第 5 章

资源的访问控制

人是生而自由的，但却无往不在枷锁之中。

——让-雅克·卢梭(法国著名思想家)

大家留意一下有关安全事件的热点新闻，经常能看到类似“儿童误食处方药品”“家畜闯入高速公路”“行人走上机动车道”这样的内容。可见，对于生命和财产方面的安全防范，最主要策略就是要做好“访问控制”，通过立法、宣传和技术手段确保人们不要到达不该进入的场所，也不要接触到不该触碰的东西。

在信息安全领域，访问控制是保护信息系统资源的最重要的安全机制，是实现数据机密性、完整性、不可抵赖性以及可用性的关键和基础。人们也经常在一些场所看到过各式各样的相关提示，比如“内部文件，仅限单位职工阅读”“关键设备，未经批准不得使用”“机要重地，禁止无关人员靠近”等等(图 5.1)。

图 5.1　生活中关于访问控制的提示

从狭义上讲，访问控制是为了限制访问主体(或称为发起者，是一个主动的实体，如用户、进程、服务等)对访问客体(需要保护的资源)的访问权限，从而使计算机系统在合法范围内使用。访问控制机制决定用户及代表一定用户利益的程序能做什么以及做到什么程度。

访问控制由两个重要过程组成：一是通过认证来检验主体的合法身份；二是通过授权来限制用户对资源的访问级别。访问包括读取数据、更改数据、运行程序、发起连接等。

5.1　身份认证

俄国作家果戈理的《钦差大臣》是一部极具讽刺性和批判性的喜剧，讲述了一个纨绔子弟在与人打赌输得倾家荡产之后冒充钦差大臣的故事。在风闻“钦差大臣微服私巡”的消息后，腐败的地方官吏们慌乱不堪，想方设法贿赂这个所谓的“钦差大臣”。市长甚至打算把女儿嫁给他，以图攀上关系、步步高升……可见，认证一个人的身份是多么的重要。

和人类一样，计算机也是通过身份认证来保证资源的合法访问，进而消除安全隐患。比如，你去自助取款，ATM 需要先核实你的身份，才能授权你继续操作；你出入高档公寓，门禁会放行住户，把其他闲杂人等挡在外面；你去单位上班，打卡机也要验证是你本人还是其他人冒名顶替。由此可以看出，一个人，能够被计算机所辨识，需要基于以下三点：①你知道什么；②你具有什么；③你是谁。下面就分别介绍这三点。

5.1.1　用户所知道的

军队晚上都要派人站岗放哨，一旦发现远处有人靠近，就要通过口令分清敌我。在战争题材的影视剧中经常出现类似的场景——我方：“口令！”对方：“长江！”对方：“回令！”我方：“黄河！”这样就核实了双方都是自己人。如对方答不上或答错，那就很可能是敌人，枪栓一拉，子弹上膛：“站住！不许动！举起手来！”可见，口令就是秘密约定好的消息，知道这个消息的人就通过了身份认证。

在互联网和电子设备上遇到的“密码”或者 Password，从严格意义上讲都应该称为“口令”。利用的就是“用户所知道的信息”判断用户的身份。这个信息只有验证的人自己知道，并且其他人都无法猜得出来。也就是说，越是难猜，就越是理想的安全口令。

常见的不安全口令有如下几种：

(1) 使用用户名(账号)作为口令。很明显，这种方法在便于记忆上有着相当大的优势，可是在安全上几乎是不堪一击——几乎所有的黑客都会首先尝试将用户名作为口令试一试。比如，很多人登录计算机的用户名和口令就都是 admin。

(2) 使用用户名(账号)的变换形式作为口令。使用这种方法的用户自以为聪明，将用户名颠倒或者加上前后缀作为口令，既容易记住，又可以防止被别人直接猜到。不过，有一些专门的黑客软件，比如 John the Ripper，如果用户名是 fool，那么它在尝试使用 fool 作为口令之后，还会试着使用诸如 fool123、123fool、loof、loof123 等口令。只要你能想到的变换方法，它也会想到，几乎不需要多少时间。

(3) 使用自己或亲友的生日作为口令。这种口令有着很大的欺骗性，因为位数是 8，理论上有上亿的可能性。其实口令中表示月份的两位数字只有 01～12 可以使用，表示日期的两位数字也只有 01～31 可以使用，表示年份的 4 位数字只能是 19××或 20××。实际的 8 位口令只有 12×31×100×2＝74 400 种可能。即使考虑到年、月、日 3 部分有 6 种排列顺序，一共也只有 74 400×6＝446 400 种可能。软件每秒尝试上万个口令不在话下，所以试出正确口令不过是分分钟的事儿。

(4) 使用学号、员工号、身份证号等作为口令。对于完全不了解用户情况的人来说，

很难猜出这种口令;但是如果是熟人或者掌握了用户的一些信息的人,猜出口令就不那么难了。就拿身份证号来说,虽然有 18 位,但很有规律,取值范围极其有限:前 6 位是最早落户地的行政区划代码;接着 8 位就是出生日期;再后面 3 位一般男性是奇数,女性是偶数;最后一位是 0～9 或 X。

(5) 使用常用的英文单词作为口令。这种方法比前几种都要安全一些。但是黑客软件一般都会配备一个很大的词库,一般有 10～20 万个常用英文单词、词组和短语。而用户选择的单词很可能在这个词库里面。就算软件每秒只尝试千把个单词,几分钟也能把词库搜完。

网上评出了"十大最烂口令",如图 5.2 左图所示,大家可以看看自己是不是也犯过同样的错误。而图 5.2 右图则展示了 CSDN① 的用户设置的复杂口令。当然,他们在拼音或英文中混杂使用了一些程序设计语言的符号,其绝妙之处恐怕只有专业人士才能体会得到。

图 5.2　简单口令(左)和复杂口令(右)示例

那么,究竟怎样的口令才是安全的呢?一般认为,安全口令应该具有以下 4 个特征:

(1) 8 位长度或更长。如果只使用口令一种认证手段,建议在 12 位以上。

(2) 必须包括大小写字母和数字字符,如果有控制字符②更好。

(3) 不要太常见。不要使用常见的单词,更不要沿用系统指定的口令。

(4) 设置一定的使用期限。就像军队的口令一样,经常更换才能保障安全。

当然,口令设置得再好,也得小心维护才行。只有执行严格的管理措施,才能让安全更有保障。下面是一些常见的注意事项:

(1) 不要将口令告诉其他人,不要几个人共享一个口令,也不要把口令记在本子上或计算机周围。

(2) 最好不要用电子邮件等网络工具传送口令。如果一定需要这样做,要对电子邮件进行加密处理。

---

① CSDN(Chinese Software Developer Network)创立于 1999 年,是中国最大的专业 IT 社区和服务平台。2011 年 12 月,由于黑客攻击,CSDN 网站数据库中超过 600 万用户的登录名和口令遭到泄露。这也促使众多网站开始对用户信息进行加密存储。

② 控制字符(control character)是出现于特定的信息文本中,表示某一控制功能的字符,比如 LF(换行)、CR(回车)、FF(换页)、DEL(删除)、BS(退格)、BEL(振铃)等。

(3) 如果账户长期不用,应将其暂停。如果员工离开公司,应及时把他的账户消除。不要保留一些不用的账户,这是很危险的。

(4) 限制登录次数,这样可以防止有人不断地尝试使用不同的口令和登录名。

(5) 限制用户的登录时间。比如,只有在工作时间,用户才能登录到计算机上。

撞 库 攻 击

提及撞库,就不能不说拖库和洗库。在黑客术语里,拖库是指黑客入侵安全防御薄弱的网络站点,把注册用户的资料数据库(包含用户名、口令等信息)全部盗走的行为,因为谐音,也经常被称作"脱裤"。如果网站没有对用户资料进行加密,那么在取得大量的用户数据之后,黑客会通过一系列技术手段和黑色产业链将有价值的用户数据变现,这通常也被称作洗库。最后,黑客利用得到的数据(用户名和口令)在其他网站上尝试登录,称作撞库。因为很多用户喜欢使用统一的用户名和口令,所以"撞库"也可以使黑客收获颇丰。

2014 年 12 月 25 日,12306 网站用户信息在互联网上疯传。对此,12306 网站称,网上泄露的用户信息系经其他网站或渠道流出。据悉,此次泄露的用户数据不少于 131 653 条。该批数据基本确认为黑客通过撞库攻击获得。可见,用户在不同网站登录时使用相同的用户名和口令,就相当于给自己的所有保险箱配了一把"万能钥匙",一旦丢失,后果可想而知。所以说,防止撞库,是一场需要用户和网站共同参与的持久战。

5.1.2　用户所拥有的

根据"用户所知道的"认证用户的身份,存在诸多显而易见的问题。就拿口令来说,最大的悖论就是:安全的口令太复杂,不容易记住;容易记住的口令一般都很简单,极不安全。而且用户面对多个应用场景,需要很多口令。口令如果都不一样,很快就忘记了;口令如果都一样,一旦有一个口令被泄露了,获取口令的人很可能拿着这个口令去其他场合一一尝试(撞库攻击)。

相对而言,根据"用户所拥有的"认证用户的身份,就有着得天独厚的优势了。当你出入校园、政府机关或者公司的时候,门卫会拦住你,让你出示证件(学生证、身份证、通行证)。这个证件就是你所拥有的,可以证实你的身份的东西。只要你随身携带,在相应的场所就可以畅通无阻。而无须像记住口令一样,必须经常"温习",一着急,还是很容易记混了或者忘了。

早期的证件大都是类似证明信那样的盖有公章的纸质文件。图 5.3 左图就是一张中国古代读书人的证件——浮票。参加科举考试的时候,在报考材料的封面上会贴有一张浮票,写着考生姓名、座次、体貌特征。考生交卷的时候,监考官会认真对比考生体貌和浮票上描述的细节是否统一。当然,仅凭文字说明不足以确认身份,所以还需要其他保障措施,比如结保证明[①]。后来,随着科学技术的发展,有了照相技术,这样就可以通过照片结

① 一般来说,结保有两种形式:一种形式是考生互相担保,5 个同时参加考试的考生互相担保,也称为"五童结";另一种形式是由官学的廪膳生充当证明人,并在结保证明,即"结状"上签字,称之为"认保"或者"派保"。这样,考生在报考和考试中有任何舞弊行为,结保者以及认保或者派保的廪膳生都要受到牵连,轻则受到降等的处分,重则会有牢狱之灾。

合相应的文字描述一起认证身份了。如图 5.3 右图所示，民国时期的学生证已经和现在比较接近了。

图 5.3　早期的证件示例

纸质证件不容易保存，带在身上时间一长，难免字迹模糊，影响辨认。而且纸质证件只能依靠人工识别，不利于信息系统的自动处理。于是，就出现了带有磁卡的证件，比如大楼的通行卡片，只要在扫描器上划卡通过验证，就可以打开大门进入大楼。磁卡如图 5.4 左图所示。磁卡携带方便，可以长期保存，而且背面的磁条（黑色）中可以存储更多的信息。但是，磁卡最大的缺点是只有数据存储能力，没有数据处理能力，也就没有对记录的数据进行安全保护的机制。因此，对于专业人员来说，伪造和复制磁卡是比较容易的。

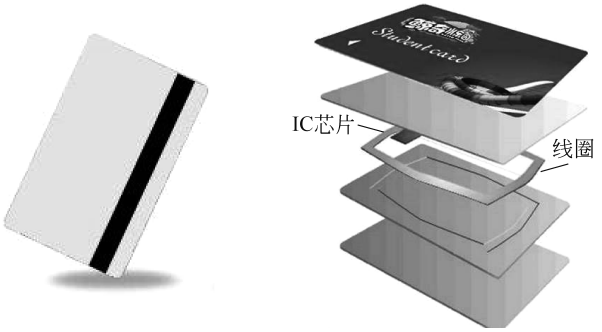

图 5.4　磁卡（左）与 IC 卡（右）

随着计算机技术的发展，尤其是微处理器的不断推陈出新，又出现了 IC 卡[①]。如图 5.4 右图所示，所有的 IC 卡中都包含一块微电子芯片，存储了持卡人的个人信息。当需要某种服务的时候，持卡人在读卡设备上进行认证。IC 卡可以说是最小的个人计算

① IC 卡（Integrated Circuit card，集成电路卡），也称智能卡（smart card）、智慧卡（intelligent card）、微电路卡（microcircuit card）或微芯片卡（microchip card）等。

机，在它的芯片上包含CPU、存储器和I/O接口，而且有操作系统的软件支持。与磁卡相比，IC卡不仅使用寿命长、存储容量大，而且安全保密性能高（具有数据处理能力），所以IC卡得到了越来越广泛的应用，比如第二代身份证、银行的电子钱包、手机SIM卡、公交卡、地铁卡以及用于收取停车费的停车卡等，都在人们日常生活中扮演了重要的角色。

无论是纸质证件还是磁卡、IC卡，都属于根据“用户所拥有的”认证用户的身份的方法。这种方式避免了像口令那样不方便记忆和管理的问题，但是其必需的物理材料导致成本也比较高，且整个流程相对复杂。其最大的缺陷就是，相关证件或卡片一旦丢失，用户就无法证实自己的身份，而捡到证件或卡片的人就可以假冒真正的用户。

双因素认证

任何身份认证方法，如果需要3种“东西”（你知道什么？你具有什么？你是谁？）中的两种，就被称为双因素认证。比如，你在ATM上取款。一方面需要插入银行卡，这是通过“你具有什么”证实你的用户身份；另一方面还需要输入口令，这是通过“你知道什么”进一步核实你的身份。如此一来，就通过双因素认证避免了因为银行卡丢失而造成损失。

USB Key，即网上银行的U盾，也是双因素认证的一个例子。USB Key是一种USB接口的硬件设备，它内置的智能卡芯片上存储了用户的密钥或数字证书，并通过加密算法实现了对用户身份的认证。每个USB Key都有一个硬件PIN（Personal Identification Number，个人识别号）码（可以理解为口令）保护，所以用户只有同时拥有PIN码和USB Key才能登录系统。即使用户的PIN码泄露，只要USB Key不被盗取，合法用户的身份就不会被仿冒；同样，如果用户的USB Key遗失，拾到者由于不知道用户的PIN码，也无法假冒真正的用户。

5.1.3　用户生物特征

在5.1.2节中提到，科举考试的浮票就是古代读书人的身份证（上面写着考生姓名、座次、体貌特征）。交卷时，监考官会认真对比考生体貌和浮票上描述的细节是否统一。这其实就是在通过“你是谁”，即生物特征认证考生的身份。当然，文字描述的生物特征是非常笼统的，只要体貌特征差别不大，就很容易蒙混过关[①]。直到有了照相技术，才让这种方式更加有效，这也算是学生证、工作证和身份证的演变历程。

随着信息技术的发展，使用计算机进行人脸特征提取和自动识别（图5.5）已经提上了日程。从技术角度看，它主要涉及两个核心工作：一是在输入的图像中定位人脸（人脸检测）；二是提取人脸特征（比如各个局部特征之间的几何关系）并进行匹配识别。在目前的人脸识别系统中，图像的背景通常是可以控制的（比如背景可以是比较容易区分的纯色），因此人脸的定位比较容易解决。但是，实际应用中的背景很可能比较复杂且不可控。另外，由于表情、位置、方向以及光照的变化都会让人脸的视觉效果产生很大的差异，这就让

① 在古代，也有通过画师画影图形的方法描摹人的形象，一般将其贴在出入关卡，用于通缉要犯。但是，一方面，画得像不像取决于画师的功底；另一方面，通过寥寥几笔很难完整地反映其外貌特征。

人脸的特征提取十分困难，虽然存在着巨大的挑战，但由于通过人脸识别进行身份认证是最为友好（可以做到让用户几乎没有觉察）和最为直接的方式，所以一直是模式识别研究和应用的热点，受到国内外相关人员的关注和追捧。

图 5.5　人脸特征提取和自动识别

应用最为广泛且最为成熟的还是指纹识别技术。在古代，人们很早就发现每个人的指纹纹路都是独一无二的，虽然手指随着身体的长大而长大，但指纹的几何形状是不会变化的。所以指纹就作为一种身份的凭证登上了历史舞台，比如在契约上按手印。计算机识别指纹就是通过其纹路的几何形状特征[①]进行匹配（比较 20 个微小特征就可以正确识别一个指纹），而每个手指上通常都有 50～200 个微小特征。

读取用户指纹的时候，需要手指和指纹采集头相互接触，以获取稳定可靠的图像。由于指纹采集头体积小、价格低廉，而指纹识别的速度快、比较方便，这就让这种身份认证方式迅速推广开来。如图 5.6 所示，掌纹识别是指纹识别的升级版，获取的特征比指纹更加丰富。但是它们有着共同的缺点：一方面是有些场景下不方便，比如医生护士经常需要洗手消毒，矿工、泥水匠这类技术工人的手上常年积攒污垢；另一方面是指纹采集的时候，在采集头上留下印痕也使得复制指纹成为可能。

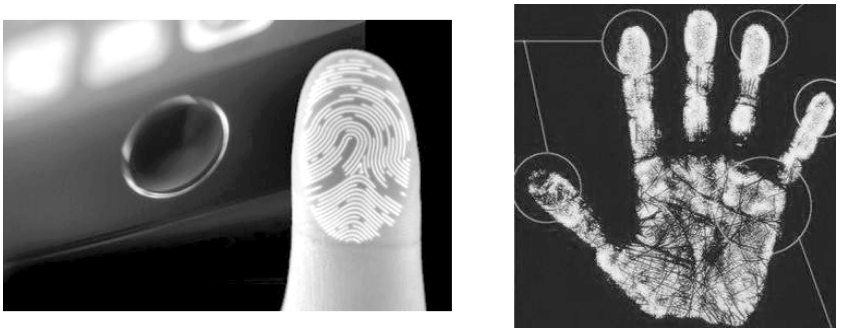

图 5.6　指纹识别（左）与掌纹识别（右）示例

相对于指纹识别在日常生活中的普及，虹膜[②]和视网膜扫描更多出现在影视作品中，被认为是针对身份认证应用的终极生物特征识别技术。如图 5.7 所示，人的眼睛由角膜、

① 目前许多国家的警察机构使用的系统是根据英国的刑侦专家爱德华·理查德·亨利于 1897 年提出的思想设计的。他将指纹划分为弓形、圈形和涡形三大类型，每一类型又分为许多子类型。

② 虹膜是位于黑色瞳孔和白色巩膜之间的圆环状部分，其包含很多相互交错的斑点、细丝、冠状、条纹、隐窝等细节特征。而且虹膜在胎儿发育阶段形成后，终生将保持不变。

虹膜、瞳孔、晶状体、视网膜等部分组成。其中，虹膜和视网膜的结构特征因人而异，即使是同卵双胞胎或者同一个人的左右眼，都不会相同。而且不可能在对视觉无严重影响的情况下用外科手术改变其特征，更不可能将一个人的特征改变得和某个特定对象一样。

虹膜可以直接看到，用通用摄像设备就可以获取图像。但是，很多情况下图像纹理不清晰，会造成识别困难（黑眼睛人群成像效果不好），而特殊的虹膜扫描装置有价格和操作等方面的高门槛。视网膜位于眼底，取像难度较大，很难降低其成本。虽然其检测结果更加稳定可靠，但可能会给被识别者带来视觉功能方面的损害。

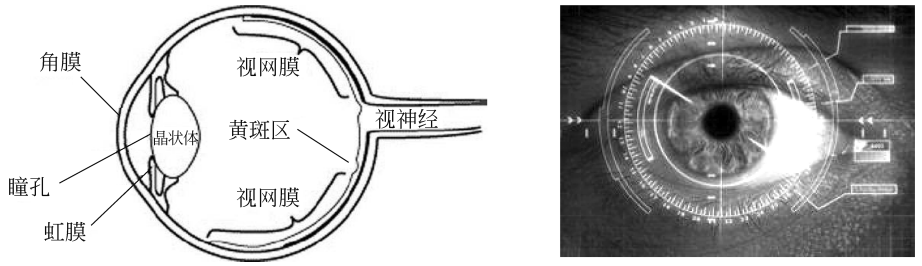

图 5.7　人的眼睛的结构（左）与虹膜识别技术（右）

总之，能够认证身份的理想的生物特征应该具备以下特点：

- 广泛性。每个人都应该具有这种特征。实际上，没有哪个生物特征能够应用于所有的人。例如，存在很小比例的人不具有可读取的指纹。
- 唯一性。每个人的具体特征各不相同，有相当大的实际可区分度。虽然在理论上有些生物特征的检测可以做到较高的区分度，错误率非常低，但是不可能期望100%的确定性。
- 稳定性。理想情况下，这些可测量的生物特征应该是永久不变的。在实践中，如果选择的生物特征能够在相当长的时间内保持稳定就足够了。
- 可采集性。选择的生物特征应该容易获取，并且不会给认证对象带来任何潜在的伤害。实际上，可采集性往往严重依赖于认证对象是否愿意合作。

行 为 特 征

用户的生物特征不仅包括上述生理特征（人脸、指纹、虹膜等），还包括一些行为特征。这两类生物特征的不同是：生理特征与生俱来，多为先天性的；而行为特征是习惯使然，多为后天性的，比如笔迹、声音、步态等。我们都有这样的生活经验：有时候，只闻其声不见其人，但是依然能够从嘈杂的人群中分辨出熟人；有时候，我们看到远方的一个身影，就能根据其走路姿势认出那个人。这两种身份认证的方式虽然错误率目前还比较高，但设备成本低廉（录音笔、摄像机），获取方便，而且基本不涉及隐私问题。

对于每个书写者而言，其笔迹总体上具有相对稳定性，而字里行间的局部变化则是每个人的固有特性。所以，对于不同的书写者而言，其笔迹的差别比较大。笔迹识别在社会生活中具有广泛的应用，比如，协议的签署，银行、金融部门

的签名对照，公安、司法部门的刑事调查和法庭取证，等等。计算机笔迹识别（包括签字识别）技术有联机和脱机两种。因为联机识别除位置信息外，还可以提取书写速度、时序、运笔压力、握笔倾斜度等动态信息，所以识别正确率比脱机识别高。当然，联机识别需要特殊的输入设备，比如手写板。

5.2 访问授权

一般来说，用以防范伪造的身份认证只有两个结果：符合和不符合。不符合的，认为是非法用户，拒绝其使用资源（比如软件、硬件、文件、网络等）；符合的，认为是合法用户，同意其使用资源。

然而，同样是通过认证的合法用户，在使用资源的时候也是区别对待的。就拿教务系统来说，教师、学生、教学秘书和系统管理员都是合法用户，权限却各不相同：教师可以录入考试成绩，学生只能查看不能改动；教学秘书可以安排课程和考试，教师只能浏览相关信息；系统管理员可以在后台修改页面布局或添加各种功能模块，教学秘书、教师和学生却不能进行此类操作。

可以这么认为：身份认证是信息安全系统中的第一道防线，是用户获取系统访问权限的第一步。在信息安全系统完成对用户的身份识别之后，便根据用户身份决定其对信息资源的访问权限。

如图 5.8 所示，访问控制包含 3 个基本要素：主体、客体和控制策略。

（1）主体是指主动的实体，是访问的发起者，它造成了信息的流动和系统状态的改变。主体通常可以是人、进程[①]和设备等。

（2）客体是指被访问的对象，包括所有受访问控制保护的资源。客体可以是文档、程序、系统、设备以及各种网络服务。

（3）控制策略也称访问策略，是指主体对客体进行访问的一套规则，用以确定一个主体是否拥有对客体进行访问的权限。

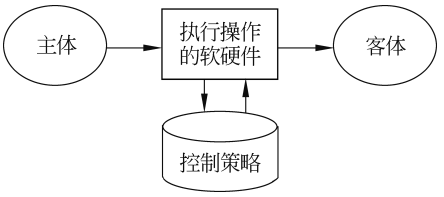

图 5.8 访问控制系统的基本框架

访问控制机制可以通过访问控制矩阵描述。如表 5.1 所示，访问控制矩阵的行对应于主体，列对应于客体；第 i 行第 j 列的元素是访问权限的集合，列出了允许第 i 个主体

① 顾名思义，进程（process）就是进展中的程序，或者说进程是执行中的程序。也就是说，一个程序加载到内存中以后就变为进程。即：进程＝程序＋执行。

对第 j 个客体可以进行的各种操作。从表 5.1 可以看出，主体 A 对客体 1 有“拥有[①]、读、写”3 种访问权限，主体 B 对客体 1 只有读的权限，主体 C 对客体 3 没有任何访问权限。

表 5.1　访问控制矩阵示例

主　体	客　体		
	客体 1	客体 2	客体 3
主体 A	拥有、读、写		拥有、读、写
主体 B	读	拥有、读、写	写
主体 C	读、写	读	

1. 基于身份的访问控制策略

前面讲到过，访问控制由两个重要过程组成：一是通过认证来检验主体的合法身份；二是通过授权来限制用户对资源的访问级别。所以人们很容易想到的授权方式就是基于身份的访问控制策略，也就是列出每一个合法用户（比如 Alice、Bob 和 Eve 等）对每一个资源的访问权限。

基于身份的访问控制策略也称自主访问控制策略，允许合法用户以用户或用户组的身份访问规定的客体，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拥有的客体的访问权限授予其他用户。

如表 5.2 所示，基于身份的访问控制策略有明显的优点：配置的粒度小，灵活易行。换句话说，就是分配权限落实到每个用户和每个资源上面，就像产品的个性化定制一样，可以让所有用户对资源的访问权限各不相同。

不过，其缺点就是配置的工作量大、效率低。因为每增加一个新用户或者增加一个新资源，都要把这个新用户对所有资源的权限重新分配一遍，或者把所有用户对这个新资源的权限重新分配一遍。如果管理的用户或资源非常多，每次改动带来的工作量非常巨大。尤其是需要同时增加多个用户或资源的时候，工作效率会变得特别低。

表 5.2　使用访问控制矩阵描述的基于身份的访问控制策略

主　体	客　体			
	1. doc	2.com	3. exe	…
Alice	拥有、读、写		执行	…
Bob	读	读、写		…
Eve	写		拥有	…
⋮	⋮	⋮	⋮	⋮

基于身份的访问控制策略是针对每个一个用户或每个一个资源进行权限配置，代价

① “拥有”权限表示管理操作，将它从读、写权限中分离出来，是因为管理员也许会对控制规则本身或文件的属性等进行修改。