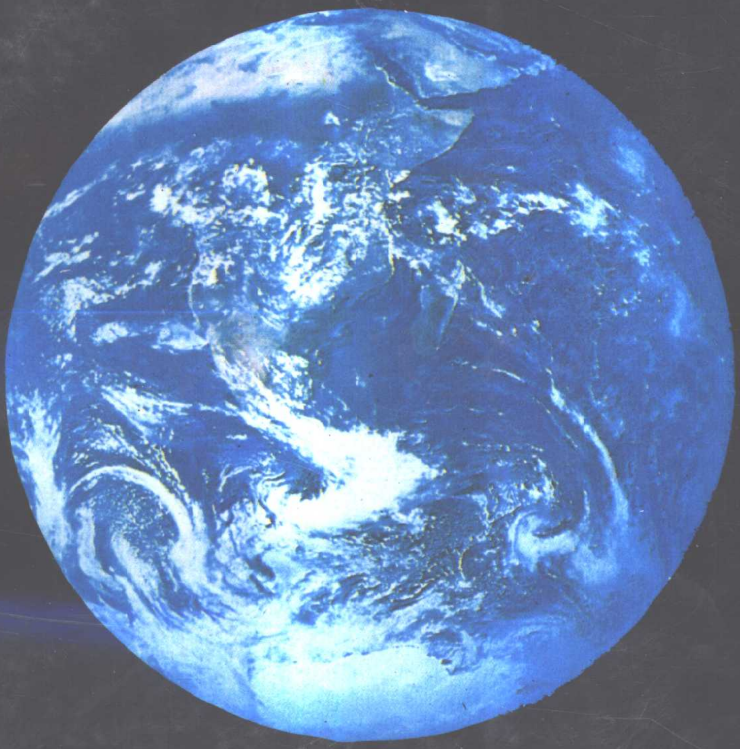

杜鹃蛋
——电脑间谍案曝光录

〔美〕克利福德·斯托尔

新 华 出 版 社

杜鹃蛋

——电脑间谍案曝光录

〔美〕克利福德·斯托尔

文学朴 等译　赵锡中 校

新华出版社

京新登字 110 号

The Cuckoo's Egg
by Clifford Stoll

Published by Doubleday
据纽约道布尔迪公司 1989 年版译

杜 鹃 蛋

——电脑间谍案曝光录

〔美〕克利福德·斯托尔著
文学朴 等译
赵锡中 校

*

新华出版社出版发行
新 华 书 店 经 销
北京新华印刷厂印刷

*

850×1168 毫米 32 开本 13.25 印张 插页 2 张 306,000 字
1992 年 2 月第 1 版 1992 年 2 月北京第一次印刷
ISBN 7—5011—1657—1/G·596 定价：8.00 元

译者前言

80年代以来，计算机技术飞速发展，大大推动了世界科学技术的进步，促进了工业生产的发展，给人类社会带来了巨大的福利。计算机不但可用于各种高速复杂的计算工作，而且几乎影响到社会生活的一切方面，使天文、物理、生物工程、化学、材料学、航天、医药卫生、通信等重要科技领域的发展相继取得突破性的进展。计算机已变得家喻户晓，整个国家以至整个世界的计算机网络已连成一片。但是与此同时，计算机的广泛适用性和高速运算效率，也为一切不法分子、间谍特务提供了有利的犯罪工具，利用计算机盗窃银行存款、窜改帐目、销毁档案和窃取军事秘密等事件屡见不鲜，应当引起社会各界尤其是使用计算机较多的部门的注意。本书第一次公开介绍美国破获的一起重大的利用计算机盗窃国防机密的国际间谍案。1989年出版后，此书成为西方世界轰动一时的畅销书。难能可贵的是，作者本人克利福德·斯托尔正是首先发现和破获这个国际间谍网的主角，因此本书内容翔实丰富，曲折动人，既可供从事计算机工作的人员参考，又可飨广大读者的兴趣口味。

斯托尔原为美国劳伦斯—伯克利实验所的一位天文学工作者，1976年调到该所计算机部门任系统管理人。他发现计算机会计帐目中一再出现75美分的误差，经过反复查对，发现有人冒充一些长期不用的用户名称，潜入他的计算机系统。于是，他不顾情报部门和官僚机构的冷漠

态度和压制，锲而不舍，穷追到底，终于在一年之后挖出了里斯一伙德国汉诺威间谍集团，为保卫国家机密建立了功勋。他的名字一再登在《纽约时报》头版上，成为美国家喻户晓的英雄。

作者虽是科研人员，但文笔流畅，摆脱了这类记实文学常见的平铺直叙的呆板性。他另辟蹊径，采用小说体裁，加入不少生活琐事和背景的描写，使作品显得生动有趣，引人入胜。

本书中“黑客”一词为 Hacker 的音译。《美国俚语大全》对这个词的解释为：“泛指使用计算机或计算机程序者，尤指好而不倦者，有时指计算机迷，……有多种解释，难以确定。”看来这是一个中性字眼，译为“黑客”似乎贬意色彩强了一些，但为了简洁起见，考虑到本书的具体内容，在找不到更合适的译法的情况下，未始不是一个权宜之计，只是不足为训。

限于译者水平，谬误之处在所难免，希望读者指正。本书译者为（按姓氏笔划为序）：文学朴、王澍秋、任美芬、沈德彝、苏潼均、钟元贞、霍爱华。赵锡中同志校订全书。

译　者

1992 年 1 月

1

我是一个奇才吗？一周以前，我还是一个天文工作者，正在心满意足地设计光学望远镜。回顾当时的情景，我是生活在充满学术气氛的幻想世界里。这些年来，我从来没有为将来筹划过，一直到我的补助金用完的那一天为止。

我真幸运，我的实验所重新录用了在那里工作过的天文工作者。我不是站在失业者的队伍里，而是从劳伦斯一伯克利实验所的凯克天文台，调到同一幢楼底层的计算机中心。

我可以冒充行家，用计算机做很多运算，给天文学家们留下深刻印象，也许可以很快读出数据，令我的同事们无法理解。尽管如此，我是一个计算机奇才吗？我不是，我是一个天文学工作者。

那时怎样呢？在我冷漠地盯着我的计算机终端的时候；我还在想着行星轨道和天体物理学。作为新来的人，我选择了窗户对着金门桥的一间小屋。这间办公室没有通风设备，有一面墙是书架。我忍受着幽闭和恐怖感，希望我在办公桌边睡觉时不会引起人注意。我的办公室左右两边是两个计算机系统人员的办公室。韦恩·格雷夫斯和戴夫·克利夫兰都是这个系统的老手。他们经常为一点小事争吵，这使我很快就熟悉了我的邻居。

韦恩认为所有的人不是不能胜任工作，就是懒惰成性，但是他却和这里工作的其他人来往频繁。他对这个系统了解得一清二楚，从磁盘驱动系统软件一直到微波天线。人们劝韦恩不要迷恋

数字设备公司的“瓦克斯”计算机，而他却非要它不可，既不要国际商用机器公司的，又不要尤尼克斯公司的，也不肯要麦金托什公司的。

戴夫·克利夫兰，在我们使用“尤尼克斯”系统的人员中是一位和善的菩萨，总是耐心地听着韦恩滔滔不绝地评论各种计算机的优劣异同。很少会议没有韦恩的推销宣传：“瓦克斯计算机是一切地方的科学家的选择，它可帮助你用12种方法编制有效的程序。”戴夫反驳说：“看，你的话只使迷恋瓦克斯计算机的人高兴，而世界上其他的人却要听我的。”戴夫从来没有让他满意地发一通脾气，这样，韦恩的怨气最后渐渐消散，只是咕哝一阵罢了。

妙极了。工作的第一天，我夹在两个人中间，他们不时的争论已经在破坏我的幻想了。

韦恩、戴夫和我要一起管理这些计算机，它们是全实验所的一种公用事业设备。我们管理12台计算机中央处理机——这是解决物理学问题的巨大运算工具，大约共值600万美元。我们期望使用这些计算机的科学家们看到的是一个简单而功能很强的计算系统，就象供电公司一样可靠。这意味着得让这些计算机昼夜不停地运转。而且正象供电公司一样，我们对使用的每个计算周期都要收费。

在4,000名实验所雇员中，也许有四分之一使用计算机主机。这1,000笔帐，每笔都天天登记，分类帐保存在计算机内。用计算机计算一小时收费300美元，因此，我们的帐目，必须分毫不爽，所以我们总是跟踪打印的每一页、磁盘上的每块空隙和处理机的每分钟处理时间。另有一台计算机用于收集这些统计数字，把每月的帐单送到实验所各个部门。

这样，碰巧在我开始工作的第二天，戴夫闲逛时来到我的办公

室，含含糊糊地提到尤尼克斯计算机会计系统出现一个差错。一定有人用了几秒钟的计算时间而没有付钱。计算机帐上收支不很平衡。上月的帐单是 2387 美元，差了 75 美分。

要是出现几千美元的误差，那是显而易见的，不难发现。但是美分栏里的误差出于一些埋藏很深的问题，所以找到这些错误自然是对初露头角的软件奇才的一次考验。戴夫说我应当考虑这个问题。

“一级盗窃案，嘿？”我回答说。

戴夫说：“把它弄清楚，克利夫，你会让每个人惊愕的。”

好吧，这看起来倒象一场有趣的游戏，于是我钻研起记帐程序来了。我发现我们的会计软件是由早就离开的夏季大学生编写的程序拼凑起来的东西。不知怎么地，这些大杂烩竟然工作得很不错，用不着管它。我在研究这些混合的程序时，发现这个软件是用 Assembler Fortran 和 Cobol 语言编写的，这些是最老的计算机语言，也许还是古典的希腊语、拉丁语和梵语。

就象大多数自制软件一样，谁也没有费心去查证我们的会计系统。只有蠢人才会在没有地图的情况下闯进这样的迷宫中去摸索。

尽管如此，现在有一个机会来探索这个系统。戴夫让我看了看每次有人与计算机联机时，这个系统是怎样记录的：记录下该用户的名字及其终端设备。每次联机时，该系统便盖下时间印记，记录用户执行什么任务、用户用了多少秒时间以及他何时与计算机断开。

戴夫解释说，我们有两套独立的会计系统。普通的尤尼克斯会计软件只把有计时印记的记录存入文件存储器里。但是为了满足某些官僚的要求，戴夫建立了第二套会计制表系统，它保留下关

于谁使用计算机的更详细的记录。

在这些年里，接连几批带着厌烦情绪的暑期学生编写了一些分析所有这些会计信息的程序。一个程序专门收集数据，把它存入文件档案。第二个程序能读出这个文件，并且计算这次运算收费多少。第三个程序可收集所有这些收费记录，打印出帐单，供邮寄到各个部门。最后一个程序把所有用户收费加起来，把这总数和计算机的内部会计程序所得出的结果相比较。这两种由不同程序并行保存的会计文件，应当得出同样的答案。

一年来，这些程序工作正常，没有出过什么差错，可是这一周的工作情况却不十分理想。可能造成这种情况的一个明显原因是舍入误差。每项会计输入很可能都是正确的，但加在一起时，十分之几美分的差额就会逐渐增加，一直积累到 75 美分的误差。通过分析这些程序如何运算，或用不同的数据检验它们，我应该能证明我的这个看法。

我不是设法了解每个程序的代码，而是写了一个短程序来核实这些数据文件。在几分钟内我就核对了第一个程序：的确，它正确地收集了会计数据。第一个程序没有问题。

检验第二个程序时，我用的时间比较长。在一个小时内，我拼凑了足够多的临时编码以证明这个程序实际上是有效的。它只是把时间间隔加起来，然后乘以我们对计算机时间的收费额。结果是，这个程序没有出现 75 美分的误差。

第三个程序工作情况非常好。这个程序查对了特许用户的名单，找到他们的研究所帐户，然后打印出一份帐单。是四舍五入造成的误差吗？不是，所有的程序都记录下金额，直至百分之几美分。奇怪，这 75 美分的误差是在哪儿发生的呢？

我为设法了解一个细小的问题花了几个小时。我犯了倔强脾

气了：该死的东西，如果有必要，我要在那里呆到夜里 12 点。

后来搞了几个试验性程序，我开始真正相信这个当地编制的会计程序的大杂烩了。毫无疑问，收支并不平衡，这些程序虽然不是万无一失的，但是不会把几十分钱遗漏掉。那时，我已找到特许用户的清单，并且弄清了这些程序是如何使用数据结构给不同的部门开帐单的。大约下午七时，一个叫亨特的用户引起我的注意。这个家伙没有一个确实的开帐地址。

哈！在过去一个月里，亨特用了 75 分钱的计算机时间，但是没有人为他付款。

这就是我们的帐上收支不平衡的根源。不知什么人把一个用户加到我们的系统里，把事情弄糟了。一个细小的误差造成了一个小小的问题。

这是该庆贺的时候。于是我打开我的笔记本，把这第一个小小的胜利写在头几页里，正当这时，我的爱人马莎顺路来看我。我们深夜来到伯克利的罗马咖啡馆，喝着克皮奇诺咖啡，共同庆贺这个胜利。

要是真正的计算机奇才，用不了几分钟就会把这个问题解决。可是对我来说，这是一个未知的领域，我能摸索着找到问题的答案真不容易。值得自慰的是，我学会了使用会计制表系统，并且练习了几种过时的计算机语言。第二天，我给戴夫发了一个电子邮件，向他指出了这个问题，借以为自己夸耀一番。

中午前后，戴夫顺道来访，放下一摞手册，并且漫不经心地提到，他从来没有增加过一个名叫亨特的用户——这一定是其他系统的一个管理人员干的。韦恩粗率地搭话说："这不是我，RTFM 。"他讲的话大多数都是以字的头一个字母的缩略词结束的。这个缩略词的意思是"看看这一摞乱糟糟的手册吧"。

但是我早就读过这些手册。按理操作人员要是加一个新用户是不会不记帐的。在其他计算机中心，你只消同一个特许帐目系统接通，让这个系统增加一个用户就成了。由于我们除此之外还必须作几种簿记登记，我们不能使用这种系统。我们的系统是很复杂的，所以我们有几个特殊的程序，能自动做文件工作和操纵管理系统。

我向周围查阅了一下，发现大家都认为这个自动化系统非常优越，谁也不能用人工加一个新用户。这个自动化系统不会犯这种错误。

嗯，我想不出这个大错是谁犯的。谁也不知道亨特其人，也没有给他立帐户。所以我从这个系统抹去了这个名字。如果他抱怨，我们可以正经八百地给他立个帐户。

一天之后，一台叫“船坞长”的不明不白的计算机给我们发来一个电子信件。这台计算机的系统管理人声称，我们实验所有人在周末曾企图闯入他的计算机。

“船坞长”的回电地址可能在任何地方，但是从种种迹象来看，是在马里兰州。这个电子邮件经过了另外 12 台计算机。每台计算机都留下了一个邮戳。

戴夫答复这封信件时，不置可否，只说：“我们要调查一下。”啊，这是当然的，在我们的所有其他问题都消除以后，我们会调查的。

我们实验所的计算机与 12 个网络上的其他数千个系统有联系。我们的任何科学家都可以与我们的计算机联机，然后和远方的某个计算机连接。一旦连接上，他们输入帐户名字和口令，就能与远方的计算机联机。在原则上，保护网络上计算机的唯一东西是口令，因为帐户名字是容易推断出来的。

“船坞长”发来的电子信件是很奇特的，戴夫把它递给韦恩，附带提了一个问题：“谁是‘船坞长’？”韦恩把它转交给我，他猜测“这很可能是某家银行”。

最后，韦恩又把这封电子信件交给我。我猜想，“船坞长”是某个海军船坞。这件事并不重要，但是看来值得花几分钟去调查一下。

这封信提供了我们的尤尼克斯计算机系统上的某个人试图与“船坞长”的计算机联机的日期和时间。我刚刚检查过会计制表系统，翻阅过这些文件，查找从星期六早晨 8 时 46 分以后的记录。同样，发现了这两个会计制表系统不一致。普通的尤尼克斯会计文件表明，在 8 时 25 分有一个叫斯文特克的用户请求联机，历时半小时，他什么也没做，然后就断机了。在这段时间没有盖上计时印记的活动。我们自制的软件也记录了斯文特克的活动，但它表明，他从 8 时 31 分直至上午 9 时 1 分一直在使用这个网络。

咦，又出现一个会计问题。计时印记不一致。从一个系统看有活动而另一个会计系统则说一切都处于休止状态。

另外一些事情似乎更为紧迫，所以我搁下了这个问题。在浪费了下午的时间去追查某个操作人员的错误以后，我不打算再去碰这个会计制表系统。

在和戴夫一起用午餐时，我提到在“船坞长”报告这次闯入事件以后，斯文特克是唯一的联过机的人，戴夫惊讶地瞪着眼说：“是乔·斯文特克吗？他在剑桥，英格兰的剑桥。他回来干什么？”原来，乔·斯文特克曾在本实验所担任尤尼克斯系统的领导人，很受人尊敬。他是一位软件奇才，在过去 10 年里他编制了 12 种重要的程序。乔在一年前已赴英格兰，在整个加利福尼亚计算机行业留下了显赫的声誉。

戴夫不能相信乔回到了本市，因为乔的其他朋友没有一个接到他的信。戴夫说："他一定是从什么网络进入我们的计算机的。"

我问戴夫："那么，你认为，乔应对这个问题负责罗？"

戴夫回答说："完全不是这样。乔是个老派的黑客(hacker)。是一个聪明、机敏而有才干的程序编制人员。不是那些玷污了'黑客'这个名词的小流氓。不管怎样，斯文特克不会想要闯入马里兰州的一台计算机的。如果他真想这样做，他是会成功的，而不留下任何痕迹。"

真奇怪：乔·斯文特克已经在英格兰呆了一年，然而却在星期六清晨出现了，企图闯入马里兰州的一台计算机，后来又断机，结果使会计制表系统出现不平衡。在门厅里，我向韦恩提起此事，他听说，乔现在正在英格兰度假。他躲到边远的林区去休养，离任何计算机都很远。"忘记'船坞长'那个电报吧。斯文特克将访问伯克利实验所，RSN，那时他将澄清这件事。"

RSN 吗？确实没有多久了。这是韦恩的"我不能肯定什么时候"的说法。

我所担心的不是斯文特克，而是帐目不平衡。这两个会计制表系统为什么记录不同的时间呢？为什么某一个活动在一个文件里有记录，而在另一个文件里却没有呢？

回过头再看看那一天下午的会计制表系统记录。我发现，这两个时间印记之间相差 5 分钟，是近几个月我们的各计算机时钟发生偏移所致。其中一个计算机的时钟每天要慢几秒钟。

但是斯文特克的活动应当在两个系统的帐目中都有记录。这是否和上周的会计问题有关呢？在我上周查找原因的时候，我是不是把事情搞糟了呢？或者是否有什么别的解释？

2

那天下午，我去开会，听完了一次关于星系结构的令人厌烦的枯燥讲演。这位博学的教授不仅讲话单调，而且在黑板上写满了一列列长长的教学方程式。

我竭力打起精神，怕睡着了，脑子里翻来复去地考虑我遇到的问题。有什么人在增加新帐户时把事情弄糟了。一周以后，斯文特克要求联机，企图闯入马里兰的某台计算机。关于这件事的会计记录似乎被窜改了。斯文特克这个用户找不到。另外，不知什么地方又有差错。这几乎象是有什么人在躲避我们的记帐程序似的。

我想知道，需要怎么做才能不花钱白白使用我们的计算机？是不是有人可能找到了一个绕过我们的会计制表系统的办法？

大计算机有两类软件：用户程序和系统软件。自己编写或设立的程序是用户程序，例如，我的天文学程序，是用来分析一个行星的大气的。

光是用户程序没有多大用处。它们不能与计算机直接谈话，而是要求操作系统操纵计算机。在我的天文学程序要记录什么的时候，它不是直接在我的荧光屏上打出一个词，而是把这个词传给操作系统，操作系统再告诉硬件写出一个词。

操作系统与编辑程序、软件库和语言解释程序一起组成系统软件。这些程序不需要你去编写，它们是和计算机配装在一起的。

这些程序一旦建立，谁也不得窜改。

记帐程序是系统软件。要修改它或绕过它，你必须是系统管理人，或设法在操作系统内获得特权地位。

好，你怎样才能获得特权地位呢？明显的办法是用系统管理人的口令和我们的计算机联机。我们好几个月没有改变过我们的口令了，但是谁也不会泄漏它。一个局外人绝对猜不出我们的秘密口令“Wyvern”——在猜测我们的口令时，有多少人会想到神话中的飞龙呢？

但是即使你成了系统管理人，你也愚弄不了记帐软件。这个名词，知道的人太少了，文件上的记载也太少了。不管怎样，我已看到这个记帐软件是可行的。

等一等——我们的自制软件也工作正常。有人增加了一个新帐户，但没有使用。也许他们不知道此事。如果有什么人从外界闯进来，他们是不会知道我们的局部革新措施的。我们的系统管理人和操作人员都知道这一点。乔·斯文特克即使在英格兰，也肯定知道。

但是，从外界来的什么人——一个精明的程序编制人“黑客”——会怎么样呢？

“黑客”一词有两个截然不同的意思。我所认识的一些自称“黑客”的人是软件奇才，他们设法创造性地设计了他们摆脱困境的办法。他们知道操作系统的一切细微的缺点。他们不是那种一周工作 40 小时的呆笨软件工程师，而是具有创造性的程序编制人员，他们不满足计算机的要求是不离开机器的。一个“黑客”简直和计算机化为一体，他了解计算机就象了解一个朋友似的。

一些天文学工作者就是这样看待我的。“克利夫，与其说他是个天文学家，倒不如说是个擅长计算机的‘黑客’”（搞计算机这一

行的人当然有不同的看法:“克利夫不是什么程序编制人,倒是了不起的天文学家!”我在研究生院学到的东西使我把双方都骗了。)

但是,常见的用法是,“黑客”是指那些闯入别人的计算机的人。① 1982 年,在一批学生使用终端设备、调制解调器和长途电话线,闯入洛斯阿拉莫斯实验所和哥伦比亚医疗中心的计算机以后,计算机界的人们突然开始明白我们联成网络的系统是脆弱的。

每隔几个月我就听到一次关于别人的计算机系统被闯入的传闻;通常这类事都发生在大学里,人们往往认为这是学生或青少年干的。一些聪明的高中学生有时会闯入有最高安全措施的计算机中心。通常这是无害的,所以也不予追究,只当作是一个“黑客”的恶作剧。

电影《战争演习》真的可能发生吗?有哪个少年“黑客”可能侵入五角大楼的一台计算机,挑起一场战争?

我不相信会有那种事,的确,在大学里,在计算机上瞎弄一通是容易的,那里没有必要采取安全措施。毕竟,大学里连大楼都很少锁门。在我的想象里,军用计算机的情况是完全不同的——它们会象军事基地一样有严密的安全保卫。即使你真的闯进一个军用计算机,要是以为你就能发动一场战争了,那也是荒谬的。我想这些事情完全不会由计算机控制。

我们劳伦斯-伯克利实验所的计算机并不特别安全可靠,但是我们必须不让外人接近计算机,并且努力防止人们不正当地使用它们。我们并不担心有人损害我们的计算机,而只是希望我们

①用什么词描写那些闯入计算机的人呢?老派的软件奇才以被称为“黑客”而自豪,最近一些公然蔑视法律的人盗用了“黑客”这个名词。

的资助机构能源部不要干扰我们。如果他们要我们把计算机漆成绿色的，那我们就得定购油漆刷子。

但是为了使访问科学家们满意，我们为这些客人设立了几个计算机帐户。任何人有了“客人”帐户名字和“客人”的口令，都能使用该系统解决他们的问题，只要他们使用的时间不超过几美元的计算时间。一个“黑客”很容易闯入这个帐户——它是完全开放的。使用时间只限一分钟，这算不上是闯入。但是从这个帐户，你可以观察这个系统的各个方面，阅读任何公开的文件，并且看到谁在联机。我们认为这为人们提供了方便，完全值得冒这个小小的安全风险。

我仔细考虑这种情形，总不相信会有一个“黑客”在我的系统内闲荡。没有人对粒子物理学感兴趣。如果有什么人愿意阅读我们的科学家的论文，那他们大多数人是会高兴的。这里没有什么特别的东西能引诱一个“黑客”——没有时髦的超级计算机，没有色情行业的秘密，没有保密的数据。的确，劳伦斯-伯克利实验所最好的工作条件就是公开的学术气氛。

在50英里以外，劳伦斯-利弗莫尔实验所做着保密工作。研究制造核弹和星球大战计划。现在，那个实验所可能是某个“黑客”要闯入的目标。但是利弗莫尔的计算机和外界没有联系，外界无法和它们接通。保护这些计算机的保密数据的办法是与外界隔绝。

如果有什么人的确闯入了我们的系统，他们能得到什么呢？他们可以阅读任何公开的文件。我们的大多数科学家是这样存储他们的数据的，以便他们的合作者能够阅读。一些系统软件也是公开的。

虽然我们称这种数据是公开的，但是外人也不应闯进来任意