第十二章 保护和安全

1. 系统安全性的主要目标是什么?

答：操作系统安全性的主要目标是方便人机交互。

1. 系统安全性的复杂性表现在哪几个方面?

答: 系统安全性的复杂性表现在应用复杂、结构复杂、结果复杂、过程复杂等。

1. 对系统安全性的威胁有哪几种类型?

答：内部威胁，包括系统自身的漏洞，计算机硬件的突发故障等

外部威胁，包括网络上的病毒，网络上的恶意攻击等

1. 可信任计算机系统评价标准将计算机系统的安全度分为哪几个等级?

答：7个级别。分别是D1 C1 C2 B1 B2 B3 A

1. 何谓对称加密算法和非对称加密算法?

答：对称加密算法是加密和解密时使用相同的密钥，主要用于保证数据的机密性。非对称加密算法也叫公开密钥算法，其加密和解密是相对独立的，使用不同的密钥。

1. 什么是易位法和置换算法?

答：易位法是按照一定的规则，重新安排明文中的比特或字符的顺序来形成密文，而字符本身保持不变。

置换算法是按照一定的规则，用一个字符去置换另一个字符来形成密文。

1. 非对称加密算法的主要特点是什么?

答：算法强度复杂、安全性依赖于算法与密钥但是由于其算法复杂，而使得加密解密速度没有对称加密解密的速度快。对称密码体制中只有一种密钥，并且是非公开的，如果要解密接得让对方知道密钥。所以保证其安全性就是保证密钥的安全，而非对称密钥体制有两种密钥，其中一个是公开的，这样就可以不需要像对称密码那样传输对方的密钥了这样安全性就大了很多。

1. 保密数据签名的加密和解密方式是什么?

答：它使用一对数学上相关的钥匙，其中一个(公钥)用来加密信息，另一个(私钥)用来解密信息。PGP采用的传统加密技术部分所使用的密钥称为"会话密钥"(sek)。每次使用时，PGP都随机产生一个128位的IDEA会话密钥，用来加密报文。公开密钥加密技术中的公钥和私钥则用来加密会话密钥，并通过它间接地保护报文内容。

1. 数字证明书的作用是什么?

答：信息的保密性、交易者身份的确定性、不可否认性、不可修改性

数字安全证书提供了一种在网上验证身份的方式。安全证书体制主要采用了公开密钥体制，其它还包括对称密钥加密、数字签名、数字信封等技术。

1. 可利用哪几种方式来确定用户身份的真实性?

答：加密技术、认证技术和电子安全协议等。

1. 在基于口令机制的认证技术中,通常应满足哪些要求?

答：口令长度适中，口令内容不能过于单一。

1. 基于物理标志的认证技术又可细分为哪几种?

答：基于磁卡的认证技术和基于IC卡的认证技术

1. 智能卡可分为哪几种类型?

答：金融卡、非金融卡、交通卡、政府应用卡

1. 被选用的生理标志应具有哪几个条件?

答：应具有足够的可变性。

1. 一个生物识别系统通常是由哪几部分组成?

答：生物识别系统通常由离线注册部分和在线识别部分组成。

16,早期常采用的内部攻击方式有哪些?

答：窃取尚未清除的有用信息

17.何谓逻辑炸弹?较常用的引爆条件有哪些?

答：“逻辑炸弹”是指在特定逻辑条件满足时，实施破坏的计算机程序，该程序触发后造成计算机数据丢失、计算机不能从硬盘或软盘引导，甚至会使整个系统瘫痪，并出现物理损坏的虚假现象。

较常用的引爆条件有事件触发、事件触发、计数器触发等

18.何谓陷阱门和特洛伊木马?

答：陷阱门其实就是一段代码，是进入一个程序的隐蔽入口点。

特洛伊木马是一种基于[远程控制](http://www.so.com/s?q=%E8%BF%9C%E7%A8%8B%E6%8E%A7%E5%88%B6&ie=utf-8&src=internal_wenda_recommend_textn)的[黑客工具](http://www.so.com/s?q=%E9%BB%91%E5%AE%A2%E5%B7%A5%E5%85%B7&ie=utf-8&src=internal_wenda_recommend_textn)，具有很强的隐蔽性和危害性。

19.何谓缓冲区溢出?

答：是一种非常普遍、非常危险的漏洞，在各种操作系统、应用软件中广泛存在。利用[缓冲区溢出攻击](https://baike.so.com/doc/2223028-2352153.html)，可以导致程序运行失败、系统宕机、重新启动等后果。更为严重的是，可以利用它执行非授权指令，甚至可以取得系统特权，进而进行各种非法操作。

20.什么是病毒和蠕虫?

答：蠕虫病毒是一种常见的计算机病毒。它是利用网络进行复制和传播，传染途径是通过网络和电子邮件。最初的蠕虫病毒定义是因为在DOS环境下，病毒发作时会在屏幕上出现一条类似虫子的东西，胡乱吞吃屏幕上的字母并将其改形。

21.什么是移动代码? 为什么说在应用程序中包含了移动代码就可能不安全?

答：如果一个程序在运行时，能在不同机器之间来回迁移，那么该程序就被称为移动代码。在应用程序中可移动变量会导致程序出错。

22.计算机病毒的特征是什么?

答：计算机病毒具有传播性、隐蔽性、感染性、潜伏性、可激发性、表现性或破坏性的特点。

23.计算机病毒有哪几种类型?

答：系统病毒、蠕虫病毒、木马病毒、脚本病毒、宏病毒、后门病毒、病毒种植程序病毒、破坏性程序病毒、玩笑病毒、捆绑机病毒。

24.什么是文件型病毒?

答：文件型病毒系[计算机病毒](https://baike.so.com/doc/336385-356249.html)的一种，主要通过感染计算机中的[可执行文件](https://baike.so.com/doc/6452170-6665855.html)(.exe)和命令文件(.com)。文件型病毒是对计算机的[源文件](https://baike.so.com/doc/5328907-5564079.html)进行修改，使其成为新的带毒文件。一旦计算机运行该文件就会被感染，从而达到传播的目的。

25.病毒设计者采取了哪几种隐藏方式来让病毒逃避检测?

答：(1)隐藏于目录和注册表空间 (2)隐藏于程序的页内零头里。

(3)更改用于磁盘分配的数据结构(4)更改坏扇区列表。

26.用户可采用哪些方法来预防病毒?

答：(1)定期在外存备份重要软件和数据 (2)使用安全性高的操作系统(3)使用正版软件 (4)使用高性能反病毒软件(5) 不轻易打开来历不明的电子邮件 (6)定期检查外存并清除病毒

27.基于病毒数据库的病毒检测方法是什么?

答：(1)建立病毒数据库 (2)扫描硬盘上的可执行文件