些是欺诈性的，但大多数人并不是。我们在这方面理解错了。考虑到黑客真正的含义，我们应该恢复他们的名声，并把那些企图非法闯入计算机系统的人归结到骇客（Cracker）一类。通常“黑客”被分为并不从事违法活动的“白帽子黑客”和从事破坏活动的“黑帽子黑客”。在人们的经验中，绝大多数“黑客”长时间呆在室内，而且并不戴帽子，所以事实上很难通过他们的帽子来区分“黑客”的好坏。

9.4.1　使用口令认证

最广泛使用的认证方式是要求用户输入登录名和口令。口令保护很容易理解，也很容易实施。最简单的实现方法是保存一张包含登录名和口令的列表。登录时，通过查找登录名，得到相应的口令并与输入的口令进行比较。如果匹配，则允许登录，如果不匹配，登录被拒绝。

毫无疑问，在输入口令时，计算机不能显示被输入的字符以防在终端周围的好事之徒看到。在Windows系统中，将每一个输入的口令字符显示成星号。在UNIX系统中，口令被输入时没有任何显示。这两种认证方法是不同的。Windows 也许会让健忘的人在输入口令时看看输进了几个字符，但也把口令长度泄露给了“偷听者”。（因为某种原因，英语有一个词汇专门表示偷听的意思，而不是表示偷窥，这里不是嘀咕的意思，这个词在这里不适用。）从安全角度来说，沉默是金。

另一个设计不当的方面出现了严重的安全问题，如9-17所示。在图9-17a中显示了一个成功的登录信息，用户输入的是小写字母，系统输出的是大写字母。在图9-17b中，显示了骇客试图登录到系统A中的失败信息。在图9-17c中，显示了骇客试图登录到系统B中的失败信息。

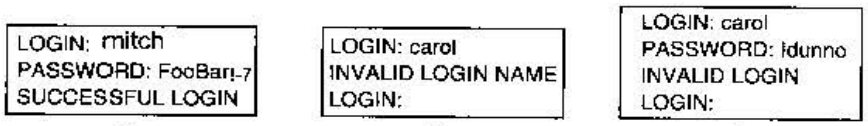

图9-17　a) 一个成功的登录；b) 输入登录名后被拒绝；c) 输入登录名和口令后被拒绝

在图9-17b中，系统只要看到非法的登录名就禁止登录。这样做是一个错误，因为系统让骇客有机会尝试，直到找到合法的登录名。在图9-17c中，无论骇客输入的是合法还是非法的登录名，系统都要求输入口令并没有给出任何反馈。骇客所得到的信息只是登录名和口令的组合是错误的。

大多数笔记本电脑在用户登录的时候要求一个用户名和密码来保护数据，以防止笔记本电脑失窃。然而这种保护在有些时候却收效甚微，任何拿到笔记本的人都可以在计算机启动后迅速敲击DEL、F8或相关按键，并在受保护的操作系统启动前进入BIOS配置程序，在这里计算机的启动顺序可以被改变，使得通过USB端口启动的检测先于对从硬盘启动的检测。计算机持有者此时插入安装有完整操作系统的USB设备，计算机便会从USB中的操作系统启动，而不是本机硬盘上的操作系统启动。计算机一旦启动起来，其原有的硬盘则被挂起（在UNIX操作系统中）或被映射为D盘驱动器（在Windows中）。因此，绝大多数BIOS都允许用户设置密码以控制对BIOS配置程序的修改，在密码的保护下，只有计算机的真正拥有者才可以修改计算机启动顺序。如果读者拥有一台笔记本电脑，那么请先放下本书，先为BIOS设置一个密码。

1. 骇客如何闯入

大多数骇客通过远程连接到目标计算机（比如通过Internet）、尝试多次登录（登录名和口令）的方法找到进入系统的渠道。许多人使用自己的名字或名字的某种形式作为登录名。如对Ellen Ann Smith来说，ellen、smith、ellen_smith、ellen-smith、ellen.smith、esmith、easmith等都可能成为备选登录名。黑客凭借一本叫做《4096 Names for Your New Baby》4096个为婴儿准备的名字的书外加一本含有大量名字的电话本，就可以对打算攻击的国家计算机系统编辑出一长串潜在的登录名（如ellen_smith可能是在美国或英国工作的人，但在日本却行不通）。

当然，仅仅猜出登录名是不够的。骇客还需要猜出登录名的口令。这有多难呢？简单得超过你的想象。最经典的例子是Morris和Thompson（1979）在UNIX系统上所做的安全口令尝试。他们编辑了一长串可能的口令：名和姓氏、路名、城市名、字典里中等长度的单词（也包括倒过来拼写的）、许可证号码和许多随机组成的字符串。然后他们把这一名单同系统中的口令文件进行比较，看看有多少被猜中的