北京科海培训中心

Web 站点安全技术

- 详细分析 Web 安全威胁及其对策
- 阐释防火墙原理与技术、安装与维护
- 探讨 Web 发布、电子邮件、文件传输、新闻网关、电子会议等服务的安全问题及防范技术
- 面向实践，循序渐进
- 处乱不惊，擒贼有术
- 权威的资源清单，顾问与咨询；产品与厂商；工具与法律……

(美) Marcus Goncalves 著
钟向群　　译

清　华　大　学　出　版　社

Prentice Hall 北京科海培训中心

Web站点安全技术

[美] Marcus Goncalves 著

钟向群 译

清华大学出版社

(京)新登字 158 号

著作权合同登记号:01－97－2050

内 容 提 要

网络安全,特别是 Web 站点安全是目前网络管理、开发人员非常关注和担心的问题。全书以准确的信息,循序渐进的方式全面阐述了规划、实现和维护 Web 站点各种应用安全的方法,重点介绍了包括防火墙在内的各种安全技术,提出了许多具体措施和策略,以最少的花费、最简单的方式来保护 Web 站点。

本书内容新、语言简炼,其中程序清单和实例分析对读者都很有实用价值。

本书面向 Internet/Intranet 网络管理人员、网络安全技术人员、网络专业的高年级学生或研究生以及信息科技的高级管理人员。

书　名:Web 站点安全技术

作　者:[美]　Marcus Goncalves

译　者:钟向群

出版者:清华大学出版社(北京清华大学校内,邮编 100084)

印刷者:北京门头沟胶印厂

发　行:新华书店总店北京科技发行所

开　本:16　印张:13.5　字数:334 千字

版　次:1998 年 4 月第 1 版　　1998 年 4 月第 1 次印刷

印　数:00001～5000

书　号:ISBN 7-302-02954-7/TP・1564

定　价:26.00 元

序

技术正在日新月异地向前发展。1993 年 3 月，60MHz 的奔腾芯片发布，次年的 3 月，100M 的处理器芯片面世，1995 年的 3 月，120MHz 的处理器芯片出现，而 1996 年 240MHz 奔腾芯片的登场更令我们惊叹：技术发展之迅速，看来比莫尔法则(Moore's Law)所预言的有过之而无不及。

这些技术发展在使许多组织从 Internet 和 Intranet 尝到甜头的同时，也给负责局域或广域系统管理和安全管理的人们一个戏剧性的挑战。安全已不再是一个组织或企业赖以炫耀的资本，而成为一种普遍责任。万维网(World Wide Web)的兴起，使得那些有入侵癖的人们有更多机会去获取敏感数据，使个人有可能捣毁一个组织或企业的整个网络。

遗憾的是，由于技术的飞速发展以及各种不良信息的广泛传播，讨论安全问题并不轻松。《Web 站点安全技术》一书提供了一个很好的方式，告诉人们如何减少对商业网络中安全的担心。此书也是负责为各种事务处理提供一个安全环境的人们案头必备之书。该书涉猎广泛，但并非浮光掠影。第 1 章和第 2 章阐述了 Web 的基本概念及其安全问题；第 3 章讨论了金融安全问题；第 4 章对各种平台的安全性及其保护策略作了介绍；第 6，7，8，9 章讨论电子邮件、文件传输、新闻讨论组以及 http 等服务的安全问题；第 10 章对防火墙的设计和实现以及其他安全考虑作了比较详尽的阐释；第 11 章简单讨论了在使用防火墙机制后对各种“可能”情况的处理；第 12 章则提供给读者有关法律法规方面的一些重要信息，以及对付那些违规犯科者的法律的和技术的手段。

该书的另一个特色是它对各种破坏网络的入侵者或敌人有比较独到的描述。作者深入探讨了那些黑客们的心理，以及他们为何对某些信息有兴趣。并在此基础上，让读者了解如何在各种级别上保护自己的网络。作者显然明白：不同的环境，需要不同的安全措施，而且，无论是专家还是新手，都必须学习新的、更强大的方法和手段来增强业已存在的安全机制。

显然，技术在进步，需要提供更多更强大的安全保护措施的交易也在增多。本书可以说是一场“及时雨”，浇灌那些对安全问题充满兴趣，对安全技术充满渴望的人们的心田，它既令人轻松愉悦，也充满洞察力和求实精神。

Jay C. Hirshberg

致　谢

短短的一页中我不可能列出我心存感激的所有人的名字。

首先我得感谢 Prentice Hall 出版社的 Mike Mechan 先生，在我完成这本书的每一步中，他都给了我最好的激励和支持；我也要感谢 Prentice Hall 出版社，它给了我一个机会让这本书与广泛读者见面；Nick Radhuber 先先在整个书稿完成中所表现出的耐心和专业素质给我留下了深刻印象。

另外，我对 Process Software Corp.（PSC 公司）的同仁们深表谢意。特别是 MIS 部门主管 Mike Brouillette 先生，它给了我许多建议、理解和激励；也感谢 MIS 组（我是其中一员）的 Gene Ferioli，Dana，stringos，Bob Weighmann，Don McCallister 以及 Chris Lok，他们的支持、思想，…还有那些令人愉快的玩笑，都使我获益匪浅，另外特别感谢 PSC 公司总裁 Phil Den-Zer 公司，他使我有机会成为如此高素质的项目中的一员。

我还要感谢 Simson Garfinkel 的建议、Phil Zommermann 的合作以及麻省理工学院 Sloan 管理学院的 Jay Hirshberg 先生所写的序言。

对于我可爱、令人尊敬且极具涵养的妻子，我一直心存感谢，她的理解、合作与爱，她的牺牲精神以及那些无数个在我废寝忘食工作时她孤枕独眠的夜晚，都使我感动，没有她的支持，本书的完成是不可想像的。

感谢上帝赐予我的一切。

Marcus Goncalves
goncalves@process.com

前 言

关于本书

本书是一本可以“挑灯夜读”的书，特别是对于 Web 站点管理者、维护者以及那些对 Web 站点安全牵神费心的系统管理员来说，更是如此。本书是利用防火墙保护 Web 站点的实用指南，而不是艰涩难懂的高技术课本，而且它对于安全老手也是很有用的，因而它实用、目的明确而又涉猎广泛。

本书对于各种信息系统和信息技术专家来说，也是不妨一读的。如今，这些领域的专家已越来越关注和参与到电子空间中来，许多系统管理者，局域网络管理者都在着手 Web 站点的建立和管理、考虑安全的建设。对于他们来讲，没有时间深入地去了解和挖掘有关 Web 安全的各种知识和技术，但又迫切地想知道 Web 站点安全的实际情况。本书以准确的信息、大量的实例和图表、循序渐进的指导以及通俗易懂的方式提供一个快捷了解 Web 安全的途径。

本书帮助读者利用防火墙和代理服务器(Proxy Server)来设计和实现 Web 站点的安全。当然，单纯只靠防火墙并不能完全保证安全，Web 站点安全是一个相当复杂的任务，但通过一个实际有效的安全策略和安全规划就可以得到一个比较安全的站点。

当然，要保证百分之百的安全是不现实的。这就像演奏交响乐，其效果取决于许多的因素，赖以演奏的乐器(硬件)，表现的舞台(操作系统)、布景(网络)，还有希望听众(用户)能做什么、不能做什么等等，这些因素都会使效果有许多差异。

如果参加过音乐会，你当然知道其规模有大小，其形式也很多样。本书丰富的案例、规则以及各种资源来帮助读者如何去选择最好的适合自己的模式，将自己的“交响乐”演奏成功。

在搞清楚防火墙是什么以及它如何保护你的 Web 资产和你的用户利益之前，我们应当知道，防火墙的基本作用就是限制 Internet 与内部网络之间的未经授权的访问。它就像管道中的筛子，即防止外部攻击者进入内部网络，也防止内部访问在未经授权的情况下到达 Internet。通过对用户的监控，防火墙还可以防止用户将比较危险的信息，比如未加密的密码口令或敏感的公司数据，发送到“危机四伏”的 Internet 上。

根据美国国家安全局(NSA)的报道，对与 Internet 相连的系统的攻击已变得越来越复杂，而且也越来越危险。比如，黑客们已有能力使用“逻辑炸弹”渗入计算机系统，该炸弹是一些可远程引爆的编码设备；另外，“电磁脉冲”与“高性能射频枪”，也可以在计算机系统中引起具有毁灭性的“电子飓风”。

为了使 Web 站点免受这些攻击，就必须有一套有效的安全系统，该系统不仅限于口令的加密或代理机制的建立，还必须将防火墙的软件和硬件以及一套设计周密的安全策略的实现紧密结合起来。

在实现防火墙之前，建立安全策略是相当重要的，它会考虑哪些服务是禁止的，哪些是允许的，同时也要考虑验证的实现方式和加密设备，以及在连入 Internet 时，Web 站点可以

承受多大的风险。

本书涵盖了上述所有的有关 Web 站点安全管理的课题。也讨论了所有服务，比如 Telnet，FTP，E-mail，news——这些都是在良好的安全防范以及部分受限下通过 Web 可以提供的服务。

本书分为四部分，并带有 10 个附录，第一部分“Web 安全规则”由四章组成，主要讨论进行 Web 安全规划的重要性及其内容。其中介绍了 Web 站点连入 Internet 可能遭受的攻击或风险以及它对安全的一些基本需求，同时讨论了有关安全实现的投资考虑以及战略构想，我们还会对一些涉及这些内容的案例进行回顾。

第 1 章“为什么要保护 Web 站点”讨论所要保护的对象（比如信息、客户和内部用户、交易、私有性等等）以及保护的理由。同时也介绍了一些值得注意的攻击形式，比如地址欺骗、E-mail 漏洞以破解密码等，最后介绍了一些相关实例以及保护 Web 站点的措施，包括防火墙在其中的作用。

第 2 章“Web 安全需求”勾勒了一个安全的 Web 站点的基本需求，比如安全责任、交易保密、数据完整性等等，也指出了通过代理（proxy）、网关以及防火墙共同构筑安全防线的重要性，说明了对通信量及 Web 站点访问进行监控的好处以及提供性能良好的传输服务的重要性。

第 3 章“金融问题”主要是考虑和安全相关的财经问题。本章中讨论了站点被攻击的潜在损失、保护好站点的潜在回报以及与之相关的客户稳定所带来的收益。

第 4 章“保护 Web 站点战略”讨论了一些基本的安全策略，比如如何识别站点的脆弱性以及如何以安全、简捷的方式来保护站点。

第二部分“实现 Web 服务”讲述如何在 Web 上在考虑基本安全问题的情况下实现 Internet 服务。其中列出了一些最常用的 Internet 服务，并讨论了与之相关的安全风险问题。

第 5 章“电子会议”讨论了可用的电子会议技术，并提供了实现的配置清单以及相应的安全防范清单。

第 6 章“Web 上的电子邮件”回顾了一些工业标准协议、特征以及它们与 Web 的作用方式。本章也提供了一个配置清单，并讨论其安全漏洞和对策。

第 7 章“文件传输协议”讨论了可用的文件传输协议及其在 Web 上的应用，当然考虑了安全问题。

第 8 章“网络新闻传输协议”讨论了新闻组网关的工作机理以及与 Web 的相互关系，它与 NNTP（网络新闻传输协议）很相似，本章特别关注了其安全问题，讨论了实现时要注意的要点。

第 9 章“Web 与 HTTP 协议”基于第 2 章所讨论的 Web 安全需求，介绍了如何构筑一个使用 HTTP 的安全策略，并讨论了 HTTP 的代理机制及其他安全考虑。涉及了高级安全技术与协议，如 S-HTTP 和 SSL。

第三部分“安全管理：用防火墙保护 Web 站点”讨论如何通过加密和授权验证系统来设置有效的防火墙。如何进行预防和有效的规划设计、如何进行例行维护，以及如何对网络事件进行跟踪。同时也讲述了如何与入侵者作斗争，如何采取必要的措施，如何擒住窃贼。另外也介绍了有关对付入侵者的法律手段，如何利用“电子法律”来保护你的利益。

第 10 章“防火墙的设计与实现”详细地讲述了防火墙的概念以及过滤的工作机理，讨论

了代理服务器和 Sock 的实现。并给出了一组 TIS 工具和一个利用这些工具和防火墙进行站点保护的例子，最后介绍了堡垒机的概念、设计及其实现与管理。

第 11 章“处乱不惊”讲述如何对付不测事件，在有不良情况发生时该如何有条不紊地处理。同时介绍了要想抓住入侵者该做哪些事，事后应如何对安全措施进行整理。

第 12 章“追捕入侵者：法律透视”介绍了新名词“电子法(cyberlaw)”，讲述如何利用有关法律保护站点不被侵犯以及如何告发和起诉黑客。

第四部分“附录”包括 10 个附录。

附录 A“防火墙相关的资源、代理商及防火墙工具”包含了一些主要有关 Web 安全的销售名单。附录 B“防火墙产品”列出了许多防火墙产品以及如何获得这些产品。附录 C“Web 服务器产品”是 Web 服务器产品的清单以及它们的比较。附录 D“内部安全弱点扫描工具”是工具清单，这些工具用来检查密码、配置、不合适的域设置等一些安全漏洞。附录 E“修补及替代程序”列出了一些能增强安全性和服务器坚固性的程序。附录 F“高级认证及密码增强工具”提供了一些能增强密码安全性的工具。附录 G“审计及入侵检测工具”提供了一系列帮助检测安全攻击和增强审计功能的工具。附录 H“密码破译工具”列出目前可用的一些对密码实施攻击的工具。这些工具清单是仅为引用，值得注意这些工具及其工作方式，附录 I“访问控制工具”列出一些增强访问控制安全的工具。

读者

此书主要是为那些对 Web 站点进行安全管理的人们写的，但对那些 Web 安全性感兴趣的读者也是非常有用的。

平台

此书主要是针对 Windows NT 和 Windows 95 的服务器平台的，但也提到并简要地讨论了 Novell 和 Unix 的 Web 服务器。附录中许多工具是针对 Unix 平台的。但总的讲来，本书大部分内容是适合于所有平台的。

当然，其中许多例子和图是基于 Windows NT 或 Windows 95 的，而且这些平台上也开发了越来越多的工具来增强其 Web 安全性。由于有许多可免费使用的工具是基于 Unix 的，因此书中也提到很多基于 Unix 的工具和资源。从我个人来讲，我的 Web 技术背景更多的是基于 Windows NT/95 平台的。

评论或建议

如果您有任何评论、意见或问题，请与我联系：goncalves@process.com。

说明：随原版书附带的 CD-ROM 包含了全面的安全资源清单，欲购本书光盘的读者请与科海培训中心联系。

通信地址：北京海淀路 82 号科海书店，邮政编码：100080

联系电话：(010)62562449 62589259

目　录

第 1 章　为什么要保护 Web 站点

Web 技术正得到广泛的应用，它架起了客户和商家之间沟通的桥梁，并以一种极具吸引力的方式使商业过程自动化。Web 大潮使资产以新的形式扩展，无论是商家、大学、Internet 用户都越来越依赖于这种新的信息方式。

当信息技术使得信息本身可以从网上联机地服务于整个 Internet 世界时，每个人都开始着手访问这个世界。但也正因为它的价值越来越高，因而要求保护的呼声也越来越高。

然而，在无所不包的 Internet 世界中，总有一帮聪明的黑客、捣蛋鬼、恶作剧者、偷盗者等纠集起来的乌合之众，在伺机闯进安全系统，并试图改进某个内部网络或者 Web 站点。

更糟的是，Internet 本身并没有保护私有和敏感信息的能力，你得靠自己的力量。而通往 Internet 之门是向每个人敞开的，使之安全的困难可想而知，这就像门上没锁却要使家安全一样。

要意识到，只要 Web 站点和 Internet 连通，它就可能被任何人访问，除非实现了某种形式的安全功能。作为 Web 管理者，必须保护你的资产、用户和客户。而 Web 上交流的信息和交流的资源都有可能为心怀不轨者攻击。

> 换换脑筋：万维网(World Wide Web)是欧洲粒子物理实验室(CERN)的 Tim Berners-Lee 先生率先启用的，它最初是一个旨在建立一个“分布式超媒体系统”的项目。Web 本质上不过是将分布于世界各处的信息文档用一种统一的方式联结起来。目前，Tim Berners-Lee 仍在这个项目中工作。该项目由 W3 联盟(W3 Consortium)资助。

▲ 什么是 W3 联盟？它是由麻省理工学院(MIT)计算机科学实验室牵头的工业联盟，其目标是制订和推出万维网标准，并鼓励万维网产品间的兼容性。可以访问站点：http://www.w3.org 以获取更多信息。

本章介绍 Web 站点安全，它只是想说明 Web 在没有安全保护的前提下是如何脆弱，并且告诉你一些威胁的表现形式，从而给出如何防范那些捣乱鬼、黑客们及其他网络上“蜇蜂”们的策略。

它也讨论了：

- 为何要保护 Web 站点
- 保护对象是什么
- 如何选择合法者与非法者

Web 可以被攻击，这是必须面对的现实；Web 的得意之处——交互性，也正是其可怕之处。不仅 Web 用户对其上的讨论、电子商务、自动 E-mail 响应等功能充满热情，那些恶作剧者、黑客们也同样手舞足蹈。站点的门开得越大，其经受恶意或犯罪访问的风险也越大。

▲ 本书认为你已对 Web 技术有基本了解，如果您希望对 Web 了解更多，可试着访问关于 Web 的 FAQ(常见问题解答)站点，它是由 Thomas Boutell 维护的：http://www.boutell.com/boutell/。

这些“黑客”们想干什么呢？没人知道，因此只能认为他们什么都可能干！他们大多数人喜欢玩一些几年前在 UNIX 上玩过的那些恶作剧。然而，如果他们把你的客户名单公布在 Internet 上怎么办？突然有一天，你公司的形象徽标被一行愚蠢的疯话取代又将如何呢？更糟的是，黑客们在你的站点上来去自由，而你却毫无觉察，这又是何等尴尬呢？有一条真理便是：或迟或早，黑客们终将惠顾！这仅仅是个概率问题。

谈到概率，“Open Computing”杂志 1995 年 7 月作过一个安全调查。结果说明如今的计算机安全问题已是非常复杂和严重。也许高层管理者“没有”时间谈论这个问题，但你必须意识到这的确很严重。

该调查由美国国家计算机安全协会(NCSA)和“Open Computing”杂志的研究部策划并调查了宾夕法尼亚州 Carlisle 市的所有该杂志的 MIS(管理信息系统)资源订阅者和 NCSA 协会的 25 000 会员。

综合结果显示：

- IS(信息系统)部门的人们对内部威胁的关注远大于对外部威胁的关注。
- 允许用户自由访问 Internet 的站点，其被攻击的次数是那些 Web 受到安全约束的站点的 8 倍。
- 在那些允许访问 Internet 且受攻击的站点中，44%的站点没有防火墙，28%甚至不知道他们用的是没有防火墙的路由器。

如果对调查结果的其他更多信息感兴趣，请与“Open Computing”杂志的研究部经理 Sean Pfister 先生联系，其电话是 415－513－6911。也可与 Tom Kelchner 先生联系，电话为 717－258－1816 转 203，传真：717－243－8642，E-mail 为 75162.2373@Compuserve.com。

也许你的 Web 站点已开始工作，也许你的整个企业都已与 Internet 相连，不知你是否想过受黑客们攻击的问题。对于这一点，下面是调查结果：

- 14%的受访问者认为他们已被攻击过。
- 11%不能肯定。
- 72%认为从未受过攻击。

图 1.1 是 MIS 专家们对过去 12 个月之内是否受过攻击的图表显示。

调查显示，允许 Internet 访问的公司确信在过去已受到过攻击，图 1.2 是允许连接 Internet 与不允许连接 Internet 公司数目的比较。看来不允许的只是极少数。

另外一个重要的信息是绝大多数受访者并不认为他们的环境足够安全。当然安全风险有各种各样。图 1.3 是 MIS 专家们所担心的安全问题。超过 77%的人担心外部的“黑客”，48%以上的人担心内部的“黑客”。

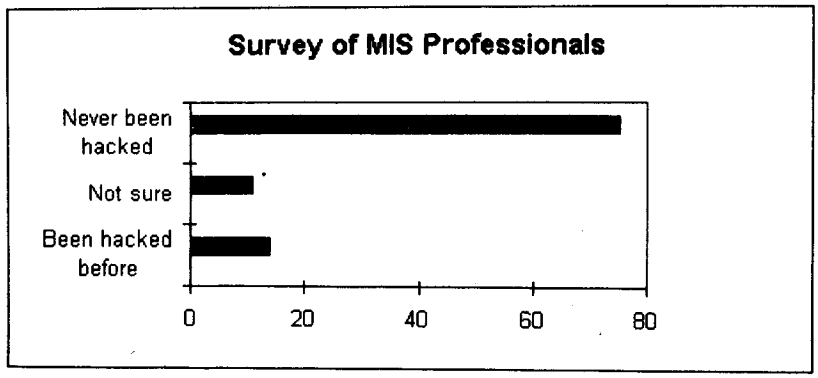

图 1.1　是否受攻击的调查结果

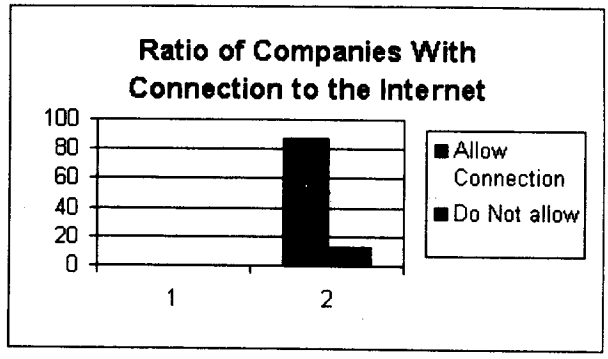

图 1.2　允许或不允许 Internet 连接的公司比较

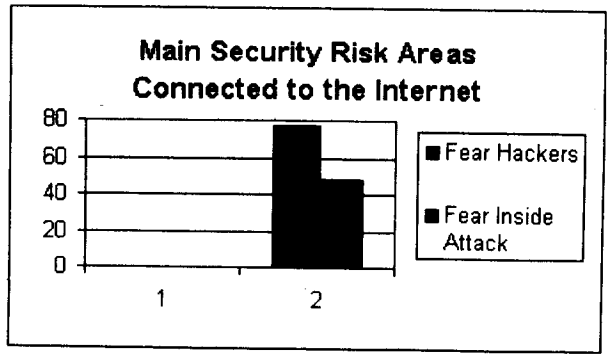

图 1.3　当连接 Internet 后主要担心的安全风险

好在大多数站点都采用了传统的安全技术，在几乎所有的站点上口令都是需要的。但还不是全部！

当问及受到攻击的站点采取了什么方法来对内、外连接进行防范时，结果是惊讶的。即使是那些已受过攻击的站点，他们都没有一个对付威胁的安全策略；竟有 44%的站点用路由器而不是防火墙来控制连接，还有 56%用了防火墙，但没有路由器一级的安全防范。

如果你运行的是一个商业 Web 站点，即责任更大，其商业动作、客户以及商业资产都仰仗于安全机制的保护，显然需要做比一般站点更多的工作。Internet 上商业交易正在成指数增长，更多的专用网络正在和 Internet 链接，对于网上的安全通信的需求将更为迫切。

1.1 保护的对象及原因

“保护 Web 信息页面的内容是目前为止最为困难的安全问题。”战略部的 Ticehurst 先生在接受 CommunicationsWeek 周刊(1996 年 4 月 8 日)的采访时曾这样说。的确，正如上面所讨论的，Internet 本身并没有提供 Web 浏览器与服务器之间的通信安全，尽管缺乏这种安全对普通用户也许影响不大，但对某些应用而言，却是很重要的。

比如，在一个与信用卡有关的销售事务中，客户很可能犹豫是否将其卡号给电子处理，因为谁能保证没有偷听者呢？

Web 安全包含两个保护对象：

- **网络安全** 它是指保护那些直接或间接与 Web 服务器打交道的计算机、硬盘、打印机、内存以及其他计算机设备。
- **交易(事务处理)安全** 它是指 Web 站点有能力提供和 Internet 上其他站点进行安全交易。包括在需要的情况下进行数字签名的能力。

上述两个方面可以组成为下面四种基本风险类型：

1. Web 文档树被非法访问的风险；它可能损害相应文档的私有性和安全性。
2. 交易截取的风险，比如金融数据或信用卡信息在远端用户发往服务器途中被截取。
3. 有关 Web 服务器的信息(如 DNS，密码等)被恶作剧使用的风险，即允许黑客可访问服务器。
4. 系统中存在缺陷(bug)从而使黑客们远程执行命令的风险。它可导致系统被修改或崩溃，包括服务器被一些不受限制的请求所淹没，而不能正常工作，最后瘫痪。

如果 Web 站点上真的要在 Internet 进行电子商务活动，其交易安全性非常重要，这在第 2 章和第 3 章将详细谈到。

1.1.1 保护信息和资源

Web 站点应该保护，以防攻击者通过内部网络对诸如打印机、工作站等资源进行控制或盗取信息。浏览器是一个对 Web 各种形式的资源都可以存取的非常强大的工具。它打开了许多扇门，不仅为用户，也为黑客们提供了便利。因此，Web 站点的保护是不言而喻的。最常见而有效的方式就是通过防火墙保护连接到 Web 服务器的内部网。

> 浏览器，何也？浏览器是用于 Web 上读取文档的强大工具。它可以访问各种形式的资源的文档，Web 站点和信息提供者通过超媒体服务器发布这些资源。而且，浏览器还可以访问 FTP，NNTP(Internet 新闻协议)以及 Gopher 提供的文件，其他访问方式也可实现。

防火墙在第 10 章将详细讨论，它是两个不信任网络之间的唯一接触点，从而使来往于两者间的通信处于被监控和保护状态。市场上有各种各样的防火墙产品，它们在性能、实现方式、保护能力等方面各有千秋。

1.1.2　保护客户和用户

安装防火墙，并完全采用合适的安全策略，就可以满足第 2 章所讨论的 Web 安全需求，从而提供一个较好的安全水平。

不过，如果要保证站点安全，完全保护客户和用户的利益，则如下的几点也甚为关键：

- **信息安全**　任何信息内容应当是专用的，不能让他人知晓，因此在 Internet 上传递信息时，必须对信息加密，以确保信息的安全性以防偷听。
- **信息交换的完整性**　信息在路由器之间传递过程中不能改变，也就是说发送者发送的信息和接收者收到的信息应该完全一致。这在处理金融交易时是很重要的，不能有任何改动。这就需要实现加密和数字签名来保证完整性。
- **发收双方的相互身份验证**　当 Web 上进行交易时，双方都必须验证彼此的确参与其中。当收方得知发方签署了交易(合同等)，这就证明了交易的可靠性，这通过数字签名是可以实现的，另一方面，它也要保证交易双方身份的真实性，也就是说不仅交易被签署，而且其签署者也是合法签署者，同时发方也得知道对方是真正的收方，而不是假冒者。这就是所谓身份验证(authentication)，它保证某人是真正的某人。

1.1.3　保证私有性

在 Internet 上保证私有性比实现生活中要困难得多。通常，我们关起门来私语，别人是无从知道的，而数字化时代情形就大不一样了，你的隐私或秘密在 Internet 上则完全有可能“曝光”。

在 Web 上，当用户发送或接收来自 Internet 上的信息时，其受拦截的机会远远大于西部的牛仔被印第安人攻击的机会。的确有一些人，会构筑巨大的数据库来跟踪别人的一举一动。

这就是创立电子私有信息中心(EPIC：Electronic Privacy Information Center)的原因，它于 1994 年在华盛顿建立，旨在提醒公众对和国家信息基础设施相关的信息私有性的关注，比如 Clipper Chip 计划；数字电话计划(Digital Telephony Proposal)；医疗记录的保密以及消费类销售数据等与信息私有性关系较大的议题。

EPIC 的宗旨是保护电子时代个人隐私的权利，使个人有更大的能力来控制自己的信息，并鼓励开发新的技术来保护隐私权。作为 Web 站点的管理员，可以经常关注 EPIC 的活动，它对相关电子立法、政治活动以及其他对隐私攻击的讨论都有最新的消息。

▲ 如果你想知道 EPIC 的更多信息，可以访问其 Web 站点：
http://cpsr.org/cpsr/privacy/epic/epic-faq.txt
也可以发电子邮件：epic@cpsr.org
写信可寄：
EPIC，666 Pennsylvania Ave，S.E.，Suite 301，Washington，D.C. 20003.