第 5 章

信息系统安全

信息系统是软/硬件运行的一个统一体，也是安全威胁的对象。访问控制是信息安全的一个重要组成部分，其目的是确保只有符合控制策略的主体才能合法地访问系统资源，通常对主机操作系统或路由器进行设置来实现相应的主机访问控制或网络访问控制。操作系统、应用系统和数据库系统构成了软件和信息管理系统运行的基础，也是本章重点讨论的对象。黑客会重点攻击操作系统、应用系统和数据库系统的弱点，以获得其控制权限和对数据的操作权限。因此，对系统的安全防范也是信息安全中的一个重要环节。

5.1 访 问 控 制

5.1.1 访问控制基本概念

身份认证技术解决了识别“用户是谁”的问题，那么通过认证的用户是不是可以无条件地使用所有资源呢？答案是否定的。访问控制(access control)技术就是指管理用户对系统资源的访问。访问控制是国际标准 ISO 7498—2 中的五项安全服务之一，对提高信息系统的安全性起到至关重要的作用，如图 5-1 所示。

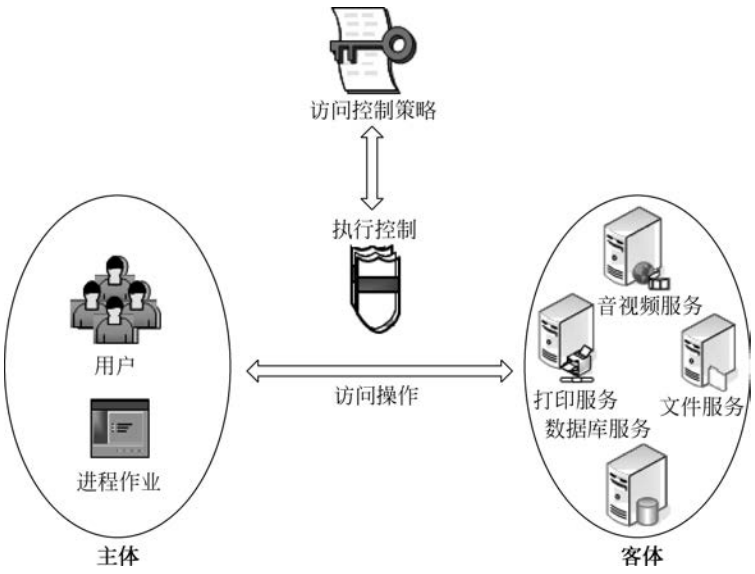

图 5-1 访问控制示意图

访问控制是针对越权使用资源的防御性措施之一。其基本目标是防止对任何资源(如

计算资源、通信资源或信息资源)进行未授权的访问,从而使资源使用始终处于控制范围内。最常见的是,通过对主机操作系统的设置或对路由器的设置来实现相应的主机访问控制或网络访问控制。例如,控制内网用户在上班时间使用 QQ、MSN 等。

访问控制对实现信息机密性、完整性起直接的作用,还可以通过对以下用户信息的有效控制来实现信息和信息系统可控性:①谁可以颁发影响网络可用性的网络管理指令;②谁能够滥用资源以达到占用资源的目的;③谁能够获得可以用于拒绝服务攻击的信息。

为了能够更精确地描述访问控制,需要对访问控制的基本组成元素进行定义说明。访问控制的基本组成元素主要包括主体、客体和控制策略。

主体(subject)是指提出访问请求的实体,是动作的发起者,但不一定是动作的执行者。主体可以是用户或其他代理用户行为的实体(如进程、作业和程序等)。

客体(object)是指可以接受主体访问的被动实体。客体的内涵很广泛,凡是可以被操作的信息、资源、对象都可以被视为客体。

访问控制策略(access control policy)是指主体对客体的操作行为和约束条件的关联集合。简单地讲,访问控制策略是主体对客体的访问规则集合,这个规则集合可以直接决定主体是否可以对客体实施特定的操作。访问控制策略体现了一种授权行为,也就是客体对主体的权限允许。访问控制策略往往表现为一系列的访问规则,这些规则定义了主体对客体的作用行为和客体对主体的条件约束。访问控制机制是访问控制策略的软硬件低层实现。

如图 5-1 所示,主体对于客体的每一次访问,访问控制系统均要审核该次访问操作是否符合访问控制策略,只允许符合访问控制策略的操作请求,拒绝违反控制策略的非法访问。访问控制可以解释为:依据一定的访问控制策略,实施对主体访问客体的控制。图 5-1 也给出了访问控制系统的两个主要工作:一个是当主体发出对客体的访问请求时,查询相关的访问控制策略;另一个是依据访问控制策略执行访问控制。通过以上分析,可以看出影响访问控制系统实施效果好坏的首要因素是访问控制策略,制定访问控制策略的过程实际上就是主体对客体的访问授权过程。如何较好地完成对主体的授权是访问控制成功的关键,同时也是访问控制必须研究的重要课题。

信息系统的访问控制技术最早产生于 20 世纪 60 年代,在 70 年代先后出现了多种访问控制模型。1985 年,美国军方提出可信计算机系统评估准则(Trusted Computer System Evaluation Criteria,TCSEC),其中描述了两种著名的访问控制模型,即自主访问控制(Discretionary Access Control,DAC)和强制访问控制(Mandatory Access Control,MAC);1992 年,美国国家标准与技术研究所(NIST)的 David Ferraiolo 和 Rick Kuhn 提出一个基于角色的访问控制(Role Based Access Control,RBAC)模型。

如何决定主体对客体的访问权限?一个主体对一个客体的访问权限能否转让给其他主体呢?这些问题在访问控制策略中必须得到明确的回答。

1. 访问控制策略制定的原则

访问控制策略的制定一般要满足如下三项基本原则。

(1) 最小权限原则:分配给系统中的每一个程序和每一个用户的权限应该是它们完成工作所必须享有的权限的最小集合。换句话说,如果主体不需要访问特定客体,则主体就不应该拥有访问这个客体的权限。

(2) 最小泄露原则:主体执行任务时所需知道的信息应该最小化。

(3) 多级安全策略：主体和客体间的数据流方向必须受到安全等级的约束。

2. 访问权限的确定过程

主体对客体的访问权限的确定过程是：首先对用户和资源进行分类，然后对需要保护的资源定义一个访问控制包，最后根据访问控制包来制定访问控制规则集。

3. 用户分类

通常把用户分为特殊用户、一般用户、审计用户和作废用户。

(1) 特殊用户：系统管理员具有最高级别的特权，可以访问任何资源，并具有任何类型的访问操作能力。

(2) 一般用户：最大的一类用户，他们的访问操作受到一定限制，由系统管理员分配。

(3) 审计用户：负责整个安全系统范围内的安全控制与资源使用情况的审计。

(4) 作废用户：被系统拒绝的用户。

4. 资源的分类

系统内需要保护的资源包括磁盘与磁带卷标、数据库中的数据、应用资源、远程终端、信息管理系统的事务处理及其应用等。

5. 对需要保护的资源定义一个访问控制包

内容包括资源名及拥有者的标识符、默认访问权、用户和用户组的特权明细表、允许资源拥有者对其添加新的可用数据的操作、审计数据等。

6. 访问控制规则集

访问控制规则集是根据第三步的访问控制包得到的，它规定了若干条件和在这些条件下准许访问的一个资源。规则使得用户与资源配对，并指定该用户可在该文件上执行哪些操作，如只读、不许执行或不许访问。“主体对客体的访问权限能否转让给其他主体”这一问题比较复杂，不能简单地用“能”和“不能”来回答。试想一下，如果回答“不能”，表面上看很安全，但按照这一控制策略做出系统后，我们就不可能实现任何信息的共享了。

5.1.2 自主访问控制

自主访问控制是一种策略，是指对某个客体具有所有权的主体能够自主地将对该客体的一种访问权或多种访问权授予其他主体，并可在随后的任何时刻将这些权限收回。这种策略因灵活性高，在实际系统中被大量采用。Linux、UNIX 和 Windows 等系统都提供了自主访问控制功能。在实现自主访问控制策略的系统中，信息在移动过程中其访问权限关系会被改变。如用户 A 可将其对目标 O 的访问权限传递给用户 B，从而使本身不具备对 O 访问权限的 B 可以访问 O。因此，这种模型提供的安全防护不能给系统提供充分的数据保护。

自主访问控制模型(DAC model)是根据自主访问控制策略建立的一种模型，允许合法用户以用户或用户组的身份来访问系统控制策略许可的客体，同时阻止非授权用户访问客体，某些用户还可以自主地把自己所拥有的客体的访问权限授予其他用户。在自主访问控制系统中，特权用户为普通用户分配的访问权限信息主要以访问控制表(Access Control List，ACL)、访问控制能力表(Access Control Capability List，ACCL)和访问控制矩阵(Access Control Matrix，ACM)三种形式来存储。

ACL 是以客体为中心建立的访问权限表，其优点在于实现简单，系统为每个客体确定

一个授权主体的列表，大多数主机都是用 ACL 作为访问控制的实现机制。如图 5-2 所示，在 ACL 示例中，(Own,R,W)表示管理、读、写操作。之所以将管理操作从读/写中分离出来，是因为管理员会对控制规则本身或文件属性等作修改，即修改 ACL。例如，对于客体 Object1 来讲，Alice 对它的访问权限集合为(Own,R,W)，Bob 只有读取权限(R)，John 拥有读/写操作的权限(R,W)。

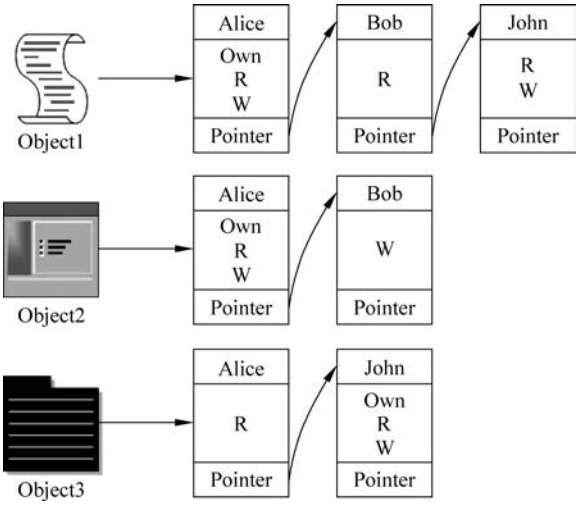

图 5-2　ACL 示例

又如图 5-3 所示，在 ACCL 示例中，ACCL 是以主体为中心建立的访问权限表。“能力”这个概念可以解释为请求访问的发起者所拥有的一个授权标签，授权标签表明持有者可以按照某种访问方式访问特定的客体。也就是说，如果赋予某个主体一种能力，那么这个主体就具有与该能力对应的权限。在此示例中，Alice 被赋予一定的访问控制能力，其具有的权限如下：对 Object1 拥有的访问权限集合为(Own,R,W)，对 Object2 拥有只读权限集(R)，对 Object3 拥有读和写的权限(R,W)。

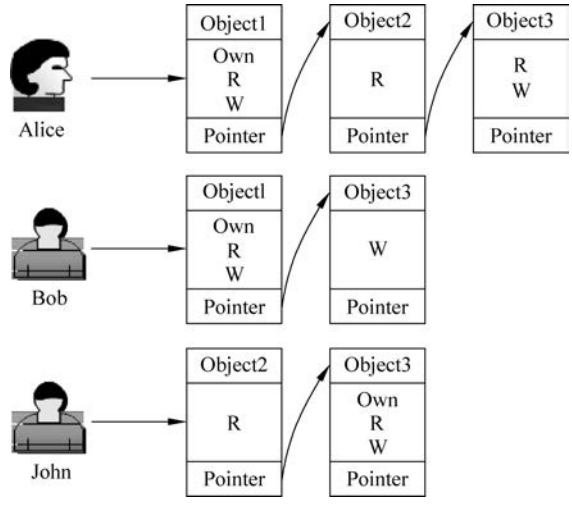

图 5-3　ACCL 示例

ACM是通过矩阵形式表示主体用户和客体资源之间的授权关系的方法。表5-1为ACM示例,采用二维表的形式来存储访问控制策略,每一行为一个主体的访问能力描述,每一列为一个客体的访问能力描述,整个矩阵可以清晰地体现访问控制策略。与ACL和ACCL一样,ACM的内容同样需要特权用户或特权用户组来进行管理。另外,如果主体和客体很多,那么ACM将会呈几何级增长,这样对于增长了的矩阵而言,会有大量的冗余空间,如主体John和客体Object2之间没有访问关系,但也存在授权关系项。

表5-1 ACM示例

主 体	客 体		
	Object1	**Object2**	**Object3**
Alice	Own,R,W	R	R,W
Bob	R	Own,R,W	
John	R,W		Own,R,W

DAC为用户提供了灵活的数据访问方式,授权主体(特权用户、特权用户组的成员以及对客体拥有Own权限的主体)均可以完成赋予和回收其他主体对客体资源的访问权限,使得DAC广泛应用于商业和工业环境中。但由于DAC允许用户任意传递权限,没有访问文件file1权限的用户A可能从有访问权限的用户B那里得到访问权限,因此,DAC模型提供的安全防护还是相对比较低的,不能为系统提供充分的数据保护。

5.1.3 强制访问控制

另一种策略是根据主体被信任的程度和客体所含信息的机密性和敏感程度来决定主体对客体的访问权。用户和客体都被赋予一定的安全级别,用户不能改变自身和客体的安全级别,只有管理员才能确定用户的安全级别且当主体和客体的安全级别满足一定的规则时,才被允许访问。这一策略称为强制访问控制。在强制访问控制模型中,一个主体对某客体的访问权只能有条件地转让给其他主体,而这些条件是非常严格的。例如,Bell-LaPadula模型规定,安全级别高的用户和进程不能向比他们安全级别低的用户和进程写入数据。Bell-LaPadula模型的访问控制原则可简单地表示为"无上读、无下写",该模型是第一个将安全策略形式化的数学模型,是一个状态机模型,即用状态转换规则来描述系统的变化过程。Lattice模型和Biba模型也属于强制访问控制模型。强制访问控制一般通过安全标签来实现单向信息流通。

强制访问控制(MAC)是一种多级访问控制策略,系统事先给访问主体和受控客体分配不同的安全级别属性,在实施访问控制时,系统先对访问主体和受控客体的安全级别属性进行比较,再决定访问主体能否访问该受控客体。为了对MAC模型进行形式化描述,首先需要将访问控制系统中的实体对象分为主体集S和客体集O,然后定义安全类SC(x)=<L,C>,其中x为特定的主体或客体,L为有层次的安全级别Level,C为无层次的安全范畴Category。在安全类SC的两个基本属性L和C中,安全范畴C用来划分实体对象的归属,而同属于一个安全范畴的不同实体对象由于具有不同层次的安全级别L,因而构成了一定的偏序关系。例如,TS(Top Secret)表示绝密级,S(Secret)表示秘密级,当主体s的安全类别为TS,而客体o的安全类别为S时,s与o的偏序关系可以表述为SC(s)≥SC(o)。依靠不同实体安全

级别之间存在的偏序关系，主体对客体的访问可以分为以下四种形式。

(1) 向下读(Read Down，RD)：主体安全级别高于客体信息资源的安全级别时，即SC(s)≥SC(o)，允许读操作。

(2) 向上读(Read Up，RU)：主体安全级别低于客体信息资源的安全级别时，即SC(s)≤SC(o)，允许读操作。

(3) 向下写(Write Down，WD)：SC(s)≥SC(o)时，允许写操作。

(4) 向上写(Write Up，WU)：SC(s)≤SC(o)时，允许写操作。

由于MAC通过分级的安全标签实现了信息的单向流动，因此它一直被军方采用，其中最著名的是Bell-LaPadula模型和Biba模型。Bell-LaPadula模型具有只允许向下读、向上写的特点，可以有效防止机密信息向下级泄露，保护机密性；Biba模型则具有只允许向上读、向下写的特点，可以有效地保护数据的完整性。

表5-2为MAC信息流安全控制，可以看出机密层次的主体对于比它级别高的客体，只有写操作权限；而对于比它级别低的客体，则拥有读操作权限。这符合RD和WU，与Bell-LaPadula模型的信息流控制一致，可以保证信息的机密性。

表5-2　MAC信息流安全控制

主　体	客　体				High
	TS	**C**	**S**	**U**	↓
TS	R/W	R	R	R	↓
C	W	R/W	R	R	↓
S	W	W	R/W	R	
U	W	W	W	R/W	Low

注：绝密(Top Secret，TS)，机密(Confidential，C)，秘密(Secret，S)，无密(Unclassified，U)

5.1.4　基于角色的访问控制

将访问权限分配给一定的角色，让用户根据自己的角色获得相应的访问许可权，这便是基于角色的访问控制策略。角色是指一个可以完成一定职能的命名组。角色与组是有区别的，组是一组用户的集合，而角色是一组用户集合外加一组操作权限集合。一般认为组是具有某些相同特质的用户集合。在UNIX操作系统中，组可以被看成拥有相同访问权限的用户集合，定义用户组时会为该组赋予相应的访问权限。如果一个用户加入了该组，则该用户即具有了该用户组的访问权限，可以看出组内用户继承了组的权限。

如图5-4所示，角色的概念可以这样理解：一个角色是一个与特定工作活动相关联的行为与责任的集合。角色不是用户的集合，也就与组不同。如果将一个角色与一个组绑定，则这个组就拥有了该角色拥有的特定工作的行为能力和责任。组和用户都可以看成角色分配的单位和载体，而一个角色可以看成具有某种能力或某些属性的主体的一个抽象。

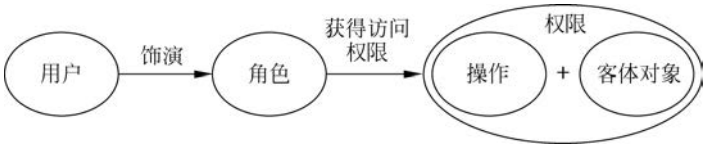

图5-4　基于角色的访问控制模型

角色的目的是隔离用户(Subject,动作客体)与权限(Privilege,指对客体)的一个访问操作,即操作(Operation)+客体对象(Object)。角色作为一个用户与权限的代理层,所有的授权应该给予角色而不是直接给用户或组。RBAC模型的基本思想是将访问权限分配给一定的角色,用户通过饰演不同的角色获得角色所拥有的访问许可权。

在基于角色的访问控制模型中,只有系统管理员才能定义和分配角色,用户不能自主地将对客体的访问权转让给别的用户。相较而言,自主访问控制配置的力度小、配置的工作量大、效率低,强制访问控制配置的力度大、缺乏灵活性,而基于角色的访问控制策略是与现代的商业环境相结合的产物,具有灵活、方便和安全的特点,是实施面向企业安全策略的一种有效的访问控制方式,目前常用于大型数据库系统的权限管理。

下面介绍一个基于角色的访问控制实例。

在银行环境中,用户角色可以定义为出纳员、分行管理者、顾客、系统管理者和审计员,相应的访问控制策略可作如下规定。

(1) 允许一个出纳员修改顾客的账号记录(包括存款和取款、转账等),并允许其查询所有账号的注册项。

(2) 允许一个分行管理者修改顾客的账号记录(包括存款和取款,但不包括规定的资金数目的范围)并允许其查询所有账号的注册项,也允许创建和终止账号。

(3) 允许一个顾客只询问他自己的账号的注册项。

(4) 允许系统的管理者访问系统的注册项和开关系统,但不允许读或修改用户的账号信息。

(5) 允许一个审计员读系统中的任何数据,但不允许修改任何内容。该策略陈述易于被非技术的组织策略者理解,同时也易于映射到访问控制矩阵或基于组的策略陈述。另外,该策略还同时具有基于身份策略的特征和基于规则策略的特征。

基于角色的访问控制具有如下优势。

(1) 便于授权管理。例如,系统管理员需要修改系统设置等内容时,必须有几个不同角色的用户到场方能操作,从而保证了安全性。

(2) 便于根据工作需要分级。例如,企业财务部门与非财务部门的员工对企业财务的访问权就可由财务人员这个角色来区分。

(3) 便于赋予最小特权。例如,即使用户被赋予高级身份时也未必一定要允许其使用特权,以便减少损失,只有必要时方能拥有特权。

(4) 便于任务分担,让不同的角色完成不同的任务。在基于角色的访问控制中,某个人用户可能是不止一个组或角色的成员,对于不同的组或角色而言拥有的权限也有所不同。

(5) 便于文件分级管理。文件本身也可分为不同的角色,如信件、账单等,由不同角色的用户拥有。

在各种访问控制系统中,访问控制策略的制定实施都是围绕主体、客体和操作权限三者之间的关系展开。有三个基本原则是制定访问控制策略时必须遵守的。

(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和错误操作带来的危险。

(2) 最小泄露原则,是指主体执行任务时,按照主体所需要知道信息的最小化原则分配

给主体访问权限。

(3) 多级安全策略，是指主体和客体间的数据流方向必须受到安全等级的约束。多级安全策略的优点是避免敏感信息的扩散。对于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对其访问。

5.2　操作系统安全

操作系统是硬件之上的第一层软件，作为计算机系统核心的软件，负责控制和管理计算机系统资源，其他软件都依赖于操作系统的支持。因此，操作系统安全是信息系统安全的基础。操作系统的设计和实现非常复杂，好的、完善的操作系统不仅要能有效地组织和管理计算机的各类资源、合理组织计算机工作流程、保证系统的高效运行，还应能阻止各类攻击、保证计算机上各类信息和数据的安全。现代操作系统存在不少的安全漏洞或后门，并且默认的安全设置容易受到攻击。因此，减少安全漏洞或后门对计算机系统的威胁，必须对操作系统设计合理的安全机制。

5.2.1　操作系统安全机制

导致操作系统不安全的主要原因是操作系统安全体制的缺陷。对操作系统构成的威胁主要有计算机病毒、特洛伊木马、隐蔽通道和天窗等。操作系统所具有的安全机制包括以下6方面。

1. 身份认证机制

身份认证是证明某人或某个对象身份的过程，是保证系统安全的重要措施。身份认证需要用一个标识来表示用户的身份。将标识和用户关联起来的过程称为认证。操作系统的许多保护措施大都基于认证系统的合法用户，身份认证是操作系统中相当重要的一个方面，也是用户获取权限的关键。

2. 访问控制机制

访问控制机制的基本任务就是防止非法用户进入系统及合法用户对系统资源的非法使用。自主访问控制根据用户的身份及允许访问权限决定其访问操作。强制访问控制是让用户与文件都有一个固定的安全属性，系统用该安全属性来决定一个用户是否可以访问某个文件。基于角色的访问控制解决了具有大量用户、数据客体和访问权限的系统中的授权管理问题。

3. 最小特权机制

最小特权是指在完成某种操作时赋予每个主体(用户或进程)必不可少的特权。最小特权机制一方面给予主体必不可少的特权，保证了所有的主体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，从而限制了每个主体所能进行的操作，确保由可能的事故、错误、网络部件的篡改等造成的损失最小。

4. 可信通路机制

可信通路(trust path)是终端人员能借以直接与可信计算基(Trusted Computing Base，TCB)通信的一种机制。可信通路机制只能由有关终端人员或可信计算基启动，并且不能被不可信软件模拟。可信通路机制主要应用在用户登录或注册时，能够保证用户确实是和安

全核心通信,防止不可信进程(如特洛伊木马等)模拟系统的登录过程而窃取口令。

5. 隐蔽通道的分析与处理

隐蔽通道是指系统中利用那些本来不是用于通信的系统资源绕过强制访问控制进行非法通信的一种机制。系统内充满着隐蔽通道。对于系统中的每一个信息比特,如果它能由一个进程修改而由另一个进程读取(直接或间接),那它就是一个潜在的隐蔽通道。

6. 安全审计机制

安全审计机制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。操作系统必须能够生成、维护及保护安全审计过程,防止其被非法修改、访问和毁坏,特别是要保护审计数据,严格限制未经授权的用户访问。

1972 年,J. P. Anderson 指出,开发安全的系统,首先必须建立系统的安全模型,完成安全系统的建模之后,再进行安全内核的设计与实现。历史上,主要安全操作系统模型有 BLP 机密性安全模型、Biba 完整性安全模型、Clark-Wilson 完整性安全模型、信息流模型、RBAC 安全模型、DTE 安全模型、无干扰安全模型等。每一种模型都用一套完善的规则来限制系统中信息的流动。操作系统的安全审计机制可以对系统中有关安全的活动进行记录、检查及审核,可以检测和阻止非法用户对计算机系统的入侵,并显示合法用户的误操作。安全审计是操作系统的重要组成部分,评价小型操作系统安全性的主要依据是 1985 年发布的美国国防部开发的可信计算机系统评价准则(Trusted Computer System Evaluation Criteria,TCSEC),该标准把安全级别从高到低分成 A、B、C、D 四个类别,又把每个类别分为若干类别。TCSEC 定义的大致内容如下。

A:校验级保护,提供低级别手段。

B3:安全域,数据隐藏与分层、屏蔽。

B2:结构化内容保护,支持硬件保护。

B1:标记安全保护,例如 System V 等。

C2:有自主的访问安全性,区分用户。

C1:不区分用户,基本的访问控制。

D:没有安全性可言,例如 MS DOS。

为了实现对信息或数据的访问控制功能,Windows 操作系统提供了特有的访问控制机制。

目前,Windows 2000 以上版本的操作系统均能达到 C2 级安全。C2 级安全标准的主要特征为:自主的访问控制;对象再利用必须由系统控制;用户标识和认证;能够审计所有安全相关事件和个人活动,只有管理员才有权限访问设计记录。

1) CPU 的工作模式

出于安全性和稳定性的考虑,从 Intel 80386 开始,该系列的 CPU 可以运行于 ring0～ring3 从高到低四个不同的权限级别,对数据也提供相应的四个保护级别。运行于较低级别的代码不能随意调用高级别的代码和访问较高级别的数据,而且也只有运行在 ring0 层的代码可以直接对物理硬件进行访问。Windows 只利用了 CPU 的两个权限级别:一个被称为内核模式,对应 80x86 的 ring0 层,它是操作系统的核心部分,设备驱动程序就是运行在该模式下;另一个被称为用户模式,对应 80x86 的 ring3 层,操作系统的用户接口部分以及

所有的用户应用程序都运行在该模式下。Windows 对运行在内核模式的组件空间不提供读/写保护。运行于内核模式的进程可以执行任何指令、访问任何地址，而运行于用户模式的进程访问的地址空间是受到限制的，能够执行的指令也是受限的，例如，这些进程不能更改其子进程之外的其他进程的状态等。

2）定时器

操作系统通过启用定时器(timer)来限制用户程序对 CPU 的使用，并能防止用户程序修改定时器，因而能够防止用户程序滥用 CPU。

3）内存保护

目前操作系统都能限制一个用户进程访问其他用户进程私有地址空间的行为，限制方法包括使用栅栏，重定位，基址/限址寄存器，对内存分段、分页等。对于共享的内存地址也提供了锁保护措施。

4）文件保护

在 Windows 中，文件和目录以及所有的基本操作系统数据结构都被称为对象，每个对象有一个拥有者。要访问对象，需要主体出示访问令牌，只有访问令牌和对象的访问控制列表中的访问控制条目匹配，系统才允许主体访问该对象。

5）安全组件

Windows 的安全组件包括安全标识符(SID)、访问令牌(access token)、安全描述符、访问控制列表(ACL)和访问控制条目(ACE)。

其中，安全标识符(SID)是用于标识用户、组和计算机账户的唯一号码。每次一个新的用户或组被建立时，它就收到唯一的 SID。当 Windows 安装和建立时，一个新的 SID 就分给那台计算机了。SID 唯一地标识用户、组和计算机，不仅应用在特定的计算机上，也在与其他计算机交互时应用。在用户被验证之后，系统会分配给用户一个访问令牌。访问令牌是访问资源的“入场券”，只要用户试图访问某种资源，就要出示访问令牌。然后系统对照请求对象的访问控制列表检查访问令牌。如果用户被许可，则以适当的方式认可访问。访问令牌只有在登录过程期间才能被分发，所以对用户访问权限的任何改变，都要求用户先注销，然后重新登录后接收更新的访问令牌。Windows 中每个对象有一个安全描述符，作为它属性的一部分。安全描述符由对象所有者的 SID、POSIX 子系统使用的组的 SID、自主访问控制列表和系统访问控制列表组成。访问控制条目即访问控制列表的表项，每个访问控制条目包含用户或组的 SID 和分配给该对象的权限。管理工具为一个对象列出访问权限时总是按照用户字母顺序列的，所以管理员的访问权限总位于前面。安全模型是对安全策略所表达的安全需求的简单、抽象和无歧义的描述，而模型的实现则描述了如何把特定的机制应用于系统中，从而实现某一特定安全策略所需的安全保护。

5.2.2　操作系统攻击技术

对操作系统的攻击有多种技术，下面从针对认证的攻击、针对漏洞的攻击、直接攻击、被动攻击以及攻击成功后恶意软件的驻留等方面进行介绍。

1. 针对认证的攻击

操作系统通过认证手段鉴别并控制计算机用户对系统的登录和访问，但由于操作系统提供了多种认证登录手段，因此利用系统在认证机制方面的缺陷或者不健全之处，可以实施

对操作系统的攻击。例如,利用字典攻击或者暴力破解等手段,获取操作系统的账号、口令;利用 Windows 的 IPC $ 功能,实现空连接并传输恶意代码;利用远程终端服务即 3389 端口,开启远程桌面控制等。

2. 针对漏洞的攻击

攻击者经常会针对展开对操作系统的攻击。在系统存在漏洞的情况下,通过攻击脚本,攻击者可以远程获得对操作系统的控制。Windows 操作系统的漏洞由微软公司每月定期以安全公告的形式对外公布,对系统威胁最大的漏洞包括远程溢出漏洞、本地提权类漏洞、用户交互类漏洞等。

3. 直接攻击

直接攻击是攻击者在对方防护很严密的情况下,通常采用的一种攻击方法。例如,当操作系统的补丁及时打上,并配备防火墙、防病毒、网络监控等基本防护手段时,针对认证和漏洞的攻击就难以奏效。此时,攻击者采用电子邮件、QQ、MSN 等即时消息软件,发送带有恶意代码的信息,通过诱骗对方点击来安装恶意代码。也就是说,可直接穿过防火墙等对系统进行攻击。

4. 被动攻击

被动攻击是在没有明确的攻击目标,并且对方防范措施比较严密情况下采用的一种攻击手段。一般通过建立或者攻陷一个对外提供服务的应用服务器,篡改网页内容,设置恶意代码,诱骗普通用户点击的情况下,对普通用户进行的攻击。由于普通用户不知网页被篡改后含有恶意代码,自己点击后被动地安装上恶意软件,从而被实施了对系统的有效渗透。

5. 攻击成功后恶意软件的驻留

恶意软件的一个主要功能是对操作系统的远程控制,并通过信息回传、开启远程连接、进行远程操作等手段造成目标计算机的信息泄露。恶意软件一旦入侵成功,将采用多种手段在目标计算机进行驻留,例如通过写入注册表实现开机自动启动,采用 rootkit 技术进行进程、端口、文件隐藏等,目的就是实现自己在操作系统中不被发现,以更长久地对目标计算机进行控制。

5.2.3 Windows 系统的安全管理

如图 5-5 所示,Windows 系统采用的是层次性的安全架构,整个安全架构的核心是安全策略,完善的安全策略决定了系统的安全性。Windows 系统的安全策略明确了系统各个安全组件如何协调工作,Windows 系统安全开始于用户认证,是其他安全机制能够有效实施的基础,处于安全架构的最外层。常见的认证机制包含登录口令和令牌。

加密和访问控制处于用户认证之后,是保证系统安全的主要手段。加密保证了系统与用户之间的通信及数据存储的机密性;访问控制则维护了用户访问的授权原则。审计和管理处于系统的内核层,负责系统的安全配置和事故处理,审计可以发现系统是否曾经遭受过攻击或者正在遭受攻击,并进行追查;管理则是为用户有效控制系统提供功能接口。

Windows 系统的安全管理主要围绕安全主体展开,目标是保护其安全性。安全主体主要包括用户、组、计算机以及域等。用户是 Windows 系统中操作计算机资源的主体,每个用户必须先行加入 Windows 系统,并被指定唯一的账户;组是用户账户集合的“容器”,也被赋予了一定的访问权限——放到一个组中的所有账户都会继承这些权限;计算机是指一台

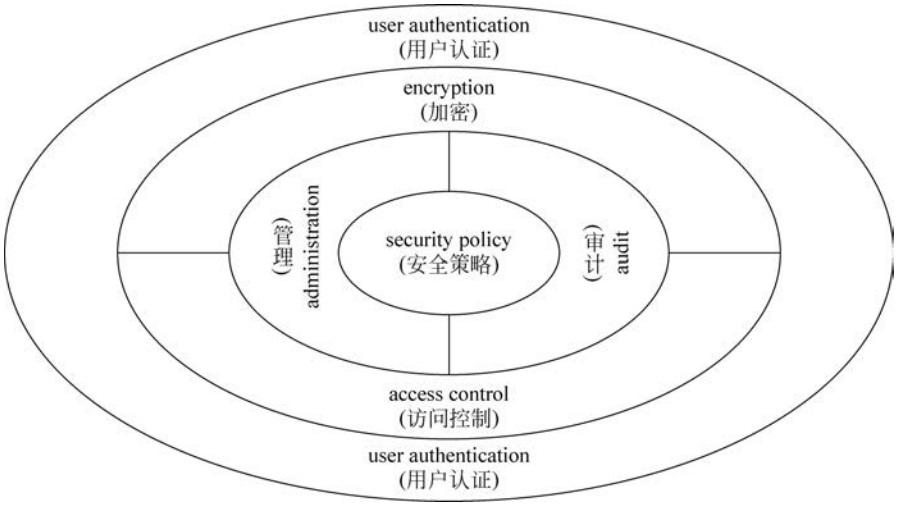

图 5-5　Windows 系统的安全架构

独立计算机的全部主体和客体资源的集合，也是 Windows 系统管理的独立单元；域是使用域控制器(Domain Controller，DC)进行集中管理的网络，域控制器是共享的域信息的安全存储仓库，同时也是域用户认证的中央控制机构。

Windows 系统的安全管理主要是由它的安全子系统来提供，安全子系统既可以用于工作站，也可以用于服务器，区别只在于服务器版的用户账户数据库可以用于整个域，而工作站版的数据库只能本地使用。如图 5-6 所示，Windows 系统的安全性服务运行在两种模式下，安全参考监视器(Security Reference Monitor，SRM)运行在内核模式下，作为 Windows Executive 的一部分；而用于与用户进行交互的主要安全服务即本地安全机构主要包括身份认证和访问控制等。

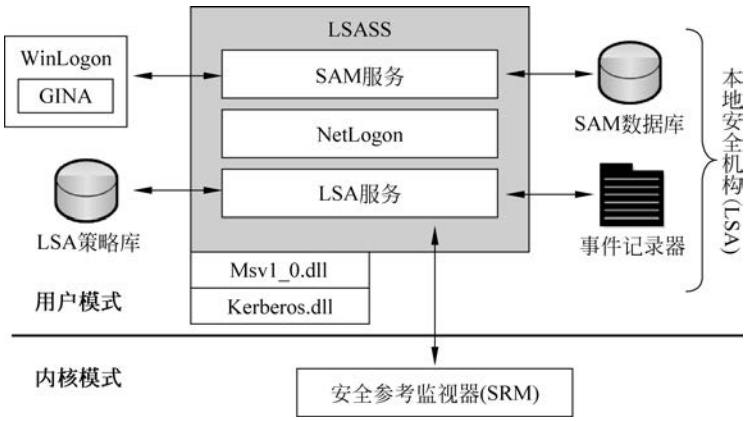

图 5-6　Windows 安全子系统

安全参考监视器(SRM)是 Windows 系统所有安全服务的基础，运行在内核模式下，负责检查一个用户是否有权限访问一个客体对象或者是否有权利完成某些动作，对每个客体对象的访问必须得到内核层 SRM 的有效性访问授权，否则访问无法完成。SRM 的另一个功能是与 LSA 配合来监视用户对客体对象的访问，并生成事件日志传送给事件记录器保存，为管理员的事件审计提供依据。

LSA安全服务主要由本地安全机构子系统(Local Security Authority Subsystem,LSASS)登录模块WinLogon两个服务来完成。WinLogon是系统启动时自动加载的一个进程,监视整个登录过程,同时可以加载GINA(Graphical Identification and Authentication)进程,提供图形化的认证界面。LSASS主要包括LSA服务、安全账户管理(Security Account Management,SAM)服务、网络登录服务NetLogon等基本组件。

LSA服务是用户与系统的交流通道,它提供了许多服务程序帮助用户完成许多工作,主要包括提供交互式登录认证服务、创建用户的访问令牌、存储和映射用户权限、设置和管理审核策略等。LSA与用户交互涉及许多服务进程,例如,与WinLogon合作完成用户登录,调用Msv1_0.dll支持NT LanMan认证的服务,调用Kerberos.dll支持Kerberos认证的服务,等等。

SAM服务是实现用户身份认证的主要依据,在SAM数据库保存着用户账号和口令等数据,为LSA提供数据查询。NetLogon是进行域登录的重要部件,首先通过安全通道与域中控制器建立连接,然后再通过安全的通道传递用户的口令,完成域登录。图5-7是Windows登录认证流程,SSPI(Security Support Provider Interface)是微软公司提供的公用API接口,可供第三方利用该接口获得不同的安全性服务而不必修改协议本身。

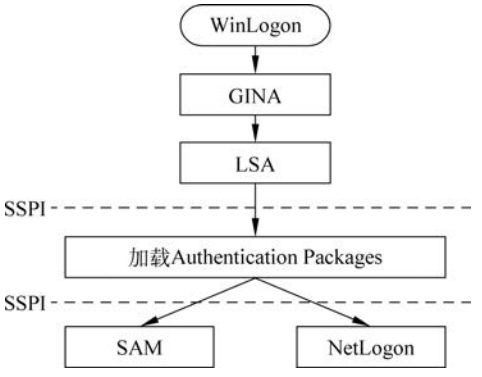

图5-7 Windows登录认证流程

5.2.4 Windows系统的访问控制

Windows系统的访问控制是其安全性的基础构件之一。访问控制模块有两个主要的组成部分:访问令牌(access token)和安全描述符(security descriptor),它们分别由访问者和被访问者持有。通过访问令牌和安全描述符的内容,Windows可以确定持有令牌的访问者能否访问持有安全描述符的对象。Windows中的每个账户或账户组都有一个安全标识符,系统的Administrator、Users等账户或者账户组在Windows内部均使用SID来标识,每个SID在同一个系统中都是唯一的。

访问令牌是一个被保护的对象,每一个访问令牌都与特定的Windows账户相关联。访问令牌包含该账户的SID、所属组的SID以及账户的特权信息。当一个账户登录时,LSA会从内部数据库中读取该账户的信息,然后使用这些信息生成一个访问令牌。当用户试图访问系统资源时,需要将拥有的令牌提供给SRM,SRM会检查用户试图访问的对象的访问控制列表。

每个被访问的客体对象都与一个安全描述符相关联,安全描述符用来描述客体对象的属性及安全规则,包含客体对象所有者的SID和ACL。ACL包含DACL和SACL。DACL由多个访问控制项(Access Control Entry,ACE)组成,每个访问控制项的内容描述了允许或拒绝特定账户对这个对象执行特定操作。SACL是为系统审计服务的,它的内容决定了当特定账户对该客体对象执行特定操作时,其行为是否会被记录到系统日志中。

如图5-8所示,Smith的进程Thread A访问客体对象FILE.txt,则SRM依据Smith

的访问令牌的信息和 FILE.txt 的安全描述符进行审核，由于安全描述符中 DACL 包含访问控制项 ACE1，其内容是拒绝 Smith 的读操作 Read、写操作 Write 和执行操作 Execute，因此 SRM 拒绝 Thread A；而 SRM 根据 DACL 的内容允许 Thread B 访问 FILE.txt。

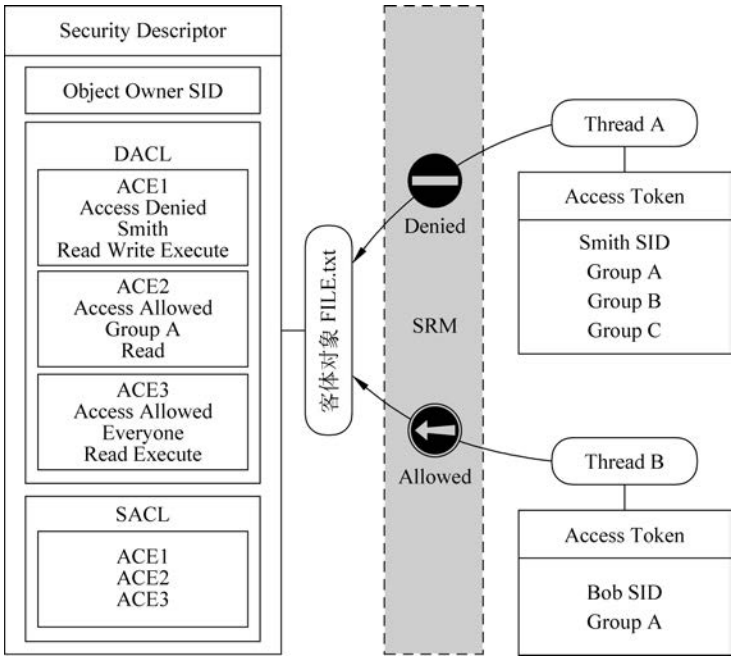

图 5-8　Windows 访问控制模型

5.2.5　Windows 系统的活动目录与组策略

Windows 操作系统安全涉及两项非常重要的服务：活动目录(Active Directory，AD)和组策略(Group Policy，GP)，它们协调工作有效提升了 Windows 操作系统的安全性。AD 存储有关网络对象的信息，让管理员和用户可以轻松查找和使用这些信息。AD 是一个面向网络对象管理的综合目录服务，网络对象包括用户、用户组、计算机、打印机、应用服务器、域、组织单元和安全策略服务。AD 是各种网络对象的索引集合和数据存储的视图，把分散的网络对象建立索引目录，存储在 AD 的数据库内。

图 5-9 为 AD 的管理划分模型，AD 把整个域作为一个完整目录进行管理，域模式要求用户进行网络登录，用户只要在域中有一个账户，登录成功即可在整个域网络中活动。同时，AD 把域划分为若干组织单元(Organizational Unit，OU)，OU 是域中用户和组、文件、打印机等网络对象以及其他 OU 的集合。可见，OU 可以划分下级 OU，下级 OU 能够继承父 OU 的访问权限。每一个 OU 有自己的管理员，负责 OU 的权限管理，从而实现 AD 的多层次管理。

AD 的功能包括基于目录的用户和资源管理、基于目录的网络服务和基于网络的应用管理。基于目录的用户和资源管理为用户提供网络对象的统一视图，基于目录的网络服务主要包括 DNS、WINS、DHCP、证书服务等，基于网络的应用管理包括管理企业通讯录、用户组管理、用户身份认证、用户授权管理和应用系统支撑等。

如果说 AD 是 Windows 网络中重要的安全管理平台，那么组策略(GP)是其安全性的

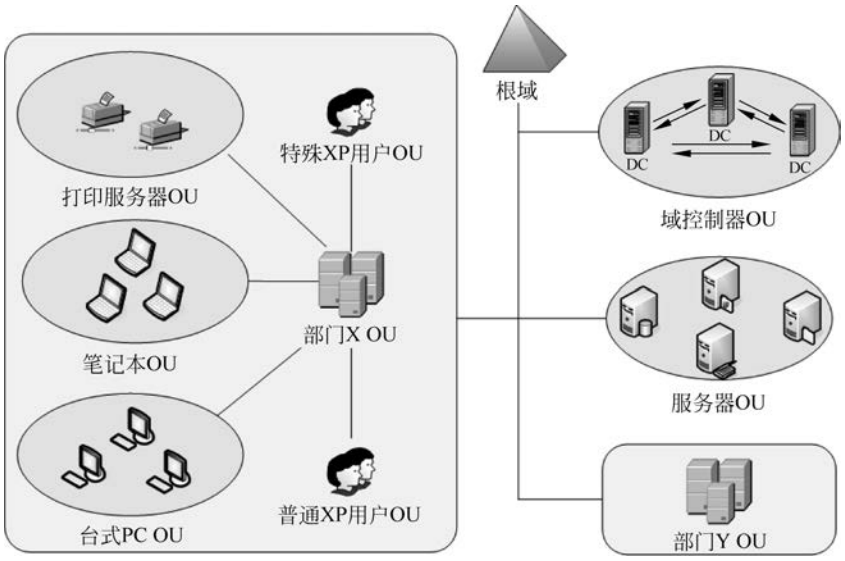

图 5-9 活动目录(AD)的管理划分模型

重要体现。GP 是依据特定的用户或计算机的安全需求定制的安全配置规则。如图 5-10 所示,管理员针对每个组织单元(OU)定制不同的 GP,并将这些 GP 存储在 AD 的相关数据库内,可以强制推送到客户端实施 GP。AD 可以使用 GP 命令来通知和改变已经登录的用户的 GP,并执行相关安全配置。

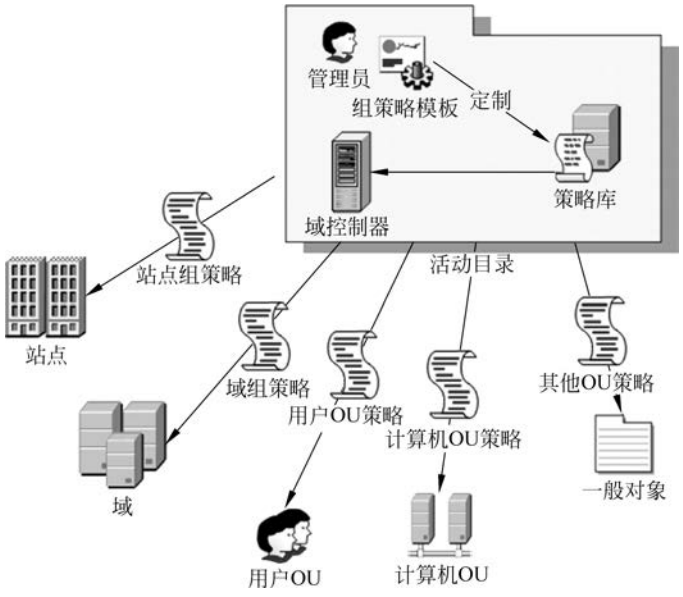

图 5-10 组策略工作流程

注册表是 Windows 系统中保存系统应用软件配置的数据库,很多配置都是可以自定义设置的,但这些配置散布在注册表的各个角落,如果手工配置,可想有多么困难和烦琐。GP 可以将系统中重要的配置功能汇集成一个配置集合,由管理人员通过配置并实施 GP,达到直接管理计算机的目的。简单地说,实施 GP 就是修改注册表中的相关配置。GP 分为基于

活动目录的GP和基于本地计算机的GP；AD GP存储在域控制器上AD的数据库中，它的定制实施由域管理员来执行；本地GP存放在本地计算机内，由本地管理员来定制实施。AD GP实施的对象是整个组织单元OU；本地GP只负责本地计算机。GP和AD配合GP部署在OU、站点或域的范围内，也可以部署在本地计算机上。部署在本地计算机时，GP不能发挥其全部功能，只有和AD配合，GP才可以发挥出全部潜力。

5.2.6　Windows系统的安全服务

Windows安全服务依托安全管理功能实现，包括账户安全、文件安全和主机安全。

1. 账户安全

只有Windows Server 2003操作系统的合法账户，才能访问网络上的资源。基于Internet的非法入侵是从寻找账户的漏洞开始的。Windows通过账户来管理用户，控制用户对资源的访问，每一个需要访问网络的用户都要有一个账户。Windows用户分为域用户账户、本地用户账户和内置用户账户。

1）域用户账户

域用户账户是用户访问域的唯一凭证，该账户在域控制器上建立，作为活动目录的一个对象保存在域的数据库中。用户在域中的任何一台计算机登录时必须提供一个合法的域用户账户，该账户将被域控制器所验证。

SAM作为保存域用户账户的数据库，位于域控制器的\%systemroot%\NTDS\NTDS.DIT文件中。每个账户都被Windows签订唯一的SID，保证账户在域中的唯一性。SID作为账户的属性不能被修改，若账户被删除，则SID将不复存在。Windows系统中SID对应用户权限，因此只要SID不同，新建账户不会继承原有账户的权限与组的隶属关系。

2）本地用户账户

Windows Server 2003在工作组模式或作为域中的成员服务器时，计算机操作系统中存在的是本地用户和本地组。本地用户账户的作用范围仅限于在创建该账户的计算机上，以控制用户对该计算机上的资源的访问。如果用户访问在工作组模式下的计算机，则必须具有被访问计算机的本地账户。本地账户存储在%SystemRoot%\system32\config\Sam数据库中，这些账户在被访问计算机上必须是唯一的。本地用户账户验证由创建该账户的计算机进行，因此这种类型账户的管理是分散的，并且也有一个唯一的SID标志，记录账户的权限和组的隶属关系。

3）内置用户账户

Windows Server 2003自带账户，系统安装好后这些账户已经存在，并且赋予相应的权限以完成某些特定的工作。Windows内置用户账户包括Administrator和Guest，内置账户不允许被删除，Administrator不允许被屏蔽，但内置账户允许被更名。Administrator账号被赋予在域中和在计算机中不受限制的权利，用于管理本地计算机或域，具体是指创建其他用户账号和组、实施安全策略、管理打印机和分配用户对资源的访问权限等。Guest是在域或计算机中的用户临时访问时使用的，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。

在规划Windows Server 2003域时，注意考虑账户的命名约定和账户的密码约定。账号命名约定包括：域用户账号的用户登录名在AD中必须唯一；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；本地用户账号在创建该账号的计算机上必须唯一；如果用户名称有重复，则应该在账号上加以区别；对于临时雇员应该做出特殊的命名，以便标示出来。账户密码约定包括：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；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；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。

2. 文件安全

Windows Server 2003 使用 NTFS 文件系统格式，该结构提供数据文件访问控制机制。NTFS 权限是基于 NTFS 分区实现，支持用户对文件的访问权限，支持对文件和文件夹的加密，NTFS 权限可以实现高度的本地安全性。

1) 通过对用户赋予 NTFS 权限可以有效地控制用户对文件和文件夹的访问

在 NTFS 分区上的每一个文件和文件夹都有一个 ACL 列表，该表记录每一个用户和组对该资源的访问权限。在默认情况下，NTFS 权限具有继承性，即文件和文件夹继承来自上层文件夹的权限。NTFS 权限分为特殊 NTFS 权限和标准 NTFS 权限两类，标准 NTFS 权限是特殊 NTFS 权限的特定组合，特殊 NTFS 权限规定了用户访问资源的所有行为。

Windows 将一些常用的特殊 NTFS 权限组合为标准 NTFS 权限，当需要分配权限时将一个标准 NTFS 权限分解为多个特殊 NTFS 权限，简化权限的分配和管理。

2) NTFS 权限的使用原则

一个用户可能属于多个组，NTFS 权限的使用原则用于判断用户对资源有何种访问权限。权限最大原则，当一个用户同时属于多个组，而这些组又有可能对某种资源赋予了不同的访问权限，按照权限最大原则，则用户对该资源的最终有效权限是在这些组中最宽松的权限，即加权限，将所有的权限加在一起即该用户的权限。

文件权限超越文件夹权限：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其被赋予访问该文件的权限，即文件权限超越其上级文件夹的权限，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。

拒绝权限超越其他权限原则：如果用户对某个资源有拒绝权限，那么该权限超越其他任何权限，即在访问该资源时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。

3) NTFS 权限的继承

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。在同一 NTFS 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移过来，因此文件和文件夹仍然保留有在原位置的一切 NTFS 权限。

在不同 NTFS 分区之间移动文件或文件夹，文件和文件夹会继承目的分区中文件夹的权限，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。

在同一个 NTFS 分区内复制文件或文件夹，文件和文件夹将继承目的位置中的文件夹的权限。在不同 NTFS 分区之间复制文件或文件夹，文件和文件夹将继承目的位置中文件夹的权限。

4）共享文件夹权限管理

共享文件夹用于向网络用户提供对文件资源的访问，可以包括应用程序、公用数据或用户个人数据。读权限：用户可以显示文件夹名称、文件名、文件属性，运行程序文件，对共享文件夹内的文件夹做出改动。修改权限：用户可以创建文件夹、向文件夹中添加文件、修改文件中的数据、向文件中添加数据、修改文件属性、删除文件夹和文件。完全控制权限：用户可以修改文件权限、获取文件的所有权并执行修改权限允许的所有任务。

5）文件的加密与解密

Windows Server 2003 的 NTFS 文件系统内置了 EFS 加密系统，利用 EFS 加密系统可以对保存在硬盘上的文件进行加密，其加密和解密过程对应用程序和用户而言是完全透明的。文件或文件夹被加密后，未经许可对其进行物理访问的入侵者都无法阅读这些文件或文件夹中的内容。通常将要加密的文件置于一个文件夹中，再对该文件夹加密，可以一次加密大量的文件。在该文件夹下创建的所有文件和子文件夹都会被加密。

3. 主机安全

主机安全是针对单个主机设置的安全规则，旨在保护计算机上的重要数据。安全策略定义了用户在使用计算机、运行应用程序和访问网络等方面的行为约束，通过这些约束避免了各种对网络安全的有意或无意的伤害。安全策略是事先定义好的一系列应用于计算机的行为准则，应用这些安全策略使用户有一致的工作方式，防止用户破坏计算机上的各种重要配置，保护网络上的敏感数据。在 Windows Server 2003 中，安全策略是以本地安全设置和组策略两种形式出现的。本地安全设置是基于单个计算机的安全性而设置的。本地安全设置应用于较小的组织或者没有应用活动目录的网络；而组策略可以在站点、组织单元或域的范围内实现，通常应用于较大规模并且应用活动目录的网络。

1）实施本地安全设置

本地安全设置只能在不属于某个域的计算机上实现，其中可设定的值较少，对用户的约束也较少。如果要在整个网络中约束用户使用计算机的行为，则必须在每一个计算机上实施本地安全设置。本地安全设置包括账户策略、本地策略、公钥策略和 IP 安全策略。

2）配置并实施组策略

在 Windows Server 2003 活动目录中，组策略的主要作用是规定用户和计算机的使用环境，还应用于成员服务器、域控制器以及管理范围内的其他计算机。组策略定义了系统管理员需要管理的用户桌面环境的各种组件。要为特定用户组创建特殊的桌面配置，可使用组策略对象编辑器创建组策略对象，并将其与选定的活动目录对象相关联。

组策略包括两部分：用户配置策略，是指定对应于某个用户账户的策略，这样不论该账户在域内哪台计算机上登录，其工作环境都是一样的；计算机配置策略，是指定对应于某台计算机的策略，这样不论哪个账户在该计算机上登录，其工作环境都是一样的。

3）使用预定义安全性模板

Windows Server 2003 包含多个适用于不同安全需求的安全性模板，利用这些模板，网络管理人员可以简化策略的设定和实施操作。预定义安全性模板包括 3 种安全级别。基本级别的模板为 Windows 定义的默认的安全级别，包括以下设定：默认的工作站、默认的服务器和默认的域控制器，它们位于\systemroot\security\templates 文件夹中。

兼容标准的模板包括商用应用程序的所有功能，使之仍然可以有效地运行，该模板为兼

容工作站或服务器模板。安全性模板有可能会影响到一些商用应用程序某些功能的运行,主要包括安全的工作站或服务器、安全的域控制器。高度安全性模板,不会考虑应用程序是否会受到这些设定的影响,主要包括高安全的工作站或服务器、高安全的域控制器。通常情况下,这类模板要慎重使用。

5.3 软件安全

在众多应用系统中,往往运行了多种软件实现其对外服务的功能。软件安全也是影响系统安全的一个重要方面。

5.3.1 开发安全的程序

大部分的溢出攻击是由不良的编程习惯造成的。现在常用的C和C++语言因为宽松的程序语法限制而被广泛使用,它们在营造了一个灵活高效的编程环境的同时,也在代码中埋下了很大的风险隐患。为避免溢出漏洞的出现,在编写程序的同时就需要将安全因素考虑在内,软件开发过程中可利用多种防范策略,如编写正确的代码,改进C语言函数库,数组边界检查,使堆栈向高地址方向增长,程序指针完整性检查等,以及利用保护软件的保护策略(如StackGuard)对付恶意代码等,来保证程序的安全性。目前有几种基本的方法可用于保护缓冲区免受溢出攻击的影响。

(1) 规范代码写法,加强程序验证。

(2) 通过操作系统使得缓冲区不可执行,从而阻止攻击者植入攻击代码。

(3) 利用编译器的边界检查来实现缓冲区的保护。

(4) 在程序指针失效前进行完整性检查。

5.3.2 IIS应用软件系统的安全性

IIS是Windows系统中的Internet信息和应用程序服务器,利用IIS可以方便地配置Windows平台,并且IIS和Windows系统管理功能完美地融合在一起,使系统管理人员获得和Windows完全一致的管理。在上面介绍了操作系统安全后,从IIS的安全性入手,简要介绍应用软件的安全性防范措施。

为有效防范针对IIS的溢出漏洞攻击,首先需要了解IIS的缓冲区溢出漏洞所在之处,然后进行修补。IIS 4.0和IIS 5.0的应用非常广泛,但由于这两个版本的IIS存在很多安全漏洞,也带来了很多安全隐患。

IIS常见漏洞包括idc&ida漏洞、.htr漏洞、NT Site Server Adsamples漏洞、.printer漏洞、Unicode解析错误漏洞、Webdav漏洞等。要了解如何加强Web服务器的安全性,防范由IIS漏洞造成的入侵就显得尤为重要。

例如,默认安装时,IIS支持两种脚本:管理脚本(.ida文件)和Internet数据查询脚本(.idq文件)。这两种脚本都由idq.dll来处理和解释,而idq.dll在处理某些URL请求时存在一个未经检查的缓冲区,如果攻击者提供一个特殊格式的URL,就可能引发一个缓冲区溢出。通过精心构造发送的数据,攻击者可以改变程序执行流程,从而执行任意代码。当成功地利用这个漏洞入侵系统后,攻击者就可以在远程获取Local System的权限了。

在“Internet 服务管理器”中，右击网站目录，选择“属性”命令，在网站目录属性对话框的“主目录”界面中，单击“配置”按钮。在弹出的“应用程序配置”对话框的“应用程序映射”界面，删除无用的程序映射。在大多数情况下，只需要留下.asp 一项即可，将.ida、.idq、.htr 等全部删除，以避免利用.ida、.idq 等这些程序映射存在的漏洞对系统进行攻击。

5.3.3　软件系统攻击技术

常见的利用软件缺陷对应用软件系统发起攻击的技术包括缓冲区溢出攻击、栈溢出攻击、堆溢出攻击、格式化串漏洞利用等。

1. 缓冲区溢出攻击

如果应用软件存在缓冲区溢出漏洞，可利用此漏洞实施对软件系统的攻击。缓冲区是内存中存放数据的地方。在程序试图将数据放到计算机内存中的某一个位置时，如果没有足够的空间，就会发生缓冲区溢出。攻击者写一个超过缓冲区长度的字符串，程序读取该段字符串，并将其植入缓冲区，由于该字符串的长度超出常规的长度，这时可能会出现两个结果：一个结果是过长的字符串覆盖了相邻的存储单元，导致程序出错，严重的可导致系统崩溃；另一个结果就是利用这种漏洞可以执行任意指令，从而达到攻击者的某种目的。程序运行的时候，数据类型等被保存在内存的缓冲区中。为了不占用太多的内存，包含动态分配变量的程序会在运行时才决定给它们分配多少内存空间。如果在动态分配缓冲区中放入超过缓冲区长度的数据，就会发生溢出。这时，程序就会因为异常而返回，如果攻击者用自己攻击代码的地址覆盖返回地址，这时通过 eip 改变返回地址，程序就会转向去执行攻击者的程序，如果攻击者编写的 shellcode 集成了文件的上传、下载等功能，获取到 root 权限，就相当于完全控制了被攻击方，也就达到了攻击者的目的。

2. 栈溢出攻击

程序每调用一个函数，就会在堆栈中申请一定的空间，我们把这个空间称为函数栈。随着进程中函数调用层数的增加，函数栈一块块地从高端内存地址向低端内存地址方向延伸；反之，随着进程中函数调用层数的减少，即各函数调用的返回，函数栈会一块块地被遗弃而向高端内存地址方向回缩。各函数的栈大小随着函数性质的不同而不等，由函数局部变量的数量决定。进程对内存的动态申请是发生在 Heap(堆)中的。也就是说，随着系统动态分配给进程的内存数量的增加，Heap(堆)有可能向高地址或低地址延伸，依赖于不同 CPU 的实现。但一般来说是向内存的高地址方向延伸的。当发生函数调用时，先将函数的参数压入栈中，然后将函数的返回地址压入栈中，这里的返回地址通常是 Call 的下一条指令的地址。例如，定义 buffer 时程序可分配 24 字节的空间，在 strcpy 执行时向 buffer 中复制字符串时并未检查长度，向 buffer 中复制的字符串如果超过 24 字节，就会产生溢出。如果向 buffer 中复制的字符串足够长，把返回地址覆盖后，程序就会出错。一般会报告错误或者非法指令，如果返回地址无法访问，则产生段错误，如果不可执行，则视为非法指令。

3. 堆溢出攻击

堆内存由分配的很多大块内存区组成，每一块都含有描述内存块大小和其他一些细节信息的头部数据。如果堆缓冲区遭受了溢出攻击，攻击者能重写相应堆的下一块存储区，包括其头部。如果重写堆内存区中下一个堆的头部信息，则在内存中可以写进任意数据。然而，不同目标软件各自特点不同，堆溢出攻击实施较为困难。

4. 格式化串漏洞利用

所谓格式化串,就是在 * printf()系列函数中按照一定的格式对数据进行输出,可以输出到标准输出,即 printf(),也可以输出到文件句柄、字符串等,对应的函数有 fprintf、sprintf、snprintf、vprintf、vfprintf、vsprintf、vsnprintf 等。能被黑客利用的地方也就出现在这一系列的 * printf()函数中。在正常情况下,这些函数只是把数据输出,不会造成什么问题,但是 * printf()系列函数有 3 个特性,这些特殊性质如果被黑客结合起来利用,就会形成漏洞。

可以被黑客利用的 * printf()系列函数的 3 个特性:参数个数不固定造成访问越界数据;利用%n 格式符写入跳转地址;利用附加格式符控制跳转地址的值。

5. shellcode 技术

缓冲区溢出成功后,攻击者如希望控制目标计算机,必须用 shellcode 实现各种功能。shellcode 是一堆机器指令集,基于 x86 平台的汇编指令实现,用于溢出后改变系统的正常流程,转而执行 shellocode 代码,从而完成对目标计算机的控制。

5.4 数据库安全

现有计算机信息系统多采用数据库存储和管理大量的关键数据,因此数据库安全问题也是系统安全的一个关键环节。了解针对数据的攻击技术,并采取相应的数据库安全防范措施,也是系统安全技术人员所需要关注的重点。

5.4.1 数据库安全技术

1. 数据库的完整性

数据库的完整性包括以下内容。

(1) 实体完整性,指表和它模拟的实体一致。

(2) 域完整性,指某一数据项的值是合理的。

(3) 参照完整性,指一个数据库的多个表中保持一致性。

(4) 用户定义完整性,由用户自定义。

(5) 分布式完整性。

数据库的完整性可通过数据库完整性约束机制来实现。这种约束是一系列预先定义好的数据完整性规划和业务规则,这些数据规则存放于数据库中,防止用户输入错误的数据,以保证所有数据库中的数据是合法的、完整的。

数据库完整性约束包括非空约束、默认值约束、唯一性约束、主键约束、外部键约束和规则约束。这种约束是加在数据库表的定义上的,它与应用程序中维护数据库完整性不同,它不用额外地编写程序,代价小而且性能高。在多网络用户的客户/服务器体系下,需要对多表进行插入、删除、更新等操作时,使用存储过程可以有效防止多客户同时操作数据库时带来的死锁和破坏数据完整一致性问题。此外,通过封锁机制可以避免多个事务并发执行存取同一数据时出现的数据不一致问题。

2. 访问控制机制

访问控制是数据库系统的基本安全需求之一,为了使用访问控制来保证数据库的安全,

必须使用相应的安全策略和安全机制保证其实施。数据库常用的存取控制机制是基于角色的存取控制机制。

基于角色的存取控制机制的特征是根据安全策略划分出不同的角色，对每个角色分配不同的操作许可，同时为用户指派不同的角色，用户通过角色间接地对数据进行存取。角色由数据库管理员管理分配，用户和客体无直接关系，他只有通过角色才可以拥有角色所拥有的权限，从而存取客体。用户不能自主地将存取权限授予其他用户。基于角色的存取控制机制可以为用户提供强大而灵活的安全机制，可以让管理员在接近部门组织的自然形式来进行用户权限划分。

3. 视图机制

通过限制可由用户使用的数据，可以将视图作为安全机制。用户可以访问某些数据，对其进行查询和修改，但是表或数据库的其余部分是不可见的，也不能进行访问。无论在基础表(1个或多个)上的权限集合有多大，都必须授予、拒绝或废除访问视图中数据子集的权限。

例如，某个表的 salary 列中含有保密职员信息，但其余列中含有的信息可以供所有用户使用。可以定义一个视图，使其包含表中除保密的 salary 列外的所有列。只要表和视图的所有者相同，授予用户视图上的 SELECT 权限，就能使用户得以查看视图中非保密列而无须对表本身具有任何权限。通过定义不同的视图及有选择地授予视图上的权限可以将用户、组或角色限制在不同的数据子集内。

4. 数据库加密

一般而言，数据库系统提供的基本安全技术能够满足普通的数据库应用，但对于一些重要部门或敏感领域的应用，仅靠上述措施难以保证数据的安全性，某些用户仍可能非法获取用户名和口令越权使用数据库，甚至直接打开数据库文件，窃取或篡改信息。因此，有必要对数据中存储的重要数据进行加密处理，以实现数据库的安全性。

较之传统的数据加密技术，数据库加密有其自身的要求和特点。数据库数据的使用方法决定了它不可能以整个数据库文件为单位进行加密。当符合检索条件的记录被检索出来后，就必须对该记录迅速解密，然而该记录是数据库文件中堆积的一段，无法从中间开始解密。因此，必须解决随机地从数据库文件中某一段数据开始解密的问题，也就是说，数据库加密只能对数据库中的数据进行部分加密。

5.4.2 数据库攻击技术

针对数据库的攻击有多种形式，攻击的最终目标是控制数据库服务器或者得到对数据库的访问权限。主要的数据库攻击手段包括以下3种。

1. 弱口令攻击

要获取目标数据库服务器的管理员口令，有多种方法和工具，例如针对 SQL 服务器的 SQLScan 字典口令攻击、SQLdict 字典口令攻击、SQLServerSniffer 嗅探口令攻击等。获取了 SQL 数据库服务器的口令后，即可利用 SQL 语言远程连接并进入 SQL 数据库内获得敏感信息。

2. SQL 注入攻击

由攻击者通过向 Web 服务器提交特殊参数，向后台数据库注入精心构造的 SQL 语句，

获取数据库中的表的内容或者挂网页木马,进一步利用网页木马再挂上木马。攻击者通过提交特殊参数和精心构造的 SQL 语句后,根据返回的页面判断执行结果、获取敏感信息。因为 SQL 注入是从正常的 WWW 端口访问,而且表面看起来与一般的 Web 页面访问没有区别,所以目前通用的防火墙都不会对 SQL 注入发出警报,如果管理员没有查看 IIS 日志的习惯,可能很长时间也不会察觉。

SQL 注入的手法相当灵活,在实际攻击过程中,攻击者根据具体情况进行分析,构造巧妙的 SQL 语句,从而达到注入的目的,而注入的程度和网站的 Web 应用程序的安全性和安全配置有很大关系。

3. 利用数据库漏洞进行攻击

利用数据库本身的漏洞实施攻击,获取对数据库的控制权和对数据的访问权,或者利用漏洞实施权限的提升。不同版本数据库的漏洞不一样。例如,Oracle 9.2.0.1.0 存在认证过程的缓冲区溢出漏洞,攻击者提供一个非常长的用户名,会使认证出现溢出,从而获得数据库的控制,这使得没有正确的用户名和密码也可获得对数据库的控制。Oracle 的 left outer joins 漏洞可以实现权限的提升。当攻击者利用 left outer joins 实现查询功能时,数据库不做权限检查,导致攻击者可以获得他们一般不能访问的表的权限。

5.4.3 数据库安全防范措施

为了有效防止针对数据库的攻击,要从前台的 Web 页面和后台的数据库服务器设置等多个层次进行统一考虑。

1. 编写安全的 Web 页面

SQL 注入漏洞是因为程序员所编写的 Web 应用程序没有严格地过滤从客户端提交至服务器的参数。所以,要防范 SQL 注入攻击,要从编写安全的 Web 应用程序开始做起。

对于客户端提交的参数,都要进行严格的过滤,检查其中是否存在特殊字符,要注意的特殊字符有单引号、双引号和当前使用的数据库服务器所支持的注释符号,例如,SQL Server 所使用的注释号是--,MySQL 所使用的注释号是/*等。除此之外,还有 SQL 语句中所使用的关键字,这些关键字包括 select、insert、update、and、where 等。除了严格检验参数,还要注意不向客户端返回程序发生异常的错误信息,这是因为 SQL 注入很大程度上是依赖程序的异常信息获取服务器的信息的,所以不能为攻击者留下任何线索。

2. 设置安全的数据库服务器

1) SQL Server

SQL Server 的安全性设置要通过安装、设置和维护三个阶段进行综合考虑。在安装阶段,将数据库默认自动或者手动安装使用 Windows 认证,这将把暴力攻击 SQL Server 本地认证机制的攻击者拒之门外。为数据库分配一个强壮的 SA 账户密码,也是安装过程中需要考虑的一件重要事情。

在设置阶段,使用服务器网络程序(server network utility)可禁用所有的 netlib,这使对数据库的远程访问无效,同时也使 SQL Server 不再响应 SQLPing 等对数据库的扫描和探测行为。激活数据库的日志功能可以在攻击者进行暴力破解时加以有效鉴别。此外,禁止 SQL Server Enterprise Manager 自动为服务账号分配权限,禁用 Ad Hoc 查询,设置操作系统访问控制列表,清除危险的扩展存储过程等措施,也可以阻止一些攻击者对数据库的非法操作。

在维护阶段，及时更新服务包和漏洞补丁，分析异常的网络通信数据包，创建 SQL Server 警报等方法，可以为管理员提供针对数据库更加有效的防范措施。

2）Oracle

Oracle 数据库的安全防范措施也需要综合考虑多方面的因素，包括可设置监听器密码，运行监听器控制程序连接相关的监听器时，可通过密码保护监听器的安全；删除 PL/SQL 外部存储功能，堵住攻击者对其的非法使用；确保所有数据库用户的默认密码已经更改为安全的新密码；为保证数据库实例的安全，及时更新补丁也是非常重要的一项安全措施。当然，如果 Oracle 数据库的前端是一个 Web 服务器，则 Web 前端将是外部攻击者的第一站，Oracle 的安全也离不开 Web 前端的安全。

3）MySQL

MySQL 数据库的安全防范措施主要包括消除授权表的通配符、使用安全密码、检查配置文件的许可、对客户端服务器传输进行加密、禁用远程访问功能和积极监控 MySQL 的访问日志。

MySQL 访问控制系统是通过一系列授权表进行的，授权表在数据库、表和列定义每一位用户的访问级别，同时定义某用户普适许可或使用通配符的权限，确保用户获得的访问权限恰好足够他们完成任务。为 MySQL 根账户设置一个密码，并且每一个用户账户都设置自己的密码，确保没有使用具有启发式信息的容易被识破的密码，例如生日、用户姓名字母等。用户账号、密码以纯文本形式存储在 MySQL 的 per-user 文件中，很容易就会被读取，因此把这些文件存储在非公共区域，或者存储在用户账户的私人主目录下，权限设置为 0600（只能被根用户读写）。

客户端服务器事务以明文信息方式传输，攻击者容易发现这些数据包并从中获取敏感信息，因此，需要激活 MySQL 设置中的 SSL 或 OpenSSH 的安全外壳实用程序，为传输数据创造一个安全加密通道，未经授权用户就很难读取传输数据。如果用户不需要远程访问服务器，那么强制所有 MySQL 连接都通过 socket 文件通信，会大大降低受到网络攻击的风险；设置服务器使用--skip-networking 选项启动，可以屏蔽 MySQL 的 TCP/IP 网络连接，确保没有用户能够远程连接到系统。MySQL 日志文件记录客户端连接、查询和服务器错误，通用查询日志（general query log）以时间戳记录了每一个客户端连接和断开连接，以及客户端执行每一次查询的情况；监控 MySQL 日志，发现网络入侵攻击的源头。

5.5　数据安全与灾难备份

在组织对信息的依赖越来越强的今天，任何关键信息系统运转的终端或者数据的丢失可能会给组织造成不可估量的损失。如何有效地保证数据信息的完整性、可用性和保密性是信息系统安全研究的重点内容。

5.5.1　数据的安全威胁

随着社会对计算机和网络的依赖性越来越大，如何保证计算机中数据的完整性、保密性和可用性成为每一个计算机使用者关心的重点。数据的完整性和可用性就是保证计算机系统上的数据和信息处于一种完整和未受损的状态。

针对数据完整性、可用性、保密性最常见的威胁来自攻击者或者计算机操作员、硬件故障、网络故障和灾难。攻击者的目的是对信息进行窃取或者破坏,计算机操作员也存在误删、误改的操作,这都对数据的安全性构成巨大的威胁。除了人为造成的问题之外,硬件故障和网络故障也是计算机运行过程中常见的故障,它们也将破坏数据的安全属性,严重时会造成数据的丢失。而往往在毫无防备的情况下突如其来的灾难,使系统数据遭到更严重的安全挑战,所有系统连同数据顷刻间被全部毁坏。为此,应针对数据的安全威胁给出应对措施,以提高数据的完整性、保密性和可用性,防止其遭到破坏。

5.5.2 数据的加密存储

保证数据安全的重要一点是保障数据的保密性,通常采用的技术是数据在存储过程中采用加密算法实现数据在介质中的加密存放。数据保密性的目的,在于当数据介质遭受盗窃或者非法复制后,仍然可以保证关键数据不被泄露。

在 Windows 操作系统中,NTFS 文件系统通过 EFS(Encrypt File System)数据加密技术实现数据的加密存储。当启用 EFS 时,Windows 创建一个随机生成的文件加密密钥(FEK),在数据写入磁盘时,透明地用这个 FEK 加密数据。然后 Windows 用公钥加密 FEK,把加密的 FEK 和加密的数据放在一起。公钥是第一次使用 EFS 时,Windows 自动生成的公私钥对中的公钥。FEK 是对称密钥,经它加密的数据只能在用户有相关私钥时才能解密出 FEK,再解密出加密的数据。

此外,PGP(Pretty Good Privacy)除了对电子邮件进行加密以防止非授权者阅读外,也可以对存储介质中的数据进行加密。PGP 采用公钥密码算法对数据进行加密,它可创建一个 PGPDisk 虚拟加密磁盘,所有数据写入此磁盘空间后,数据都处于加密状态,只有输入正确的 passphrase,才能访问加密的数据信息。此块磁盘空间的数据即使被窃取,也始终处于加密状态,从而保证了数据的安全。

5.5.3 数据备份和恢复

数据备份作为信息安全的一个重要内容,其重要性却往往被人们忽视。只要发生数据传输、数据存储和数据交换,就有可能产生数据故障,如果没有采取数据备份和数据恢复手段与措施,就会导致数据的丢失,甚至造成无法弥补与估量的损失。数据故障是多种多样的,通常可以划分为系统故障、事务故障和介质故障 3 类。计算机的应用越来越广泛,但使用计算机系统处理日常业务在提高效率的同时,也产生了新的问题,即数据失效。一旦发生数据失效,组织就会陷入困境:客户资料、技术文件、财务等数据可能被损坏得面目全非,而允许恢复时间可能只有短短几天或更少。如果系统无法顺利恢复,最终结局不堪设想。所以组织的信息化程度越高,数据备份和恢复措施就越重要。

数据备份和恢复是保护数据的最后手段,也是防止主动型信息攻击的最后一道防线。数据备份不仅仅是简单的文件复制,在多数情况下是指数据库备份。所谓数据库备份,是指制作数据库结构和数据的副本,以便在数据库遭到破坏时能够恢复数据库。备份的内容不但包括用户的数据库内容,而且包括系统的数据库内容。需要注意的是,大容量的备份不等于简单的文件复制,也不等于文件的永久性归档,它是要求用一种高速、大容量的存储介质将所有的文件(网络系统、应用软件、用户数据)进行全面的复制与管理。

1. 数据备份的方式

数据备份有多种方式，在不同的情况下，应该选择最合适的方法。按备份的数据量来说，数据备份的方式可以分为完全备份、增量备份、差分备份与按需备份4种。完全备份，是指备份系统中的所有数据，其特点是所需时间最长，但恢复时间最短，操作最方便，也最可靠；增量备份，是指只备份上次备份以后有变化的数据，其特点是所需时间较短，占用空间较少，但恢复时间较长；差分备份，是指只备份上次完全备份以后有变化的数据，其特点是所需时间较长，占用空间较多，但恢复时间较快；按需备份，是指根据临时需要有选择地进行数据备份。

采用何种备份方式，还取决于以下两个重要因素：备份窗口，即完成一次给定备份所需的时间，这个备份窗口由需要备份数据的总量和处理数据的网络架构的速度来决定；恢复窗口，即恢复整个系统所需的时间，恢复窗口的长短取决于网络的负载和磁带库的性能及速度。在实际应用中，必须根据备份窗口和恢复窗口的大小以及整个数据量，决定采用何种备份方式。一般来说，差分备份既避免了完全备份和增量备份的缺陷，又具有它们的优点。差分备份无须每天都做系统完全备份，并且实现灾难恢复很方便，只需要上一次完全备份磁带和灾难发生前一天磁带就可以完全恢复数据，因此采用完全备份结合差分备份的方式较为适宜。

2. 数据备份的状态

按状态来划分，数据备份有物理备份和逻辑备份两种。物理备份是指将实际物理数据库文件从一处复制到另一处的备份，冷备份、热备份都属于物理备份。所谓冷备份，也称脱机(offline)备份，是指以正常方式关闭数据库，并对数据库的所有文件进行备份。其缺点是需要一定的时间来完成，在备份期间，终端用户无法访问数据库，而且这种方法不易做到实时备份。所谓热备份，也称联机(online)备份，是指在数据库处于打开状态且用户对数据库进行操作的情况下进行的备份；也指通过使用数据库系统的复制服务器，连接正在运行的主数据库服务器和热备份服务器，当主数据库的数据有所修改时，变化的数据通过复制服务器可以传递到备份数据库服务器中，保证两个服务器中的数据一致。这种热备份方式实际上是一种实时备份，两个数据库分别运行在不同的计算机上，并且每个数据库都写到不同的数据设备中。逻辑备份就是将某个数据库的记录读出并将其写入一个文件中，这是经常使用的一种备份方式。MS-SQL 和 Oracle 等都提供 Export/Import 工具来用于数据库的逻辑备份。

3. 数据备份的层次

从层次上划分，数据备份可分为硬件容错和软件备份。目前的硬件冗余技术有双机容错、磁盘双工、磁盘阵列(RAID)与磁盘镜像等多种形式。硬件容错也有它的不足，一是不能解决因病毒或人为误操作引起的数据丢失以及系统瘫痪等灾难；二是如果错误数据也写入备份磁盘，硬件容错也会无能为力。理想的数据备份应使用硬件容错来防止硬件障碍，使用软件备份和硬件容错相结合的方式来解决软件故障或人为误操作造成的数据丢失。此外，从地点来划分，数据备份还可分为本地备份和异地备份。

4. 高可用性系统

高可用性系统的主要功能是保证在计算机系统的软硬件出现单点故障时，通过集群软件实现业务的正常切换，保证业务不间断、不停顿。高可用性系统是一组通过高速网络连接

的计算机集合,通过高可用集群软件相互协作,作为一个整体对外提供服务。集群中的每台服务器都分别运行后台检测进程和控制进程,定时收集磁盘、网络、串口等信息,检测进程发现集群中的某台服务器出现故障后,将对这台故障服务器进行接管处理,接管后 IP 地址动态切换,并由集群中的正常服务器自动启动故障服务器的应用程序和数据库,保证系统和应用服务不间断。高可用性系统通过多个服务器的相互备份实现了服务器单点故障时业务的正常进行,例如服务机的双网卡或者多网卡,以及 RAID(冗余磁盘阵列)等。由于集群系统在计算上的内在关联性,决定了节点之间的数据交换量较大,特别当集群内节点数增加到几十乃至几百时,内部网络传输数据的速率是整个系统计算速度的瓶颈。较高的传输带宽和尽量低的传输延时是高可用系统所追求的主要目标。

5. 网络备份

就传统的单机备份而言,备份设备连接到服务器,所以服务器负担重,备份操作安全性差。当服务器采用双机或集群时,备份设备只能通过其中的一台服务器进行备份。当网络中业务主机较多,并且需要实施备份操作的系统平台和数据库版本不同时,通过网络备份服务器对局域网中的不同业务主机数据进行备份就是一个最佳的选择。网络备份是通过在网络备份服务器上安装备份服务器端软件,在需要进行数据备份的业务主机上安装网络备份客户端软件,客户端软件将备份的数据通过网络传到备份服务器进行备份。网络备份使每台服务器负担减轻,备份操作安全性高,而且可通过一台网络备份服务器备份多台业务主机和服务器。网络备份可通过网络备份软件跨平台实时备份正在使用的数据库和文件,支持多服务器环境平行作业备份操作。通过网络备份软件也可以很好地对备份介质进行管理,实现全自动备份和恢复,可实现定时备份,并支持完全备份、增量备份、差量备份等多种备份策略。网络备份为局域网中的数据备份提供了高效的备份管理手段。

网络备份的缺点也十分明显,它占用大量网络资源,也占用一定的主机资源,同时备份时间较长。更加高效的备份技术存储区域网(Storage Area Network,SAN)解决了这些问题。存储区域网(SAN)是一种采用了光纤接口将磁盘阵列和前端服务器连接起来的高速专用子网。SAN 结构允许服务器连接任何存储设备,即 SAN 将多个存储设备通过光交换网络与服务器互联,使存储系统有更好的可靠性和扩展性。SAN 减少了对局域网网络资源的占用,改善了数据传输性能;改善了数据访问途径和访问速度,服务器可以通过光纤网络高速、远距离地访问共享存储设备;使得管理人员也可以集中管理存储系统,强化备份和恢复策略,提高整个系统的效率。同时,通过光纤交换机和集线器,存储设备可以无限扩展,主机节点的增加和替换可以减少对系统的影响。SAN 结构以一种共享存储系统的方式支持异构服务器的集群,保证了系统的高可用性。它支持所有服务器和存储设备的硬件互联,使得服务器增加存储容量变得非常简单。

6. 归档和分级存储管理

归档和分级存储管理是与网络备份不同的另一种数据备份技术,可用来解决因网络上的数据不断增长而造成数据量过大,计算机存储空间无法满足数据库存储需求的情况。归档是指将数据复制或者打包存放,以便能长时间地进行保存。归档的主要作用是长期保存数据,将有价值的数据安全地保存较长的时间。文件归档可以通过文档服务器对重要文档进行统一备份管理。普通信息数据一般通过数据压缩工具进行压缩,然后定期复制后存储下来。另一种常用的归档方法是使用备份系统,将关键数据备份到可移动介质中存放。分

级存储管理是一种对用户和管理员而言都透明的、提供归档功能的自动化备份系统。分级存储管理与归档的不同之处在于它把数据进行了迁移，而不是纯粹复制。分级存储管理系统选择将文件进行迁移，然后将文件复制到存储介质中，当文件被正确地复制后，一个与原文件具有相同名字的标志文件被创建，但它只占用比原文件小得多的磁盘空间。当用户想访问这个标志文件时，分级存储管理介入进来，将原始数据从正确的存储介质中恢复过来。分级存储管理主要用于当数据变得越来越陈旧时，将其从计算机的存储介质中转移到另一种存储介质中存放，以节省原计算机系统中有限的存储空间。

数据备份系统和高可用性系统可以避免由软硬件故障、人为操作失误和病毒造成的数据完整性、可用性的破坏。但是，当计算机系统遭到如地震、火灾等意外时，上述技术仍然无法解决。这时，就要靠数据容灾系统保护数据的完整可用性。数据容灾系统的基本原理是远程建立一套和本地计算机系统功能相同的计算机系统，当本地计算机系统遭受意外后，仍然远程保存了完整的数据。数据容灾系统除了在本地包含高可用性系统和数据备份系统之外，还包括数据远程复制系统和远程高可用性系统。数据远程复制系统主要保证本地数据中心和远程备份数据中心的数据一致性，数据远程复制一般通过软件数据复制和硬件数据复制技术实现，具体复制方式主要包括同步方式和异步方式。远程高可用性系统主要保证本地发生灾难后，业务及时切换到远程备份系统，它基于本地高可用性系统之上，实现远程故障的诊断、分类，并及时采取相应的故障接管措施。

当发生数据故障或者系统失效时，需要利用已备份的数据或其他手段，及时对原系统进行恢复，以保证数据安全性以及业务的连续性。对于一个计算机业务系统，所有引起系统非正常宕机的事故，都可以称为灾难。当无法预计的各种事故或灾难导致数据丢失时，及时采取灾难恢复措施，可以将企业或组织的损失降低到最低。一般灾难发生时，留给系统管理员的恢复时间往往相当短。但现有的备份措施没有任何一种能够使系统从大的灾难中迅速恢复过来。

通常情况下，系统管理员想要恢复系统至少需要下列几个步骤：①恢复硬件；②重新装入操作系统；③设置操作系统（驱动程序设置、系统、用户设置）；④重新装入应用程序，进行系统设置；⑤用最新的备份恢复系统设置。

系统备份与普通数据备份的不同在于，它不仅备份系统中的数据，还备份系统中安装的应用程序、数据库系统、用户设置、系统参数等信息，以便需要时迅速恢复整个系统。

系统备份方案必须包含灾难恢复措施。灾难恢复措施同普通数据恢复措施的最大区别在于：在整个系统都失效时，用灾难恢复措施能够迅速恢复系统而不必重装系统。需要注意的是，备份不等于单纯的复制，因为系统的重要信息无法用复制的方式备份下来，而且管理功能也是备份的重要组成部分。管理包括自动备份计划、历史记录保存、日志管理、报表生成等，没有管理功能的备份，不能算是真正意义上的备份，因为单纯的复制并不能减轻繁重的备份任务。数据备份与灾难恢复密不可分，数据备份是灾难恢复的前提和基础，而灾难恢复是在此基础之上的具体应用。灾难恢复的目标与计划决定了所需要采取的数据备份策略。

在网络环境中，系统和应用程序安装起来并不是那么简单，系统管理员必须找出所有的安装盘和原来的安装记录进行安装，然后重新设置各种参数、用户信息、权限等，这个过程可能要持续好几天甚至更久。因此，最有效的方法是对整个网络系统进行备份。这样，无论系统遇到多大的灾难，都能够应付自如。为保证数据的完整性和可用性，常采用备份、归档、分

级存储、镜像、RAID以及远程容灾等技术实现对数据的安全保障。

5.5.4 信息系统灾难备份技术

信息系统灾难备份是指信息系统的灾难备份与恢复,包括灾难前的备份与灾难后的恢复两层含义。灾难备份是指利用技术、管理手段以及相关资源确保关键数据、关键数据处理系统和关键业务在灾难发生后可以恢复的过程。

信息化发展的趋势也是我们要建设以及确定今后灾难备份方向的一个重要因素。现在,信息的重要性已经远远超过了系统设备本身,信息系统的信息量增长非常惊人,信息有效的保存已经成为一个很严峻的问题。在信息领域,灾备系统可以理解为以存储系统作为基本支持系统、以网络作为基本传输手段、以容错软/硬件技术为直接技术手段、以管理技术为重要辅助手段的综合系统。

一般情况下,信息系统灾难发生的原因有三种,分别是自然灾难、人为灾难和技术灾难。自然灾难所产生的直接后果就是本地数据信息难以获取或保全、本地系统难以在短时间内恢复或重建、灾难对信息系统的影响和范围难以控制。人为灾难的后果是丢失或泄漏重要数据信息、性能降低乃至丧失系统服务功能、软件系统崩溃或者硬件设备损坏。技术灾难的后果是造成信息、数据的损害或丢失。

灾难备份的目的就是通过建立远程备用数据处理中心,将生产中心数据实时或非实时地复制到备份中心。

灾难备份核心技术主要包括存储技术、信息系统评估和系统重构技术、信息安全技术和系统管理技术。

灾难备份存储技术主要包括虚拟化存储技术、多存储版本的管理技术、删除重复数据技术、集群并行存储技术、高效能存储技术等。灾难备份体系结构技术的核心包括容错系统结构、数据恢复技术、系统恢复技术、业务连续性服务。灾难备份信息安全技术主要用于保障数据在存储与传输过程中的安全性问题、网络系统的可靠和安全连接问题、计算机系统的安全性问题、使用用户的身份安全问题和系统操作的不可抵赖性问题等。其核心包括数据安全性技术、网络安全技术、系统安全技术、身份安全技术、安全审计技术。灾难备份系统管理技术是灾难备份的关键支撑技术,包括数据信息管理、灾难应急管理、系统恢复管理、灾难影响评估与决策支持。

灾难备份技术未来发展方向:从围绕着数据存储向围绕着应用服务转变,存储技术由集中式向分布式、虚拟化发展,从孤立专用系统向综合服务系统转变;围绕服务的灾难备份技术发展方向,保障业务连续性方向发展,要求数据完整而可用、系统快速重建、应用快速部署;新型容灾体系结构研究;灾难备份存储未来方向包括虚拟化灾难备份存储技术、重复数据删除与压缩技术、分布式灾难备份存储技术;灾难备份综合服务系统建设,即建立第三方中立机构形式的外包灾难备份系统,重点解决的问题包括公信力问题、数据的安全性、维护的便捷性、可扩展性、可共享性等。

5.6 实　　训

实训　EasyRecovery 数据备份与恢复

实训目的:理解数据备份的概念,熟悉常用的数据备份方法;理解数据恢复的原理,了

解常见的恢复种类，熟悉常用数据恢复软件；能用数据恢复软件 EasyRecovery Professional 进行数据恢复。

实训准备：数据备份工作是系统管理员的重要工作和职责，数据备份的方法很多，备份的手段也多种多样，双机异地备份是商业服务器数据安全的基本要求。实验前要求复习备份的概念和方法，深入理解备份、增量备份、系统备份、数据备份、持续性数据保护等概念，掌握数据备份的常用方法。

确定备份计划主要考虑以下几方面。

（1）确定备份的频率。确定备份频率要考虑两个因素：一是系统恢复时的工作量，二是系统活动的事务量。数据库备份可以是每个月、每一周甚至是每一天进行，而事务日志备份可以是每一周、每一天甚至是每一小时进行。

（2）确定备份的内容、介质和存放地点。

（3）确定备份采用动态备份还是静态备份。

（4）估计备份需要的存储空间量。在执行备份前，应该估计备份需要使用的存储空间量。

（5）确定备份的人员。

执行数据库恢复以前，应注意以下两点。

（1）在数据库恢复前，应该删除故障数据库，以便删除对故障数据库的任何引用。

（2）在数据库恢复前，必须限制用户对数据库的访问，数据库的恢复是静态的，应使用企业管理器或在系统存储过程中设置数据库为单用户。

实训内容：

1. Windows XP 文件备份与还原

（1）运行备份工具：选择“开始”→“程序”→“附件”→“系统工具”→“备份”命令。初次运行是以向导模式运行的，为了方便讲解，单击“高级模式”进入备份工具的主界面，如图 5-11 所示。

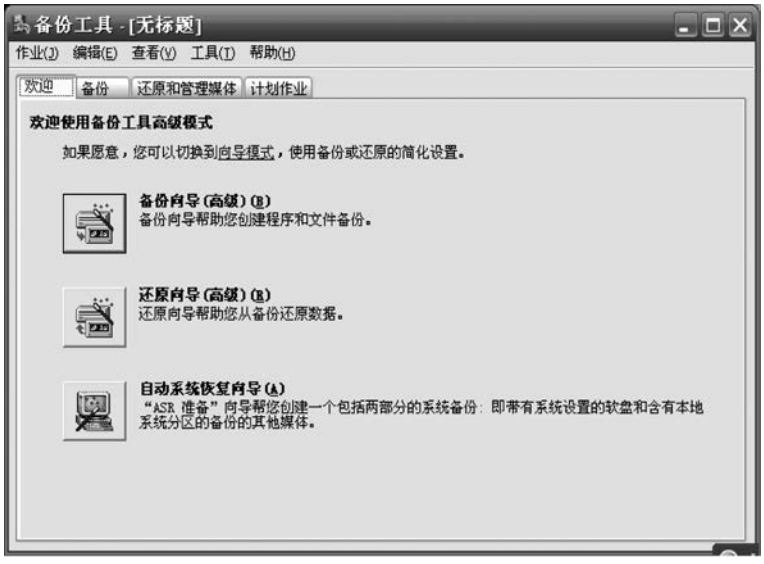

图 5-11　备份工具主界面

(2) 对某些资料进行备份："备份向导"→"下一步"→"备份选定的文件、驱动器或网络数据"→"要备份的项目"中勾选所要备份的文件夹(在文件列表框勾选需要备份的文件),如图 5-12 所示。

图 5-12 利用备份向导备份

单击"下一步"→"浏览",选择备份文件保存位置并输入备份的名称,如图 5-13 所示。

图 5-13 选择备份位置

单击"下一步"→"完成",这样就建立了一个名为 Backup 的备份文件,如图 5-14 所示。

最好把备份文件放到另外的存储器中,例如第二个硬盘、U 盘、刻录光盘等,以免因主硬盘有问题而导致数据与备份一起丢失。

(3) 对备份进行还原(以还原刚创建的 Backup.bkf 这个备份文件为例)。在图 5-11 中,单击"还原向导"→"下一步",在"要还原的项目"中选择需要还原的项目和对应的文件夹(在文件列表框勾选需要还原的文件),如图 5-15 所示。如果用户重装了系统导致没有还原项目列表,可以单击"浏览"按钮来找到备份文件。

图 5-14　备份进度

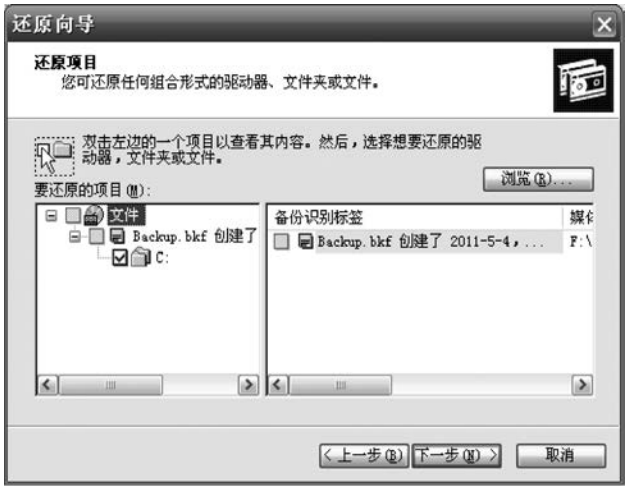

图 5-15　利用备份还原向导进行还原

在图 5-15 中，单击“下一步”→“完成”就把原来的备份还原到以前备份的源地址了。选择“高级”还原选项，可以对还原位置做出选择，如图 5-16 所示。

图 5-16　高级还原选项设置

“原位置”：备份时的文件位于哪里就恢复到哪里。

“替换位置”：自己选择还原的文件保存的位置，但保持原有的目录结构。

“单个文件夹”：自己选择还原文件保存的位置，但不保存原有的目录结构。

2. Windows 7 文件备份与还原

(1) 在 Windows 7 桌面，双击“计算机”，选择“系统属性”→“系统保护”，然后选择想要开启高级备份与还原功能的磁盘，这里选择“D 盘”，单击“配置”按钮。

(2) 创建系统还原点，填入还原点描述，这里填入 D，然后单击“创建”按钮，创建成功后单击“关闭”按钮。

(3) 双击桌面“计算机”，右击“D 盘”，选择“属性”→“以前的版本”，在这里能看到刚刚开启备份与还原功能的磁盘为我们创建的还原点文件，它是一个版本文件。

(4) 打开 D 盘，选择一个文件夹，然后删除该文件夹，并清空回收站。

(5) 双击桌面“计算机”，右击“D 盘”，选择“属性”→“以前的版本”，单击“D 盘”(这就是系统为我们备份的以前的版本信息)，再单击“还原”按钮。系统现在就在进行以前版本的还原操作。

(6) 打开“计算机”，双击“D 盘”，检查被删除的文件是否已经恢复。

3. 使用数据恢复软件 EasyRecovery Professional 进行数据恢复

(1) 解压缩并安装 EasyRecovery Professional v6.10.07。

(2) 打开 EasyRecovery.exe，选择“数据恢复”选项，如图 5-17 所示。

图 5-17 EasyRecovery 软件界面

单击“高级恢复”按钮，首先会弹出“目标文件警告”对话框，在此对话框中，EasyRecovery 要求用户将要恢复的文件复制到除源文件位置以外的安全位置。

如果系统中有多个被损坏的分区，不要将文件从一个分区恢复到另一个损坏的分区，这种情况下，可以使用可移动的介质或者另一个未损坏的硬盘驱动器作为目标位置。在该对话框中，选中“不要再显示此消息”复选框，然后单击“确定”按钮，如图 5-18 所示。

(3) 在“高级恢复”界面中，选择要查找的分区，然后单击“高级选项”按钮，如图 5-19 所示。

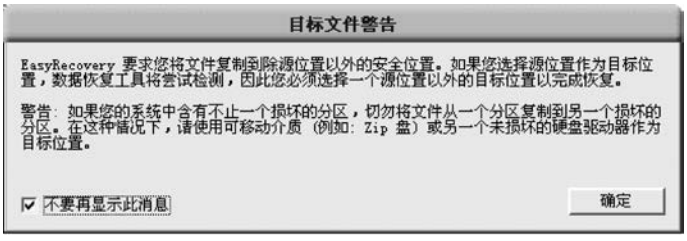

图 5-18　将文件恢复至安全位置

图 5-19　高级恢复界面

（4）在弹出的“高级选项”对话框中，包含“分区消息”“文件系统扫描”“分区设置”“恢复选项”4 个选项卡。在“分区信息”选项卡中，可以设置“起始扇区”和“结束扇区”。当分区不可见时，可以在此输入起始扇区和结束扇区，如果分区可见，则保留默认值，如图 5-20 所示。

图 5-20　设置高级选项

在“文件系统扫描”选项卡的“文件系统”下拉列表中选择分区的文件类型，可以在 FAT12、FAT16、FAT32 和 NTFS 之间选择，如图 5-21 所示。在选中“高级扫描”单选按钮后，单击“高级选项”按钮，从中可以设置“簇大小”和“起始数据”。

在“分区设置”选项卡中，如果分区已经损坏，选择“使用 MFT”选项可以使用当前 MFT

图 5-21 确定文件系统

扫描文件；如果分区被意外格式化了，选择“忽略 MFT”选项，即可忽略所有文件系统结构并简单地扫描文件数据。在“恢复选项”选项卡中，允许用户忽略扫描过程中找到的含有无效属性或已被删除的文件。当所有设置完成后，单击“确定”按钮，再单击“下一步”按钮。

(5) 这时 EasyRecovery 将开始扫描分区，当扫描到数据后，选中要恢复的文件或者文件夹，然后单击“下一步”按钮。

(6) EasyRecovery 可以将数据恢复到本地驱动器，或者通过网络恢复到 FTP 服务器。如果要将数据恢复到本地驱动器，选中“恢复至本地驱动器”单选按钮，再单击“浏览”按钮选择目标文件夹；如果要将数据恢复到 FTP 服务器，则选择“恢复至 FTP 服务器”选项，并单击“FTP 选项”按钮，在弹出的“FTP 选项”对话框中键入 FTP 服务器的地址、端口及具有“上传”权限的用户名及密码，然后单击“确定”按钮。

在进行数据恢复时，还可以使用“过滤器”选项，以恢复指定类型的文件。选中“使用过滤器”复选框，然后单击“过滤器选项”按钮，在弹出的“过滤器选项”对话框中，选择要过滤的文件，在“指定文件名”文本框中指定要恢复文件的文件名或扩展名(支持 * 和? 通配符，* 代表所有，? 代表一个字符)。在下拉列表中选择要恢复的文件类型，单击“确定”按钮返回，然后再进行恢复时，将恢复指定的文件，如图 5-22 所示。

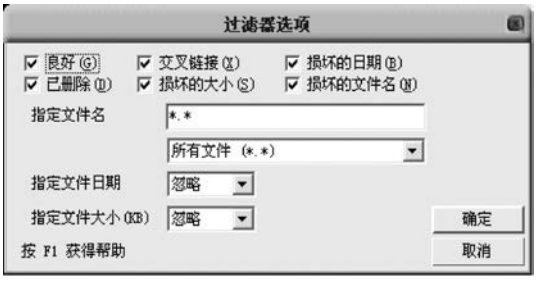

图 5-22 恢复指定文件