第 3 章　身份认证与访问控制

3.1　第 3 章知识提要

本章主要介绍了身份认证和数字签名，基于生物特征、静态口令、动态口令、密钥分发、数字证书的身份认证，以及采用非对称密码体制的数字签名。为了保证消息的完整性，还需要采用消息认证或报文摘要法。常见的国际数字证书标准 X.509 以及以公开密钥加密法为中心的密钥管理体系结构 PKI、Kerberos 体制的数字认证，为了对合法用户进行权限划分，还介绍了自主、强制、基于角色的访问控制策略。从访问者的角度把系统分为主体和客体两部分，涉及访问控制矩阵、授权关系表、访问能力表、访问控制表等形式。

3.2　第 3 章习题和答案详解

一、选择题（答案：BBCCA DADBA DACB）

1. 用数字办法确认、鉴定、认证网络上参与信息交流者或服务器的身份是指_____。
   A. 接入控制
   B. 数字认证
   C. 数字签名
   D. 防火墙

答案：B

解答：只有B的定义与题中的描述相符。

2. 身份鉴别是安全服务中的重要一环，以下关于身份鉴别的叙述中，不正确的是_____。
   A. 身份鉴别是授权控制的基础
   B. 身份鉴别一般不用提供双向的认证
   C. 目前一般采用基于对称密钥加密或公开密钥加密的方法
   D. 数字签名机制是实现身份鉴别的重要机制

答案：B

解答：身份鉴别包括采用双向认证的方法，因此选择B。

3. 以下关于CA认证中心说法正确的是_____。
   A. CA认证是使用对称密钥机制的认证方法
   B. CA认证中心只负责签名，不负责证书的产生
   C. CA认证中心负责证书的颁发和管理，并依靠证书证明一个用户的身份

D. CA认证中心不用保持中立，可以随便找一个用户作为CA认证中心

答案：C

解答：CA（认证中心）负责证书的颁发和管理，并依靠证书证明一个用户的身份。

4. Kerberos的设计目标不包括_____。

A. 认证
B. 授权
C. 记账
D. 审计

答案：C

解答：Kerberos的设计目标不包括记账。

5. 访问控制是指确定_____以及实施访问权限的过程。

A. 用户权限
B. 可给予哪些主体访问权利
C. 可被用户访问的资源
D. 系统是否遭受入侵

答案：A

解答：访问控制是指确定用户权限以及实施访问权限的过程。

6. 下列对访问控制影响不大的是_____。

A. 主体身份
B. 客体身份
C. 访问类型
D. 主体与客体的类型

答案：D

解答：对访问控制影响不大的是主体与客体的类型。

7. 为了简化管理，通常对访问者_____，以避免访问控制表过于庞大。

A. 分类组织成组
B. 严格限制数量
C. 按访问时间排序，删除长期没有访问的用户
D. 不作任何限制

答案：A

解答：为了简化管理，通常对访问者分类组织成组，以避免访问控制表过于庞大。

8. PKI支持的服务不包括_____。

A. 非对称密钥技术及证书管理

B. 目录服务
C. 对称密钥的产生和分发
D. 访问控制服务

答案：D

解答：PKI服务不包括访问控制。

9. PKI的主要组成不包括_____。
A. 证书授权CA
B. SSL
C. 注册授权RA
D. 证书存储库CR

答案：B

解答：PKI的主要组成不包括SSL。

10. PKI管理对象不包括_____。
A. ID和口令
B. 证书
C. 密钥
D. 证书撤销

答案：A

解答：PKI管理对象不包括ID和口令。

11. 下面不属于PKI组成部分的是_____。
A. 证书主体
B. 使用证书的应用和系统
C. 证书权威机构
D. AS

答案：D

解答：PKI的组成部分包括政策批准结构（Policy Acception Authority，PAA），政策认证机构（Policy Certification Authority，PCA），认证机构（Certification Authority，CA），在线注册机构（Online Registration Authority，ORA），不包括AS。

12. PKI能够执行的功能是_____和_____。
A. 鉴别计算机消息的始发者
B. 确认计算机的物理位置
C. 保守消息的机密
D. 确认用户具有的安全性特权

答案：AC

解答：PKI能够执行的功能是鉴别计算机消息的始发者和保守消息的机密。

13. PKI的主要理论基础是_____。

A. 对称密码算法

B. 公钥密码算法

C. 量子密码

D. 摘要算法

答案：B

解答：PKI的主要理论基础是公钥密码算法。

二、填空题

答案：1. 身份认证，信源，信宿

2. 访问控制，访问权限

3. 数字证书，认证中心

1. 身份认证是验证信息发送者是真的，而不是冒充的，包括信源、信宿等的认证和识别。
2. 访问控制的目的是为了限制访问主体对访问客体的访问权限。
3. 数字证书是PKI的核心元素， 认证中心是PKI的核心执行者。

三、问答题

1. 简述生物特征身份认证的发展趋势。

答：提高生物特征识别的精确性和可靠性是未来的发展趋势。

2. 简述口令可能会遭受哪些攻击。

答：攻击口令的方式多种多样，常见的有以下 4 种。

（1）社会工程学。

（2）暴力破解。

（3）弱口令扫描。

（4）密码监听。

3. 假定只允许使用 26 个字母构造口令，在下列情况下各可以构造出多少条口令？

（1）口令最多可以使用 n 个字符，$n = 4$，6，8，不区分大小写。

（2）口令最多可以使用 n 个字符，$n = 4$，6，8，区分大小写。

答：（1）分别是 26 的 4 次方，26 的 6 次方，26 的 8 次方。

（2）分别是 52 的 4 次方，52 的 6 次方，52 的 8 次方。

4. 编写一个口令生成程序。程序以长度 s（可以取 s=8，16，32，64）的随机二进制种子作为输入。

（1）让多名用户使用你的程序生成口令，记录有多少人选择了相同的事件。

（2）生成一个口令并加密，然后让人通过尝试随机数种子的所有值进行口令攻击。事先要给定一个猜测次数的期望值。

答：略

5. 略

6. 比较动态口令的 3 种实现方式。

答：短信密码、软件令牌、硬件令牌。短信密码是通过手机短信形式发送 6 位或更多随机数的动态口令。软件令牌是通过软件生成随机密码。硬件令牌每 60s 变换一次动态口令。

7. 比较静态口令与动态口令。

答：静态口令不随时间变化，动态口令随时间而变化。

8. 常用动态令牌有哪几种？

答：（1）短信密码。

（2）手机令牌。

（3）硬件令牌。

（4）软件令牌。

9. 在身份验证中，可能会遇到重放攻击。重放具有如下几种形式：

（1）简单的重放：攻击者简单地复制信息，经过一段时间后，再重放原来的信息。

（2）重放不能被检测到：这时，原始的信息不能到达，只有重放信息到达目的地。

（3）没有定义的重放返回：发送者这时很难确定是发送信息，还是接收信息。

如何确定信息是否是重放的信息？

答：重放（replay）攻击是指在消息没有时间戳的情况下，攻击者利用身份认证机制中的漏洞先把别人有用的消息记录下来，过一段时间后再发送出去。

如果在发送信息中加上时间戳，就可以有效检测信息是否是重放信息。

10. 如何保护 IC 卡的安全？

答：对于 IC 卡，常用的攻击行为有以下 3 种。

（1）截取信道中的信息：通过非法设备以及相关技术手段读取 IC 卡中存储的数据信息以及在 IC 卡与读卡器进行操作时截取数据交换信息。

（2）破译 IC 卡中的信息：攻击者采用上述两种方式截获数据信息后，根据 IC 卡中数据信息的变化情况以及数据交换过程中数据流的变化对数据进行分析，从而确认 IC 卡中所有数据的含义以及数据流的变化规则，完成对 IC 卡中数据信息的破译，进而达到非法改变数据信息的目的。

（3）复制 IC 卡中的数据信息：攻击者在截获数据信息后，并不对数据进行分析破译，而是记录在特定操作中数据流的变化情况，在需要时将记录的数据流直接复制发送到 IC 卡，从而达到非法改变数据信息的目的。这种情况经常发生在当 IC 卡与读卡器之间进行数据交换采用加密处理的时候。

在上述描述的攻击方法中，第一种方式是手段，由于 IC 卡是由用户掌握和使用的，管理方无法实现实时跟踪，因此在现实中是无法阻止攻击者进行这种尝试的。第二、三种方式是数据分析处理，是攻击的目的所在。为此，在设计 IC 卡及其相关管理系统时，必须对数据的安全性给予高度重视，从某种角度来说，一个 IC 卡系统设计是否成功，关键在于其对数据安全性的处理。在 IC 卡及系统中使用的都是集成电路卡（IC 卡），集成电路卡的核心是采用集成电路芯片进行数据的存储。目前广泛使用的 IC 卡使用的是电可擦除数据存储芯片（EEPROM），这种芯片读写速度快，掉电后数据可以长期保存，并且数据可以反复进行擦写。IC 卡根据对 EEPROM 读写处理方式的不同，可以分为存储卡、逻辑加密卡以及智能卡（CPU 卡）三大类，它们具有不同的数据保护安全级别。

其中，存储卡是直接将 EEPROM 芯片封装在卡片上，外部设备可以直接访问到 EEPROM 中的任何一个单元。由于存储卡中只有 EEPROM 一个芯片，因此 IC 卡的对外接口实际上就是 EEPROM 的对外接口，这样，外部读写设备就可以十分方便地对 EEPROM 进行数据读写操作，作为 IC 卡而言，无法对合法或非法的读写设备进行判断和识别，非常容易进行攻击。存储卡只是用来对数据进行存储，而无法对数据进行安全性保护，因此存储卡不具备数据安全性保护措施，数据安全级别很低。

而逻辑加密卡是在将 EEPROM 芯片封装在卡片上的同时，将一组硬件逻辑电路也封装在卡片上，外部读写设备必须通过硬件逻辑电路的判断后，才能访问到 EEPROM 中的任何一个单元。由于在 IC 卡中存在一组硬件逻辑加密电路，EEPROM 芯片的接口并不直接对外，在初始状态，IC 卡芯片中的数据开关处于断开状态。外部读写设备在访问 IC 卡芯片中的 EEPROM 单元之前，必须首先发一组数据给硬件逻辑电路，硬件逻辑电路在判断数据的合法性后（即密码校验），才决定是否将 IC 卡内的开关闭合。只有密码校验正确后，硬件逻辑电路才能将开关闭合，这时外部读写设备才能对 EEPROM 中的数据进行读写操作，这样逻辑加密卡就可以对外部合法和非法的读写设备进行识别判断。通过这种方式，逻辑加密卡对内部 EEPROM 中的数据进行了安全性保护，因此逻辑加密卡具备数据安全性保护措施。但逻辑加密卡的安全性级别并不是很高，有两种攻击方式可以对其进行攻击测试：一种是当合法读写设备在发送数据进行密码校验时，非法设备可以跟踪到校验密码，这样，今后非法设备通过重放也可以通过密码校验，从而对逻辑加密卡进行数据攻击；另一种方法是非法设备在跟踪到合法设备已经通过逻辑加密卡的密码校验，IC 卡内部开关闭合后，再通过数据线对逻辑加密卡中 EEPROM 的数据进行攻击破坏。因此，逻辑加密卡虽然具备一定的数据安全性保护，但它的安全级别依然较低。

所以，要保证 IC 卡的安全性，须采用智能卡（CPU 卡）。智能卡是在将 EEPROM 芯片封装在卡片上的同时，将微处理器（CPU）芯片也封装在卡片上，外部读写设备只能通过 CPU 与 IC 卡内的 EEPROM 进行数据交换，在任何情况下都不能再访问到 EEPROM 中的任何一个单元。由于在智能卡中封装了微处理器芯片，这样，EEPROM 的数据接口在

任何情况下都不会与 IC 卡的对外数据线连接。外部读写设备在与智能卡进行数据交换时，首先必须发指令给 CPU，由 CPU 根据其内部 ROM 中存储的卡片操作系统（COS）对指令进行解释，并进行分析判断，在确认读写设备的合法性后，允许外部读写设备与智能卡建立连接。之后的数据操作仍然要由外部读写设备发出相应的指令，并且 CPU 对指令进行正确解释后，允许外部读写设备和智能卡中的数据存储区（RAM）进行数据交换，数据交换成功后，在 CPU 的控制下利用智能卡中的内部数据总线，再将内部 RAM 中的数据与 EEPROM 中的数据进行交换。可以看到，在数据处理过程中，外部读写设备只是和 CPU 打交道，同时数据交换也只能和数据缓存区 RAM 进行，根本无法实现对智能卡中 EEPROM 数据的直接访问，这样就实现了对智能卡 EEPROM 中数据的安全保护。由于智能卡内部具有 CPU 芯片，在具有数据判断能力的同时，也具备了数据分析处理能力，因此智能卡可以随时区别合法和非法读写设备，并且由于有了 CPU 芯片，具备数据运算能力，还可以对数据进行加密解密处理，因此具备非常高的安全性，其安全级别很高。

因此，为了保护 IC 卡的安全，应尽量选用智能卡作为 IC 卡系统的信息传递的介质。

11. 请画出带有时间戳的基于秘密密钥的身份验证过程。

答：Kerberos 身份验证过程如图 3-1 所示。

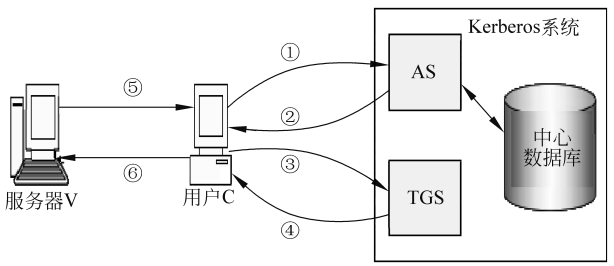


图 3-1　Kerberos 身份验证过程

（1）认证服务交换，用户从 AS 取得入场券。

① 客户向 AS 发出访问 TGS 请求（用 TS_1 表示新请求）：

$$C \rightarrow AS：E_{KC}[ID_C||ID_{TGS}||TS_1]$$

② AS 向 C 发出应答：

$$AS \rightarrow C：E_{KC}[K_C,TGS||ID_{TGS}||TS_2||Lifetime_2||Ticket_{TGS}]$$

其中

$$Ticket_{TGS}= E_{KT}[K_{CT}||ID_C||AD_C ||ID_T||TS_2||Lifetime_2]$$

（2）入场券许可服务交换，用户从 TGS 获取服务许可凭证。

③ C 向 TGS 发出请求，内容包括服务器识别码、入场券和一个认证符。

$$C \rightarrow TGS：E_{KCT}[ID_S||Ticket_{TGS}||Authenticator_C]$$

其中

$$Ticket_{TGS}= E_{KT}[K_{CT}|ID_C||AD_C ||ID_T||TS_2||Lifetime_2]$$

$$Authenticator_C= E_{KCT}[ID_C||AD_C||TS_3]$$

④ TGS 验证后，向 C 发出服务许可凭证：

TGS→C：$E_{KCT}[K_{CS}||ID_S||TS_4||\ Ticket_S]$

其中

$Ticket_S= E_{KTS}[K_{CS}||ID_C||AD_C\ ||ID_S||TS_4||Lifetime_4]$

（3）客户-服务器相互认证交换，用户从服务器获取服务。

⑤ C 向服务器证明自己身份（用 $Ticket_S$ 和 $Authenticator_C$）

C→S：$E_{KCS}[Ticket_S||Authenticator_C\ ]$

其中

$Ticket_S= E_{KTS}[K_{CS}||ID_C||AD_C\ ||ID_S||TS_4||Lifetime_4]$

$Authenticator_C= E_{KCS}[ID_C||AD_C||TS_5]$

⑥ 服务器向客户证明自己身份。

S→C：$E_{KCS}[TS_5+1]$

这个过程结束，客户 C 与服务器 S 之间就建立起了共享会话密钥，以便以后进行加密通信或交换新密钥。

12. 简述认证机构的严格层次结构模型的性质。

答：层次结构中的所有实体都信任唯一的根 CA。在认证机构的严格层次结构中，每个实体(包括中介 CA 和终端实体)都必须拥有根 CA 的公钥，该公钥的安装是在这个模型中为随后进行的所有通信进行证书处理的基础，因此，它必须通过一种安全（带外）的方式完成。

值得注意的是，在一个多层的严格层次结构中，终端实体直接被其上层的 CA 认证（也就是颁发证书），但是它们的信任锚是另一个不同的 CA（根 CA）。

13. 证书管理由哪 3 个阶段组成，每个阶段包括哪些具体内容？

答：证书管理的 3 个阶段及具体内容说明如下。

（1）初始化阶段。

A. 终端实体注册

终端实体注册是单个用户或进程的身份被建立和验证的过程。注册过程能够通过不同的方法实现。终端实体注册是在线执行的，是用注册表格的交换说明的。注册过程一般要求包括将一个或更多的共享秘密赋给终端实体，以便后来在初始化过程中 CA 确认那个个体。

B. 密钥对产生

密钥资料可以在终端实体注册过程前或直接响应终端实体注册过程时产生。在 RA 中或在 CA 中产生密钥资料是可能的。每个终端实体多个密钥可以被用作支持分离的和截然不同的服务。例如，一个密钥对可以被用作支持不可否认性服务，而另一个密钥对可以被用作支持机密性或密钥管理功能（双密钥对模型）。

C. 证书创建和密钥/证书分发

无论密钥在哪里产生，证书创建的职责都将单独地落在被授权的 CA 上。如果公钥是被终端实体，而不是 CA 所产生的，那么该公钥必须被安全地传送到 CA，以便其能够被放入证书。

一旦密钥资料和相关的证书已经被产生，它们就必须被适当分发。请求证书和从可信实体（即 CA）取回证书（以及相关的密钥，如果适用的话）的必要条件是要求有一个安全协议机制。

D. 证书分发

如果私钥和相应的公钥证书已经被分发，那么就有一种或多种传送给另一个实体的方法。

- 带外分发。
- 在一个公众的资料库或数据库中公布，以使查询和在线检索简便。
- 带内协议分发。例如，包括带有安全 E-mail 报文的适用的验证证书。

被用作数字签名目的的证书可以仅需要分发给它们的所有者，被用作机密性目的的证书对于发信方必须是容易获得的。

E. 密钥备份和托管

一定比例的加密密钥将因为许多原因（忘记密码、磁盘被破坏、失常的智能卡或雇员被解雇）使这些密钥的所有者无法访问，这就需要事先进行密钥备份。

密钥托管是指把一个秘密的密钥或私钥交由第三方保管，这样做的问题是哪些密钥应委托保管以及谁是可以信任的第三方（政府？）。

（2）颁布阶段。

A. 证书检索

证书检索与访问一个终端实体证书的能力有关。检索一个终端实体证书的需求可能被两个不同的使用要求所驱动。

- 加密发给其他实体的数据的需求。
- 验证一个从另一个实体收到的数字签名的需求。

B. 证书验证

证书验证与评估一个给定证书的合法性和证书颁发者的可信赖性有关。证书验证是在基于那个证书被准许加密操作前进行的。

C. 密钥恢复

密钥管理生命周期包括从远程备份设施（如可信密钥恢复中心或 CA）中恢复私有加密密钥的能力。密钥的恢复能使 PKI 管理员和终端用户的负担减至最小，这个过程必须尽可能最大程度自动化。

D. 密钥更新

当证书被颁发时，其被赋予一个固定的生存期。当证书“接近”过期时，必须颁发一个新的公/私钥和相关证书，这被称为密钥更新。应该允许一个合理的转变时间使依托方取得新证书，从而避免与过期证书所有有关的服务中断。这个过程是自动的，并对终端用户完全透明。

（3）取消阶段。

A. 证书过期

证书在颁布时被赋予一个固定的生存期，在其被建立的有效期结束后，证书将会过期。当一个证书过期后，与该证书有关的终端实体可能发生 3 件事。

- 没有活动：终端实体不再参加 PKI。
- 证书恢复：相同的公钥被加入新有效期的新证书（当与最初证书的颁布有关的环境没有变化时使用，并且它仍然认为是可靠的）。
- 证书更新：一个新的公/私钥对被产生，并且一个新的证书被颁发。

B. 证书撤销

在证书自然过期前对给定证书的即时取消（可疑的密钥损害、作业状态的变化或者雇用终止等）。

一个终端用户个人可以亲自初始化自己的证书撤销（例如，由于相应私有密钥的可疑损害）。RA 可以代表终端用户被用作初始化证书撤销。经授权的管理者也可以有能力撤销终端实体的证书。

C. 密钥历史

由于机密性加密密钥最后要过期，因此可靠安全地存储用作解密的私有密钥是必需的，这被称作密钥历史，否则无法恢复。

D. 密钥档案

可靠地保存已经过期的用于验证数字签名的公钥，以便对历史文档的数字签名进行验证。

14. 简述使用密钥的身份认证的分类方法。

答：有基于公钥加密认证协议的双向认证和单向认证，以及基于单钥加密认证协议的双向认证和单向认证方法。

15. 简述 Kerberos 身份认证的异域认证过程。

答：如图 3-2 所示。

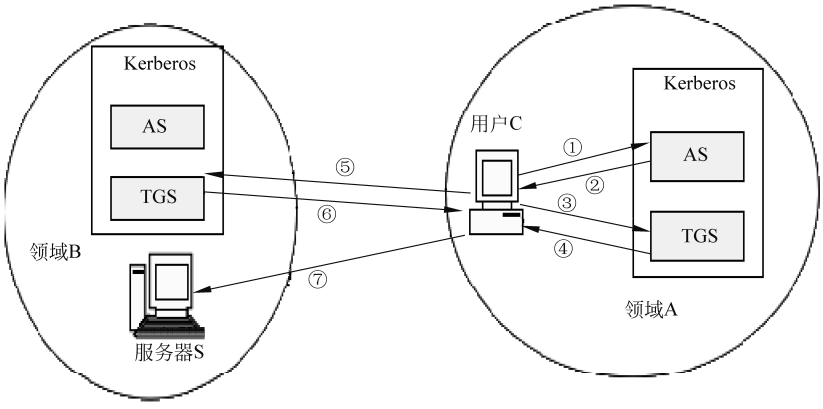


图 3-2　Kerberos 身份认证的异域认证过程

① C→AS：E_{KC} [ID_C || ID_T ||TS_1]。

② AS→C：E_{KC}[K_{CT} ||ID_T || TS_2 || $Lifetime_2$ || $Ticket_{TGS}$]。

③ C→TGS：E_{KCT} [ID_{TB} || $Ticket_{TGS}$ || $Authenticator_C$]（ID_{TB} 为 B 域 TGS_B 标识）。

④ TGS→C：E_{KCT} [K_{CTB}||ID_{TB}||TS_4|| $Ticket_{TB}$] （K_{CTB} 为 C 与 TGS_B 会话密钥）。

$Ticket_{TB}$= E_{KTB}[K_{CTB}||ID_C||AD_C ||ID_{TB}||TS_4||$Lifetime_4$]

⑤ C→TGS_B：E_{KCTB} [ID_{TB}||$Ticket_{TB}$||$Authenticator_C$]。

⑥ TGS_B→C：E_{KCTB} [K_{CS} || ID_{TB} || ||TS_6 || $Ticket_{TB}$]。

⑦ C→S：E_{KCS} [$Ticket_{TB}$||$Authenticator_C$]。

其中，K_C 为 C 的用户主密钥，由 C 上的用户口令导出；可与 AS 共享，记为 K_{CA}。

K_S 为 S 服务器主密钥，可与 TGS 共享，也记为 K_{ST}。

K_T 为 TGS 主密钥，可与 AS 共享，记为 K_{AT}。

K_{CT} 为 C 与 TGS 会话密钥。

K_{TS} 为 TGS 与 S 会话密钥。

K_{CS} 为 C 与 S 会话密钥。

16. 简述 X.509 证书包含的内容。

答：X.509 公开密钥证书包含下列内容。

（1）版本，指明这个证书符合 ITU-T X.509 建议的哪个版本格式。X.509 现在已经有 1，2，3 共 3 个版本。

（2）序列号，由发布证书的 CA 分配。这个序列号在该 CA 发布的所有证书中是唯一的。

（3）算法标识符，指明证书数字签名的算法。

（4）发布者，表明发布和签署该证书的 CA。

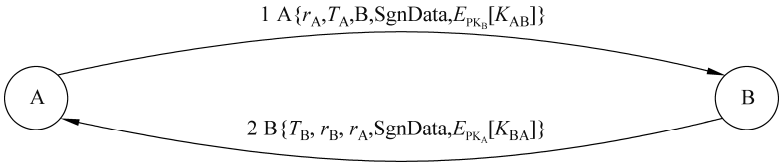
（5）有效期，包含起始两个日期。

（6）主体，定义名字或者是其他的身份标识，表明这个证书发给哪个用户。例如，主体域可能包含名字和住址。

（7）公开密钥信息，包含用户的公开密钥和使用这个密钥的算法。

（8）签名，证书的数字签名。

17. 简述 X.509 的双向认证过程。



答：X.509 建议 3 种认证过程：一次认证（也称单向认证）、二次认证（也称双向验证）和三次认证过程。

双向认证过程即 A 不仅要向 B 发送验证凭证消息，B 也要通过应答证明以下几点：ID_B 的身份，应答是由 B 发出的，应答的接收者是 A，应答报文是完整和及时的。

18. 试述数字证书的原理。

答：数字证书采用公开密钥体制（如 RSA）。每个用户设定一仅为本人所知的私有密

钥，用它进行解密和签名；同时设定一公开密钥，为一组用户所共享，用于加密和验证签名。

采用数字证书，能够确认以下两点。

（1）保证信息是由签名者自己签名发送的，签名者不能否认或难以否认。

（2）保证信息自签发后到收到为止未曾做过任何修改，签发的信息是真实信息。

19. 查阅资料，简述有关 PKI 的标准及其相关产品。

答：PKI 标准：

（1）X.209（1988）ASN.1 基本编码规则的规范。

（2）X.500（1993）信息技术之开放系统互联。

（3）X.509（1993）信息技术之开放系统互联。

（4）PKCS 系列标准。

随着网络应用的不断普及深入，PKI 的市场正在不断扩大。现在，市场上涌现出了很多 PKI 产品，如

（1）Baltimore 公司的 UniCERT。

（2）Entrust 公司的 PKI 产品-Entrust/PKI 5.0。

（3）VeriSign 公司的 OnSite。

20. PKI 可以提供哪些安全服务？PKI 体系中包含了哪些与信任有关的概念？

答：通过数字证书，可以提供身份的认证与识别，完整性、保密性和不可否认等安全服务。在 PKI 中，我们可以把信任定义具体化为：如果一个用户假定 CA 可以把任一公钥绑定到某个实体上，则他信任该 CA。

21．叙述基于 X.509 的数字证书在 PKI 中的作用。

答：PKI（Public Key Infrastructure）是一个以公开密钥加密法为中心的密钥管理体系结构，它能提供公开密钥加密和数字证书服务，采用证书管理公钥，通过第三方的可信任机构 CA (Certificate Authority)把用户的公钥和用户的其他标识信息（如名称、E-mail、身份证号等）捆绑在一起，在 Internet 上验证用户的身份，即使用数字证书提供用户的公开密钥，让可信任第三方——数字证书认证中心（CA）签署用户的公开密钥。目前广泛认可的 PKI 是以 ITU-T 的 X.509 数字证书第 3 版为基础的结构。

22. 解释访问控制的基本概念。

答：访问控制是建立在身份认证基础上的，通过限制对关键资源的访问，防止非法用户的侵入或因为合法用户的不慎操作而造成的破坏。

访问控制的目的是限制主体对访问客体的访问权限（安全访问策略），从而使计算机系统在合法范围内使用。

23. 访问控制有几种常用的实现方法？它们各有什么特点？

答：（1）访问控制矩阵。

行表示客体（各种资源），列表示主体（通常为用户），行和列的交叉点表示某个主体对某个客体的访问权限。通常，一个文件的 Own 权限表示可以授予（authorize）或撤销（revoke）其他用户对该文件的访问控制权限。

（2）访问能力表。

实际的系统中虽然可能有很多的主体与客体，但两者之间的权限关系并不多。为了减少系统的开销与浪费，可以从主体（行）出发，表达矩阵某一行的信息，这就是访问能力表（capabilities）。

只有当一个主体对某个客体拥有访问能力时，它才能访问这个客体。但是，要从访问能力表获得对某一特定客体有特定权限的所有主体就比较困难。在一个安全系统中，正是客体本身需要得到可靠的保护，访问控制服务也应该能够控制可访问某一客体的主体集合，于是出现了以客体为出发点的实现方式——ACL。

（3）访问控制表。

也可以从客体（列）出发，表达矩阵某一列的信息，这就是访问控制表（Access Control List）。它可以对某一特定资源指定任意一个用户的访问权限，还可以将有相同权限的用户分组，并授予组的访问权。

（4）授权关系表。

授权关系表（authorization relations）的每一行都表示了主体和客体的一个授权关系。对表按客体进行排序，可以得到访问控制表的优势；对表按主体进行排序，可以得到访问能力表的优势。授权关系表适合采用关系数据库实现。

24. 在信息系统内主体通常指什么？客体通常指什么？

答：主体通常指用户，客体通常指资源。

25. 查找资料，分别给出几个自主访问控制、强制访问控制和基于角色的访问控制的实例。

答：（1）“拥有者/同组用户/其他”模式：在 UNIX、Linux、VMS 等系统中，实现了一种十分简单、常用而有效的自主访问控制模式，就是在每个文件上附加一段有关访问控制信息的二进制位，这些二进制位反映了不同类别用户的存取方式，即文件的拥有者、文件拥有者同组的用户和其他用户。

这种模式的一个很大缺点就是，客体的拥有者不能够精确控制某个用户对其客体的访问权，如不能够指定与 owner 同组的用户 A 能够对该客体具有读、写、执行权限，而与 owner 同组的用户 B 不可以对该客体有任何权限。

（2）强制访问控制已经在许多基于安全内核的系统中得以实现，并转换到许多非内核化的操作系统中，包括 Honeywell 公司的 Multics、DEC 公司的 SES/VMS 以及 Sperry 公司的 1100 操作系统。这里，以 UNIX SVR 4.1ES 安全操作系统的强制访问控制机制为例加以说明。

安全操作系统 UNIX SVR 4.1ES 的强制访问控制机制分别对系统中的主体和客体赋予了相应的安全级，并采用了多级安全规则。

A. 主体的安全级。主体的安全级即用户的安全级以及代表用户进行工作的进程的安全级。用户的安全级是系统管理员根据安全策略，使用 adduser 命令创建用户时设置的。系统在用户安全文件档中为每个用户建立一项，表明该用户的安全级范围，并说明其默认安全级。默认安全级在该用户的安全级范围之内。

用户登录系统时，他可以指定本次登录的安全级，指定安全级必须在其安全级范围之内。成功登录后，系统将用户本次指定的安全级设置给为该用户创建的 shell 进程。如果用户不指定登录安全级，系统则将该用户的默认安全级设置给为该用户创建的 shell 进程。

B. 客体的安全级。客体安全级的确定和赋值是根据客体的类型按以下规则进行的文件、有名管道的安全级。文件、有名管道的安全级为创建该客体进程的安全级，且客体的安全级必须等于其父目录的安全级，保存在相应的磁盘 Inode 节点和内存 Inode 节点中。

进程、消息队列、信号量集合和共享存储区的安全级。这组类型的客体不具有文件系统表示形式，其安全级为创建进程的安全级，保存在内存相应的数据索引结构中。

目录的安全级。目录同普通文件一样，在它们的生存周期内具有一个安全级，所不同的是目录的结构须满足兼容性。一个进程创建一个目录，目录的安全级即为创建其进程的安全级，且目录的安全级须大于或等于其父目录的安全级。同文件一样，它保存在相应的磁盘 Inode 节点和内存 Inode 节点中。

C. 设备的安全级。系统在设备安全文档中说明系统中每个设备的安全属性，如设备的最高安全级、最低安全级等。设备还具有当前安全级，一个设备的当前安全级为调用该设备的用户进程、系统进程或系统服务进程的安全级。设备的当前安全级必须在设备的最大安全级与最小安全级之间。

另外，设备分为单级设备和多级设备。多级设备可以包含多个安全级数据。这个设备只能由具有适当特权的进程打开（open），包括内核和系统进程、具有适当特权的管理员进程。磁盘和存储器设备就是多级设备。单级设备在某个时刻只能处理单一安全级的数据。这类设备包括终端和用于某个相应状态的磁带机和软盘驱动器。如果一个设备用作一个公用（public）资源，那么它必须是单级设备。具有适当特权的管理员可以将这些设备用作多级设备，如产生一个系统的磁带备份。

通常，一个用户在登录时访问一个终端设备，这个用户将以某个安全级在该终端上进入系统。如果这个安全级不在这个终端所定义的安全级范围之内，这个登录就会失败。如果登录成功，这个设备的安全级就被设置成用户登录时使用的安全级。

要使用磁带或软盘设备，或者不是在登录时访问终端设备，用户必须要求管理员分配（allocate）设备，管理员以某个安全级将此设备分配给这个用户。如果这个安全级不在设备的安全级范围之内，这个分配将失败。如果成功，用户就成为这个设备的所有者（owner）。此时文件的 DAC 设置为 600，设备安全级为分配命令中给定的安全级，并且管理员将通知用户这个操作已经成功。如果用户当前的安全级等于分配的安全级，用户就可以任意使用这些设备了。

还有少量设备不属于以上两种分类而需要特别处理，包括/dev/null、/dev/zero、/dev/tty。由于数据并不流过这些设备，所以用户随时都可以访问这些设备。

（3）基于角色的访问控制的实例包括北仑国际集装箱码头有限公司基于该控制系统的

软件，包括 *Polaris*（码头生产管理系统）、《费收发票管理系统》《人事工资管理系统》等。基于 RBAC 模型的权限管理系统的实现技术方案简化了开发人员的开发工作，也使用户在进行权限分配时更加直观灵活，并支持岗位、权限多变的需求。

26. 比较自主访问控制、强制访问控制和基于角色的访问控制。

答：自主访问控制（Discretionary Access Control，DAC）由客体的属主对自己的客体进行管理，由属主自己决定是否将自己的客体访问权或部分访问权授予其他主体，这种控制方式是自主的。也就是说，在自主访问控制下，用户可以按自己的意愿，有选择地与其他用户共享他的文件。强制访问控制的基本思想是不允许单个用户确定访问权限，只有系统管理员才可以确定用户或用户组的访问权限。MAC 主要用于多层次安全级别的系统（如军事系统）中。优点是具有更强的访问控制能力，缺点是工作量大，管理不便以及不灵活。基于角色的访问控制（Role-Base Access Control，RBAC）是以角色而非个体设计的访问控制策略，一个个体可以有多重角色，一个角色可以由多人承担，由于角色比个体具有较大的稳定性，这种访问控制比针对个体的自主访问控制和强制访问控制在可操作性和可管理性方面都要强得多。

27. 查找资料，说明还有哪些新的访问控制策略。

答：利用层次分析法，根据用户流量特征对用户的信任度进行评估，采用基于信任度的访问控制策略，并根据信任度动态调整网络防御路径，实现对内部威胁的实时防护。具体实现如下：访问控制应用（ACA）为 SDN 控制器的上层应用，是整个系统的核心。ACA 通过 SDN 控制器获取数据层面的信息和用户的身份信息，通过流量分析设备获得用户的行为信息，并能够从用户信息数据库中获取用户的权限信息。利用层次分析法（Analytic Hierarchy Process，AHP），结合层次结构模型将用户的总体信任度分解为子信任度，再将子信任度分解为更细的数据单元，即信任度证据，然后再从下层到上层进行系统的组合。这种先分解再组合的方法能够解决用户信任评估中的不确定性、主观性。AHP 可分为 5 个步骤：①建立层次结构模型；②构造判断矩阵；③层次单排序及一致性检验；④层次总排序；⑤层次总排序一致性检验。

根据常见的内部威胁类型，将用户总体信任度分解为 5 个子信任度，即身份安全子信任度、越权访问安全子信任度、流量安全子信任度、畸形数据包安全子信任度、扫描攻击安全子信任度。身份安全子信任度主要代表用户身份的可信程度；越权访问安全子信任度主要代表越权访问的严重程度；流量安全子信任度主要代表用户发动流量型攻击的可能性；畸形数据包安全子信任度代表用户发动畸形包攻击的可能性；扫描攻击安全子信任度代表用户扫描网络中主机和端口的可能性。

通过层次分析法可以得到总体信任度和 5 个子信任度的值。上述 6 个信任度值作为系统选取访问控制策略的依据。系统每隔一段时间计算一次信任度的值，并根据得到的信任度决定是否需要进行访问控制策略的变更。

第 4 章　网络安全防护

4.1　第 4 章知识提要

本章习题详细解答了关于防火墙、Internet 安全协议、VPN、入侵检测系统、网络诱骗、蜜罐技术等方面的常见问题和实践思路。

4.2　第 4 章习题和答案详解

一、选择题（答案：BCADC BDBDD DBACA DABBC CADDA）

1．防火墙用于将Internet和内部网络隔离，是_____。

A. 防止Internet火灾的硬件设施
B. 网络安全和信息安全的软件和硬件设施
C. 保护线路不受破坏的软件和硬件设施
D. 起抗电磁干扰作用的硬件设施

答案：B

解答：防火墙的主要作用是保护系统安全，由硬件和软件联合实现。

2. 防火墙最主要被部署在_____位置。

A. 网络边界
B. 骨干线路
C. 重要服务器旁
D. 桌面终端

答案：C

解答：根据题意，防火墙主要被部署在重要服务器旁最切合答案。

3. 下列关于防火墙的说法中错误的是_____。

A. 防火墙工作在网络层
B. 防火墙对IP数据包进行分析和过滤
C. 防火墙是重要的边界保护机制
D. 部署防火墙，就解决了网络安全问题

答案：A

解答：目前的硬件防火墙可以在第二层至第七层工作，即可以作链路层访问控制（MAC）到应用层访问控制（关键字过滤等），不只是在网络层，因此选A。

4. 在一个企业网中，防火墙应该是_____的一部分，构建防火墙时首先要考虑其保护的范围。

A. 安全技术
B. 安全设置
C. 局部安全策略
D. 全局安全策略

答案：D

解答：防火墙是全局安全策略的一部分。

5. 一般而言，Internet防火墙建立在一个网络的_____。

A. 内部子网之间传送信息的中枢
B. 每个子网的内部
C. 内部网络与外部网络的交叉点
D. 部分内部网络与外部网络的结合处

答案：C

解答：一般而言，Internet防火墙建立在一个网络的内部网络与外部网络的交叉点。

6. 包过滤型防火墙从原理上看是基于_____进行数据包分析的技术。

A. 物理层
B. 数据链路层
C. 网络层
D. 应用层

答案：B

解答：根据包过滤型防火墙的定义，应该选B。

7. 对非军事DMZ而言，正确的解释是_____。

A. DMZ是一个真正可信的网络部分
B. DMZ网络访问控制策略决定允许或禁止进入DMZ通信
C. 允许外部用户访问DMZ系统上合适的服务
D. 以上3项都是

答案：D

解答：对非军事DMZ而言，正确的解释是 DMZ是一个真正可信的网络部分，DMZ网络访问控制策略决定允许或禁止进入DMZ通信，允许外部用户访问DMZ系统上合适的服务，所以选D。

8. 对动态网络地址交换（NAT），不正确的说法是_____。

A. 将很多内部地址映射到单个真实地址

B. 外部网络地址和内部地址一对一地映射
C. 每个连接使用一个端口
D. 最多可有64 000个同时的动态NAT连接

答案：B

解答：对动态网络地址交换（NAT），外部网络地址和内部地址不是一对一的映射，借助于NAT，私有（保留）地址的“内部”网络通过路由器发送数据包时，私有地址被转换成合法的IP地址，一个局域网使用少量IP地址（甚至1个）即可实现私有地址网络内所有计算机与Internet的通信需求，因此选B。

9. 以下_____不是包过滤防火墙主要过滤的内容。
A. 源IP地址
B. 目的IP地址
C. TCP源端口和目的端口
D. 时间

答案：D

解答：包过滤防火墙主要过滤的内容不包括时间，因此选D。

10. 在被屏蔽的主机体系中，堡垒主机位于_____中，所有的外部连接都经过滤路由器到它上面去。
A. 内部网络
B. 周边网络
C. 外部网络
D. 自由连接

答案：D

解答：在被屏蔽的主机体系中，堡垒主机位于自由连接处。

11. 外部数据包经过过滤路由只能阻止_____的唯一IP欺骗。
A. 内部主机伪装成外部主机IP
B. 内部主机伪装成内部主机IP
C. 外部主机伪装成外部主机IP
D. 外部主机伪装成内部主机IP

答案：D

解答：外部数据包经过过滤路由只能阻止外部主机伪装成内部主机IP的唯一IP欺骗。

12. IPSec协议工作在网络的_____。
A. 数据链路层
B. 网络层
C. 应用层

D. 传输层

答案：B

解答：IPSec协议工作在网络的网络层。

13. IPSec协议中涉及密钥管理的重要协议是_____。

A. IKE
B. AH
C. ESP
D. SSL

答案：A

解答：IPSec协议中涉及密钥管理的重要协议IKE（Internet Key Exchange）。

14. SSL产生会话密钥的方式是_____。

A. 从密钥管理数据库中请求获得
B. 每一台客户机分配一个密钥的方式
C. 随机由客户机产生并加密后通知服务器
D. 由服务器产生并分配给客户机

答案：C

解答：SSL产生会话密钥的方式是：随机由客户机产生并加密后通知服务器。

15. 传输层保护的网络采用的主要技术是建立在_____基础上的_____。

A. 可靠的传输服务　安全套接字层（SSL）协议
B. 不可靠的传输服务　S-HTTP
C. 可靠的传输服务　S-HTTP
D. 不可靠的传输服务　安全套接字层（SSL）协议

答案：A A

解答：传输层保护的网络采用的主要技术是建立在可靠的传输服务基础上的安全套接层（SSL）协议。

16. 主要用于加密机制的协议是_____。

A. HTTP
B. FTP
C. Telnet
D. SSL

答案：D

解答：主要用于加密机制的协议是SSL。

17. 通常所说的移动VPN是指_____。

A. Access VPN
B. Intranet VPN
C. Extranet VPN
D. 以上均不是

答案：A

解答：通常所说的移动VPN是指 Access VPN。

18. 以下属于第二层的VPN隧道协议有_____。
A. IPSec
B. PPTP
C. GRE
D. 以上均不是

答案：B

解答：属于第二层的VPN隧道协议有PPTP。

19. 将公司与外部供应商、客户及其他利益相关群体相连接的是_____。
A. 内联网VPN
B. 外联网VPN
C. 远程接入VPN
D. 无线VPN

答案：B

解答：将公司与外部供应商、客户及其他利益相关群体相连接的是外联网VPN。

20. 以下不属于隧道协议的是_____。
A. PPTP
B. L2TP
C. TCP/IP
D. IPSec

答案：C

解答：TCP/IP 不属于隧道协议。

21. 以下不属于VPN核心技术的是_____。
A. 隧道技术
B. 身份认证
C. 日志记录
D. 访问控制

答案：C

解答：日志记录不属于VPN核心技术。