网络与信息安全技术丛书

Firewalls and Internet Security

repelling the wily hacker

防火墙与因特网安全

(美) William R. Cheswick
Steven M. Bellovin 著

戴宗坤 罗万伯 等译

吴世忠 审校

机械工业出版社
China Machine Press

Addison-Wesley

网络与信息安全技术丛书

防火墙与因特网安全

(美) William R.Cheswick
Steven M.Bellovin 著

戴宗坤 罗万伯 等译

吴世忠 审校

机械工业出版社
China Machine Press

本书从介绍安全问题入手，讨论了TCP/IP协议簇的重要部分；随后，详尽描述了防火墙的结构，分析了几种常用防火墙网关，详细阐述了各种鉴别策略的选择及多种网关工具的使用；并在此基础上，通过对黑客行为和各种攻击进行分类、分析，论述了如何在具体实践中对付黑客的入侵，如何维护系统的安全；最后，讨论了计算机安全所涉及的法律问题以及如何在高风险环境中应用密码学知识来保护信息。

本书作者是AT&T公司计算机安全方面的高级专家，本书凝聚了他们多年来的研究与实践经验，是系统与网络设计、管理人员的一本必不可少的参考书。

本书版权登记号：图字：01-1999-3212

图书在版编目(CIP)数据

防火墙与因特网安全/（美）切斯维克(Cheswick, W. R.）贝罗维(Bellovin, S. M.)著；戴宗坤等译. - 北京：机械工业出版社，2000.4

(网络与信息安全技术丛书)

书名原文：Firewalls and Internet Security: repelling the wily hacker

ISBN 7-111-07856-X

Ⅰ.防… Ⅱ.①切… ②贝… ③戴… Ⅲ.①防火墙-基本知识②因特网-安全技术 Ⅳ.TP393.08

中国版本图书馆CIP数据核字(2000)第03372号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）

责任编辑：陈 谊

北京昌平第二印刷厂印刷 · 新华书店北京发行所发行

2000年4月第1版第1次印刷

787mm × 1092mm 1/16 · 14印张

印数：0 001-6 000册

定价：25.00元

译 者 序

本书是美国计算机安全专家William R. Cheswick 和Steven M. Bellovin 所著《Firewalls and Internet Security: repelling the wily hacker》(1994年出版)的中文译本。根据作者在因特网上公布的若干修订和补充意见，我们在中文译本中一一做了修改和补充。

William R. Cheswick 和Steven M. Bellovin系AT&T公司长期从事局域网、广域网和因特网安全技术及系统配置研究的高级专家。他们根据自己对OSI及TCP/IP网络体系结构，以及UNIX操作系统中与网络通信有关的模块及其裁剪、配置原则的理解，对防火墙与因特网安全的关系进行了系统、深入的研究和工程实践，并以此为基础完成了《Firewalls and Internet Security: repelling the wily hacker》一书。

1995年下半年，经中国工程院院士何德全先生的指点和推荐，我们有幸接触该书，获益匪浅。这几年中，该书对我们在有关信息安全理论研究和工程实践方面的工作，起到了重要参考作用。尽管该书出版于1994年，但其结构体系、思维逻辑、技术实用及文字可读性，在今天看来，仍有相当可取之处。因此，尽管目前已有大量同类中文技术书籍，但我们仍认为有必要将其译为中文，推荐给对网络及信息安全有兴趣的读者朋友们。

该书内容翔实，技术细节描述生动、具体而深入，书中所列例子基本上基于UNIX操作系统，尽管其中有些技术可能有些过时，但总的来看，这些例子所表明的概念及思想方法、技术路线，无论是经作者反复推敲过的，或是引用他人的，仍具有很大的参考价值。该书另一特点是，在网络安全的宏观体系结构与微观技术细节的描述上结合紧密，丝丝入扣。尤其是作者将网络安全作为手段以实现信息安全目的这种思维方式凝聚了作者多年来的研究与实践经验。此外，在研究防火墙与因特网安全的关系和工程实现方法时，强调了安全技术、安全服务与安全管理的相互依赖、共存亡的思想，很值得借鉴。其中在谈及与网络安全有关的法律法规、规章制度、社会工程以及道德规范时，思维清晰，入情入理，既有说服力，又提出了大量需要研究的问题。最后，也是需要特别提醒读者朋友的，作者在描述某些概念和技术细节时，往往并不直接给出结论，而是采用借喻、类比和引用等方式以幽默的语言间接予以表达。

我们在翻译过程中，尽可能准确地表达原文概念和重要的论述。对于原文难以理解的地方，我们做了必要的意译，力求表达得清楚易懂。

本书的出版，得益于机械工业出版社华章公司的远见卓识，得益于中国国家信息安全测评认证中心吴世忠主任的极力推荐，得益于四川能士信息工程技术公司提供的良好工作条件，在此深表衷心的感谢!

四川大学信息安全研究所戴宗坤、罗万伯、罗建中、唐三平、陈麟和国际关系学院图书馆的马芳同志直接参加了本书的翻译工作。其中戴宗坤翻译了第1、3、4、5、6章，罗万伯翻译了前言、第7章和第8章，罗建中翻译了第6、10、12章，陈麟初译了第9和第11章，唐三平翻译了第13和14章及附录、参考文献。马芳翻译了第2章，戴宗坤、罗万伯对全书进行了综合

统稿。吴世忠研究员审校了全书并提出许多中肯的修改意见。

由于时间仓促，错误在所难免，诚望读者赐教。

译　者

1999年12月

于四川大学信息安全研究所

前　言

运行一个安全的计算机系统并不难。你只需断开全部拨号连接设备，只与终端相连，并将计算机及其终端都置于坚如铁壁且戒备森严的屋子里就万事大吉了。

——F.T. Grampp and R.H.Morris

当今绝大多数计算机系统，无论其情况如何，都不会以上述极端的方式运行。一般来说，安全性与方便性是折衷平衡的，大多数人并不会放弃通过网络进行远程访问的方便性，显然，这样做会损失一些安全性。我们的目的就是要讨论如何将安全损失降到最低程度。

当计算机系统挂接到某些类型的网络上后，情况会更糟。至少有下述三个主要原因导致了网络的安全风险。第一个原因，也是最明显的原因，就是网点越多，黑客从这些地方发起攻击的可能性就越大。无法接近计算机系统的人，自然不能对其发起攻击；而为合法用户提供的连接机制越多，系统就越脆弱。

第二个原因是网络扩大了计算机系统的物理边界。在一台计算机内，所有东西都在一个机箱里。CPU可以从存储器中提取鉴别数据，不必担心被人窜改或暗中监视。传统机制——状态位、存储器保护以及类似技术——能够保护重要区域。但在网络中这些就不适用了。收到的消息可能来历不明，而发出的消息则会暴露给网络的其他系统。很显然，在网络中需要更加小心。

第三个原因则更加微妙，并与普通拨号调制解调器和网络之间的基本区别有关。通常，调制解调器提供某种服务，如登录，在你的计算机连接到网络上时，就会得到一个login或Username的提示符；再如通过这个控制界面发送邮件。在登录服务过程中也许有脆弱性，但这毕竟是一个单一服务，而且是比较简单的服务。另一方面，联网的计算机提供了很多的服务：登录、文件传输、磁盘存取、远程操作、电话号簿、系统状况等等。因此，更多的站点需要保护——站点越复杂，则保护越难。例如，一个联网的文件系统，不能够依靠键入的口令去处理每项事务。进一步地，许多服务的开发利用是以假定网络范围受到一定限制为前提的。在一个跨越全球的联网时代，这一假设已不成立，有时还会产生严重后果。

联网的计算机还有另一个特别值得注意的问题：它们通常并不是一个单一的统一体。即，把一台计算机连接到网络以便单独与一台“陌生”的计算机进行对话，并不是经常发生的事。更为普遍的是，一些组织拥有许多计算机，而它们互相连接并通向外部世界。这里既有祸又有福：祸——因为联网的计算机常常需要信任对方并获得某些扩展；福——网络可以配置成只有一台计算机需要与外部世界进行对话。这种专用计算机，通常称为“防火墙网关”，处于我们所建议的安全方案的核心位置。

我们的目的有两个。第一，我们希望说明，安全方案是有效的。即，只要对预期威胁的防范部署适当，防火墙就能大大增强一个组织的安全性。第二，我们希望说明，网关是必要的，并且确实存在真正的威胁，需要认真对付。

致读者

本书主要是写给网络管理员的，他们必须保护自己的组织，以免不加防范地暴露到因特网上。读者最好应具备系统管理和网络方面的背景知识。某些章节需要涉及较深的技术知识。大多数章节具有趣味性。只对部分内容感兴趣的读者，完全可以跳过那些枯燥无味的资料去欣赏本书的其他部分。

我们也希望系统和网络设计人员读这本书。书中讨论的许多问题都是缺乏安全意识的设计直接导致的结果。我们希望更新的协议和系统将是更安全的。

我们的例子和讨论都是相对于UNIX系统和程序而言的。因为，因特网上的多用户机器大多数都是运行在UNIX操作系统的某个版本上。大多数的应用级网关也是在UNIX上实施的。这并不是说其他操作系统更安全，而是因为在因特网上其他操作系统很少。不过，这些准则和原理也适用于建立在其他操作系统上的网关，甚至包括MS-DOS这样的操作系统。

我们将重点放在TCP/IP协议簇上，它在因特网上使用得最多。同样的道理，这并不表明TCP/IP比其他协议栈更安全（我们也怀疑是否如此），而是因为TCP/IP的应用已经相当成功。最重要的是，它是多种网络的协议，不仅仅包括工作站，还包括从台式个人机到最大型超级计算机范围内的所有机器。因特网连接了美国和世界其他各国的大多数主要的大学、研究实验室、政府代理机构及众多的商业公司。我们的机构——AT&T贝尔实验室、也连在因特网上，我们在本书中提供的许多忠告都是与联网有关的经验之谈。相信我们的经验同样适用于具有类似特性的任何网络上。我们阅读过对X.25公共数据网络上的计算机进行严重攻击的资料。防火墙也可用于该网络，当然，在一些细节上会有所不同。

本书不是一本关于如何用安全方式管理计算机系统的书，尽管我们也提出过这方面的建议。有关这一题目的书很多，如[Farrow, 1991]、[Garfinkel and Spafford, 1991]和[Curry, 1992]。本书也不是一本告诉你如何管理各种组装防火墙网关的“食谱”。由于涉及的技术太新，任何一本这样的著作甚至在它出版前就可能过时。我们希望本书是一套指南，它定义有关安全问题，并粗略地勾勒出可能的解决办法。我们也描述了怎样构造最新网关的技术，以及为什么这样做的原因。我们的设计决策直接归功于我们关于探测和防御网络攻击者的经验。

我们偶尔也提到已经发生的某些情况的“报告”。对这一含糊的说法，我们表示歉意。虽然我们已尽力标明文献出处，但仍不尽人意，因为有些信息来源于与其他安全管理员的秘密讨论，他们不愿透露姓名。网络安全的裂口可能使人十分难堪，特别是当它们发生在那些本应对此有清楚认识的组织内部的时候，就更是如此。

术语

在进一步叙述之前，值得对某些术语做一些解释。我们将攻击者叫做黑客(hacker)。在某种程度上说，这种称谓是大众媒体对数以千计的有创造力程序员名声的一种侮辱。事实确实如此。Bruce Sterling在[Sterling,1992,55～56页]中对此做了绝妙的描述：

> 术语hacking被沿用至今，几乎所有法律机构都把它用于那些专业的计算机欺骗和滥用行为。美国警方把几乎任何涉及到“利用”、“借助”、“通过”或“阻挠”计算机的犯罪行为都描述为hacking。
>
> 更为重要的是，hacker这个词是计算机“入侵者”（intruder）用来称呼他们自己的。

在千方百计侵袭他人系统的人中，却没有（或极少有）人把他们自己称作“计算机侵入者”（computer intruder）、“计算机侵害者”（computer trespasser）、“破坏者”（cracker）、“蠕虫”（wormer）、“蒙面大盗“（dark-side hacker）或“高技术街匪”（high-tech street gangster）。虽然已经发明了几个其他贬义词，希望能在出版物和公众中保留词意的原始含义。但很少有人真正使用这些词。

本书的结构

本书从介绍安全问题（第1章）入手，随后详细讨论了TCP/IP协议簇的重要部分（第2章），并对安全问题给予了特别关注。

本书第二部分详细描述了防火墙的结构。分析了已经建立过的几种防火墙网关（第3章），接下来详细阐述了我们的第三个和最新的一个网关的结构情况(第4章)，各种鉴别策略的选择(第5章)及我们用过的其他工具（第6章），已实现的几种监视器（第7章）。我们也描述了已实现的、用来测试安全性的黑客工具（第8章）：在有人决心尽力将你的系统防御撕开前，你不知道是否安全。这一部分非常详尽，如果需要，你完全可以直接移植我们的工作，或稍做修改后使用。

安全不仅仅是像现在时和将来时那样简单的事情。在第9章，我们尝试对黑客行为进行分类，对不同攻击种类进行分析。第10章是相当具体：描述了企图入侵我们的系统的所谓Berferd事件以及此过程中发生的趣事。第11章给出了我们及其他人多年来收集的日志数据。

第12章讨论了计算机安全所涉及的法律问题。这类问题并不都是直接而明了的。第13章说明了在高风险环境里如何应用密码学。第14章给出了若干建议。

关于本书的勘误

虽然我们已经尽了最大努力，仍然难免存在个别错误。可以在FTP. RESEARCH. ATT. COM站点的/dist/internet_security/firewall.book目录下找到勘误表及其他信息(我们已经下载了本书的勘误表，并在翻译过程中做了更正。—译者注)。当然，我们十分欢迎你帮助我们找出错误，并将电子邮件发送到firewall-book@research.att.com。

William R. Cheswick
ches@research.att.com
Steven M. Bellovin
smb@research.att.com

原书书号：ISBN 0-201-63357-4

第一部分 入 门

第1章 安全问题概述

1.1 为什么要研究安全问题

什么是“计算机安全”？广义地讲，安全是指防止其他人利用、借助你的计算机或外围设备，做你不希望他们做的任何事情。当然，这一定义过于泛泛了。然而，这一定义却引出了我们不得不面临的一些极为重要的问题，这些问题是任何希望设置一种有效的安全机制的人必须回答的。

首要问题是：“我们力图保护的是些什么资源？”答案并不总是明确的。是CPU周期吗？在一定时期内，这个问题很有意义，因为那时计算机时间非常昂贵。但如今这已不再是问题了，当然超级计算机是一个例外。与CPU周期相比，更为严重的是，CPU——或者更确切地说，运行按一定配置文件定制的特定软件的CPU——的名字或标识，这使它可以访问其他更重要的资源。这些通常比CPU时间更敏感。一个打算破坏或模仿一台主机的黑客通常将对该主机全部资源进行访问：文件、存储设备、电话线等。通过实际的分析发现，某些黑客最感兴趣的是滥用主机标识，而不是过分触及主机的专门资源，他们利用这些标识，暗渡陈仓，向外连接其他可能更感兴趣的目标。有些人可能实质上对你机器中的数据感兴趣，不管它们是否是公司的敏感材料或政府机密。

通常，对这个问题的答案是采取必要的主机专用措施。存有敏感文件的计算机可要求额外的口令级别，或者甚至(在少数场合)对文件加密。同样，如果感兴趣的目标机器可以向外连接，管理人员可以选择，需要一定特权才能访问该网络。可能的话，所有这些访问都应该通过一个后台守护程序(daemon)来进行，它将执行额外的日志记录。

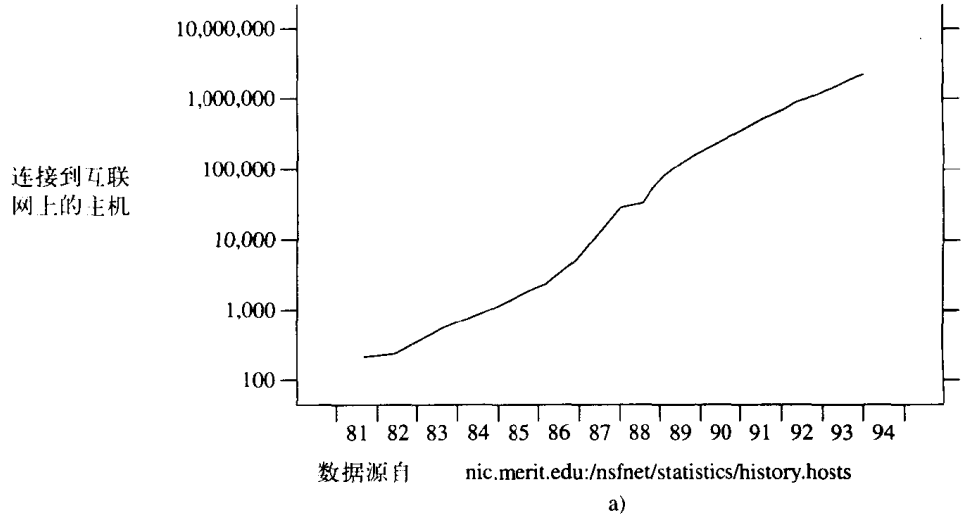
当然，人们通常想保护所有资源，在这种情况下，最明显的答案是把攻击者拒之于门外，即首先不让他们进入计算机系统。这样一种方法是一个有用的开端，虽然，它假设系统安全问题来自外部。

这导出了第二个主要问题：“计算机系统必须防范谁？”足以对付一个使用调制解调器的年轻人的技术，在重要的情报部门面前却无能为力。对于前者，增强口令安全性即可解决问题，然而后者却能够、并且可能借助于搭线窃听和密码分析，监视你的计算机和电缆的电子发射，甚至瞄准你在计算机房的“暗箱操作”。计算机安全并不是目的，它是达到信息安全这一目的的手段。如果必要和合适的话，还应该采用其他手段。计算机安全防范的强度与其所受的威胁成比例，其他防范措施虽已超出了本书的讨论范围，但同样必不可少。

图1-1用两种方法显示了因特网增长的情况。图a显示的是因特网自动扫描探测到的主机总数。近几年的统计比实际数量低，因为没有可靠的技术来统计连接到互联网上的所有计算机。图b表明了过去几年里在NSFnet中注册的网络数目。请注意：两个图的垂直坐标都是对数

坐标。这些增长是指数型的。假如有两百万主机登录，那么有多少人访问这些计算机呢？又有多少人试图在这些机器上一试黑客身手，甚至以黑客为职业呢？

在配置安全机制之前必须回答的第三个问题，是硬币的另一面："你能在安全方面付出多大代价？"安全问题的部分代价是直接的财政开支，诸如建立防火墙网关需要额外的路由器和计算机。通常，容易忽视设置和运行网关的管理费用。而且还有一些更微妙的开支——方便性、生产性甚至道德问题引起的开支。过分的安全性可能像过低的安全性一样有害。找出适当的安全性平衡点是一件棘手的、却完全必要的事——并且，只有当你从两个极端对你的组织机构的安全风险进行了恰当评估后才可能做到这一点。



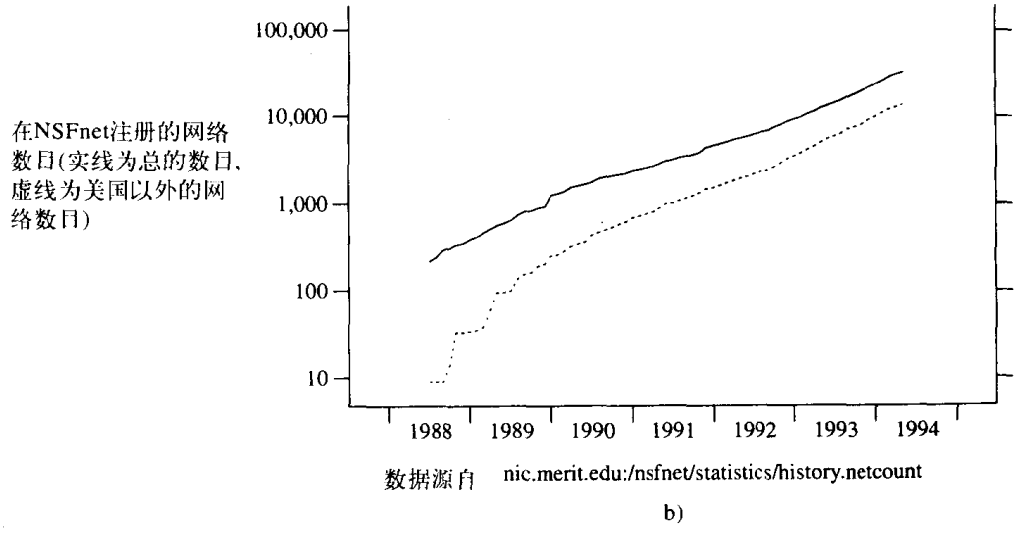


图1-1　因特网的增长

还有一点值得一提。即使你不相信你的财产有多大价值，仍值得将黑客拒之于你的机器之外。你可以对安全问题持宽容态度，但攻击者对此可能并不明白。黑客在他们认为已经被人探测到时，便将这些系统的记录像丢垃圾一样废弃，这种情况实在是太多了。(有人甚至企

图对我们的系统下手，参见第10章。）

1.2 选择安全策略

即使是偏执狂也有对手。

——无名氏

安全策略(security policy)是决策的集合，它们集中体现了一个组织对安全的态度。更准确地说，安全策略对于可接受的行为以及应对违规做出何种响应确定了界限。从本质上讲，安全策略对不同的组织来说是有区别的。大学里一个系的安全需求不同于一个公司的产品开发部的需求，同样，后者又不同于一个军事部门。但是，每个组织，如果要求它在不可接受事件发生时就采取行动的话，都应有一整套安全策略。

本书不过多地涉及对事件如何响应的问题，这些在其他书籍中已有十分充分的说明，例如[Holbrook and Reynolds, 1991]。但是对防火墙来说，其基础便是定义可接受行为的界限。

第一步是决定“允许什么”和“不允许什么”。在一定程度上，这一处理受业务或组织的结构需要所驱动；因此，还可能发布一道命令，禁止个人使用公司计算机。一些公司希望限制流出的通信，以防止雇员将公司有价值的数据泄漏出去。其他方面可受到技术考虑的影响：某一特定协议尽管很有用处，由于不能安全地管理它，也不能采用。还有一些涉及到诸如雇员未经适当授权而进口软件之类的问题：公司并不希望由于侵害其他人的权利而被起诉。很清楚，做出这样一些决定是一个反复的过程，因而某一个人的答案绝不可能像雕刻在石头上，或刻蚀在半导体器件中一样一成不变。

设计态度

本故事的意义在于，任何东西在你没有认识它之前都是危险的。

Beowulf Schaefer in Flatlander

——Larry Niven

安全策略中的关键是设计防火墙的态度。这个态度也就是设计人员的态度。它根据防火墙失效的代价以及设计人员对失效可能性的估计来确定。同时也基于设计人员对其自身能力的估计。在天平的一端放着一个哲理，说：“我们将使用它，除非你能向我表明它是坏的。”在另一端的人说：“请你说明它的安全性与必要性，否则我们不会用它。”那些完全远离天平的人宁愿从网络上拔出插头，断开连接，也不愿冒一点风险。这样的举动当然过于极端，但可以理解。为什么一个公司会因网络连接获利而甘冒丢失机密的风险呢？从美国军方禁止把存有机密数据的机器连接到不安全网络这件事上，人们可意识到，美国军方对计算机安全技术是多么缺乏信心。

一般说来，我们倾向于天平另一端的多疑的观点(就我们公司所处的环境而言，我们应该强调此点)。我们试图对防火墙进行一种失效保护(fail-safe)设计：即使我们忽略了一个安全漏洞或者安装了一个受到损害的程序，但我们相信防火墙本身仍是安全的。让我们将这一方法与一个简单的数据包过滤方法进行比较。如果过滤表被删除或者安装不正确，或者当路由器软件中有若干缺陷，网关可能被渗透。如果你的态度是允许稍微宽松地对待网关安全，那么这种非失效保护(nonfail-safe)的设计，就是便利和可以接受的解决方案。

我们不主张断开与大多数站点的连接。道理很简单：没有绝对的安全。要想解决问题不花钱，只能是空想。网络有很多优点，脱离网络则是自动放弃这些优点。也许脱离连接是一种正确的选择，但这是需要权衡风险与利益的关系后才能做出的决定。

我们提倡谨慎，并非出于神经质。基于以下所解释的理由，我们认为防火墙是一个重要工具，它能将风险降到最小，同时还提供大部分——并非全部——网络连接利益。但对很多站点来说，设置防火墙的时候，需要对安全持“偏执”的态度，对此我们可以证明。

公理1　摩菲定理　所有的程序都有缺陷。

定理1　大程序定律　大程序的缺陷甚至比它包含的内容还多。

证明　通过调查统计。

推理1-1　一个安全相关程序有安全性缺陷。

定理2　只要不运行这个程序，那么这个程序是否有缺陷，也无关紧要。

证明　在所有逻辑系统中，均有(假→真)= 真。

推理2-1　只要不运行这个程序，即使这个程序有安全性漏洞，也无关紧要。

定理3　对外暴露的计算机，应尽可能少地运行程序，且运行的程序也应尽可能小。

证明　直接从推理1-1和推理2-1导出。

推量3-1　防火墙基本法则　大多数主机不满足我们的要求：因为它们运行太多太大的程序。因此，唯一的解决办法是将真正希望运行的程序隔离在防火墙的另一边。

上述数学论述，虽然并不十分严谨，但仍可以导出有益的结论。防火墙必须配置得尽可能小，才能降低风险。如果不存在风险，还要防火墙干什么？在此，我们并不打算把这个说法标为公理，但是某些妄想狂患者具有真正的敌人，这是绝对真实的。

我们还可以引出另外一些结论。首先，我们感到任何程序，不管它看起来多么地完美，但仍可能隐藏着安全漏洞。(谁能料到，在某些机器中，一个整数除法错误[⊖]，竟然会导致系统被穿透？)因此我们坚信，任何东西在被证明是无罪之前，均是有罪的。于是，我们把防火墙配置成对任何东西都加以拒绝，除非我们明确地做出决定允许它，并接受这一风险。相反的做法是，只阻断那些已知的对我们具有极端危险性的犯罪者。

进而言之，安全策略无论是否正式成文，但却客观存在。如果没有说或做其他事情，那么缺省的安全策略就是“任何东西都可通行”。无疑，在一个必须注重安全的环境中，这种策略是不可能接受的。如果不做出明确的决定，那么实际上是做出了缺省决定，即允许几乎所有东西。

这并不是判定什么服务可以或不可以接受。如前所述，这些决定必须视具体环境而定。但我们给出的规则是通用的。

1.3　安全网络对策

1.3.1　主机安全

在某些人看来，真正的防火墙概念就像一道咒符。在多数情况中，网络并不是处于风险

⊖　见CERT Advisory CA-92: 15, July 21, 1992. 附录A中给出了怎样获得CERT Advisory的有关信息。

中的资源；相反，是网络终端面临威胁。通过分析得知，诈骗专家几乎极少偷窃电话服务本身，而是利用电话系统作为工具去接近他们的受骗者。所以网络安全显然有意义。假定攻击者的目标是网络上的主机，那么为何不对其进行适当配置和装备，以抗御攻击呢？

答案是应该如此，实际却可能并非如此。定理3表明，这种打算可能是徒劳的。无论在网络程序中，还是在系统管理方面，都会有缺陷。计算机安全是这样一种方式：攻击者只需赢一次。无论你的防火墙有多厚，也无论你的阵地有多巍峨，只要攻击者找到一个薄弱点——比如说，延伸至隐密处的暗道(或后门)——系统便被穿透了。不幸的是，这并不是你的灾难的尽头。

根据定义，联网的机器是不被隔离的机器。一般情况下，其他机器以某种方式信任这些机器，可能是完全盲目地信任rlogin，或者是由Kerberos鉴别系统使用的复杂的密码校验[Bryant, 1998; Kohl and Neuman, 1993; Miller *et al.*, 1987; Steiner *et al.*, 1988]，在这种情况下，特定用户将成为被信任者。如果入侵者能够破坏这个系统，那么他或她可以通过接管root权限并得到系统标识或某些用户帐户来攻击其他系统。

这样看来，我们似乎对计算机安全状况是过分悲观了。不过这只有一半正确：我们并不乐观，但也不过于悲观。纵观近年来网络安全或软件工程的历史，没有理由让我们相信还有其他说法。也不是只有我们才有这种感觉。

例如，看看著名的橘皮书[DoD, 1985a]。它列出的每一种安全等级的特性——审计，访问控制，可信路径以及其他类似的东西——得到了大家重视，但是更高等级的安全需要更多、更为苛刻的保证条件。这就是说，必须有更多的理由让人信服，系统实际上实现了设计的功能。除这些要求外，即使是具有A1等级评估的最可信的系统，只要有一个糊涂用户访问过这一系统，那么这个系统中最为敏感的信息也是不可信的了[DoD, 1985b]。在因特网上，很少有系统能满足C2要求，因此它们的安全性是不够的。

我们面临的另一个挑战与生成安全系统的困难完全无关：对系统的管理问题。无论编写的代码如何好，设计如何清楚，后来出现的人为差错能够使整个保护失效。考虑下列事件的后果：

(1) 在假日或周末，当没有系统管理员值班时，出现网关机器故障。

(2) 备份专家不能通过电话诊断故障，而需要产生一个客户帐号。

(3) 操作人员增加客户帐号，却没有指定口令。

(4) 专家忘了增加口令。

(5) 操作人员忘记删除该帐号。

(6) 某些大学生发现了该帐号并在一天之内告诉了他们的朋友们。

可能否？当然可能，此事确实在我们的一个网关中出现过。当不速之客在探测我们其他的网关机器时，触发了一个报警器，我们才发现被穿透了。

相对说来，管理我们的防火墙机器比较简单。它们运行最小配置，免除了人们对某些事情的担心。成品的网关机器有大量调节旋钮、按钮和开关需要操作，并且许多装配是不安全的。更糟的是，很多是按销售商指定的方式运输的。机器安全性越高，通常使用和管理就越不方便，但一些制造商却把他们的产品选择定位于“易于使用”的市场。我们的内部网络有许多机器是受到专业性管理的。不过有许多部门的机器，一旦开箱、插入和通电，就万事大吉，被人忽略了。它们工作在旧的操作系统版本上，当且仅当其中的缺陷直接影响到很多用

户时，它们才被修改过来。既然系统在工作，为什么还要改变它？相当时间里，这成为一种合理的态度，但这种模式交错地传递网络信任，是有风险的。

1.3.2　网关和防火墙

它是简单的礼物，
它是免费的礼物，
它是使我们降低到合适位置的礼物，
我们发现这个正确的地方，
它是爱和欢乐的河谷。
只要获得真正的简单，
即使为之鞠躬、致敬，也不觉羞愧。
我们满怀喜悦，旋转，旋转，
不停地旋转，旋转，直至完全正确。

——Shaker Hymn

基于这种观点，我们推荐使用防火墙来保护网络就不是什么惊人之举了。我们把防火墙定义为：安装在同时具有下列特征的两个网络之间的(硬/软)部件的集合：

- 从里到外和从外到里的所有通信都必须通过防火墙。
- 只有本地安全策略授权的通信才允许通过。
- 防火墙本身是免疫的，不会被穿透的。

并非所有的安全漏洞都只是一般化的坏事而已。有些完全是令人恐怖的。我们采用“炸弹”符号以指出一个特别严重的风险。这并不意味着你对其他问题可持乐观态度——攻击者并不十分在意他们怎样进入——但该符号提示确实就有关优先考虑的问题给出了粗略的指导。

我们应注意到这些只是设计的目标。简单地说，一个方面的失效并不意味着该集合就不是防火墙，只不过它不是一个好的防火墙。

理想的防火墙直接遵循我们在前面讲述的原则。很多主机——也许是绝大多数——不能保护它们自己免受确定的攻击。而防火墙有几个明显的优势。

防火墙能够确保安全的一个最大的理由其实很简单，因为它不是一台通用的主机。因而，没有必要既具有双倍的安全性，又极大地增加用户的方便性——NIS, rlogin等等。对于与防火墙功能无关的很多未知的安全性则可以省去。

第二个好处来自防火墙机器受到的专业管理。我们并不主张防火墙管理员必须比普通系统管理员更能干，但却要求他们具有更强的安全意识。然而，几乎肯定他们要比只照料自己机器的非管理人员强。这后一类人应包括物理科学家、教授以及那些对自己所在岗位极负责任的人。要求他们具有更多的安全意识，可能合理，也可能不合理；显然，安全意识并不是他们最优先考虑的事情。

普通用户中更少有人能对此有所帮助。拙劣的口令就是一种严重的风险，如果用户及其

口令不存在，这并不是个问题。同样，可以对各种接口程序做出或多或少的改变以期对提高安全性有所帮助，但条件是不得打扰习惯于用不同方式工作的人们。一个例子是第5章讲述的使用手持式鉴别机进行登录。许多人讨厌它，或者由于它过于昂贵而不便在整个机构上装配。然而，一个网关机器应该有一个十分有限的用户共同体，他们完全忽略这些考虑。

更微妙的是，网关机器不需要、也不应该接受任何其他机器的信任。因此，即使网关机器已经遭到损坏，也不会导致其他机器自动遭殃。另一方面，只要你愿意(并且如果你决定反对使用手持式鉴别机)，网关机器还能信任其他机器，因而在少数帐号上拥有的大多数口令都是不必要的。再重申一遍，不在防火墙上的那些东西并不会遭受损坏(防火墙的其他部件还能保护网关机器上脆弱的服务，参见第3章)。

网关机器还有其他非安全性优点。例如，它们是邮件和FTP管理的中心点。对于处理延迟邮件，检查报头语法正确性，重写返回地址(即重写成:*Firstname. Lastname* @Org.Domain格式)等，只需监视一台机器；对于邮件问题，外部的人有一个单一接触点；对于输出的文件，有一个单一位置进行搜索。

尽管如此，我们的焦点仍是安全性。对于我们已经说到的所有那些与防火墙有关的利害关系，应该强调的是，我们既不提倡也不宽恕以草率的行为对待主机安全性。即使防火墙是不可摧毁的，并且管理人员和操作人员不犯任何错误，但因特网并不是唯一的风险源头。除内部人员攻击风险外——在某些环境中，那是一种严重的风险——外部人员可以通过其他手段获得访问权。至少有一个案例，一名黑客是通过调制解调器通信池进入，并从内部攻击防火墙[Hafner and Markoff, 1991]。强大的主机安全策略是一个必需品，而非奢侈品。因此，为了保护机构网络中极为敏感的部位，设置内部防火墙是个好主意。AT&T就使用了它们。究竟什么受到了保护，留给你自己去想象吧。

1.3.3 保护口令

(说话，朋友，请进。)

"'说话，朋友，请进'指的是什么意思？"梅里问。

"那是最明白不过的"，吉姆利说，"如果你是朋友，说出正确口令，门就会打开，你就可进入。"

……

"但是，甘达尔夫，你不知道那个口令，是不是？"玻若米尔惊讶地问。

"是的！"巫士说……"我确实不知道那个口令，但是我们很快就会知道的。"

Lord of the Rings
——J.R.R.Tolkien

系统缺陷是一种破坏系统十分刺激的方法，但不是最常用的攻击方式。因为其固有的特性，"用户口令"攻击方式获得了这一"殊荣"。由于整个口令系统失效引发的系统穿透占了相当高的百分比。

我们的"口令系统"失败的原因有几种。然而最常见的问题在于人们习惯选择拙劣的口令。重复的研究表明，猜测口令极易成功，例子可见[Klein, 1990]或[Morris and Thompson, 1979]。我们不是说每个人都选用拙劣的口令，但是，却有相当一部分人把那种可猜测口令留

给了那些擅长猜测口令的攻击者。

猜测口令式攻击采用两种基本形式。第一种是在登录时尝试使用已知的或假设的用户名和类似的猜测口令。这种方法常常惊人地获得成功。站点常常有帐户-口令对，如*field*-service, *guest*-guest等。这些帐户-口令对，居然经常出现于系统手册中！第一次可能不成功，再试也不成，10余次是家常便饭，总有一次会成功——攻击者一旦进入，你的主要防线就会崩溃。遗憾的是，很少有操作系统能抗击来自内部的攻击。

这种方法并不是不可能的！不应当允许用户使用不正确的口令尝试无限次地登录，登录失败应被记录下来，应提醒用户，在他们的帐户上有登录失败的尝试等。这些没有一件是新技术，但是却很少有人这样做，做得正确的就更少了。在[Grampp and Morris, 1984]中指出了许多常犯的共同错误，但很少有研发人员听从这些劝告。更为糟糕的是，目前在UNIX系统上存在的很多日志记录，是用*login*和*su*实现的。其他一些在大多数系统上使用口令的程序——如ftpd, rexecd，各种屏幕锁定程序等——都没有记录失败的登录。

黑客设法寻求口令的第二种方法是，对偷来的口令文件(例如UNIX系统上的/etc/passwd)进行匹配推测。这些可能是从被攻破的系统中偷来的，在这种情况下攻击者将在其他机器上去试这些破译了的口令(用户趋向于重复使用口令)，或者可以从一个尚未被穿透的系统中获得。这就叫做字典攻击(dictionary attacks)，并且常常都是极为成功的。不要犯下面的错误：你的口令文件一旦落入敌人手中，你的机器极可能将遭到损害。Klein[1990年]报告口令破译率约为25%。如果这个数字对你的机器是准确的，而且你正好有16个用户帐号，那么这些口令中至少一个有99%的机率是脆弱的。

第三种方法是从一个合法的终端上搭接电缆窃听会话并记录所使用的口令。采用这种方法，无论你选择的口令如何好都无济于事，你的帐户，而且很可能你的系统，都将被损坏。

由此我们能够得出几个结论。第一，当然也是至关重要的，就是教育用户如何正确地选择一个好的口令。可悲的是，自从Morris和Thompson在1979年发表关于这一主题的论文以来，15年过去了，用户的习惯并未改进多少。尽管进行过很多努力，如[Spafford, 1992b; Bishop, 1992]，也没有就可容许的口令采取更严格的系统限制以帮助改善这种问题。已尝试过的其他一些提高口令安全性的办法，是通过逆行校检[Muffett, 1992]。但是固执的用户总是倾向于最大限度地使用同一口令，而黑客只需要赢一次就行了。

假如你无法使人们不选择不好的口令，那么重要的是绝不能让口令文件落入敌人手中。这就意味着应该:

- 小心地配置系统服务(例如Sun的NIS)的安全特性。
- 限制*tftpd*可使用的文件。
- 避免把一个真正的/etc/passwd文件放在匿名FTP区域。

当然，也有与黑客开玩笑的机会。例如，我们的ftpd会很高兴地把/etc/passwd文件交付给你(见图1-2)，包含许多完整的口令，可借助一本字典[Klein, 1990]，尝试用词语即可破译。提醒他们，“为什么还要浪费时间，赶快进攻吧”。由于所谓的root实际上并不存在，显示在黑客公告板上的第一件事，就是有关黑客特性控制的某些东西。

某些UNIX系统提供了一种能力，即使对合法用户也隐匿经散列运算的口令。如果你的系统有这种特性(有时叫做影象(shadow)或辅助(adjunct)口令文件)，我们强烈主张你采用它。其他许多操作系统都明智地散列并隐藏它们的口令文件。

```
root:DZo0RWR.7DJuU:0:2:0000-Admin(0000):/:
daemon:*:1:1:0000-Admin(0000):/:
bin:*:2:2:0000-Admin(0000):bin:
sys:*:3:3:0000-Admin(0000):/usr/v9/src:
adm:*:4:4:0000-Admin(0000):/usr/adm:
uucp:*:5:5:0000-uucp(0000):/usr/lib/uucp:
nuucp:*:10:10:0000-uucp(0000):/usr/spool/uucppublic:/usr/lib/uucp/uucico
ftp:anonymous:71:14:file transfer:/:no soap
research:nologin:150:10:ftp distribution anccount:/forget:/it/baby
ches:La9Cr9ld9qTQY:200:1:me:/u/ches:/bin/sh
dmr:laHheQ.H9iy6I:202:1:Dennis:/u/dmr:bin/sh
rtm:5bhD/k5k2mTTs:203:1:Rob:/u/rtm:/bin/sh
adb:dcScD6gKf./z6:205:1:Alan:/u/adb:/bin/sh
td:deJCw4bQcNT3Y:206:1:Tom:/u/td:/bin/sh
```

图1-2 我们匿名FTP区域的假/etc/passwd文件

口令到底多长为宜?

一般认为UNIX系统强行把口令限制在8个字符是不适当的[Feldmeier and Karn，1990; Leong and Tham, 1991]。但是口令到底多长为宜呢?

UNIX系统口令散列算法的问题是，它把每一个输入字符的7个有效位直接作为加密密钥。由于所使用的算法(DES，参见第13章)只允许56位密钥，因此限制在8个字符，别无选择。

7位有128种可能的组合，但这并不等于使用了128种组合。不但多数人避免在他们的口令中使用控制字符，而且多数人甚至只用字母。实际上，大部分人倾向于采用由小写字母组成的口令。

我们可以通过采用信息论(information theory)[Shannon, 1949]把口令值的真值表示为密钥。对于一个8个字母的普通英文文本，其信息内容是每个字母约2.3位，或许更少[Shannon, 1948, 1951]。因此用英文单词组成的口令，实际上就只有一个约19位的有效密钥长度，而不是56位。

一些人选择名字(自己的，配偶的，孩子的，等等)作为口令。这就造成一个最坏的结果，因为存在同名的现象。利用AT&T在线电话簿进行实验，结果表明第一个名字在整个名字中只有约7.8位的信息。这的确是极坏的选择。

较长的英文短语，每个字母有更低的信息内容，约在1.2～1.5位/字母的等级上。因此一个16字节的口令，如果使用英文短语，那么它也并不是强得让人猜不出来，其中信息量只有约2^{19}～2^{24}位。如果用户挑选独立的字作为口令，那么情况会有所改善，信息量将增加到约2^{38}位。但是如果用户用名字的组合填满这些字节，那么我们对此无能为力。

1.3.4 加密

加密在计算机安全战争中常被视为最基本的武器。但实际情况并不如此。当然，它是一