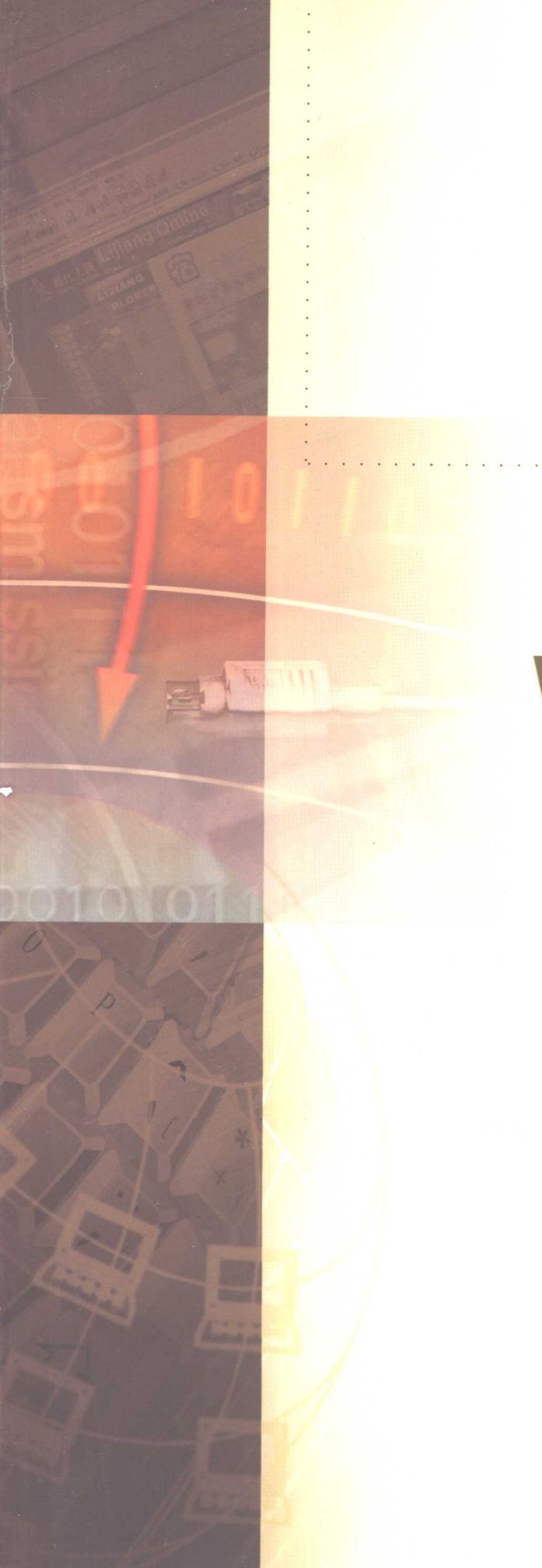

新编计算机网络安全实用丛书

构建安全 Web 站点

北京启明星辰信息技术有限公司 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
URL:http://www.phei.com.cn

新编计算机网络安全实用丛书

构建安全 Web 站点

北京启明星辰信息技术有限公司　编著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书详细地阐述了如何构建一个安全的 Web 站点，内容翔实，例证丰富。全书的主要内容包括：Web 安全需求，Web 服务器的安全策略，分布式拒绝服务攻击的原理、工具和对策，CGI 的安全管理，Cookies 及其安全，Java 的安全性，加密技术在安全管理中的应用，Web 浏览器的安全，Apache 服务器的安全性，IIS 服务器的安全管理，以及利用防火墙和入侵检测系统加强 Web 服务器的安全等。

图书在版编目(CIP)数据

构建安全 Web 站点/北京启明星辰信息技术有限公司编著 .—北京：电子工业出版社，2002.1
(新编计算机网络安全实用丛书)
ISBN 7-5053-6888-5

Ⅰ.构… Ⅱ.北… Ⅲ.因特网—安全技术 Ⅳ.TP393.4

中国版本图书馆 CIP 数据核字(2001)第 063064 号

丛 书 名：新编计算机网络安全实用丛书
书　　名：**构建安全 Web 站点**
编　　著：北京启明星辰信息技术有限公司
责任编辑：贾贺　张旭
排版制作：电子工业出版社计算机排版室监制
印 刷 者：北京四季青印刷厂
装 订 者：河北省涿州桃园装订厂
出版发行：电子工业出版社　http://www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787×1092　1/16　印张：15.25　字数：390 千字
版　　次：2002 年 1 月第 1 版　2002 年 1 月第 1 次印刷
书　　号：ISBN 7-5053-6888-5 / TP·3914
印　　数：5000 册　　定价：25.00 元

丛 书 序

全球信息高速公路的建设给整个社会的科学与技术、经济与文化带来了巨大的推动与冲击，同时也给我们带来了许多挑战。Internet/Intranet 的信息安全是一个综合的系统工程，需要我们在网络安全技术的研究和应用领域做长期的攻关和规划。

在 Internet/Intranet 的大量应用中，Internet/Intranet 安全面临着重大挑战。事实上，资源共享和信息安全历来是一对矛盾。随着 Internet 的飞速发展，计算机网络的资源共享进一步加强，随之而来的是信息安全问题日益突出。在人们对网络的优越性还没有完全接受的时候，黑客攻击开始肆虐全球的各大网站；而病毒制造者们也在各显其能，从 CIH 到爱虫，中毒者不计其数。一般认为，计算机网络系统的安全威胁主要来自黑客攻击、计算机病毒和拒绝服务攻击三个方面。目前，人们也开始重视来自网络内部的安全威胁。

黑客攻击早在主机终端时代就已经出现，随着 Internet 的发展，现代黑客则从以系统为主的攻击转变到以网络为主的攻击。新的攻击手法包括：通过网络监听获取网上用户的账号和密码；监听密钥分配过程、攻击密钥管理服务器，得到密钥或认证码，从而取得合法资格；利用 UNIX 操作系统提供的守护进程的缺省账户进行攻击，如 Telnet Daemon、FTP Daemon、RPC Daemon 等；利用 Finger 等命令收集信息，提高自己的攻击能力；利用 Send Mail，采用 Debug、Wizard、Pipe 等进行攻击；利用 FTP，采用匿名用户访问进行攻击；利用 NFS 进行攻击；通过隐蔽通道进行非法活动；突破防火墙等。目前，已知的黑客攻击手段多达 500 余种。

计算机病毒与“蠕虫”程序有所不同，它们主要的区别是，“蠕虫”寄生于操作系统之上，而计算机病毒寄生于一般的可执行程序上。计算机病毒种类繁多，极易传播，影响范围广。它动辄删除、修改文件，导致程序运行错误，甚至死机，已构成对 Internet/Intranet 的严重威胁。

拒绝服务攻击是一种破坏性攻击，最早的拒绝服务攻击是“电子邮件炸弹”。它的表现形式是用户在很短的时间内收到大量无用的电子邮件，从而影响正常业务的运行，严重时会使系统关机、网络瘫痪。

总而言之，对 Internet/Intranet 安全构成的威胁可以分为以下若干类型：黑客入侵、来自内部的攻击、计算机病毒的侵入、秘密信息的泄漏和修改网络的关键数据等，这些都可以造成 Internet 的瘫痪等。可见我们面临的计算机网络系统的安全威胁日益严重。

那么，黑客攻击等威胁行为为什么经常能够得逞呢？主要原因在于 Internet/Intranet 系统内在的安全脆弱性；其次是人们思想麻痹，没有正视黑客入侵所造成的严重后果，因而舍不得投入必要的人力、财力和物力来加强 Internet/Intranet 的安全性，没有采取有效的安全策略和安全机制；另外，缺乏先进的网络安全技术、工具、手段和产品等原因也导致网络的安全防范能力较弱。

由于我国网络研究起步晚，网络安全技术还有待整体的提高和发展。我很高兴看到这套丛书的诞生，该丛书系统全面地介绍了计算机网络安全各方面的问题，并且从一些新的角度进行探讨，例如，如何针对 Internet/Intranet 系统的安全威胁建立正确的安全策略；如何提出 Internet/Intranet 系统安全的整体解决方案；如何严格规范建立 Internet/Intranet 系统的安全机制等。这对提高我国网络安全防范能力将有重要的参考作用。

这套新版的计算机网络安全实用丛书具有起点高、内容新、技术覆盖面广等特点，包括了对业界最新的网络安全技术、操作系统漏洞和防范方法、网络安全工具以及防范黑客攻击手段等内容的详细分析和介绍。读者可以带着各种问题，从不同的角度来了解这些技术，一定会有所收获。

中国工程院院士　沈昌祥

目　录

第 1 章

Web 简介

本章概要：

- Web 的发展简史，使读者了解 Web 的起源与发展概况；
- 常用的 Web 功能，初现其丰富多采的一面；
- Web 的工作原理，为 Web 的安全分析与策略打下良好的基础。

Web 的发展与兴起是计算机及网络技术迅猛发展的产物。从简单的文本信息交流到安全成功的网上商业交易，Web 的进展可谓日新月异。各种标准、协议日渐走向成熟，并步入到人们的日常生活当中。了解 Web 的历史和基本工作原理，对于 Web 安全工作者而言应该是大有裨益的。

1.1 Internet Web 简史

1.1.1 引言

Internet 的中文名称为因特网，它不是一个公司的名字，也不属于某个机构专有，它是联接遍布世界各地的规模较小的计算机网络的超大规模网络。Internet 的发展是 Web 出现的起因，而 Web 技术的出现和发展则进一步促使 Internet 飞速成长。如今，Internet 正以迅猛强劲之势渗透到社会的各个层面，无论是在商业领域、教育科研机构或政府组织，人们日益感受到它的魅力与巨大益处，人们的生活方式也因此而增添了新的内容和形式，Internet 俨然成了信息时代的代名词。通常而言，当我们谈及 Internet 时，更多的是围绕 Web 技术来展开的。从网上信息发布到电子商务，从个人主页到公司广告，Web 技术支撑着 Internet 的方方面面，可以说，Web 技术是 Internet 技术的核心与关键所在。在谈及 Web 的发展时，我们不能不提及 Internet 的发展。Internet 发展至今，已经走过了 30 年历程。虽然在人类发展史的漫漫长河中，30 年只不过是短暂一瞬，但 Internet 上汇集的高新科技精华、深刻社会影响和浓郁文化氛围，对人们的生活产生了深远的影响。

1.1.2 Internet 的起源

Internet 的起源可以追溯到 20 世纪 50 年代末的冷战时期。1957 年，前苏联发射了人类历史上第一颗人造卫星。作为对策，美国国防部成立了高级研究计划署（ARPA）来确保美国在军事科技上的领先地位。随后，ARPA 在 1969 年启动了一项计算机互联计划——ARPANET 计划。ARPANET 使用网络控制协议（NCP）传送数据，最初联接的四个节点包括加州大学洛杉矶分校、斯坦福研究学院、加州大学 Santa Barbara 分校和犹他州州立大学。这项工程由 BBN 负责实施，并于当年 12 月获得了成功。这个传输速度为 50kb/s 的简单网络可以说是当今 Internet 的雏形。随后又有不少院校相继加入到联网计划中，截至 1972 年，在网的计算机已达 23 台。这时，BBN 的雷·托里森（Ray Tomlinson）编写的第一个电子邮件（E-mail）程序也投入使用。

同年，ARPA 更名为国防部高级研究计划署（DARPA），以突出其服务于军事国防的初衷。

1.1.3　Internet Web 的发展

Internet 的早期用户仅限于计算机专家、工程师及科学家，网络中没有友好的用户界面，也没有家用或办公用的计算机，每个用户所面临的首先是熟悉一个繁杂的系统。尽管如此，Internet 仍然在 ARPA 及其他机构的组织和协调下一步一步地深入与完善，羽翼日丰，渐露峥嵘。迄今为止，Internet 的发展大体经历了 4 个阶段。

1．军用实验阶段（1969~1984 年）

从 20 世纪 60 年代开始，ARPA-DARPA 一直致力于多种联网技术的研究，而且逐步将这些联网技术向军队中推广。与此同时，ARPA-DARPA 也敏锐地意识到按不同技术构成的各个体系结构不同的网络中的计算机无法进行通信的问题。1973 年，由 DARPA 的卡恩（Bob Kahn）和 Stanford 大学的塞夫（Vint Cerf）领衔，组织研制一种能使各种计算机网络之间相互通信的技术，他们的研究成果就是后来被称为 TCP/IP 的 Internet 核心协议。Bob Kahn 和 Vint Cerf 在他们的阐述传输控制协议的论文中第一次使用了 Internet 一词。正是这种极具前瞻性的研究，引发了计算机界的一场空前规模的革命。而日后的发展也证明，尽管这种协议本身并不完美，但它的实用、简洁的理念和思想，促成了一个世界性网络的建立。1976 年，麦卡夫（Robert M.Metcalfe）博士提出了以太网（Ethernet）的概念，它使得数据分组能够在共享的铜线上快速传输，从而为局域网的蓬勃发展奠定了理论基础。局域网的普及为 Internet 的进一步扩展提供了良好的基础。

1978 年，另一种 UNIX 联网协议 UUCP（UNIX to UNIX Copy Protocol）在贝尔实验室产生并随 UNIX 系统而分发，作为其代表性应用的 Usenet 新闻组（News Group）开始成为人们交流信息的一种有效的工具和手段。Usenet 借助于 Internet 的物理联接，将全世界的 UNIX 系统联接起来，而且很多 Internet 的主干网点也得益于新闻组的存在，新闻组中一些有关 Internet 技术的讨论与交流成为集思广益、解惑答疑的重要场所，这无疑给 Internet 的全球性普及提供了良好的环境与先例，也促成了许多 Internet 有关标准的形成。

IBM 在这个时期启动了 BITNET（Because It's Time Network）的联网计划，将教学机构和世界各地的 IBM 主机联接起来，引入了“存储转发”网络的概念，并于 1981 年开始提供邮件和邮件组服务，同时通过网关软件将 BITNET 与 Internet 联接起来，以便于交换信息。邮件组（即邮件列表 Mailing List）的出现成为继 Usenet 之后团体协作讨论的又一重要手段，它们都为 Internet 的发展提供了优良的土壤与氛围：疑难、争议、统一与协作。

网络通用语言 TCP/IP 协议在这个时期也逐渐成熟并进入实用阶段。1982 年，在 DARPA 的资助下，加州大学伯克利分校将 TCP/IP 嵌入到 UNIX BSD4.1 中，从而极大地推进了 ARPANET 的发展。同时，以套接字（Socket）为标志的应用开发接口以及一系列实用程序的出现进一步展示了 TCP/IP 的广阔前景。1983 年 1 月，TCP/IP 正式成为 ARPANET 的标准核心通信协议，每一台联入 ARPANET 的机器必须采用 TCP/IP 协议。这种强制性的标准虽然有其独断的一面，但从客观上，它避免了许多的困扰与纷争，进

一步加速了网络互联的进程。

域名解析系统 DNS 也在此时由 Wisconsin 大学提出，DNS 通过分布式的数据库将难以记忆的一长串数字——IP 地址，转换为符合人们日常习惯的名字——主机名的形式，大大方便了人们对各个主机的访问。

DARPA 对网络进行了扩充，将几乎所有军事节点都包括到了 Internet 之中。这时，在网主机达到 562 台。TCP/IP 的广泛使用，在网主机数量的成倍增加，表明实验型网络——ARPANET 开始走向实用型网络——Internet。第一个 Internet 组织 IAB（Internet Active Board）也应运而生，负责协调 Internet 的研究与发展，著名的 RFC（Request for Comments）技术文档从此层出不穷，为 Internet 的发展提供技术和标准导向。这一切都标志着真正意义上的 Internet 的出现。

2. Internet 进入学术应用阶段（1984~1992 年）

1984 年，Internet 的主机总数达 1024 个，比上一年度翻了一番。ARPANET 也被分为两个子网：MILNET 和 ARPANET，前者直接服务于军事目的，而后者着眼于高级研究与开发，这两个网络继续由美国国防部支持。这时，其他的政府和组织开始对 Internet 产生兴趣并提供资金，积极参与 Internet 的建设，其中包括 NASA 和美国科学基金会 NSF。

早在 1981 年，NSF 为无法直接接入 ARPANET 的大学院校建设了一个称为 CSNET 的骨干网，在 Vinton Cerf 的建议下，ARPANET 实现了与 CSNET 的互联。时至 1984 年，羽翼未丰的 Internet 还一直以 56kb/s 的联接速度运行，没有任何网络分层或控制。

NSF 在这个时期表现出来了令人称道的远见卓识，它开始了 NSFNET 计划，为网络提供全面的体系结构控制，以便 Internet 能够扩张和发展。这个计划有三个中标者：MERIT（是以 Michigan 大学为中心的一个非营利研究组织，负责提供工程和运作支持）、IBM（负责开发先进的路由平台）、MCI（美国第二大电信公司）负责提供广域带宽。

NSFNET 计划的第一步是建设一个具有层次结构的主干网 NSFNET，新的主干网速度为 T1（1.544Mb/s），25 倍于原有网络。为此，三家中标公司联合投资，专门成立了一个非营利的公司 ANS（Advance Network Services）来管理这一网络。1991 年，ANS 更名为 NAS CO+RE 系统有限公司，成为第一个国家商业 Internet 服务提供商，它的使命是培育商业和研究网络的商机。

1986 年，Internet 工程任务小组 IETF（Internet Engineering Task Force）成立，负责为 ARPANET、美国国防数据网以及 Internet 核心网关系统的建筑师们提供技术协调。IETF 涉及的内容几乎涵盖了 Internet 建设所急需解决的问题：从应用、组织、标准化、安全性到网络管理、与 OSI（开放系统互联参考模型）的结合等。它的存在对 Internet 的规范运作起到了重要的协调和领导作用。

伴随着 NSFNET 的发展壮大及其 T1 主干网的建成，1988 年夏天，NSFNET 取代了 ARPANET 而成为 Internet 的主干网，1989 年，ARPANET 完成了它的历史使命，宣布解散。Internet 流量的增长是如此之快，以至 NSFNET 的 T1 主干网刚刚建成便立即开始目标为传输速度 T3（45Mb/s）的干线升级。

1991 年，美国国会通过了一项法案，准备建立国家教育研究网络（NREN），作为 NSFNET 的后继，以期达到千兆位的主干网速度，这就是后来“信息高速公路”计划的

起始。

需要指出的是，伴随着因特网络的发展，与其相应的应用软件也成为人们关注的焦点。有效地利用已有的网络资源和信息的需求驱动，共享众人的智慧，促成了一系列独具匠心的概念和工具的出现。电子邮件（E-mail）、文件传输（Ftp）、远程登录（Rlogin）和新闻组（News）四种主要的应用早已深入人心，但由于网络信息资源与日俱增，且繁杂无序，这些手段捉襟见肘。1989 年加拿大蒙特利尔麦基大学（McGill University）的 Peter Deutsch 和他的同事们为更好地利用匿名 FTP 站点的资源，建立了称为 Archie 的索引数据服务器，开创了 Internet 信息的分类检索及简易操作先河，Brewster Kahle 开发了广域信息服务器 WAIS，用于全文本方式的索引和查询，它的数据库中集中了所有 USENET 的常见问题 FAQ 集、Internet 标准的相关报告等。当然，所有这些工具都要求用户对系统有一定程度的了解，没有提供直观、友好的用户界面。

这一年，被称为万维网之父的 Tim Berners Lee 和他的同事在欧洲粒子物理实验室（CERN）提出了一种新的协议，用于信息的分布和传播。1991 年该协议发展为传播信息到世界每个角落的全球万维网 WWW（World Wide Web）协议，此即众所周知的 HTTP（Hyper Text Transfer Protocol）协议。这是一种基于超文本（HyperText）全新理念的协议，在该体系中，每个文档中可以嵌入指向其他文档的链接，每当用户选中某一个感兴趣的文档链接时，它将转而直接显示相应的内容，用户无需了解该链接文档的实际位置。正是这个协议为 Internet 日后轰轰烈烈的发展播下了火种，奠定了 Web 技术的基石。当时它的发展步履蹒跚，普及的速度远不如明尼苏达大学（University of Minnesota）所发明的 Gopher 系统。应该说，Gohper 系统是第一个拥有友好界面的 Internet 应用，该系统采用了客户/服务器方式，尽管这在当时引发了不少争论，但它的菜单驱动和便捷高效的开发方式，展示了自身的优势，在很短的时间内，世界各地的 Gopher 服务器迅速增加到 1 万多个。此后，内华达大学（University of Nevada）开发的 Veronica（Very Easy Rodent-Oriented Net-wide Index of Computerized Archives）Gopher 菜单检索系统使 Gopher 系统更上一层楼。所有这些都使 Internet 在易于使用方面迈上了一个新的台阶，也为日后 Internet 的发展方向提供了经验和借鉴。

截至 1992 年，在网主机数目已经突破 110 万，此时的 Internet 真正迈进了学术应用的黄金阶段，超越了军事实验网络的界限。非营利性的学术研究和交流是该时期 Internet 应用的典型特征。

3．Internet 进入商业应用过渡阶段（1992~1995 年）

Internet 协调、组织部门的成立和逐步健全、完善，先进的网络的铺设，新型应用软件的出现，为 Internet 向商业化过渡做好了充分的准备。

1992 年，Internet 学会（Internet Society）成立，商业组织的代表开始参与到 Internet 的日常运作中，表明了 Internet 商业化的发展趋势。1993 年 NSF 成立了 Internet 信息中心 InterNIC，负责提供目录和数据库服务、注册服务、信息服务，协调 Internet 中需要惟一识别的域名、地址等相关资源的分配。

在此期间 NSF 允许更多的私人网络与 NSFNET 相联，建成了一个全新的、富有商业竞争力的 Internet 体系结构。

1993 年，在美国国家超级计算应用（NCSA）实验室工作的 Marc Andreessen 和 Eric