口令。结果有86%的口令出现在他们的名单里。Klein（1990）也得到过同样类似的结果。

也许有人认为优秀的用户会挑选特别的口令，实际上许多人并没有这么做。一份1997年伦敦金融部门关于口令的调查报告显示，82%的口令可以被轻易猜出。通常被用户采用的口令包括：性别词汇、辱骂语、人名（家庭成员或体育明星）、度假地和办公室常见的物体（Kabay，1997）。这样，骇客不费吹灰之力就可以编辑出一系列潜在的登录名和口令。

网络的普及使得这一情况更加恶化。很多用户并不只拥有一个密码，然而由于记住多个冗长的密码是一件困难的事情，因此大多数用户都趋向于选择简单且强度很弱的密码，并且在多个网站中重复使用他们（Florencio和Herley，2007；Gaw和Felten，2006）。

如果口令很容易被猜出，真的会有什么影响吗？当然有。1998年，《圣何塞信使新闻》报告说，一位在Berkeley的居民Peter Shipley，组装了好几台未被使用的计算机作为军用拨号器（war dialer），拨打了某一个分局内的10 000个电话号码[如（415）770-xxxx]。这些号码是被随机拨出的，以防电话公司禁用措施和跟踪检测。在拨打了大约260万个电话后，他定位了旧金山湾区的20 000台计算机，其中约200台没有任何安全防范。他估计一个别有用心的骇客可以破译其他75%的计算机系统（Denning，1999）。这就回到了侏罗纪时代，计算机实际只需拨打所有260万个电话号码。⊖

并不只有加利福尼亚州才有这样的骇客，一个澳大利亚骇客曾经做过同样的尝试。在这个骇客闯入的系统中有在沙特阿拉伯的花旗银行的计算机，使他能够获得信用卡号码、信用额度（如500万美元）和交易记录。他的一个同伴也曾闯入过银行计算机系统，盗取了4000个信用卡号（Denning，1999）。如果滥用这样的信息，银行毫无疑问会极力否认自己有错，而声称一定是客户泄露了信息。

互联网是上帝赐给骇客的最好的礼物，它帮助骇客扫清了入侵计算机过程中的绝大多数麻烦，不需要拨打更多的电话号码，军用拨号器可以按下面的方式工作。每一台联入互联网的计算机都有一个（32位的）IP地址（IP Address）。人们通常把这些地址写成十进制点符号，如w.x.y.z，每一个字母代表从0到255的十进制IP地址。骇客可以非常容易地测试拥有这类IP地址的计算机，并通过向shell或控制台中输入命令

```
ping w.x.y.z
```

来判断该计算机是否在网上。如果计算机在网上，它将发出回复信息并告知走一个来回需要多少毫秒（虽然某些网站屏蔽了ping命令以防攻击）。黑客很容易写一个程序来自动发射大量的IP地址，当然也可以让军用拨号器来做。如果某台计算机被发现在网上的IP地址为w.x.y.z，骇客就可以通过输入

```
telnet w.x.y.z
```

尝试进入系统。

如果联机尝试被允许（也可能被拒绝，因为不是所有的系统管理员欢迎通过Internet来登录），骇客就能够开始从他的名单中尝试登录名和口令。起初可能会失败，但随着几次尝试后，骇客最后总是能进入系统并获取口令文件（通常位于UNIX系统的/etc/passwd下，而且对公众是可读的）。然后，他开始收集关于登录名使用频率等统计信息来优化进一步的搜索。

许多telnet（远程登录）后台程序在骇客尝试了许多不成功的登录后会暂停潜在的TCP连接，以降低骇客的连接速度。骇客这时会同时启动若干个并行线程，一次攻击不同的目标。他们的目标是在一秒中内进行尽可能多的尝试，利用尽可能多的带宽。从他们的观点来说，同时攻击好几台计算机并不是一个严重的缺陷。

除了依次ping计算机的IP地址外，骇客还可以攻击公司、大学或其他政府性组织等目标，如地址为foobar.edu的Foobar大学。骇客通过输入

```
dnsquery foobar.edu
```

⊖ 在获得奥斯卡奖的科幻电影《侏罗纪公园I》中，一位名叫Dennis Nedry的计算机系统总设计师暗地里将由计算机控制的保安系统全部关闭并逃离了主控室，以便窃取并带走恐龙的DNA。另一位计算机技术人员面对混乱的系统，对现场的其他人说，由于没有保存任何信息，所以要想恢复保安系统，只有一个一个地测试，才能在总共200万个号码中将需要的号码找出来，一听是200万个号码，在场的人都泄了气。作者在这里调侃了电影《侏罗纪公园I》的创作者们，既然现场计算机系统还能工作，为什么不让计算机去拨打这些号码呢！？——译者注