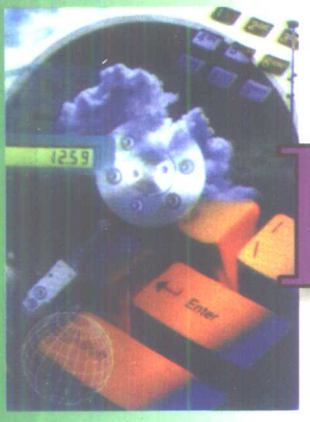
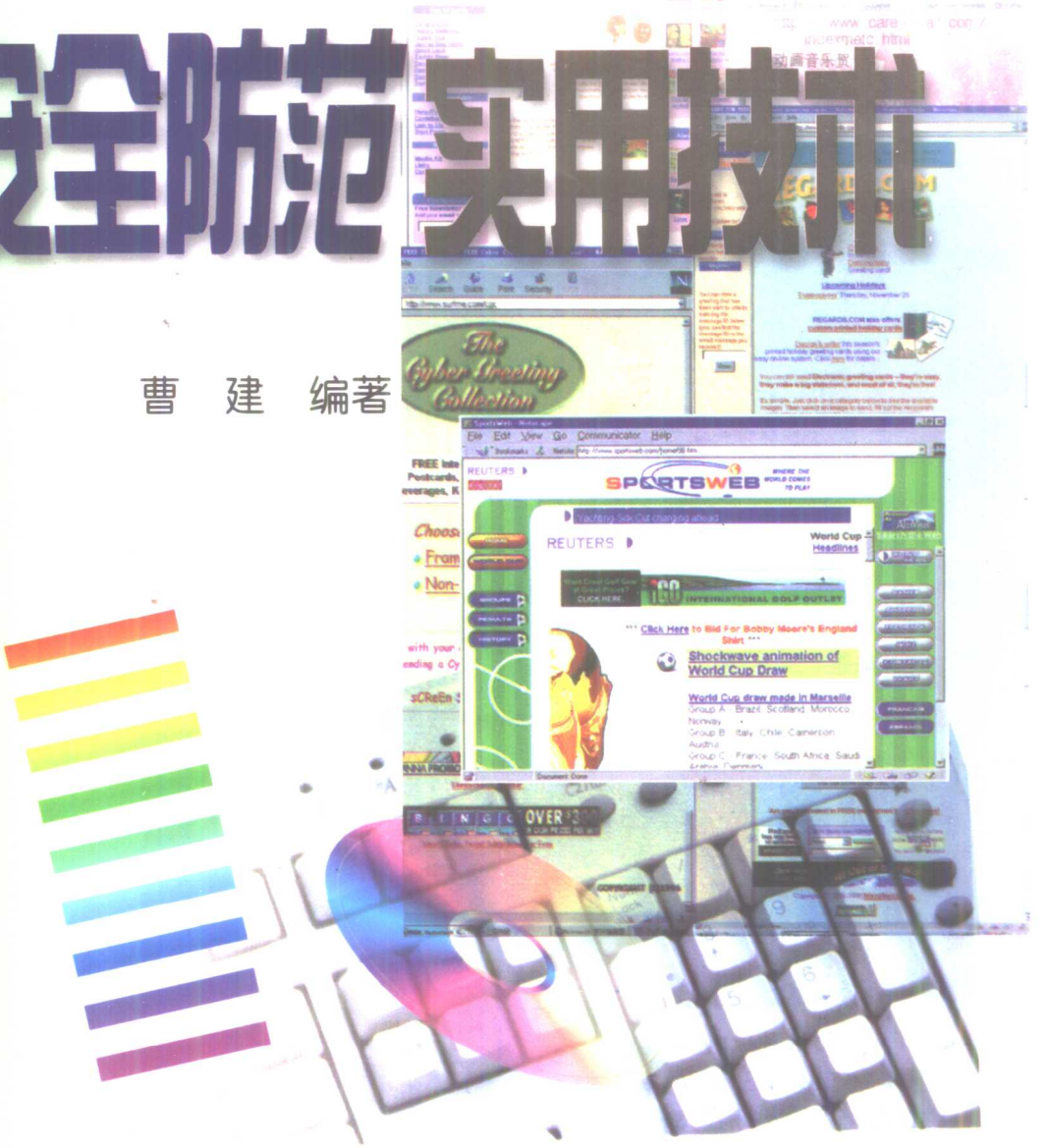


Internet与E-mail安全防范实用技术

曹 建 编著



电子科技大学出版社

Internet 与 E-mail 安全防范实用技术

曹 建 编著

电子科技大学出版社

内 容 提 要

本书详细探讨了网络袭击的常见形式，深入分析了 Internet 与 E-mail 的安全要求、加密原理和加密算法，全面介绍了 Internet 内容分级审查和安全浏览的实现方法，十分透彻地讲解了常用防火墙和 Internet 过滤软件的操作技术及使用技巧。在此基础上，详细讲述了数字凭证的申请与获取操作，以及利用数字凭证、数字签名和 PGP 加密软件、双密钥技术等实现 E-mail 安全收发的具体途径。此外，本书还给出了切实可行的病毒防范方法。

为便于初学者介入，本书还详细讲解了计算机网络基础、Internet 上网操作、E-mail 收发以及免费 E-mail 信箱申请操作等知识。

本书语言流畅，举例丰富，内容讲解深入浅出，适合所有使用 Internet 并需要保护信息安全和过滤网络内容的各层次读者学习使用。

Internet 与 E-mail 安全防范实用技术

曾　建　编著

出　　版：电子科技大学出版社　　(成都建设北路二段四号,邮编 610054)
责任编辑：唐雅邻
发　　行：电子科技大学出版社
经　　销：新华书店
印　　刷：四川建筑印刷厂
开　　本：787mm×1092mm　1/16　　印张　16　字数　399　千字
版　　次：1999 年 11 月第一版
印　　次：1999 年 11 月第一次印刷
书　　号：ISBN 7—81065—283—4/TP・165
印　　数：1—4000 册
定　　价：19.50 元

前　言

近几年，随着 Internet 的应用范围越来越广，网络信息浏览和 E-mail 收发越来越普及，用户越来越多。与此同时，网络黑客和低道德水平的网络用户也日益增多，网络安全和信息保护问题也因此变得日益突出起来。越来越多的普通网络用户需要保护自己的 Internet 信息，尤其是 E-mail 信息的安全和保密，以便能够免受非法用户的侵犯和袭击。另一方面，随着 Internet 上色情、暴力类站点的增多，如何有效地过滤网络内容，屏蔽色情、暴力站点，为未成年人创造健康、文明的网络信息环境，已成为全社会共同关心的话题，尤其成为家长和老师所迫切需要解决的问题。

本书就是在这种形势下，结合笔者的技术经验和国内外一些最新实用的安全防范技术写成的。书中详细讲解了一些防火墙过滤软件和加密软件的使用方法，这些软件都可以从 Internet 上下载，笔者均给出了下载网址及安装、设置方法。

本书除以案例介绍网络安全性的“引子”外共有 8 章内容，各章内容简介如下：

第 1 章详细讲解计算机网络与 Internet 基础知识。本章是为了便于初学者使用本书而准备的，在透彻地讲述一些基本概念的基础上，十分详细地介绍了 Internet 的产生与发展历程，Internet 上网决策、安装与调试方法，Internet 浏览的基本操作技术，E-mail 使用技术以及免费 E-mail 信箱的申请与使用方法等。

第 2 章介绍网络袭击的常见形式。主要涉及口令袭击与网络诈骗、偷用网络服务与网络偷窃、网络破坏、侵犯知识产权与个人隐私、电脑黑客及其网络袭击行为等内容。

第 3 章讲述 Internet 与 E-mail 的安全要求及一般实现方法，详细讲解了信息加密原理和基于单密钥技术的传统加密算法及基于双密钥技术的现代加密算法，并给出了安全防范技术的选用标准。

第 4 章讲解 Internet 安全浏览的实现方法。内容主要涉及操作系统安全与 Bug 问题的解决方法，Internet 的安全性及区域安全级设置，分级审查与安全屏蔽等。

第 5 章在剖析防火墙技术原理及实现方式的基础上，详细讲解安装与使用网络防火墙和过滤软件的操作方法，如 Secure PC FireWall，ConSeal PC Firewall，Cyber Patrol 等。

第 6 章介绍个人数字凭证和企业数字凭证的申请与使用方法，详细讨论使用数字凭证和数字签名实现 E-mail 安全收发的操作技术。

第 7 章在讨论计算机病毒基本情况的基础上，分析并给出了防治计算机病毒的一般方法，以及几种常见计算机病毒的防治途径。

第 8 章详细讲解 PGP 加密软件的使用方法。在众多信息加密软件中，PGP 是其中十分优秀的一种，而且目前应用也比较广泛。使用它可以加密用户的 E-mail 信件，也可以

加密其他各种重要数据文件。本章详细讨论 PGP 加密软件的功能、使用方法与获取途径，通过例子讲解使用 PGP 加密与解密信件的具体操作，并探讨该软件的安全性能与使用技巧。

需要说明的是，由于加密技术和网络安全技术本身就比较复杂，所以本书某些章节的内容对初学者来说可能有一定的难度，比如加密算法；但这并不影响本书的实用性，初学者刚开始学习时可以跳过这些章节和自己感到有一定难度的部分内容，先学习那些实际的具体操作，等掌握了有关 Internet 安全浏览和 E-mail 加密的操作方法后，再浏览和进一步学习以前跳过的那些内容，将理论与实践相结合，在实践中学习理论，这样就可以从更高的境界把握网络安全防范技术的实质，进而指导自己更好地实现 Internet 与 E-mail 信息的安全与保密。

由于笔者水平有限，书中内容可能会有一些疏漏或差错，敬请广大读者和专家、学者批评指正。网络和通信技术在不断发展，软件水平在不断提高，相应地，网络安全技术与安全防范方法也在不断变化，实践中读者还会遇到各种各样的疑难问题，所以笔者非常希望广大读者能通过 E-mail 方式与笔者时常联系，共同探讨有关 Internet 与 E-mail 安全防范的技术与方法。

曹 建

1999 年 8 月

目　录

引子：你的信息安全吗？

本章概要：

- 案例 1：国内首起 E-mail 侵权案
- 案例 2：恋爱隐私泄密案
- 案例 3：网络病毒“损”你没商量
- 案例总结与本书主题

我们周围有个别人总是以获取他人秘密和隐私为乐，或从中谋利，或发泄私愤，或寻求刺激，或陷害别人。随着 Internet 的兴起与广泛应用，人们借助网络能够更为便捷地传递和获取信息，但与此同时，信息的危险性也在逐级增加。我们先看几起案例，并从中引出本书主题。

案例 1：国内首起 E-mail 侵权案

1996 年 7 月 9 日，国内首起 E-mail 侵权案在 B 市人民法院开庭审理，该案原告和被告均系 B 大学心理学系 93 级女研究生。

4 月 9 日，原告甲收到美国 M 大学教育学院通过 Internet 寄给她的 E-mail，告知她该学院已同意她的入学申请，并将向她提供 18 000 美元的全额奖学金。这是一个令人高兴的事情，因为经过数年寒窗苦读，她终于得到了美国名牌大学的奖学金，得到了出国深造的机会。

此后，她便等待美国 M 大学的正式通知；但左等右等，过了半个多月也没能等来。焦急之中她便请美国的朋友去 M 大学询问。4 月 27 日，美国的朋友告诉她，M 大学教育学院收到了一封于北京时间 4 月 12 日 10:16 发出的，且以她的姓名署名的 E-mail，该 E-mail 拒绝了 M 大学的奖学金及入学邀请。因此，M 大学已将原准备给她的奖学金和入学机会转给了其他人。

原告在法庭上说，4 月 9 日，她和被告乙一起去 B 大学认知心理学实验室时，接收到了 M 大学发来的 E-mail，被告也看到了这封信的内容，而且这封 E-mail 存放在了被告的电子信箱里。原告上诉法庭，是被告在 4 月 12 日 10:16 冒用原告的名义给 M 大学教育学院发出了一封 E-mail，谎称原告已接受了其他学校的入学邀请，不能去该校学习，拒绝了该校提供的全额奖学金。

原告从 B 大学计算中心提取了 4 月 12 日的 E-mail 记录，与美国取证来的材料完全吻合。因此，原告要求被告承认错误，以书面形式公开道歉，并支付原告调查取证以及与美国学校交涉的费用，营养和医疗费用，精神损失费等，共人民币 15 000 元。法庭上，被告

辩解她从未以原告的名义给M大学发过拒绝奖学金的E-mail，与此事没有任何责任。

虽然法庭审理中没有确认究竟是谁假冒原告名义向M大学发出E-mail，但是，休庭后，被告终于向原告承认，确实是她冒用原告的名义发出了E-mail，并愿意为此向原告道歉，赔偿因此给原告造成的精神损失等费用。后经过法院从中调解，原告和被告双方自愿达成协议，被告赔偿原告精神损失、经济损失12 000元，并以书面形式向原告道歉。

该案发生后，E-mail信息的安全性问题，以及有关网络信息使用的道德和法律问题等，引起了社会公众的广泛关注。美国M大学对此案也非常关注，就在原告收到B市人民法院调解书的同一天，该校以最快的速度给她发来了通知，恢复她的全额奖学金，并热情邀请她入该校深造。本案的被告原本已经获得了美国D大学的奖学金，B大学心理学系主任向该校发去了带有自己签名的证明信，明确被告的问题，并表示该学生不适合成为任何一所美国大学的学生。D大学很快作出反应，取消了被告的奖学金和入学机会。

此案过后，我们想一想，如果原告收到的E-mail是加密过的，或者具有不被别人偷窥的安全性，那么她就不会经历这么一段坎坷，身心也不会遭受这么多刺激。另一方面，被告的人品我们暂不评论，但如果因为这封E-mail保密而她看不到，那她也不会失去美国深造的机会。

案例2：恋爱隐私泄密案

这件事情虽然没有诉诸法庭，但却实实在在地发生在一位青年女教师身上。这位教师姓H，人长得如花似玉，性格又非常活泼，极讨人喜爱。她在L市某大学完成本科和研究生学业后分配到S市一所大学任教。在L市读书时，她曾谈了一位男朋友，后因感情不合，两人于研究生毕业前夕分手。H赌气南下，来到S市工作，成为一名大学教师。工作一年多后，经人牵线联系，与一位在公司工作的小伙子交上了朋友。小伙子性格温和而宽容，对女友体贴入微。而且两人志趣相同，共同话题很多，关系很快发展起来。

两人工作的地点相距比较远，一位在S市的西部，一位在S市的东部，加上彼此工作又都非常忙，因此他们通常不能天天见面，一般周末相聚，所以平日他们还常常使用E-mail通信联系，互相表达彼此的感情和爱意。由于年青教师不结婚只能住集体宿舍，所以H老师不便把电脑买到集体宿舍来，只好使用教研室里的电脑和调制解调器收发E-mail。教研室里的电脑是公用计算机，不仅一些年青教师用，而且一些研究生也使用。虽然每个人都有自己的E-mail帐号，但由于计算机没有装载网络操作系统，所以他们还是共用一套E-mail收发软件，不能实现用户间信息的完全隔离。接收和发送完的E-mail都放在同一软件系统中，大家彼此都能选择某个E-mail并可以读到其中的内容；但这一点并不是每位老师都知道，只有几位比较熟悉计算机的老师和研究生才知道这一点。不少老师还以为，自己使用自己的帐号，把信发出去，机器里面就没有了。

这位可怜的H老师也不知道这一点。随着她与男友关系的发展，而且两人已经都老大不小的了，都已过了晚婚年龄，所以两人就开始讨论结婚问题了。当然，所有这些情况，包括下面我要谈到的情况都是H老师出事以后，人们通过各种途径零零碎碎地打听到的。H老师的男友爱她很深，很真诚。H老师也是一位心地善良，热情待人的诚实的好女孩。虽然两人一年多的交往，彼此都比较了解了，但邻近结婚登记，H老师还是想把最后一个心底的秘密告诉她的男友。她不想对自己爱也同时爱自己的人隐瞒什么。

不过这种秘密当面说，很难说得出口，所以她选择了以信的形式告诉他；但没有选择普通信件，而是选择了 E-mail。真不知道她当时为什么选择 E-mail，或许她可能怕写在信纸上的字太真切，或者容易保留下来；她不想回忆这件事，所以她想发一个 E-mail，男友读完后从硬盘上删除掉，就没有任何东西了，她日后也不会看到，更不会钩想起这件事。这是我们推测，当时她也不一定是这么想的；但她确确实实是给他男友发了一封 E-mail，谈起了这件事情，并请求男友的原谅。她还是使用教研室里的电脑发出的这封 E-mail。信发出去，她就以为这边机器里面没有这封信的内容了。

事实上，收发 E-mail 的软件里面还保留有她这封信的副本，只是她没有看到，也不知道。可这封信不知道怎么就被别人看到了。可能是老师，也可能是研究生，使用教研室里的电脑收发 E-mail 时，从保留 E-mail 副本的文件夹中看到了这封信。一星期后，很多人都知道了，而且有不少人就此事在议论、在嚼舌头。H 老师慢慢地觉察出这事，等她了解这件事后，顿觉羞愧难当，一时没想开，给男友写下一封信，然后服毒自杀了。这样年青，这样美丽的生命，就这样僵冷在 S 市的夏天里。

想一想，如果我们能够以对待普通信件的道德和行为准则对待 E-mail，H 老师的恋爱隐私则不大可能泄露，她还会继续享受美好生活。我们知道，对普通信件我们是不能未经允许擅自拆看别人信件的，那是违法的；我们的道德约束也不允许我们随便去从别人已经拆开的信封里抽出信件阅读，即使这封信放在没人的地方。因此，如果法律和道德规范不能保护 E-mail 的安全，那我们就应当寻求加密或其他途径来保护我们 E-mail 的个人隐私。

案例3：网络病毒“损”你没商量

计算机网络病毒是网络信息安全的另一重要方面。以前，没有联网的个人计算机主要通过磁盘传播病毒，只要读写磁盘前进行必要的查毒和杀毒，就能有效地预防病毒；而现在，计算机病毒是通过 Internet 传播的，你只要一上网，一收到 E-mail，你的计算机就有可能遭到病毒的袭击。这类网络病毒一般具有“逻辑炸弹”或“特洛伊木马(Trojan Horse)”特性，能够伪装成无害信息进入用户的计算机系统，并进行大规模破坏活动。

1996 年 9 月，Internet 上出现了一种名为“好时光(Good Time)”新病毒。这种病毒以 Internet 上的 E-mail 系统为传播途径，不需要传统病毒所要求的交换程序，具有更易和更快的感染可能性。“好时光”病毒含有“逻辑炸弹”，用户的计算机系统一旦感染它，它就会毁坏系统的整个硬盘，继而破坏微处理器的正常运行。与此同时，Internet 上还出现了一种隐藏在解压缩程序内的病毒，程序名为 PKZIP300.ZIP，其实是一匹“特洛伊木马”，用户一旦下载，病毒就会在计算机中不断复制大量的文件，直到复制的文件占满用户硬盘且将硬盘损坏为止。

到年底，Internet 上又出现了一种名为 Penpal Greetings 的特洛伊木马型的病毒。它以 E-mail 信息的形式出现，表面上征集志同道合的笔友，实际上一旦用户下载，它就会捣毁硬盘数据，并自动向用户 E-mail 信箱中所有已经存在的地址转发这份含有病毒的 E-mail，危害更多的网络用户。

在 Penpal Greetings 肆意横行的同时，Internet 上还出现了一种名为 Deeyenda 的病毒，它远比 Penpal Greetings 更为可怕。它能够对侵人的计算机系统进行全面搜索，寻找所有有价值的信息，如用户个人数据、系统口令、信用卡号码等，并将这些信息发往不知何地的

地方。

几年来，Internet传播的病毒有增无减，1997年、1998年和1999年都出现了更新的网络病毒，且“毒性”更强，危害更大。例如，1999年4月初，一种名为“蒙丽莎(Melissa)”的新型网络病毒通过Internet在16小时内便席卷全球。该病毒起源于西欧一个色情站点的新闻讨论组，几天内便造成全球数家大型Internet入网公司被迫关闭E-mail服务，同时感染了几百万台计算机系统。该病毒为Word 97宏病毒，运行染上它的Word软件时，该软件“工具栏”菜单中的“宏”命令便成为无效命令。

网络病毒的流行，使得网络安全防范问题日益受到全社会的广泛关注，许多软件公司开发出了专门的防病毒的E-mail收发软件或可以加载的功能模块，帮助用户免受网络病毒之苦。

在网络病毒史上，有一个非常著名的事件，即“蠕虫(Worm)”病毒事件。1988年11月2日，与Internet相连的成千上万的计算机运行得越来越慢，许多计算机最后达到死机状态，无法工作。虽然系统内的文件和数据完好无损，但数百万美元的计算机时间却被这种病毒“吞噬”而白白地浪费掉了。这种病毒能从网络上的一台计算机传到另一台计算机，并在传播过程中进行复制，它利用了程序员在Unix系统中留下的一个鲜为人知，也不易引人注意的“后门”，直接进入计算机系统，袭击存储器。它把自己隐藏在存储器的某处，并四处传递误导信息，这样就使得它极难被发现，也极难被控制。“蠕虫”病毒繁殖的速度之迅速异常惊人，在不到10个小时的时间里便掠过美国，导致6000多台计算机系统关机。几天后，查出病毒制造者是罗伯特·莫里斯(Robert Morris)，系康奈尔大学23岁的研究生。他制造这个病毒程序的目的是想验证它能进入多少台计算机，但由于他在程序设计中有一个错误，结果病毒的复制速度大大出乎他设计的速度。由于莫里斯触犯了美国联邦法律，被判以缓刑3年、10 000美元罚款和400小时无偿公益劳动。

自从蠕虫事件后，Internet上成立了计算机应急小组CERT(Computer Emergency Response Team)，用以保护网络安全；但计算机病毒就像生物病毒一样，此消彼长，防不胜防。不论反病毒技术有多么先进，总会有人发明“毒性”更大，危害更奇特的新病毒。因此，作为使用计算机和Internet的普通用户，需要掌握一些基本的防范病毒的方法和技巧，以不变应万变，保护自己计算机系统和信息资源的安全性。

不论是病毒的编制者还是网络的非法入侵者，他们都是各色计算机“黑客(Hacker)”中的一员。所谓黑客，是指利用通信软件，通过计算机及其网络非法进入他人系统，截获或篡改计算机数据，危害信息安全的电脑入侵者或入侵行为。Hacker的原意是指热衷于计算机程序设计的人，他们对计算机非常着迷，且具有一种畸形的道德与价值观念，以入侵他人计算机及网络系统为乐。例如，据报道，有一小撮人对美国五角大楼的计算机系统展开了“高度组织与系统化的袭击”；美国国家航空及太空总署(NASA)、美国海军及全美10多所著名大学运行微软Windows NT及Windows 95操作系统的计算机同时遭到黑客袭击；存放有美国在线AOL(American Online)虚拟社区负责人敏感信息的数据库遭到黑客袭击；纽约时报站点(http://www.nytimes.com)遭到黑客袭击。

案例总结与本书主题

随着经济信息化进程的加快，计算机网络在政府、军事、金融、医疗卫生、交通、电