万水网络与数据库丛书

网络安全技术

——风险分析、策略与防火墙

[美] Othmar Kyas 著
王霞 铁满霞 陈希南 译

中国水利水电出版社

网络安全技术

——风险分析、策略与防火墙

[美] Othmar Kyas 著

王霞　铁满霞　陈希南　译

中国水利水电出版社

内 容 提 要

Internet 是由计算机网络互连而成的全球性信息网。近年来，Internet 的安全问题越来越引起人们的关注。本书包括了 Internet 安全的方方面面。首先回顾了早期的电话窃用、计算机病毒及计算机犯罪的历史，并从 Internet 潜在的风险入手，对各种安全漏洞、侵袭方法及侵袭者的形象作了详尽的描述。

本书着重分析了 Internet 上各种安全隐患、应用风险及其病毒危害，论述了 Internet 安全体系结构的规划与建立以及防火墙系统的设计与实施方案，并详细介绍了数据加密技术与侵袭模拟器。

本书内容新颖独特，实用性强，是广大 Internet 用户的必备手册，可为 Internet 网络的安全管理、操作及维护提供实用指南，适合于大专院校、科研机构、商业及政府部门的网络管理人员、技术人员及研究人员使用。

图书在版编目(CIP)数据

网络安全技术/(美) 基亚斯(Kyas, O.)著;王霞等译. -北京:中国水利水电出版社, 1998.6

(万水网络与数据库丛书)

书名原文：Internet Security

ISBN 7-80124-219-X

I. 网… II. ①基… ②王… III. 因特网-安全技术 IV.TP393.4

中国版本图书馆 CIP 数据核字(98)第 13768 号

书　　名	网络安全技术—风险分析、策略与防火墙
作　　者	[美] Othmar Kyas
译　　者	王 霞 铁满霞 陈希南
出版、发行	中国水利水电出版社（北京市三里河路 6 号 100044） 北京万水电子信息有限公司（北京车公庄西路 20 号 100044）
排　　版	北京万水电子信息有限公司
印　　刷	水利电力出版社印刷厂印刷
规　　格	787×1092 毫米 16 开本 12.75 印张 279 千字
版　　次	1998 年 6 月第一版 1998 年 6 月北京第一次印刷
印　　数	0001—5000 册
定　　价	21.00 元

译 者 序

计算机网络的迅速发展使得Internet 全球信息网在世界各个领域中发挥着日益重要的作用，但随着Internet 使用范围的不断扩大与用户的不断增加，网络安全也愈来愈成为日益突出的严重问题。目前有关 Internet 安全方面的研究与探讨尚不深入，参考资料也比较缺乏，尤其在我国更是如此。鉴此，我们将《网络安全技术——风险分析、策略与防火墙》一书奉献给大家。本书不仅为网络的安全设计与构造指明了方向，而且可为网络的安全管理、操作及维护提供实用指南。

本书论述了网络安全的方方面面。从潜在的风险分析入手，详细描述了Internet 的各种安全隐患、应用风险及病毒危害，给出了相应的防范措施与安全准则，并论述Internet 安全体系结构的规划与建立以及防火墙系统的设计与实施方案。全书共包括十八章，各章内容按排如下：第一章介绍了Internet 上的各种风险及风险分析与风险评估方法；第二、三章详细描述了各种形形色色的侵袭者与计算机犯罪，并分析了犯罪的目的；第四章综述了Internet 的众多薄弱环节；第五、六、七、八章就Internet 的访问控制、TCP/IP 通信协议以及多种应用服务的安全风险作了详尽的叙述，并给出了相应的防范措施；第九章专门讨论了计算机与网络病毒，并对病毒的类型及危害进行了特别说明；第十章给出了网络安全准则的制定策略与安全体系结构的实施方案；第十一至十六章针对各种防范措施，如各种各样防火墙系统、数据加密技术及侵袭模拟器等方面均作了详细的介绍与论述；第十七章给出了有关网络安全的联机信息；最后，在第十八章展望了未来Internet 安全体系结构的发展趋势——防火墙系统。

本书由西安交通大学王霞、西安电子科技大学铁满霞及西安交通大学陈希南三位同志共同翻译完成。其中第一至第六章、第九、第十章及附录部分由王霞同志翻译，第七、八章及第十二至十六章由铁满霞同志翻译，第十一章及第十七、十八章由陈希南同志翻译。本书全稿由西安航空计算技术研究所王世奎同志进行了统校，并给予技术指导，在此表示诚挚的感谢。由于译者水平有限，时间仓促，本书难免存在一些缺点和错误，殷切希望广大读者批评指正。

经 WWW、Gopher、FTP 或 EMAIL 进入 Internet

WWW: http://www.itcpmedia.com
GOPHER: gopher.thomson.com
FTP: ftp.thomson.com
EMAIL: findit@kiosk.thomson.com

WebEXtra

就本书论述的主题，WebExtra 提供了极为有价值的新颖独特的信息。如关于 Internet 安全的风险分析、防范策略以及防火墙系统等诸多方面的信息如下：

• 标题新闻条目。敦促人们及时掌握有关 Internet 与 Web 的安全、防火墙及信息／数据安全方面的时代发展脉搏。

• Internet 发展方面的重要新闻。

只需到 Web 网点查询国际 Thomson Computer Press，上述 WebExtra 的特别信息即可免费获得（仅通过 Internet 与 WWW 的访问需交费）。URL 为：

http://WWW. itcpmedia.com

ITP 特别服务

引　言

通过Internet 侵袭专用计算机网络的事件迅速增多，与近年来Internet 用户的爆炸性增长相同步。据计算机紧急情况处理小组(CERT)报道，1989年仅发生132起计算机安全事故，到1994年，安全事故的数量竟已多达到2241起，先后共有4万多个网络受到损害。

随着Internet 在经济领域中重要性的逐步提高，Internet 上的犯罪活动预计将加速增长。尽管如此，与Internet 联网的公司机构所采取的预防措施还远不完备，以至于不熟练的计算机窃贼也能轻易入侵访问。

本书讨论了网络安全的方方面面，从分析潜在的风险人手，对安全漏洞、各种各样的袭击方法及侵袭者的形象都给出了详细的描述(深入了解各种侵袭技巧是有效安全系统设计的基础)。

后续章节不仅论述了全面安全体系结构的规划与建立，而且给出了防火墙系统的设计与实施方案，并对加密系统与袭击模拟器做了充分说明。

Internet 作为全球通信媒体，其战略上的重要性与内部数据网络的安全标准，均需对有争议的网络安全做出专业约定。与Internet 相连的网络，若不具备相应安全的体系结构，就有可能造成严重后果。总而言之，按照结构化的设计思想合理设计的防火墙体系结构，能提供充分的保障以防止计算机犯罪，并能保证毫无限制地访问Internet 上的各种资源。

目　　录

第一章　Internet 安全：风险分析

1.1　Internet 安全风险——信息高速公路上的危险

自从 1993 年 Internet 上首次采用第一种图形用户界面 NCSA MOSAIC 以来，这一全球最大网络的用户数量与服务内容都有了迅猛增加。商业集团和个人用户都很快意识到，由 Internet 带来的革命化通信时代，为通信应用领域开辟了无限的前景。事实上，Internet 已成为全球市场的基础设施。未来几年内，它也将是整个社会发展的关键技术。

另一方面，随着利用 Internet 从事商业活动的加大，犯罪活动与滥用现象已日益增多。当公司考虑是否要与 Internet 联网以及如何联网时，需考虑的主要问题就是涉及其中的风险因素。如果没有适当的安全保护措施，一旦与 Internet 联网，将会带来意想不到的风险。今天，几乎所有的公司都依靠着计算机系统平静地运作。若由于 Internet 上的安全风险，有几台或全部计算机系统崩溃，将不可避免地带来大量的财政损失。该损失有可能超过使用 Internet 所带来的效益。

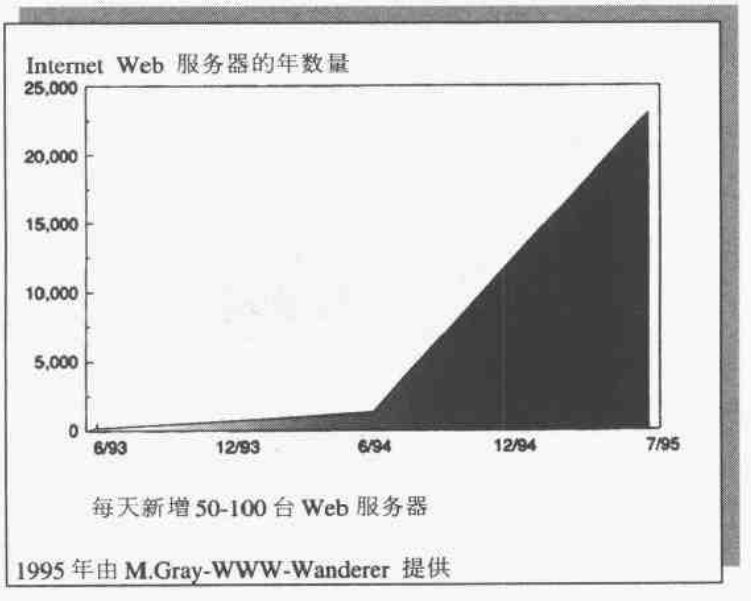


图 1.1　1993 年以来 Internet 服务器的增长趋势

1.2　DP 基础设施中的基本风险

探讨 Internet 安全时，常被忽视的事实是，公司的计算机系统面临的严重风险并不仅仅

在Internet 上。例如，1994年，Ernst和Young对发生问题的美国公司所进行的研究表明：在最近12个月内，由于数据安全问题，有半数公司遭受了财政损失。受损失的公司中，超过2/3是由于公司的工作人员造成的，而其中的一半仅是由于误操作引起的。下面列举一些典型情况：

- 没有备份
- 由磁盘带进了病毒
- 出于“我仅仅想看看，如果…”的好奇心
- 误操作（如删除数据等等）

一旦公司出现上述任何一种情况，其计算机系统不管是否连在外部通信网络的上，与Internet 的联网极大地增加了成为蓄意袭击目标的机会。

1995年5月，NCSA（国家计算机安全联合会）所作的调查表明，连在Internet 上的公司平均遭受的袭击是未与Internet 联网公司的8倍（见图1.2）。由图上可见，未与Internet 联网的公司仅为3%，而与Internet 联网的公司遭受的侵袭却为24%。其它的风险因素是，与其它公司连接的数据链路，允许员工经由modem（调制解调器）拨进公司网络的基础设施等。1994年，美国国防部“计算机智能与安全组”所做的研究却打破了这些数字。其主要发现是，80%以上的袭击者都是借助于Internet 从外部侵袭到内部数据系统的（见图1.3）。

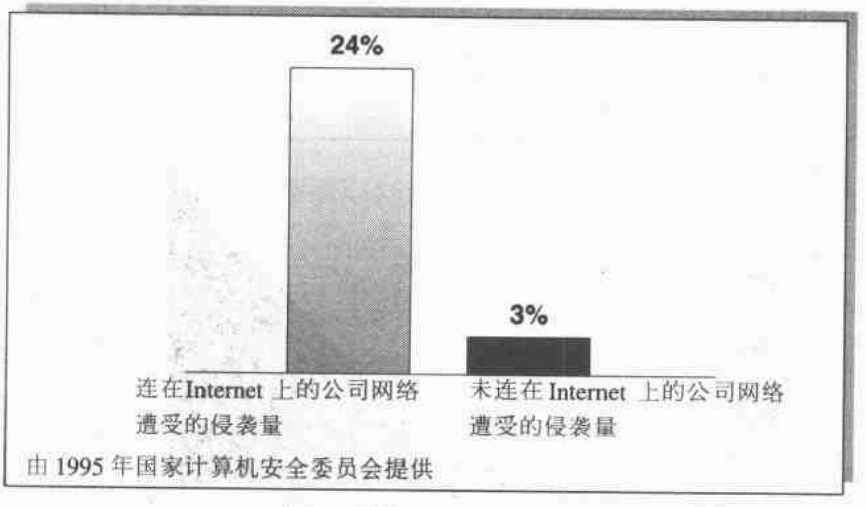


图 1.2 连接 Internet 的风险率

1.3 Internet 存在的风险

来自 Internet 对内部信息系统带来的潜在风险的主要因素有：

- 外部访问未被授权的信息系统
- 数据丢失（插入／删除／滥用）
- 机要信息丢失（泄露／竞争）
- 公共通用网络上的固有问题（病毒、人为破坏等）

- “Trojan horses”（Trojan horses 程序）和病毒混杂在 Internet 的传输数据中
- 利用虚假身份（地址欺骗、第三方 ID 等）

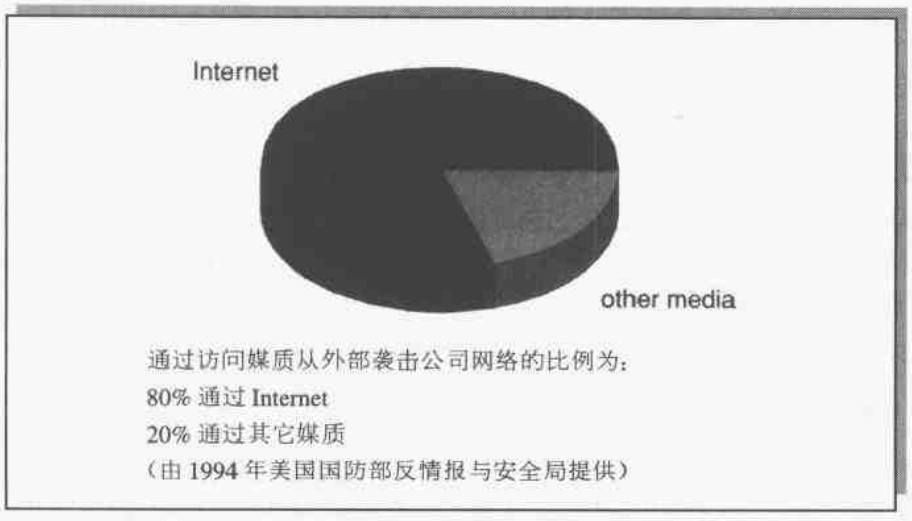


图 1.3 计算机犯罪：访问媒质

1.4 Internet 风险分析

风险分析是用来确定 Internet 风险给公司带来损失的程度。

1.4.1 定义“风险”

DIN VDE 标准（德国工业标准）将“风险”（“risk"）定义为：

- 如果事故发生，预计损失的程度（DIN85）
- 预测事故发生的概率

近几年，随着计算机系统的不断普及，上述风险的两个方面已有极大增加。人们大量利用信息资源，由于访问未被授权的内部资料与通信系统而引发的破坏显著上升。Internet 安全事故的数量与破坏发生的概率今后将增加的更快。

1.4.2 风险分析的基本原则

一般说来，风险分析划分为四个阶段：

(1) 确定分析的范围
(2) 找出风险
(3) 评估风险
(4) 分析结果

1.4.2.1 确定范围

第一步，首先划分风险分析所覆盖的区域。由于风险分析复杂，就不能在整个 DP（数据处理）系统上进行，而只能在单个区域内。因此，只能在单个分析区域间确定界面。后续

章节给出划分的结果。

1.4.2.2 找出风险

第二步是找出风险。这需要详细地描绘所有现存的风险，并调查风险的影响结果。分析风险采用以下两种方法：

- 风险情况分析
- 模拟研究

若用风险情况分析，就需将引起安全事故的假设事件集中在一起（处在同一界面上），通过对主要情况的研究，较快地得到原始结果。另一方面，若用模拟研究，通过如实反映所分析区域的情况，模拟潜在风险所带来的影响，最后查出风险所在。上述两种分析方法都较昂贵且费时，并且还涉及到特殊软件（比如来自 Siemens Nixdorf 中的 ASIS）。

1.4.2.3 风险评估

第三步为风险评估。它是在对风险发生的概率及潜在损失的分析和确定基础上进行的。基本的风险评估，就是安全事故带来的损失值（以美元计）乘以一年内事故发生的概率。例如，将基本风险评估应用于假设全部数据丢失引起网络崩溃的事故中。

- 数据丢失带来的直接与间接损失值为：25000000 美元
- 概率：1/10(10 年一次)

基本的风险评估为：25000000 × 0.1=2500000 美元 / 年。

基本的风险评估系统常采用统计表格和范畴分类来帮助确定风险事件。结果表明精确度并没有太偏离现实生活。该评估主要用在美国，可利用许多适合的风险分析软件包（比如 BDSS、Bayesian 判决辅助系统，OP&S）。

常规的风险分析借助于列表和矩阵，首先将信息系统分解为可确定风险的客体。与基本分析方法相反，对风险不做精确计算而是按范畴分类。比如划分为可接受的风险、不可接受的风险、非常不可能及非常可能发生的风险等。

1.4.3 风险分析：网络问题及数据完整性破坏所带来的损失

由于人们经由 Internet 进行互访，就潜在着许多安全事故，通过对此类事故的最初评估，就能估计网络崩溃和数据完整性破坏所带来的损失值。

从 80 年代末以来，有效的数据通信基础设施对几乎所有的公司来讲，都是生死攸关的问题。计算机系统一旦出现问题和崩溃，不管怎样，就会立刻造成极大的损失。在最近 10 年内，每次网络瘫痪所造成的损失呈逐年增长趋势（图 1.4）。

尽管现在计算机网络停工期的平均时间为十年前的十分之一，但伴随更多富有弹性的操作系统与更复杂的硬件设施的采用，使得损失的价值大大提高。当然，这也是由于公司更加依赖数据通信技术的结果。1989 年，网络停工期所带来的损失为每小时 3500 美元，到 1993 年，已上升到 52000 美元。

目前，几乎所有公司的重要数据都贮存在计算机上，保证数据记录的完整性也愈加显的重要。在最近五年内，许多公司都借助于网络化 PC 机开展业务，这一状况带来了两个主要

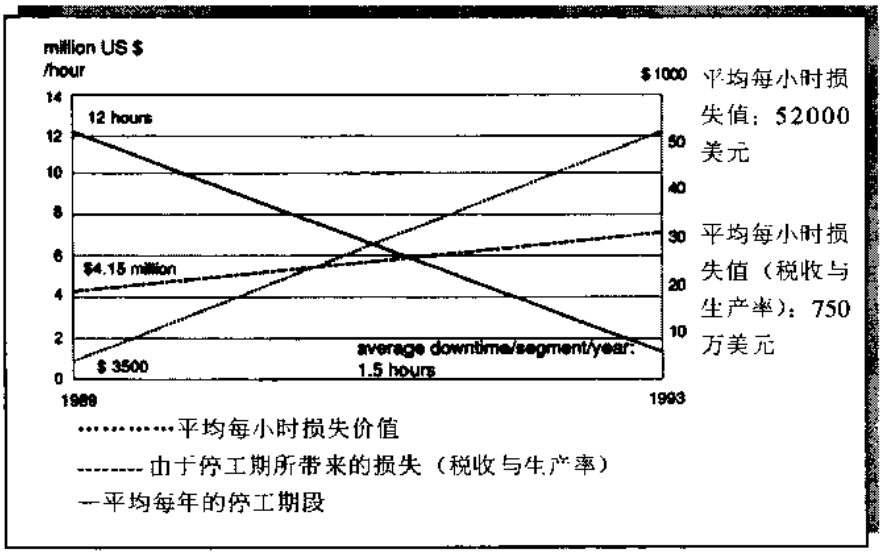


图 1.4 1989 年以来公共网络停工期的损失价值

风险：第一，强大的工作站好比是巨大的集中器，将大量的数据集中在一起，一旦系统数据丢失或受到破坏，就会丢失大量数据，并且数据越集中，丢失的也就越多；第二，越来越多的用户经由 LAN（局域网）访问数据，这使得要做到可靠地确认用户，并确保用户仅访问被批准的数据是很困难的，与此同时，一旦潜在侵袭者侵入公共网络，便可随意访问所有的系统。

1989 年，仅有 1/5 的 PC 机联网，而今天已超过 50%。UNIX 工作站已取代许多专用计算机，但其强大的存储能力与开放式操作系统却成为侵袭者袭击的潜在目标。

尽管这一转变引起的安全事故，过去一直主要是由于内部的原因，但随着计算机都涌向

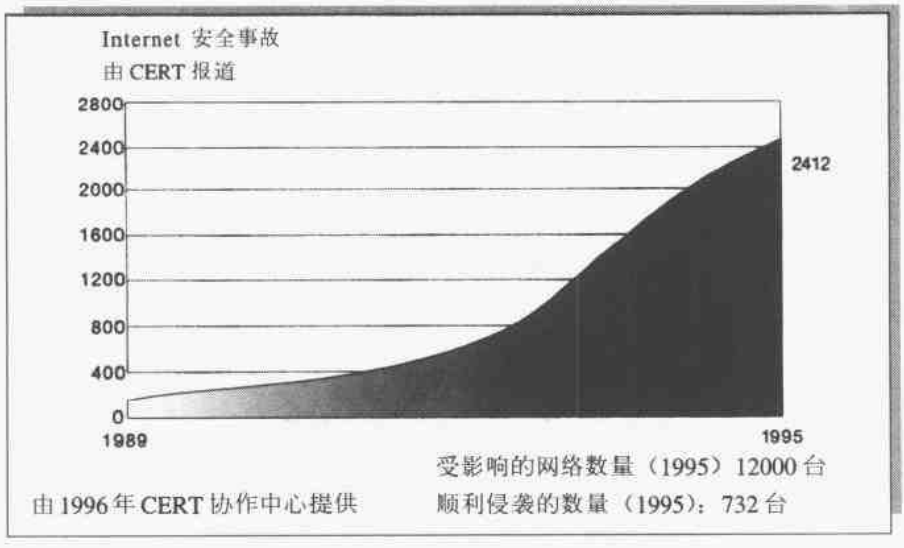
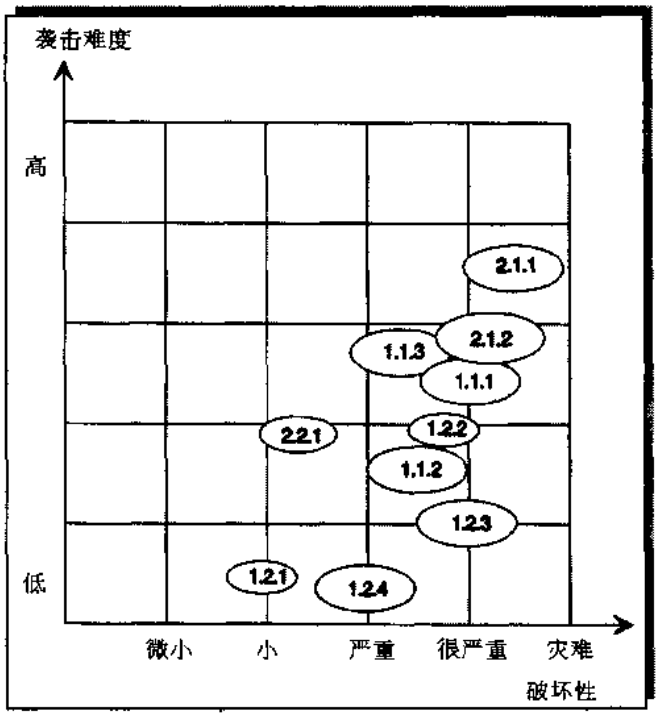


图 1.5 1989～1994Internet 安全事故的数量

与公共数据网络连接，从各个方面来看，该安全问题将会变得日益突出。

1.4.4 风险发生的概率

经由Internet 越权侵袭计算机系统的事件逐年增加，基本上与计算机数量的快速增长相同步。1988年，ARPA（高级研究项目署）成立了Internet 安全组织CERT（计算机紧急情况处理小组）。据CERT报道，1989年仅有132起计算机安全事故，到1995年安全事故的数



1 内部袭击：
1.1 未授权访问公司数据（插入、删除，破坏数据）
1.1.1 通过认证系统破坏
1.1.2 NFS 袭击
1.1.3 X-Windows 袭击
1.1.4 …
1.2 网络基础结构的破坏
1.2.1 网络过载的发生
1.2.2 对网络部件的袭击(ICMP 袭击、路由袭击)
1.2.3 对物理网络基础结构的破坏(hubs、路由器等)
1.2.4 病毒感染
1.3 机密信息的丢失
1.3.1 网络嗅探器
2 外部袭击(Internet，拨号线等)
2.1 未授权访问公司数据（插入、删除、破坏数据）
2.1.1 TCP 序号袭击
2.1.2 路由袭击
2.2 网络基础结构的破坏
2.2.1 网络过载的发生

图 1.6 数据网络的风险分析

量已多达2412起，共有12000多个网络受到影响。实际数字也许还要高几倍。美国NCCC（“计算机犯罪国家中心”）估计，发现的计算机犯罪仅为1%，上诉到法庭的也只有14%。

美国国防部(DoD)信息服务局，通过对自身计算机系统的多次调查，证实了上述结论。他们有计划企图入侵8932台服务器和计算机，其中有7860种情况获得成功，被发现了的仅390种情况，而只报道了19种情况。

许多正在使用Internet的计算机侵袭者利用高性能、复杂的代理软件有计划地寻找系统中的安全漏洞。几个小时内，侵袭者可查找几百个网络和计算机系统的脆弱点，以找到适当的袭击办法。

许多情况下，侵袭者输入一完整的Internet 地址范围（通过Internet 地址扫描器获得），在几天的时间内，可完成安全漏洞的系统调查。

侵袭者可轻而易举地改变了网络化DP基础设施的正常工作，而这对英国哥伦比亚大学的系统管理员来说，发现它们却很困难。1995年3月，在四千多台计算机上发现了“Sniffer”（嗅探器）程序，该程序可自动地捕捉口令。到发现时为止，已有三千多个口令被泄露出去。

1.5 风险的详细分析

利用风险矩阵，我们可进行详细的风险分析，使具体评估安全风险给公司带来损害的程度成为可能。潜在的安全事故可看作是损害程度和所发生事故概率的函数。

每种闯入事件的概率都与所用的计算机和网络系统、现有的基础设施（外部数据线、联网情况、拨号网等），以及现有的安全保护措施（防火墙、拨号应答等）有关。影响基本安全风险的其它因素有：

- 公司的运作情况是潜在指标（产品、竞争者等）
- 公司所处的位置
- 公司规模和员工数量

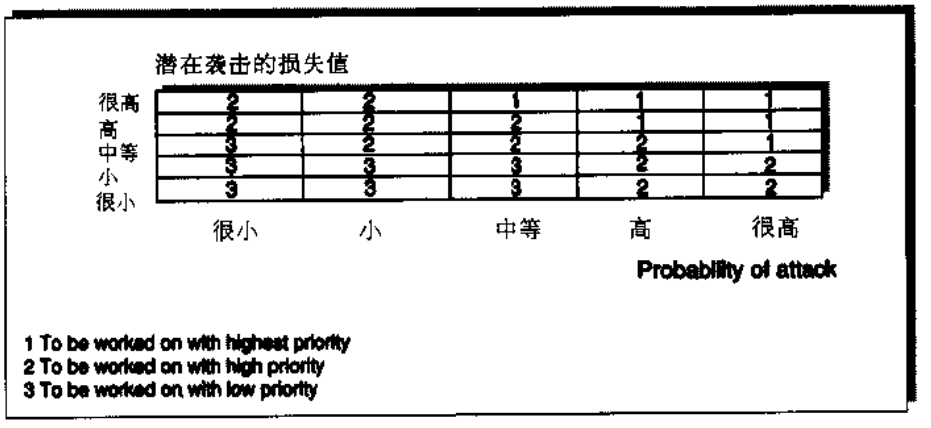


图 1.7 潜在袭击的概率和损失价值关系