制的有效性建立在如下的哪些条件上？（ ＡＣ ）

A）用户进入系统前，需要鉴别与确证

B）每一个用户都要授与一定的权限

C）用户或程序的访问权信息是受保护的，是不会被非法修改的

D）每一用户的权限能相互转授

13、访问控制矩阵模型中包括三个要素，那么他们是（ ＡＣＤ ）

A）系统中的客体集

B）系统中的用户集

C）系统中的主体集

D）系统中主体对客体的访问权限集合

14、用数据库来实现对数据信息的管理，在许多方面都有强于文件系统，具体体现在如下几个方面（ ＡＢＣＤＥ ）

A）共享性

B）最小的冗余度

C）数据的一致性

D）数据的完整性

E）强有力的访问控制

15、数据库主要的安全要求主要体现在如下几个方面（ ＡＢＣＤ ）

A）数据库的完整性

B）数据库的可靠性

C）数据库的保密性

D）数据库的可用性

E）数据库的冗余度

16、

二、判断题

三、填空题

1、从广义上讲，一般有三类加密算法可以用来对数据进行加密，他们是：

非对称 和 散列 。

2、在数字证书的组件中，通常包括如下的几个基本结构：要被证实的实体的名字、这个实

体的公开密钥、 证书机构的名字、 一个数字签名 、 签名所使用的算法
、和时间期限。

3、根据安全服务与网络层次的关系，对于对等实体鉴别服务，在OSI的7个层次中，与之相关的层次分别为： 3 ， 4 ， 6 。

4、在操作系统中，要有实现对客体保护机制，其中访问目录表机制容易实现，但存在需要解决的三个问题： 共享客体的控制 、 访问权的回收 和 多重许可权问题 。

5、SSL握手协议(SSL Handshake
Protocol)的主要过程可以划分为三个阶段：这三个阶段分别为： hello阶段 、 key agreement阶段 和 finish阶段 。

6、对于给定的客体x和y，根据信息流的流动策略，信息从x流向y是授权的当且仅当 SC(x)<=SC(y)
，如果x，y都是可变类，那么SC(y)是SC(x)是它在流动之前的类。假设x是在范围[0，31]中的整数变元，所有的取值都是等概率的。如果y初始时不存在，通过执行赋值句“y := x” ，则产生 5 比特的x-->y的信息流。

7、在大型的数据库系统中，DBMS提供触发器功能，用于监视正在输入或修改的值是否破坏数据库的完整性，触发器的可以完成的功能为： 检查取值类型与范围 ，

。

8、信息安全的最根本属性是防御性的，主要目的是防止己方信息的保密性 、与可用性 遭到破坏。

四、名词解释

1、公钥密码体制

指一个加密系统的加密密钥和解密密钥时不一样的，或者说不能由一个推导出另一个，其中一个称为公钥用于加密，是公开的，另一个称为私钥用于解密，是保密的。其中用公钥计算私钥是难解的，即所谓的不能由一个推出另一个。

2、数据保密服务

用来保护网络中交换的数据，防止未经许可地暴露数据内容。根据OSI标准协议中规定的数据交换方式，它提供连接方式和无连接方式的数据保密服务。此外它还提供从观察信息流就能推导出信息的保护和允许用户选择协议数据单元中的某些字段进行保护。

3、访问控制矩阵

是通过矩阵形式表示访问规则和授权用户权限的方法，也就是说，对每个主体而言，都拥有对哪些客体有哪些访问的权限；而对客体而言，又有哪些主体对他可以实施访问。将这种关联关系加以阐述，就形成了控制矩阵

4、拒绝服务攻击

拒绝服务攻击是一类个人或多人利用Internet协议组的某些工具，拒绝合法用户对目标系统（如服务器）和信息的合法访问的攻击。

5、虚拟专用网

VPN被定义为通过一公共网络（如INTERNET）建立的临时的、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，它是对企业内部网的扩展。

6、两阶段提交

为了保证数据更新结果的正确性，必须防止在数据更新过程中发生处理程序中断或出现错误，而采用的技术成为两阶段提交技术。第一阶段称为准备阶段。收集为完

成更新所需要的信息和其它资源。但不数据库作实际的改变。第二阶段的工作是对需要更新的字段进行真正的修改，这种修改是永久的。

7、防火墙

防火墙就是一个位于内部网络和它所连接的网络之间的软件或硬件。流入流出的所有网络通信均要经过此防火墙。防火墙可以看成保护内部网边界的哨卡，阻塞进出防火墙的恶意信息流。

五、计算、证明题

1、系统中有N个人需要两两保密通信，

若使用对称加密算法，每个人需要保存多少个密钥，系统中一共有多少个密钥？

若使用公开加密算法，每个人需要保存多少个密钥，系统中一共有多少个密钥？

2、有某单位职工工资表（见附表1），请计算如下数据：（6分）

职工工资表

3、访问控制矩阵

是通过矩阵形式表示访问规则和授权用户权限的方法，也就是说，对每个主体而言，都拥有对哪些客体有哪些访问的权限；而对客体而言，又有哪些主体对他可以实施访问。将这种关联关系加以阐述，就形成了控制矩阵

4、拒绝服务攻击

拒绝服务攻击是一类个人或多人利用Internet协议组的某些工具，拒绝合法用户对目标系统（如服务器）和信息的合法访问的攻击。

5、虚拟专用网

VPN被定义为通过一公共网络（如INTERNET）建立的临时的、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，它是对企业内部网的扩展。

6、两阶段提交

为了保证数据更新结果的正确性，必须防止在数据更新过程中发生处理程序中断或出现错误，而采用的技术成为两阶段提交技术。第一阶段称为准备阶段。收集为完成更新所需要的信息和其它资源。但不数据库作实际的改变。第二阶段的工作是对需要更新的字段进行真正的修改，这种修改是永久的。

7、防火墙

防火墙就是一个位于内部网络和它所连接的网络之间的软件或硬件。流入流出的所有网络通信均要经过此防火墙。防火墙可以看成保护内部网边界的哨卡，阻塞进出防火墙的恶意信息流。

五、计算、证明题

1、系统中有N个人需要两两保密通信，

若使用对称加密算法，每个人需要保存多少个密钥，系统中一共有多少个密钥？
若使用公开加密算法，每个人需要保存多少个密钥，系统中一共有多少个密钥？

2、有某单位职工工资表（见附表1），请计算如下数据：（6分） 职工工资表

a) median(男，奖金)=?

b) 设特征公式为：C=女*（销售部+计划处）+安监部，则|C|=?，
rfreq(c)=？avg(c,工资)=？ c）在“1-响应，98%-
支配”标准下，为何要限制Sum(销售部,工资)或Sum(男*销售部,工资)
这两个统计? 答：

a) median(男，奖金)=150（2分）

b) |C|=4， rfreq(c)=4/11 avg(c,工资)=575（2分）

c）Sum(销售部,工资)- Sum(男*销售部,工资)=500
根据外部知识，泄漏了销售部唯一女职工黄爱玲的工资情况（2分）

六、简述题

1、简述两阶段提交技术，及其在保证数据完整性和一致性方面的作用。

答：为了保证数据更新结果的正确性，必须防止在数据更新过程中发生处理程序中断或出现错误，而采用的技术成为两阶段提交技术。第一阶段称为准备阶段。收集为完成更新所需要的信息和其它资源。但不数据库作实际的改变。第二阶段的工作是对需要更新的字段进行真正的修改，这种修改是永久的。
保证了同表数据的完整性，

保证了多表间数据的一致性。

2、Java采用什么机制来实现JavaApplet的安全性？
答：JAVA采用了如下一些安全措施

1）采用字节码验证器 2）运行内存布局 3）文件的访问控制 4）类装入器

5）类的内置安全措施

3、在军用安全模型下，一个批准为<机密，{常规，导弹、火炮}>的用户能否有权访问下列方式

归档的文献，并说出理由。

1）<绝密，{常规，导弹、火炮}> 2) <机密，{导弹}> 3）<机密，{坦克，导弹}> 4) <机密，{飞机}> 5）<秘密，{常规，导弹，火炮}> 6) <秘密，{机枪}> 答：

1）<绝密，{常规，导弹、火炮}> 不可以 2) <机密，{导弹}> 可以

3）<机密，{坦克，导弹}> 不可以 4) <机密，{飞机}> 不可以

5）<秘密，{常规，导弹，火炮}> 可以 6) <秘密，{机枪}> 不可以
4、采用分组与通配符的方法有助缩短ACL表的长度，提高系统效率。根据客体File1的ACL的结构和内容，简述客体File1的访问控制。

File1 客体

答：

组prog中只有Joann有REW权，同组其他成员只有R权

任意组中，用户zbs有RE权 其他情况没有任何权限

5、系统状态的转换是依靠一套本原命令来实现的，这些命令是用一系列改变访问矩阵内容的本原操作来定义的，在访问矩阵模型中定义了6种本原操作，对文件f有所有权的进程p，可以把对f的任何权利（除所有权外）转授给其他进程，请完成下面的命令序列，以实现p把对文件f的read和write权限转授给进程q

command confer_read_write(p,q,f) if own in then end

6、简述产生缓冲区溢出的主要原因

答：1）程序员缺少编程经验，程序中没有检查缓冲区边界的功能
2）程序编制错误造成的。 3）程序员故意遗留下来的程序漏洞。
4）程序设计语言编译器本身的缺陷。

7、图示化描述1、2组成的线性格与{A,B }组成的子集格的积代数

8、简述IPv4的安全问题。

答：TCP/IP本身不提供加密传输功能

TCP/IP本身不支持信息流填充机制 TCP/IP本身不提供对等实体鉴别功能

TCP/IP协议体系本身存在缺陷，容易遭受到攻击

由TCP/IP支持的Internet中的各个子网是平等的，难以实现分级安全的网络结构（如树状结构），无法实现有效的安全管理。

许多厂商提供的TCP/IP应用层协议实用软件中存在严重的安全漏洞，常常被黑客用作网络攻击的工具。

9、比较分析常用的生物特征认证方法。

答：一般而言，生物统计学设备是用于保证某种安全的有效和简单的设备。它可以测量与识别某个人的具体的生理特征，如指纹、声音图象、笔迹、打字手法或视网膜图象等特征。生物统计学设备通常用于极重要的安全场合，用以严格而仔细地识别人员身份。 指纹识别技术是一种已经被接受的可以唯一识别一个人的方法。

手印识别与指纹识别有所不同，手印识别器需要读取整个手而不仅是手指的特征图象。

识别声音图象的能力使人们可以基于某个短语的发音对人进行识别。声音识别技术已经商用化了，但当一个人的声音发生很大变化的时候（如患感冒），声音识别器可能会发生错误。
视网膜识别技术是一种可用技术，但还没有象其他技术那样得到广泛的利用。

10、分析分析数据库的两种加密方式。 答：

1）库外加密

方法简单，密钥管理相对简单 2） 库内加密

记录加密 属性加密 元素加密 问题：密钥多，管理复杂。

11、分析密码体制的基本要求 基本要求：

(1)对所有密钥，加、解密算法迅速有效□对加解密的软硬件要求低□容易推广普及
(2)体制的安全性不依赖于算法的保密□筛选抗分析□用户有关□与开发者无关

12、简述数字签名的基本要求 基本要求：

1、签名不能伪造：签名是签名者对文件内容合法性的认同、证明、和标记，其他人的签名无效；

2、签名不可抵赖：这是对签名者的约束，签名者的认同、证明、标记是不可否认的；
3、签名不可改变：文件签名后是不可改变的，这保证了签名的真实性、可靠性；

4、签名不可重复使用：签名需要时间标记，这样可以保证签名不可重复使用。

5、签名容易验证：对于签名的文件，一旦发生纠纷，任何第三方都可以准确、有效地进行验证。

13、简述访问控制的基本任务和实现方法。

基本任务：是保证对客体的所有直接访问都是被认可的。它通过对程序与数据的读、写、更改和删除的控制，保证系统的安全性和有效性，以免受偶然的和蓄意的侵犯。 实现：由支持安全策略的执行机制实现

14、简述访问监控器的不知之处。

1）访问监控器主要还是作为单级安全模型使用的，受监视的目标要么允许被访问，要么不允许被访问

2）系统中所有对受监控目标的访问要求都由监控器检查核实，监控程序将被频繁调用，这将使监控器可能成为整个系统的瓶颈，影响系统效率。
3）监控器只能控制直接访问，不能控制间接访问。

13、简述数据库的安全威胁体现在哪些方面
1）向数据库中输入了错误或被修改的数据。
2）支持数据库系统的硬件环境故障。

3）数据库系统的安全保护功能弱或根本没有安全机制。
4）数据库管理员专业知识不够。

5）网络黑客或内部恶意用户对网络与数据库的攻击手段不断翻新。
6）计算机病毒的威胁日益严重。

7）对于象中国这样的发展中国家，操作系统、网络系统与数据库系统和计算机这样核心的软、硬件都是外国公司研制的，整个国家信息的安全建筑在外国公司的“良知”与“友好”上，这是最大的不安全因素。

14、数据库的完整性体现在哪些方面，以及如何保证数据库的完整性。

1）在物理完整性方面，要求从硬件或环境方面保护数据库的安全，防止数据被破坏或不可读。应该有灾后数据库快速恢复能力。数据库的物理完整性和数据库留驻的计算机系统硬件可靠性与安全性有关，也与环境的安全保障措施有关。

2）在逻辑完整性方面，要求保持数据库逻辑结构的完整性，需要严格控制数据库的创立与删除、库表的建立、删除和更改的操作。逻辑完整性还包括数据库结构和库表结构设计的合理性，尽量减少字段与字段之间、库表与库表之间不必要的关联，减少不必要的冗余字段，防止发生修改一个字段的值影响其他字段的情况。

3）在元素完整性方面，元素完整性主要是指保持数据字段内容的正确性与准确性。元素完整性需要由DBMS、应用软件的开发者和用户共同完成。

七、论述题

1、和操作系统相比，为什么说数据库的访问控制的难度要大的多？（6分）答：

1）管理对象量的差别（2分）

操作系统要管理的客体量比较小

数据库系统要控制的对象如记录的量可能很大，

2）管理对象之间关系的差别（2分）

操作系统要管理的客体之间的关系简单

数据库系统要控制的对象之间的关系复杂

3）控制粒度上的差别（2分）

操作系统要的控制粒度最多达到文件一级

数据库系统要控制粒度可以是表，记录，属性

4）推理攻击控制上的差别

使数据库的访问控制机制不仅要防止直接的泄漏，而且还要防止推理泄漏的问题
操作系统中一般不存在这种推理泄漏问题，它所管理的目标（文件）之间并没有逻辑关系

2、举例说明：要构造一个即满足安全性又满足精确性的信息流控制机制是困难的。（6分）答：考虑赋值语句“y := k*x”。（3’）

假定在一个策略中，SC(k)≤SC(y)成立，但SC(x)≤SC(y)不成立。

如果总是禁止其执行，是安全的，但不精确。

如果k=0或H(x)=0，执行语句不导致流x□y的发生。

设计“仅对实际流x□y证明关系SC(x)≤SC(y)”的机制，远比设计“对能够潜在地引起流x□y的任何运算，证明关系SC(x)≤SC(y)”的机制困难。

考虑语句（3’）

if f(n) halts then y:=x else y:=0

其中f是任意函数，且关系SC(x)≤SC(y)不成立。

考虑两个系统，一个总是允许该语句的执行，而另一个则禁止执行它。显然，不解决停机问题，第一个系统是否安全，或第二个系统是否精确的都是不可判定的。

上面两个例子表明，构造一个既是安全的、又是精确的机制在理论上是不成立的

3、试述IPv4版本TCP/IP的缺陷及其造成的安全问题，并讨论可以从网络什么层次上提供哪些安全增强技术。（6分）

答：TCP/IP本身不提供加密传输功能 □容易受到被动攻击

TCP/IP本身不支持信息流填充机制□容易受到信息流分析的攻击

TCP/IP本身不提供对等实体鉴别功能□容易遭到欺骗攻击

TCP/IP协议体系本身存在缺陷，容易遭受到拒绝服务攻击攻击

由TCP/IP支持的Internet中的各个子网是平等的，难以实现分级安全的网络结构（如树状结构），无法实现有效的安全管理。
许多厂商提供的TCP/IP应用层协议实用软件中存在严重的安全漏洞，常常被黑客用作网络攻击的工具。（3分）

应用层□Kerberos系统

应用层＋传输层□SSL

10

网络层□IPsec（3分

4、图示化描述数字签名的过程，并讨论其中散列函数所起的作用。

使用散列函数的优点：

1）扩大了原文的大小空间，如2的64次幂（SHA）

2）大大减少了加密和解密的开销

3）使得数字签名快速有效。

使用散列函数的不足：

由于散列函数存在碰撞问题，这就给攻击者利用碰撞进行攻击提供了可能，例如，

1）求原文的摘要

2）按自己的意图修改原文，

3）插入无意义的字符，构造其散列值，使其散列值与原文的摘要一致即可

4）这样有最终的消息，替换原文。

5、对比分析对称与非对称密码体制

11

6、论述数据库的安全威胁主要体现在哪些方面

1）向数据库中输入了错误或被修改的数据，有的敏感数据在输入过程中已经泄漏了，已经失去应有的价值；在数据维护（增、删、改）和利用过程中可能对数据的完整性造成了破坏。

2）支持数据库系统的硬件环境故障，如无断电保护措施而发生断电造成信息丢失；硬盘故障致使库中数据读不出来；环境灾害和人为破坏也是对数据库系统的威胁。

3）数据库系统的安全保护功能弱或根本没有安全机制（如dBASE类数据库），对数据库的攻击者而言够不成屏障作用。

4）数据库管理员专业知识不够，不能很好地利用数据库的保护机制和安全策略，不能合理地分配用户的权限，或经若干次改动后造成用户权限与用户级别混乱配合，可能会产生超过用户应有级别权限的情况发生。

5）网络黑客或内部恶意用户对网络与数据库的攻击手段不断翻新、他们整天琢磨操作系统和数据库系统的漏洞，千方百计地设法侵入系统；相反，各部门对数据库的安全防护的经费投入不足，研究深度显得不足，系统的安全设施改进速度跟不上黑客对系统破解的速度。

6）计算机病毒的威胁日益严重，现在不仅DOS病毒到处蔓延，而且已经出现了针对Windows、UNIX等各种操作系统的病毒，直接威胁网络数据库服务器的安全。目前还没有解决病毒的根本措施。

7）对于象中国这样的发展中国家，操作系统、网络系统与数据库系统和计算机这样核心的软、硬件都是外国公司研制的，整个国家信息的安全建筑在外国公司的“良知”与“友好”上，这是最大的不安全因素。

7、数据库的完整性体现在哪些方面，以及如何保证数据库的完整性。

1）在物理完整性方面，要求从硬件或环境方面保护数据库的安全，防止数据被破坏或不可读。例如，应该有措施解决掉电时数据不丢失不破坏的问题，存储介质损坏时数据的可利用性问题，还应该有防止各种灾害（如火灾、地震等）对数据库造

成不可弥补的损失，应该有灾后数据库快速恢复能力。数据库的物理完整性和数据库留驻的计算机系统硬件可靠性与安全性有关，也与环境的安全保障措施有关。

2）在逻辑完整性方面，要求保持数据库逻辑结构的完整性，需要严格控制数据库的创立与删除、库表的建立、删除和更改的操作，这些操作只能允许具有数据库拥有者或系统管理员权限的人才能够进行。逻辑完整性还包括数据库结构和库表结构设计的合理性，尽量减少字段与字段之间、库表与库表之间不必要的关联，减少不必要的冗余字段，防止发生修改一个字段的值影响其他字段的情况。

3）在元素完整性方面，元素完整性主要是指保持数据字段内容的正确性与准确性。元素完整性需要由DBMS、应用软件的开发者和用户共同完成。

相关文档：

- 信息安全导论论文
- 信息安全导论答案
- 信息安全导论试题
- 信息安全导论实验报告
- 信息安全导论第二版
- 信息技术考试练习题
- 信息安全论文
- 信息安全自查报告
- 信息安全技术论文
- 信息安全检查总结报告