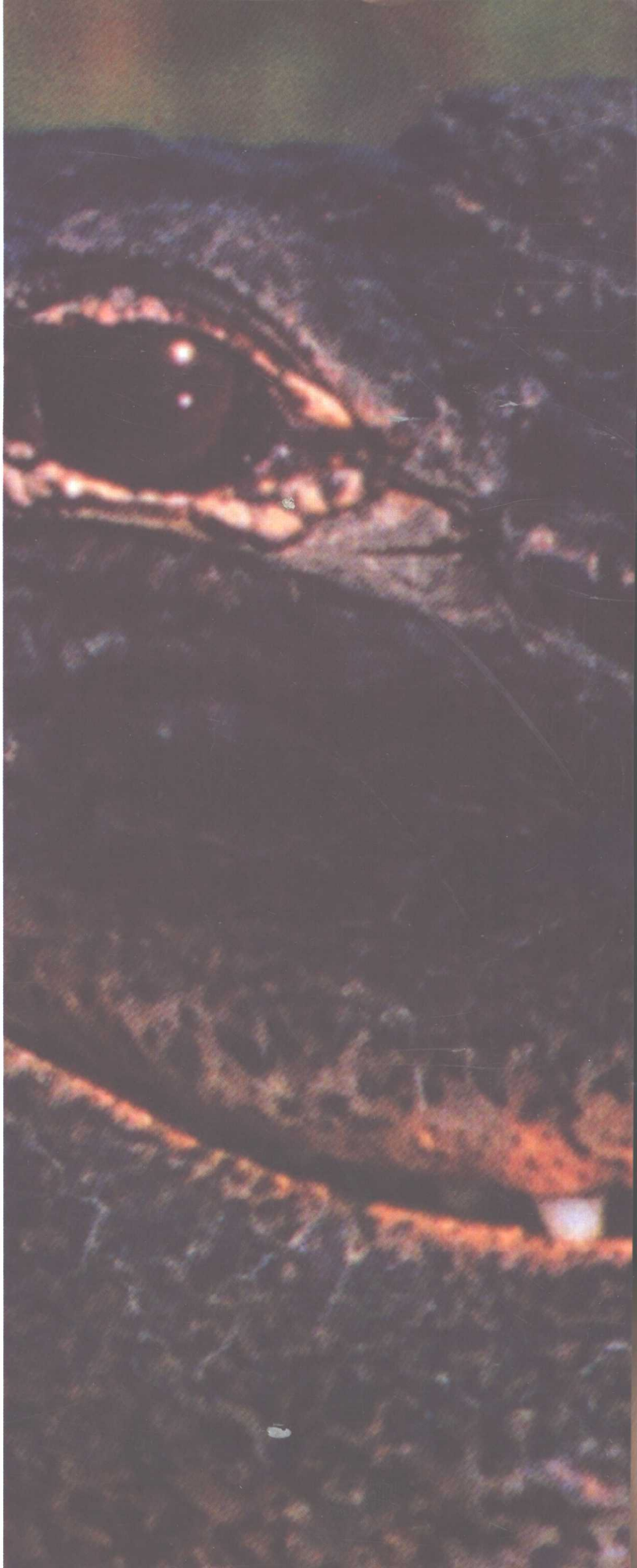
SAMS

〔美〕Richard Blum 著
杜 鹏 译

开放源码邮件系统安全



人民邮电出版社
POSTS & TELECOMMUNICATIONS PRESS

开放源码邮件系统安全

[美]Richard Blum 著

杜 鹏 译

人民邮电出版社

图书在版编目（CIP）数据

开放源码邮件系统安全/（美）布卢姆（Blum，R.）著；杜鹏译。
—北京：人民邮电出版社，2002.4
ISBN 7-115-10081-0

I. 开… II. ①布… ②杜… III. 电子邮件—安全技术 IV. TP393.098

中国版本图书馆 CIP 数据核字（2002）第 011178 号

版权声明

开放源码邮件系统安全

◆ 著 [美] Richard Blum
译 杜 鹏
责任编辑 陈冀康

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
读者热线 010-67180876
北京汉魂图文设计有限公司制作
北京顺义向阳胶印厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：21.5
字数：512 千字 2002 年 4 月第 1 版
印数：1-4 000 册 2002 年 4 月北京第 1 次印刷

著作权合同登记 图字：01－2001－4076 号

ISBN 7-115-10081-0/TP・2765

定价：40.00 元

本书如有印装质量问题，请与本社联系 电话：（010）67129223

内容提要

本书对开放源码电子邮件系统及其安全做了全面而详细深入的介绍。

全书分为三个部分 17 章。第一部分包括 1 到 6 章，介绍了电子邮件系统的基础知识。第二部分是 7 到 13 章，选取了目前最为流行的 3 种开放源码邮件软件 sendmail、qmail 和 Postfix，有针对性地介绍了怎样使用它们建立安全的邮件环境，另外着重介绍了防止开放式转发和阻挡垃圾邮件的方法。第三部分是 14 到 17 章，介绍了邮件服务安全方面的高级知识，包括防火墙、SASL、POP3 和 IMAP 服务器安全等技术。

本书内容安排循序渐进，实例丰富，无论是对专业的电子邮件管理员还是普通的电子邮件技术学习者均能有所帮助。

译者的话

电子邮件系统是互联网的一个成功典范，作为一种全新的通信工具，它诞生时间不长却给人们工作和生活的诸多方面都带来了深刻的变化，在某种程度上已经成为人们工作和生活中不可或缺的重要部分。随着互联网的进一步普及，电子邮件的作用也将越来越重要。

然而，电子邮件系统在给人们提供便捷通信手段的同时也遭到了一些人的滥用。由于早期的电子邮件系统采用的都是开放式接收并转发所有的邮件，这就给广告商和恶意的黑客钻了空子。广告商利用开放式转发发送成千上万的垃圾邮件，塞满了用户的邮箱，降低了邮件服务器的效率；黑客们利用开放式转发可以轻易地入侵服务器，使邮件系统瘫痪，并有可能进一步破坏系统资源。尽管今天的邮件软件基本上都禁止开放式转发，同时也提供了很多防止黑客攻击的手段，但是对于经验不是很丰富的邮件管理员来说，或者是在复杂的邮件环境中，如何根据特定的条件选用合适邮件软件、正确地进行安装和配置，并保障邮件系统的安全也不是一件很容易的事情。

本书正是为了解决这个问题。通过本书的介绍，读者将会了解到互联网上电子邮件系统工作的基本原理，邮件的格式，邮件在互联网上采用什么协议进行传输以及又是通过哪些软件由客户端发出、从服务器上收取。接下来本书以UNIX 系统为例，分析了怎样保护邮件系统的载体——服务器系统的安全，并重点介绍了 3 种使用最广泛的开放源码邮件软件 sendmail、qmail 和 Postfix 的配置、安装以及各自的安全保护措施，然后讨论了阻挡垃圾邮件和过滤病毒的方法。本书第三部分介绍了怎样保护邮件服务的安全，给出了一些实际运行的邮件系统的例子，分别针对 sendmail、qmail 和 Postfix 邮件软件介绍了怎样建立邮件防火墙，怎样对网络连接进行认证，怎样使用安全协议以及怎样安装和配置安全的基于 Web 的邮件服务器。

本书在内容安排上循序渐进，所介绍的软件又都是免费软件，因此电子邮件技术人员和爱好者们可以按照本书的讲解一步一步地建立自己的安全的电子邮件系统。

对于开放源码的支持者来说，本书系统地介绍了电子邮件领域的有代表性的开放源码邮件软件，也不失为一本有益的参考书。

由于时间较短，译者水平有限，本书中难免有不准确之处，请读者不吝指正。

译者

2002 年 1 月

前 言

据说每一种计算机平台都有使它获得成功的“杀手锏”，很多人认为电子邮件是互联网的“杀手锏”。

互联网电子邮件已经成为一项重要的商用和家用资源。很多公司使用电子邮件作为公司内部通信以及同外部顾客联系的手段。邮件服务器的死机时间将会给很多公司的通信造成严重影响。

不幸的是，并不是每一个电子邮件用户都遵守相同的规则。随着互联网的普及，对邮件系统的滥用也日渐增多。那些利用常规邮件系统大量发送邮件试图销售各种各样商品的人也开始利用互联网电子邮件系统。使用一个计算机程序就能给成千上万的人发送信息的商业前景把很多讨厌的商业行为也吸引到了互联网上。洪水般的无用的商业邮件不但挤占了网络带宽也塞满了用户的邮箱，导致邮件系统的超负荷运行。

另一种对互联网邮件系统的滥用是黑客利用发送恶意的病毒程序进行攻击。电子邮件尚未普及时，病毒制造者只能依靠人们通过软盘共享文件或从公告牌下载文件的方式传播它们的破坏性程序。随着电子邮件（以及界面友好的邮件客户端程序）的普及，只需要简单地把病毒发给少数几个人就可以轻易使成千上万台计算机受到感染。

作为邮件管理员，你的工作就是保护你的用户免受不需要的垃圾邮件和恶意病毒的侵害，但是在今天的邮件环境中，这不是一件很容易的事情。

对 UNIX 环境下的邮件管理员来讲，有许多开放源码电子邮件服务器软件可供选择，这就给你提供了多种不同的方法来保护你的网络不受垃圾邮件和病毒的侵害。当然，任何一种 UNIX 邮件服务器产品在不同的邮件环境中都有优点和缺点。

在 UNIX 电子邮件简短的历史中，有 3 种独立的开放源码软件产品同其他同类产品相比得到了更广泛的流行。到目前为止，UNIX 环境下最流行的邮件软件是 Sendmail 联合体开发的 sendmail 软件。除此之外，还有两种软件也吸引了大量的用户，一个是 Dan Berstein 开发的 qmail，另一个是 Wietse Venema 开发的 Postfix。这 3 种软件都是完整的邮件服务器软件包，也都可以通过配置来阻止垃圾邮件和病毒。本书的目的就是帮助邮件管理员认识这 3 种软件在防止垃

圾邮件和病毒侵害方面的功能，并在实际系统中应用这些功能。

知识是邮件管理员所能利用的最好的安全工具。理解互联网上邮件系统使用的协议对于提高你对邮件安全性的认识很重要，因此本书的第一部分将帮助一些邮件管理员新手理解电子邮件协议以及电子邮件相关的病毒和攻击的原理。如果你已经对电子邮件系统的工作原理有很好的理解，可以跳过本书的第一部分，把它当作阅读后面章节时的参考。

第二部分从 UNIX 系统和邮件服务器的角度出发，集中介绍了怎样构建一个安全程度较高的邮件服务器。在你获得一个安全的邮件环境前，必须先有一个安全的 UNIX 系统来检测并阻止攻击者的入侵。类似地可以对邮件服务器进行配置，阻止垃圾邮件和病毒的侵害。通过对各种不同的 UNIX 邮件服务器软件的学习，你可以确定出哪一种是最适合你自己的邮件环境。

本书在最后一部分给出了一些在真实运营的电子邮件服务器环境下应用安全功能的例子。对于电子邮件系统的安全性来说，邮件防火墙是最好的工具之一，它可以防止互联网上的搜索程序从你的邮件服务器上收集信息。接下来讨论了安全的 POP3 和 IMAP 服务器以及安全的 Webmail 服务器，它们为你的用户提供了从远端安全地读取邮件的方法。

本书的内容

本书包括 3 个部分，每部分又分成了若干章节：

第 1 章“电子邮件基础知识”，介绍了电子邮件的历史以及电子邮件是怎样在 UNIX 平台上工作的。

第 2 章“SMTP 协议”，介绍了简单邮件传输协议（Simple Mail Transfer Protocol，SMTP），在互联网上发送邮件的核心协议。

第 3 章“POP3 协议”和第 4 章“IMAP 协议”介绍了邮局协议（Post Office Protocol，POP）和交互邮件访问协议（Interactive Mail Transfer Protocol，IMAP），这两个协议允许远程用户从邮件服务器上读取邮件。

第 5 章“MIME 协议”，介绍了邮件内容和附件使用的标准格式，包括增强邮件安全性的 S/MIME 和 PGP 方法。

第 6 章“读取邮件头”，帮助邮件管理员新手分析电子邮件的邮件头信息，从而可以对垃圾邮件和恶性病毒进行追查。

第 7 章“保护 UNIX 服务器安全”，帮助邮件管理员理解 UNIX 服务器安全的基本知识，以及一些增强服务器安全性、识别入侵企图的开放源码产品的例子。

第 8 章“sendmail 邮件软件”、第 9 章“qmail 邮件软件”和第 10 章“Postfix 邮件软件”介绍了 sendmail、qmail 和 Postfix 这 3 种开放源码邮件服务器软件，每一章都介绍了一种软件的安装以及怎样在一个比较安全的环境中进行配置。

第 11 章“防止开放式转发”，讲述了怎样防止垃圾邮件发送者使用你的邮件服务器向其它用户发送垃圾邮件，以及怎样避免从互联网上已知的开放式转发服务器收到垃圾邮件。

第 12 章“阻挡垃圾邮件”，讲述了怎样在标准的开放源码邮件服务器软件中嵌入垃圾邮件过滤功能。

第 13 章“过滤病毒”，讲述了两种用来阻止病毒进入你的邮件系统的方法：病毒过滤和使用商业反病毒软件进行病毒扫描。

第 14 章“使用邮件防火墙”，介绍了创建单独的邮件防火墙服务器使用的技术。邮件防火墙服务器可以保护你的用户地址和邮箱免受黑客的攻击。

第 15 章“使用 SASL”，介绍了常用的要求远程服务器在你的服务器进行认证的方法，只有通过认证才允许它们发送邮件。

第 16 章“安全的 POP3 和 IMAP 服务器”，介绍了怎样在 POP3 和 IMAP 服务器中嵌入 OpenSSL 开放源码软件以支持 SSL 协议，从而为你的用户提供一种更安全的从远程读取邮件的方法。

第 17 章“安全的 Webmail 服务器”，作为本书的结束，介绍了怎样使你的邮件服务器为远程用户提供一个功能全面的、安全的 WebMail 界面。

本书声明

本书举例时使用了大量的邮件地址和网络域名，所有的例子都尽可能使用虚构的地址和域名，在本书写作时这些地址和域名还没有在分配域名和在数字互联网组织（Internet Corporation for Assigned Names and Numbers，ICANN）注册。如果本书出版后这些地址被注册，本书声明同它们的拥有者没有任何关系。

另外，所有本书中使用的 IP 地址也只是为了举例。如果有可能，本书尽量使用公共 IP 地址，你应该把它们替换成分配给你的特定组织的 IP 地址；不得已的情况下，本书选择使用那些同任何现有 IP 网络无关的虚构地址。在给你的网络分配 IP 地址时，如果该网络同互联网相连，请先咨询一下你的互联网服务提供商。

本书中使用的一些约定

本书中使用的一些约定如下：

注意

注意提供给你一些关于当前话题的评论和辅助信息，以及某个概念的详细解释。

小心

这是一些警告信息，防止你可能把事情弄糟，并提示你怎样避免网络中的陷阱。

每章结束都有一段小结，概括这一章介绍的主要内容。

此外，本书中还使用了一些印刷上的约定：

- 斜体用来区分新的条目，有时也用于强调；
- 命令、变量和代码使用特殊的等宽字体显示；
- 在代码列表和代码例子中，使用加黑的等宽字体强调用户输入的命令行；
- 语法描述中的占位符用斜等宽字体显示，表示你必须使用真实的文件名、参数或其他内容来替换占位符。

目　录

第一部分　电子邮件原理

第二部分 服务器安全

第三部分 邮件服务安全