# 第 3 章 操作系统安全

## 3.1 国际安全评价标准的发展及其联系

计算机系统安全评价标准是一种技术性法规。在信息安全这一特殊领域，如果没有这一标准，与此相关的立法、执法就会有失偏颇，最终会给国家的信息安全带来严重后果。由于信息安全产品和系统的安全评价事关国家的安全利益，因此许多国家都在充分借鉴国际标准的前提下，积极制订本国的计算机安全评价认证标准。

第一个有关信息技术安全评价的标准诞生于 20 世纪 80 年代的美国，就是著名的《可信计算机系统评价准则》(Trusted Computer System Evaluation Criteri，TCSEC，又称桔皮书)。该准则对计算机操作系统的安全性规定了不同的等级。从 20 世纪 90 年代开始，一些国家和国际组织相继提出了新的安全评价准则。1991 年，欧共体发布了《信息技术安全评价准则》(Information Technology Security Evaluation Criteria，ITSEC)。1993 年，加拿大发布了《加拿大可信计算机产品评价准则》(Canadian Trusted Computer Product Evaluation Criteria，CTCPEC)，CTCPEC 综合了 TCSEC 和 ITSEC 两个准则的优点。同年，美国在对 TCSEC 进行修改补充并吸收 ITSEC 优点的基础上，发布了《信息技术安全评价联邦准则》(FC)，参见图 3.1。

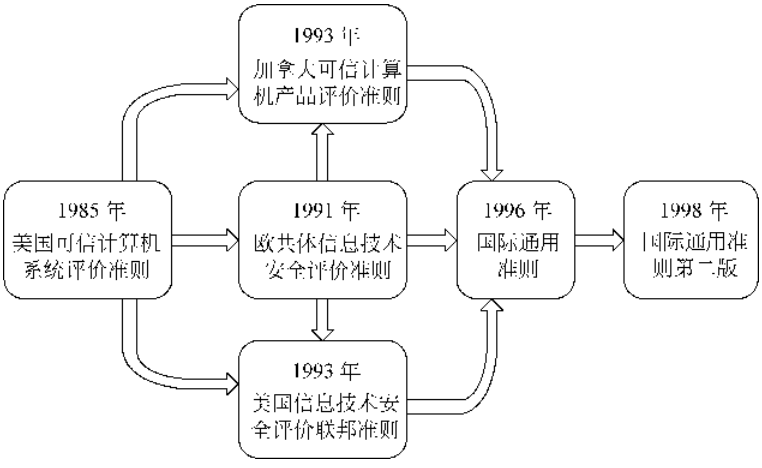


图 3.1 安全评价标准的发展

1996 年 6 月，上述国家共同起草了一份通用准则(CC)，并将 CC 推广为国际标准。CC 发布的目的是建立一个各国都能接受的通用的安全评价准则，国家与国家之间可以通过签订

互认协议来决定相互接受的认可级别，这样能使基础性安全产品在通过 CC 准则评价并得到许可进入国际市场时，不需要再作评价。此外，国际标准化组织和国际电工委也已经制定了上百项安全标准，其中包括专门针对银行业务制定的信息安全标准。国际电信联盟和欧洲计算机制造商协会也推出了许多安全标准。

### 3.1.1 计算机安全评价标准

计算机安全评价标准——TCSEC 是计算机系统安全评估的第一个正式标准，具有划时代的意义。该准则于 1970 年由美国国防科学委员会提出，并于 1985 年 12 月由美国国防部公布。TCSEC 最初只是军用标准，后来延至民用领域。TCSEC 将计算机系统的安全划分为 4 个等级 7 个级别。

D 类安全等级：D 类安全等级只包括 D1 一个级别。D1 的安全等级最低，D1 系统只为文件和用户提供安全保护。D1 系统最普通的形式是本地操作系统，或者是一个完全没有保护的网络。

C 类安全等级：该类安全等级能够提供审慎的保护，并为用户的行动和责任提供审计能力。C 类安全等级可划分为 C1 和 C2 两类。C1 系统的可信任运算基础体制，通过将用户和数据分开来达到安全的目的。在 C1 系统中，所有的用户以同样的灵敏度来处理数据，即用户认为 C1 系统中的所有文档都具有相同的机密性。C2 系统比 C1 系统加强了可调的审慎控制。在连接到网络上时，C2 系统的用户分别对各自的行为负责。C2 系统通过登录过程、安全事件和资源隔离来增强这种控制。C2 系统具有 C1 系统中所有的安全性特征。

B 类安全等级：B 类安全等级可分为 B1、B2 和 B3 三类。B 类系统具有强制性保护功能。强制性保护意味着如果用户没有与安全等级相连，系统就不会让用户存取对象。B1 系统满足下列要求：系统对网络控制下的每个对象都进行灵敏度标记，系统使用灵敏度标记作为所有强迫访问控制的基础。系统在把导入的、非标记的对象放入系统前标记它们。灵敏度标记必须准确地表示其所联系的对象的安全级别。当系统管理员创建系统或者增加新的通信通道或 I/O 设备时，管理员必须指定每个通信通道和 I/O 设备是单级还是多级，并且管理员只能手工改变指定。单级设备并不保持传输信息的灵敏度级别，所有直接面向用户位置的输出（无论是虚拟的还是物理的）都必须产生标记来指示关于输出对象的灵敏度，系统必须使用用户的口令或证明来决定用户的安全访问级别，系统必须通过审计来记录未授权访问的企图。

B2 系统必须满足 B1 系统的所有要求。另外，B2 系统的管理员必须使用一个明确的、文档化的安全策略模式作为系统的可信任运算基础体制。B2 系统必须满足下列要求：系统必须立即通知系统中的每一个用户所有与之相关的网络连接的改变。只有用户能够在可信任通信路径中进行初始化通信，可信任运算基础体制能够支持独立的操作者和管理员。

B3 系统必须符合 B2 系统的所有安全需求。B3 系统具有很强的监视委托管理访问能力和抗干扰能力。B3 系统必须设有安全管理员。B3 系统应满足以下要求：除了控制对个别对象的访问外，B3 必须产生一个可读的安全列表，每个被命名的对象提供对该对象没有访问权的用户列表说明，B3 系统在进行任何操作前，要求用户进行身份验证。B3 系统验证每个用户，同时还会发送一个取消访问的审计跟踪消息。设计者必须正确区分可信任的通信路径和其他路径，可信任的通信基础体制为每一个被命名的对象建立安全审计跟踪，可信

任的运算基础体制支持独立的安全管理。

A 类安全等级：A 系统的安全级别最高。目前，A 类安全等级只包含 A1 一个安全类别。A1 类与 B3 类相似，对系统的结构和策略不作特别要求。A1 系统的显著特征是，系统的设计者必须按照一个正式的设计规范来分析系统。对系统分析后，设计者必须运用核对技术来确保系统符合设计规范。A1 系统必须满足下列要求：系统管理员必须从开发者那里接收到一个安全策略的正式模型，所有的安装操作都必须由系统管理员进行，系统管理员进行的每一步安装操作都必须有正式文档。

### 3.1.2 欧洲的安全评价标准

欧洲的安全评价标准——ITSEC 是欧洲多国安全评价方法的综合产物，应用领域为军队、政府和商业。该标准将安全概念分为功能与评估两部分。功能准则从 F1～F10 共分 10 级。1～5 级对应于 TCSEC 的 D～A。F6～F10 级分别对应数据和程序的完整性、系统的可用性、数据通信的完整性、数据通信的保密性以及机密性和完整性的网络安全。评估准则分为 6 级，分别是测试、配置控制和可控的分配、能访问详细设计和源码、详细的脆弱性分析、设计与源码明显对应以及设计与源码在形式上一致。

### 3.1.3 加拿大的评价标准

加拿大的评价标准——CTCPEC 专门针对政府需求而设计。与 ITSEC 类似，该标准将安全分为功能性需求和保证性需要两部分。功能性需求共划分为四大类：机密性、完整性、可用性和可控性。每种安全需求又可以分成很多小类，来表示安全性上的差别，分级条数为 0～5 级。

### 3.1.4 美国联邦准则

美国联邦准则——FC 是对 TCSEC 的升级，并引入了“保护轮廓”(PP)的概念。每个轮廓都包括功能、开发保证和评价三部分。FC 充分吸取了 ITSEC 和 CTCPEC 的优点，在美国的政府、民间和商业领域得到广泛应用。但 FC 有很多缺陷，是一个过渡标准，后来结合 ITSEC 发展为国际通用准则。

### 3.1.5 国际通用准则

国际通用准则——CC 是国际标准化组织统一现有多种准则的结果，是目前最全面的评价准则。1996 年 6 月，CC 第一版发布；1998 年 5 月，CC 第二版发布；1999 年 10 月 CC v2.1 版发布，并且成为 ISO 标准。CC 的主要思想和框架都取自 ITSEC 和 FC，并充分突出了“保护轮廓”的概念。CC 将评估过程划分为功能和保证两部分，评估等级分为 eal1、eal2、eal3、eal4、eal5、eal6 和 eal7 共 7 个等级。每一级均需评估 7 个功能类，分别是配置管理、分发和操作、开发过程、指导文献、生命期的技术支持、测试和脆弱性评估。

## 3.2 我国安全标准简介

我国信息安全研究经历了通信保密、计算机数据保护两个发展阶段，正在进入网络信息安全的研究阶段。通过学习、吸收、消化 TCSEC 的原则进行了安全操作系统、多级安全数

据库的研制，但由于系统安全内核受控于人，以及国外产品的不断更新升级，基于具体产品的增强安全功能的成果，难以保证没有漏洞，难以得到推广应用。在学习借鉴国外技术的基础上，国内一些部门也开发研制了一些防火墙、安全路由器、安全网关、黑客入侵检测、系统脆弱性扫描软件等。但是，这些产品安全技术的完善性、规范化实用性还存在许多不足，特别是在多平台的兼容性及安全工具的协作配合和互动性方面存在很大距离，理论基础和自主的技术手段也需要发展和强化。

以前，国内主要是等同采用国际标准。现在，由公安部主持制定、国家技术标准局发布的中华人民共和国国家标准 GB17895—1999《计算机信息系统安全保护等级划分准则》已经正式颁布并使用了。该准则将信息系统安全分为五个等级，分别是用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。主要的安全考核指标有身份认证、自主访问控制、数据完整性、审计、隐蔽信道分析、客体重用、强制访问控制、安全标记、可信路径和可信恢复等，这些指标涵盖了不同级别的安全要求。

### 3.2.1 第一级 用户自主保护级

本级的可信计算基通过隔离用户与数据，使用户具备自主安全保护的能力。它具有多种形式的控制能力，对用户实施访问控制，即为用户提供可行的手段，保护用户和用户组信息，避免其他用户对数据的非法读写与破坏。具体表现在如下几个方面：

(1) 可信计算基定义和控制系统中命名用户对命名客体的访问。实施机制(例如，访问控制表)允许命名用户以用户和(或)用户组的身份规定并控制客体的共享，阻止非授权用户读取敏感信息。

(2) 可信计算基初始执行时，首先要求用户标识自己的身份，并使用保护机制(例如，口令)来鉴别用户的身份，阻止非授权用户访问用户身份鉴别数据。

(3) 可信计算基通过自主完整性策略，阻止非授权用户修改或破坏敏感信息。

### 3.2.2 第二级 系统审计保护级

与用户自主保护级相比，本级的可信计算基实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。它增加了客体重用以及安全审计方面的内容，并进一步增强了自主访问控制以及身份鉴别机制，具体表现在：

(1) 自主访问控制机制根据用户指定方式或默认方式，阻止非授权用户访问客体。访问控制的粒度是单个用户。控制访问权限扩散，没有存取权的用户只允许由授权用户指定对客体的访问权。

(2) 通过为用户提供唯一标识、可信计算基能够使用户对自己的行为负责。可信计算基还具备将身份标识与该用户所有可审计行为相关联的能力。

(3) 在可信计算基的空闲存储客体空间中，对客体初始指定、分配或再分配一个主体之前，撤销该客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时，当前主体不能获得原主体活动所产生的任何信息。

(4) 可信计算基能创建和维护受保护客体的访问审计跟踪记录，并能阻止非授权的用户对它访问或破坏。可信计算基能记录下述事件：使用身份鉴别机制；将客体引入用户地址空间(例如，打开文件、程序初始化)；删除客体；由操作员、系统管理员或(和)系统安全

管理员实施的动作，以及其他与系统安全有关的事件。对于每一事件，其审计记录包括事件的日期和时间、用户、事件类型、事件是否成功。对于身份鉴别事件，审计记录包含的来源（例如，终端标识符）；对于客体引入用户地址空间的事件及客体删除事件，审计记录包含客体名。对不能由可信计算基独立分辨的审计事件，审计机制提供审计记录接口，可由授权主体调用。这些审计记录区别于可信计算基独立分辨的审计记录。

### 3.2.3 第三级 安全标记保护级

本级的可信计算基具有系统审计保护级的所有功能。此外，还提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述；具有准确地标记输出信息的能力；消除通过测试发现的任何错误。它增加了强制访问控制机制，具体表现为：

（1）可信计算基对所有主体及其所控制的客体（例如，进程、文件、段、设备）实施强制访问控制。为这些主体及客体指定敏感标记，这些标记是等级分类和非等级类别的组合，它们是实施强制访问控制的依据。可信计算基支持两种或两种以上成分组成的安全级。可信计算基控制的所有主体对客体的访问应满足：仅当主体安全级中的等级分类高于或等于客体安全级中的等级分类，且主体安全级中的非等级类别包含了客体安全级中的全部非等级类别，主体才能读客体；仅当主体安全级中的等级分类低于或等于客体安全级中的等级分类，且主体安全级中的非等级类别包含了客体安全级中的非等级类别，主体才能写一个客体。可信计算基使用身份和鉴别数据，鉴别用户的身份，并保证用户创建的可信计算基外部主体的安全级和授权受该用户的安全级和授权的控制。

（2）可信计算基应维护与主体及其控制的存储客体（例如，进程、文件、段、设备）相关的敏感标记。这些标记是实施强制访问的基础。为了输入未加安全标记的数据，可信计算基向授权用户要求并接受这些数据的安全级别，且可由可信计算基审计。

（3）在审计记录的内容中，对于客体引入用户地址空间的事件及客体删除事件，审计记录包含客体名及客体的安全级别。此外，可信计算基具有审计更改可读输出记号的能力。

（4）在网络环境中，使用完整性敏感标记来确信信息在传送中未受损。

### 3.2.4 第四级 结构化保护级

本级的可信计算基建立于一个明确定义的形式化安全策略模型之上，它要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。本级的可信计算基必须结构化为关键保护元素和非关键保护元素。可信计算基的接口也必须明确定义，使其设计与实现能经受更充分的测试和更完整的复审。加强了鉴别机制；支持系统管理员和操作员的职能；提供可信设施管理；增强了配置管理控制。系统具有相当的抗渗透能力。增加的内容主要表现在如下几个方面：

（1）可信计算基对外部主体能够直接或间接访问的所有资源（例如，主体、存储客体和输入输出资源）实施强制访问控制；

（2）可信计算基能够审计利用隐蔽存储信道时可能被使用的事件；

（3）系统开发者应彻底搜索隐蔽存储信道，并根据实际测量或工程估算确定每一个被标识信道的最大带宽；

（4）对用户的初始登录和鉴别，可信计算基在它与用户之间提供可信通信路径。该路

径上的通信只能由该用户初始化。

### 3.2.5 第五级 访问验证保护级



本级的可信计算基满足引用监视器需求。引用监视器仲裁主体对客体的全部访问。引用监视器本身是抗篡改的；必须足够小，能够分析和测试。为了满足引用监视器需求，可信计算基在其构造时，排除那些对实施安全策略来说并非必要的代码；在设计和实现时，从系统工程角度将其复杂性降低到最小程度。支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很高的抗渗透能力。增加的内容主要表现在如下几个方面：

(1) 在审计方面，可信计算基包含能够监控可审计安全事件发生与积累的机制，当超过阈值时，能够立即向安全管理员发出报警。并且，如果这些与安全相关的事件继续发生或积累，系统应以最小的代价中止它们；

(2) 可信路径上的通信只能由该用户或可信计算基激活，且在逻辑上与其他路径上的通信相隔离，且能正确地加以区分；

(3) 可信计算基提供过程和机制，保证计算机信息系统失效或中断后，可以进行不损害任何安全保护性能的恢复。

## 3.3 安全操作系统的基本特征

### 3.3.1 最小特权原则

最小特权原则是系统安全中最基本的原则之一。所谓最小特权指的是“在完成某种操作时所赋予网络中每个主体(用户或进程)必不可少的特权”。最小特权原则，则是指“应限定网络中每个主体所必需的最小特权，确保可能的事故、错误、网络部件的篡改等原因造成的损失最小”。

最小特权原则一方面给予主体“必不可少”的特权，这就保证了所有的主体都能在所赋予的特权之下完成所需要完成的任务或操作；另一方面，它只给予主体“必不可少”的特权，这就限制了每个主体所能进行的操作。

最小特权原则要求每个用户和程序在操作时应当使用尽可能少的特权，但允许主体以参与某特定工作所需要的最小特权去进入系统。被授权拥有强力角色的主体，不需要动辄运用到其所有的特权，只有在那些特权有实际需求时，主体才去运用它们。如此一来，将减少由于不注意的错误或是侵入者假装合法主体所造成的损坏发生，限制了事故、错误或攻击带来的危害。它还减少了特权程序之间潜在的相互作用，从而使对特权无意的、没必要的或不适当的使用不太可能发生。这种想法还可以引申到程序内部：只有程序中需要那些特权的最小部分才拥有特权。

### 3.3.2 自主访问控制和强制访问控制

自主访问控制(DAC)是一个接入控制服务，它执行基于系统实体身份和它们到系统资源的接入授权。这包括在文件、文件夹和共享资源中设置许可。

强制访问控制(MAC)是“强加”给访问主体的,即系统强制主体服从访问控制政策。强制访问控制的主要特征是对所有主体及其所控制的客体(例如,进程、文件、段、设备)实施强制访问控制。为这些主体及客体指定敏感标记,这些标记是等级分类和非等级类别的组合,它们是实施强制访问控制的依据。系统通过比较主体和客体的敏感标记来决定一个主体是否能够访问某个客体。用户的程序不能改变他自己及任何其他客体的敏感标记,从而系统可以防止特洛伊木马的攻击。

强制访问控制一般与自主访问控制结合使用,并且实施一些附加的、更强的访问限制。一个主体只有通过了自主与强制性访问限制检查后,才能访问某个客体。用户可以利用自主访问控制来防范其他用户对自己客体的攻击,由于用户不能直接改变强制访问控制属性,所以强制访问控制提供了一个不可逾越的、更强的安全保护层以防止其他用户偶然或故意地滥用自主访问控制。

强制访问策略将每个用户及文件赋予一个访问级别,如最高秘密级 T(Top Secret)、秘密级 S(Secret)、机密级 C(Confidential)及无级别级 U(Unclassified)。其级别为 T>S>C>U,系统根据主体和客体的敏感标记来决定访问模式。访问模式包括:

- 下读(read down)　用户级别大于文件级别的读操作。
- 上写(write up)　用户级别小于文件级别的写操作。
- 下写(write down)　用户级别等于文件级别的写操作。
- 上读(read up)　用户级别小于文件级别的读操作。

### 3.3.3　安全审计功能

安全审计是识别与防止网络攻击行为、追查网络泄密行为的重要措施之一。具体包括两方面的内容:一是采用网络监控与入侵防范系统,识别网络各种违规操作与攻击行为,即时响应(如报警)并进行阻断;二是对信息内容的审计,可以防止内部机密或敏感信息的非法泄露。

审计作为安全系统的重要组成部分,在美国的 TCSEC 中对于安全审计的定义是这样的:一个安全系统中的安全审计系统,是对系统中任一或所有安全相关事件进行记录、分析和再现的处理系统。因此,在 TCSEC 中规定了对于安全审计系统的一般要求,主要包括如下的五个方面:

(1) 记录与再现,要求安全审计系统必须能够记录系统中所有的安全相关事件,同时,如果有必要,应该能够再现产生系统某一状态的主要行为;

(2) 入侵检测,安全审计系统应该能够检查出大多数常见的系统入侵的行为,同时,经过适当的设计,应该能够阻止这些入侵行为;

(3) 记录入侵行为,安全审计系统应该记录所有的入侵行为,即使某次入侵已经成功,这也是事后调查取证和系统恢复必需的;

(4) 威慑作用,应该对系统中具有的安全审计系统及其性能进行适当宣传,这样可以对企图入侵者起到威慑作用,又可以减少合法用户在无意中违反系统的安全策略;

(5) 系统本身的安全性,安全审计系统本身的安全性必须保证,这包括两个方面的内容,一是操作系统和软件的安全性,另一个是审计数据的安全性;一般来说,要保证审计系统本身的安全,必须与系统中其他安全措施(例如认证、授权、加密等)相配合。

另外，TCSEC 还要求 C2 级以上的安全操作系统必须包含审计功能。我国计算机信息系统安全保护等级划分准则(GB l7859—1999)对安全审计也有相应的要求。审计为系统进行事故原因的查询、定位、事故发生前的预测、报警以及事故发生之后的实时处理提供详细、可靠的依据和支持，以便有违反系统安全规则的事件发生后能够有效地追查事件发生的地点和过程。

### 3.3.4 安全域隔离功能

安全域是指在其中实施认证、授权和访问控制的安全策略的计算环境。当用户安装和配置操作系统时，将创建称为管理域的初始安全域。安全域理论不仅为建设信息安全保障体系提供基础，而且在风险评估当中如果能较好地应用安全域，还会起到事半功倍的作用。安全域可以将一个单独资产联系起来，在等级保护当中也有比较好的应用。总之，安全域理论是安全方面的最佳实践，对于信息安全建设具有非常重要的指导意义。

## 3.4 Windows 2003 的安全设置

### 3.4.1 Windows 安全漏洞及其解决建议

Windows 系统上的重大安全漏洞，主要包括两大部分：Windows 服务器安全漏洞和工作站的安全漏洞。

对于这些安全漏洞更佳的解决方案是建设一个强壮的防火墙，精心地配置它，只授权给可信赖的主机能通过防火墙。在防火墙上，截止所有从端口 137～139 的 TCP 和 UDP 连接，这样做有助于对远程连接的控制。另外，在内部路由器上，设置 ACL，在各个独立子网之间，截止从端口 137～139 的连接。这是一种辅助措施，以限制该安全漏洞。值得注意的是，有些黑客程序可以具有选择端口号的能力，它可能成功地攻击其他端口。

### 3.4.2 Windows 2003 的认证机制

Windows 2003 身份认证的重要功能就是它对单一注册的支持。单一注册允许用户使用一个密码一次登录到域，然后向域中的任何计算机认证身份。

单一注册在安全性方面提供了两个主要优点：对用户而言，单个密码或智能卡的使用减少了混乱，提高了工作效率；对管理员而言，由于管理员只需要为每个用户管理一个账户，域用户所要求的管理支持减少了。

身份认证分以下两种方式执行：

(1) 交互式登录。交互式登录过程向域账户或本地计算机确认用户的身份，这一过程根据用户账户的类型而不同。如果使用域账户登录，被授权的用户可以访问该域以及任何信任域中的资源。如果使用密码登录到域账户，Windows 2003 将使用 Kerberos V5 进行身份认证。如果使用智能卡，Windows 2003 将使用带证书的 Kerberos V5 身份认证。

(2) 网络身份认证。网络身份认证确认用户对于试图访问的任意网络服务的身份。为了提供这种类型的身份认证，Windows 2003 安全系统支持多种不同的身份认证机制，包括 Kerberos V5、安全套接字层/传输层安全(SSL/TLS)以及为了与 Windows NT 4.0 兼容而

提供的 NTLM。

### 3.4.3 Windows 2003 账号安全

(1) 域用户账号。域用户账号是用户访问域的唯一凭证,因此在域中必须是唯一的。域用户账号在域控制器上建立,作为活动目录的一个对象保存在域的数据库中。用户在从域中的任何一台计算机登录到域中的时候必须提供一个合法的域用户账号,该账号将被域控制器所验证。

(2) 本地用户账号。本地用户账号只能建立在 Windows 2003 独立服务器上,以控制用户对该计算机资源的访问。

(3) 内置的用户账号。Administrator(管理员)账号被赋予在域中和在计算机中具有不受限制的权利,该账号被设计用于对本地计算机或域进行管理,可以从事创建其他用户账号、创建组、实施安全策略、管理打印机以及分配用户对资源的访问权限等工作。Guest(来宾)账号一般被用于在域中或计算机中没有固定账号的用户临时访问域或计算机时使用的。该账号默认情况下不允许对域或计算机中的设置和资源做永久性的更改。出于安全考虑,Guest 账号在 Windows 2003 安装好之后是被屏蔽的。如果需要,可以手动启动,应该注意分配给该账号的权限,该账号也是黑客攻击的主要对象。

(4) 账号命名约定。由于账号在域中的重要性和唯一性,因此账号的命名约定十分重要。一个好的账号命名约定将有助于规划一个高效的活动目录。Windows 2003 的账号命名约定包括如下内容:

① 域用户账号的用户登录名在活动目录中必须唯一。

② 域用户账号的完全名称在创建该用户账号的域中必须唯一。

③ 本地用户账号在创建该账号的计算机上必须唯一。

④ 如果用户名称有重复,则应该在账号上区别出来。

(5) 密码约定。通常设定密码有如下原则:

① 尽量避免带有明显意义的字符或数字的组合,最好采用大小写和数字的无意义混合。在不同安全要求下,规定最小的密码长度。通常密码越长越不易被猜到(最长可以达到 128 位)。

② 对于不同级别的安全要求,确定用户的账号密码是由管理员控制还是由账号的拥有者控制。

③ 定期更改密码,尽量使用不同的密码。有关密码的策略可以由系统管理员在密码策略管理工具中加以规定,以保护系统的安全性。

### 3.4.4 Windows 2003 文件系统安全

文件系统安全是操作系统安全的核心。Windows 2003 文件系统控制谁能访问信息以及他们能做些什么。即使外层账号安全被突破,攻击者还必须击败文件系统根据文件拥有权和权限精心设置的防御措施。当建立文件的权限时,必须先确定文件系统格式为 Windows NT 文件系统(NTFS),当然也可以使用 FAT 格式,但是并不支持文件级的权限。一旦已经实施了 NTFS 的文件系统格式,就可通过 Windows 的资源管理器直接来管理文件的安全。

NTFS 权限及使用有以下几个原则：

(1) 权限最大原则。当一个用户同时属于多个组，而这些组又有可能被赋予了对某种资源的不同访问权限，则用户对该资源最终有效权限是在这些组中最宽松的权限，即加权权限，将所有的权限加在一起即为该用户的权限("完全控制"权限为所有权限的总和)。

(2) 文件权限超越文件夹权限原则。当用户或组对某个文件夹以及该文件夹下的文件有不同的访问权限时，用户对文件的最终权限是访问该文件的权限，即文件权限超越文件的上级文件夹的权限，用户访问该文件夹下的文件不受文件夹权限的限制，而只受被赋予的文件权限的限制。

(3) 拒绝权限超越其他权限原则。当用户对某个资源有拒绝权限时，该权限覆盖其他任何权限，即在访问该资源的时候只有拒绝权限是有效的。当有拒绝权限时权限最大法则无效。因此对于拒绝权限的授予应该慎重考虑。

在同一个 NTFS 分区内或不同的 NTFS 分区之间移动或复制一个文件或文件夹时，该文件或文件夹的 NTFS 权限会发生不同的变化。这时 NTFS 权限的继承性就起到了作用，关于 NTFS 权限的继承性有以下几个方面：

(1) 在同一个 NTFS 分区内移动文件或文件夹。在同一分区内移动的实质就是在目的位置将原位置上的文件或文件夹"搬"过来，因此文件和文件夹仍然保留有在原位置的一切 NTFS 权限(准确地讲就是该文件或文件夹的权限不变)。

(2) 在不同 NTFS 分区之间移动文件或文件夹。在这种情况下文件和文件夹会继承目的分区中文件夹的权限(ACL)，实质就是在原位置删除该文件或文件夹，并且在目的位置新建该文件或文件夹(要从 NTFS 分区中移动文件或文件夹，操作者必须具有相应的权限。在原位置上必须有"修改"的权限，在目的位置上必须有"写"权限)。

(3) 在同一个 NTFS 分区内复制文件或文件夹，在这种情况下复制文件和文件夹将继承目的位置中的文件夹的权限。

(4) 在不同 NTFS 分区之间复制文件或文件夹，在这种情况下复制文件和文件夹将继承目的位置中文件夹的权限(当从 NTFS 分区向 FAT 分区中复制或移动文件和文件夹都将导致文件和文件夹的权限丢失，因为 FAT 分区不支持 NTFS 权限)。

### 3.4.5 Windows 文件保护

微软公司为 Windows 2000/XP 系统增添了一项新功能 WFP (Windows File Protection)。这个组件的主要功能是，在系统文件遭到意外删除，或在安装/卸载应用程序时被无意识破坏后，利用备份文件恢复 Windows 系统。

初次安装 Windows XP 时，部分以 dll、exe、fon、ocx、sys 和 tff 结尾的文件将被 WFP 标识为重要的系统文件，并在 dllcache 文件夹下为这些文件备份。在用户使用 Windows 2000/XP 系统的过程中，WFP 将在默认设置下把以 ax、cpl、cpx、dll、exe、fon、inf、ocx、rsp、sys、tff 和 tlb 结尾的文件备份在 WINDOWS\system32\dllcache 文件夹下。如果这些系统文件被误删除或是被破坏，WFP 能够利用在 dllcache 下的备份文件，轻而易举地恢复 Windows 的文件系统。

由于 WFP 能自动利用备份恢复原有系统文件，所以不能用一般的方法升级装有 WFP 的操作系统文件。下面介绍几种升级的常用方法：

(1) 安装 Windows 服务组件。

(2) 升级 Windows 系统。

(3) 运行 hotfix.exe。hotfix 能自动更新 WFP 所备份的系统文件。目前大多数 hotfix 程序已经被打包在 Windows 服务组件内。如果安装了 Windows XP SP1,那么打开"添加/删除程序"能看到两个 hotfix 程序。

(4) 使用 Winnt32.exe 运行系统的安装/升级程序。

此外,还有一种简单的手工升级方法,把要升级的文件复制到 dllcache 文件夹下,然后 WFP 就能自动升级 Windows 文件系统。

在运行 WFP 程序之前,用户必须先以系统管理员身份登录。系统管理员的身份会为用户修改与 WFP 有关的配置提供相当方便的条件。在完成相关设置后,退出系统以正常用户身份再次登录,这样就可以使用 WFP 了。

### 3.4.6 Windows 2003 的加密机制

文件加密系统(Encryption File System,EFS)是 Windows 2003/XP 所特有的一个实用功能,对于 NTFS 卷上的文件和数据,都可以直接被操作系统加密保存,在很大程度上提高了数据的安全性。

EFS 加密是基于公钥策略的。在使用 EFS 加密一个文件或文件夹时,系统首先会生成一个由伪随机数组成的文件密钥(File Encryption Key,FEK),然后将利用 FEK 和数据扩展标准 X 算法创建加密后的文件,并把它存储到硬盘上,同时删除未加密的原始文件。随后系统利用公钥加密 FEK,并把加密后的 FEK 存储在同一个加密文件中。而在访问被加密的文件时,系统首先利用当前用户的私钥解密 FEK,然后利用 FEK 解密出文件。在首次使用 EFS 时,如果用户还没有公钥/私钥对(统称为密钥),则会首先生成密钥,然后加密数据。如果登录到了域环境中,密钥的生成依赖于域控制器,否则它就依赖于本地机器。

EFS 加密有以下两点好处,首先,EFS 加密机制和操作系统紧密结合,因此不必为了加密数据安装额外的软件,这节约了使用成本。其次,EFS 加密系统对用户是透明的。这也就是说,如果加密了一些数据,那么对这些数据的访问将是完全允许的,并不会受到任何限制。而其他非授权用户试图访问加密过的数据时,就会收到"访问拒绝"的错误提示。EFS 加密的用户验证过程是在登录 Windows 时进行的,只要登录到 Windows,就可以打开任何一个被授权的加密文件。

要使用 EFS 加密,首先要保证操作系统符合要求。目前支持 EFS 加密的 Windows 操作系统主要有 Windows 2000、Windows Server 2003 全部版本和 Windows XP Professional。其次,EFS 加密只对 NTFS 5 分区上的数据有效(注意,这里提到了 NTFS 5 分区,这是指由 Windows 2003/XP 格式化过的 NTFS 分区;而由 Windows NT 格式化的 NTFS 分区是 NTFS 4 格式的,虽然同样是 NTFS 文件系统,但它不支持 EFS 加密),无法加密保存在 FAT 和 FAT 32 分区上的数据。

对于想加密的文件或文件夹,只需要用鼠标右键单击,然后选择"属性",在常规选项卡下单击"高级"按钮,之后在弹出的窗口中选中"加密内容以保护数据",然后单击"确定"按钮,等待片刻数据就加密好了。如果加密的是一个文件夹,系统还会询问,是把这个加密属性应用到文件夹上还是文件夹以及内部的所有子文件夹。按照实际情况来操作即可。解密