HZ BOOKS

UNIX
实用工具
译丛

SSH

UNIX Secure Shell

工具

UNIX Secure Shell

(美) Anne Carasik 著

张 蓬 匡 巍
张建杰 陈水珑 等译
徐国平 王 军 审校

机械工业出版社
China Machine Press

McGraw-Hill

UNIX实用工具译丛

SSH：UNIX Secure Shell工具

(美) Anne Carasik 著

张 蓬 匡 巍 等译
张建杰 陈水珑

徐国平 王 军 审校

机械工业出版社
China Machine Press

随着网络的不断发展，网络的安全也变得越来越重要。本书针对这一问题专门介绍了Secure Shell(SSH)工具。SSH包括三个主要部分：UNIX进程、TCP/IP网络以及加密。它改善了UNIX的不足，并使安全性管理的复杂程度降到很低。本书从一名系统管理员和使用者的角度出发，教你如何最大程度地利用Secure Shell，让你了解它的功能和安装配置过程。本书共分五个部分：第一部分“获得并安装Secure Shell”；第二部分“Secure Shell 1”；第三部分“Secure Shell 2”；第四部分“Secure Shell的高级使用”；第五部分“附录”。通过这五部分的学习，读者就可以完全掌握SSH的使用。

版权登记号：01-1999-3672

图书在版编目(CIP)数据

SSH: UNIX Secure Shell工具 / (美) 卡雷西克 (Carasik, A.) 著；张蓬等译. -北京：机械工业出版社，2000.8
(UNIX实用工具译丛)
书名原文：UNIX Secure Shell
ISBN 7-111-08122-6

Ⅰ.U… Ⅱ.①卡… ②张… Ⅲ.UNIX操作系统 Ⅳ.TP316.81

中国版本图书馆CIP数据核字(2000)第32866号

机械工业出版社(北京市西城区百万庄大街22号 邮政编码 100037)
责任编辑：瞿静华
北京昌平第二印刷厂印刷·新华书店北京发行所发行
2000年8月第1版第1次印刷
787mm×1092mm 1/16·11.75印张
印数：0 001-6 000册
定价：35.00元(附光盘)

译 者 序

UNIX操作系统自1969年在AT&T Bell实验室诞生以来，迄今已有近30年的历史。UNIX以其简洁而且强大的优点成为当前应用领域最为广泛的主流操作系统之一。实践表明，UNIX系统一直是当前重点行业和关键事务领域的可靠平台。它作为高端的解决方案，正与其他操作系统协同工作，处理着大大小小的IT事务。

随着Internet的迅猛发展，出现了越来越多的网络应用程序。然而，实践表明，许多网络应用程序并不像人们想象的那样安全。这样，如何确保在新的工作环境下的工作安全就成为许多从事网络维护与管理的人员所必须关注的一个重要问题。通常情况下，系统管理员必须使用一整套网络管理软件来维护他们的系统。而由于许多安全管理软件过于复杂，使得维护和管理成为一件令人头疼的事。在这些管理软件中，Secure Shell(SSH)正以其简洁和高效逐渐为系统管理员和公司的首席信息执行官们所青睐。SSH适用于几乎所有的UNIX平台——包括HP-UX、AIX、Solaris、Digital UNIX、Irix、Linux、SCO。它简单易用，无需太多的培训即可掌握。为了帮助UNIX环境的系统管理员能尽快熟练掌握安全Shell的使用方法，我们组织翻译了这本《UNIX Secure Shell》。

本书将从一名系统管理员和使用者的角度出发，教你如何最大程度地利用Secure Shell。在此基础之上，还有专门一章来解答疑难问题，这些问题都是些已经发现的常见问题。全书共分为五部分：第一部分介绍关于Secure Shell的预备知识，包括如何获得并安装Secure Shell；第二部分介绍Secure Shell 1的内容，这部分的介绍将有助于熟悉该环境；第三部分则是对Secure Shell 2的描述；在此基础之上，第四部分介绍了Secure Shell的高级使用，对如何使用Secure Shell实现多种附加功能进行了深入的探讨。第五部分附录将提供一些有关加密的背景知识，包括加密技术的基础知识、术语以及相关的法律问题。

本书是作者多年经验的结晶、内容丰富，由浅入深，实用性强。特别是书中给出了大量的有价值的代码实例，读者可以在自己的机器上运行它们，从而能尽快地熟悉Secure Shell环境。本书适于自学，具有不同应用背景的读者都可以从中获益。

我们在尊重原著的基础上，力求准确、严谨地翻译本书。但由于时间仓促，加上译者水平有限，书中难免有错误或不妥之处，敬请读者批评指正。

本书由匡巍(1～3章)、张蓬(4～5章)、陈水珑(6～7章)、张建杰(8～10章)、刘璐(附录)等翻译，徐国平、王军审校。在此感谢中国UNIX用户协会(CUUG)UNIX培训中心给予的支持和帮助。

译 者

2000年3月

序

在过去的五年中，Internet发生了爆炸性的变化并开拓了崭新的市场。对于那些富于勇气尝试新事物和新方法的人们来说，只要有足够的想象力就意味着有无数的机遇。数百万的人涌向Internet，无论是作为客户还是为客户提供服务与商品的商家，都从中获取到许多好处。其结果是电子商务的涌现并成为新千年的技术引擎。

与已经逝去的19世纪中曾经魔术般地出现的黄金一样，新世纪的信息巨流带来的不仅是新的机遇，也包含了新的风险。与旧时的强盗及梁上君子一样，黑客们正给那些不在意的和缺乏准备的人的生活增添很多烦恼。简而言之，欺骗无所不在。一旦你在某时拥有了一个功能性的站点，下一分钟你就可能因交易列表的消失而困惑不已。在网上从事商业活动实在是一件使人感到不踏实的事情。

为了解决这些问题，对网络性能的需求促使分布式系统及分布式管理技术得以诞生。如果你想保持你的工作不受侵害，就必须使用安全技术。对那些并不十分精通技术的人来说，向他们解释清楚造成管理过程崩溃的安全漏洞是一件非常困难的事情。财务经理及首席执行官就是这样的人。对于他们来说，出了事就是你的错误和责任。任何的意外事件都会使你感觉自己像一个傻子，而且很有可能，是一个将失业的傻子。

作为系统管理员，我们意识到我们的生活是一个搜集使我们的工作富于效率的工具的过程，无论这些工具是什么样的。现在，我们必须将安全工具加进这个工具清单中了。这样，我们就不必再担心由黑客造成的让人烦恼的系统崩溃了。Secure Shell，或SSH，是一个能使我们的工作更为安全的工具。

许多操作系统都有内建的工具，用以使系统的使用者能方便地工作。例如远程登录、文件拷贝和Shell等。每个工具都具备进一步开发的能力。最普遍的，如伯克利(Berkeley)的远程命令集就为系统管理员提供了一套基本的工具，可以长时间方便地管理整个企业网。

遗憾的是，伯克利的这套命令集广为人知，这就使得它像一颗一触即发的地雷一样危险。工具毕竟是工具，作为工具，r命令当然要面向大众。实际上，r命令集仿佛是一套螺钉旋具，功能齐全并且分工明确。当你要上螺丝或干类似的活儿时，它们使起来一定很顺手。但是人们还希望它们能作为榔头或钳子使用。而Secure Shell正如一把多功能瑞士军刀一样。Anne很好地描述了Secure Shell的功能和它的安装和配置过程。你将学习什么是Secure Shell，它能做什么，以及它不能做什么。此外，通过举例，Anne还将带你一起经过整个安装和配置过程，并且列出了实际操作的细节。本书同时还介绍了SSH1和SSH2，其中命令选项的一些特殊细节也将述及，以及如何与主机命令一起来创建一个健壮的会话或者一个不太健壮的会话。

Mark S.Kadrich

前　言

关于这本书

你可能已经意识到有太多的网络应用程序是不安全的。所幸，本书并不是讲那些不安全的应用程序的，相反，是讲如何去替代它们。

太多的安全管理应用程序过于复杂，使得维护和管理成为一件令人头疼的事。Secure Shell不会让你头疼，事实上，它使安全性管理的复杂程度降到最低，你无需经太多的培训就可以胜任，并且使得维护和管理尽量简化。

本书将向你介绍Secure Shell是什么和不是什么，并且如何执行它。因此，本书对你的重要性就在于：通过使用Secure Shell将使你的网络会话更加安全。Secure Shell非常类似一把瑞士军刀，使用它，可以干许多你不曾想到过的事。

SSH通信安全小组的Tatu Ylonen重写了这个程序，当时是1995年7月，他还只是赫尔辛基技术大学的一名研究人员。Tatu编写了一个安全的应用程序来替代许多今天仍然在UNIX网络上使用的不安全的应用程序。

Secure Shell包括三个主要部分：UNIX进程[⊖]、TCP/IP网络以及加密。它弥补了众所周知的UNIX的弱点，诸如伯克利提供的一些服务(应用)，或者是 r 命令。r 命令虽然提供了两个系统之间无缝的连接，但它有一个重要缺点：非常差的身份认证，以致几乎可以被任何人所蒙骗。Secure Shell可以用来替代 r 命令，还可以替代Telnet和FTP。

但是，使用Secure Shell仍然难以防范会话截取和IP欺骗等技术。因此它提供了加密技术作为一种可靠的手段以确保你安全地登录。这就好像指纹认证一样，你可以被识别，而别人却很难冒充你的身份。并且，加密技术还防止有人截获你的网络连接信息，如你输入的个人电子邮件[⊜]或密码。

本书将从一名系统管理员和使用者的角度出发，教你如何最大程度地利用Secure Shell。而且，还用一章专门来解答疑难问题，这些问题都是一些已发现的常见问题。

还有大量与Secure Shell有关的附加资源可以帮助你。从Web网页到Usenet组你都可以找到各种信息，你还可以通过邮件列表或从网上获得帮助。

另外，你还可以了解Secure Shell不能干什么。Secure Shell并不会加固你的系统或网络——你不得不自己去做相应的工作。Secure Shell没有去除 r 命令和Telnet，它起到信息的传送作用——从本地客户端传送到另一种类型的网络客户端，如POP、DNS或PPP。

可喜的是：Secure Shell几乎可以运行在各种类型的UNIX之上。随着Linux(一种UNIX的自由软件)变得越来越流行，Secure Shell也越来越成为一种保护我们系统至关重要的产品。Secure Shell不仅可以防止入侵者截取你的密码和你的会话内容，还为你在运行网络应用程序时提供了一套可自行设置的安全性保护。

⊖ 是的，Secure Shell还可以运行在多种操作系统之上，如Windows、OS /2等等。

⊜ Secure Shell并不能替代PGP。如果你给自己的信件加密，请使用PGP，可以在以下网址得到它：http://web.mit.edu/network/pgp.htm。

适用对象

本书适用于UNIX系统和网络管理员，也适用于那些在编写脚本或代码时使用Secure Shell的程序员。然而，本书并不深入讨论Secure Shell代码的修改,因为这已超出管理的范畴。

如果你是一位网络或安全顾问，本书将是你最合适的参考书，它将告诉你如何使用Secure Shell以及它能做什么。而且，如果你需要在许多地方实现Secure Shell，那么本书也会有助于你。

如果你有UNIX系统管理和网络的基本技能，那么你会做得更好。你无须知道加密是如何实现的——基本的加密知识可以参考附录A“加密技术基础”以及附录B“国际加密技术法律”。

我想提醒大家的是，本书并不专门讨论如何在Window95、NT以及其他平台上使用Secure Shell。SSH为Windows和其他平台提供有许多不同的工具，所以本书只能是讨论各种工具，而不是SSH程序本身。

本书的结构

本书被分为五个部分：“获得并安装SSH”、“Secure Shell 1”、“Secure Shell 2”、“Secure Shell的高级使用”和附录。这五个部分可以帮助你安装Secure Shell，学习SSH1和SSH2的使用和一些高级应用，包括密钥管理(key management)，如何与防火墙一起工作以及端口转发(port forwarding)。

第一部分：获得并安装SSH

这部分包括两章，即Secure Shell的介绍和在UNIX下安装Secure Shell。这两章为你提供了预备知识。

第1章：什么是Secure Shell? 本章将介绍Secure Shell是什么？它能保护什么和它不能保护什么，r命令与Secure Shell的s命令的不同点。

第2章：在UNIX上安装Secure Shell。 如果你还没有安装Secure Shell，本章将介绍有关内容，包括从编辑配置文件到如何安装Secure Shell应用程序。还包含如何设置各种配置开关和适用的附加功能，如SOCKS、TCP包和RSAREF。

第二部分：Secure Shell 1

这部分包括两章，涉及到Secure Shell的第一种实现，即SSH1。它包含了客户端和服务器端两方的使用。第3章和第4章将帮助你熟悉SSH1环境。

第3章：Secure Shell 1服务器守护进程——sshd。 如果你希望了解Secure Shell 1的服务器守护进程(sshd)的工作原理及基本操作，本章将向你介绍一些基本知识，同时还为你提供了一些基本配置实例。还有一些语法示例，教你如何在实时环境中使用sshd。

第4章：Secure Shell客户端——ssh和scp。 本章阐述Secure Shell 1客户程序(ssh和scp)的工作原理和基本操作。同样也列举了一些基本配置实例和应用实例，以演示启动客户程序并运行它。你也会找到一些包含语法的例子，并学会如何在实时环境中使用ssh和scp。

第三部分：Secure Shell 2

这部分包括两章，介绍Secure Shell的第二种实现——SSH2。也包含了客户端和服务器端

两方的使用。该工具有一个IETF的草稿(draft)，可以在以下网址得到：http://www.ietf .org /ids .by.wg/secsh.html。

第5章：Secure Shell 2服务器守护进程——sshd2和sftp-server2。如果你希望了解Secure Shell 2服务器守护进程的工作原理及基本操作，本章将向你介绍一些基本知识。本章还列举了一些语法示例，并教你如何在实时环境中使用sshd2和sftp-server2。同时也列举了一些基本配置实例。

第6章：Secure Shell 2客户端——ssh2、scp2和sftp2。本章阐述了Secure Shell 2客户程序(ssh2、scp2和sftp2)的工作原理和基本操作。这里也列举了一些基本配置实例和应用实例，以演示启动客户程序并运行它。同样可以找到一些语法示例，并学会如何在实时环境中使用ssh2、scp2和sftp2。

第四部分：Secure Shell的高级使用

当你已经具备了Secure Shell的服务器守护进程和客户程序的基本知识以后，这部分将深入讨论如何使用Secure Shell实现多种附加的功能。其中包括SSH密钥管理，使SSH同防火墙一起工作，以及用SSH完成一些很酷的事情。

第7章：Secure Shell密钥管理。本章介绍了SSH1和SSH2的密钥管理内容。涉及主机密钥(host key)、服务器密钥、用户密钥、密钥的生成和身份认证代理。此外，本章还介绍了这些密钥的配置文件。

第8章：Secure Shell与防火墙。如果你有兴趣把SSH和防火墙结合起来或让SSH透过防火墙进行发送，本章会对你有所帮助。它定义了防火墙，阐述如何为SSH的防火墙定义一套规则，以及SSH和防火墙的一些用途，如创建一个伪VPN和使用SOCKS。

第9章：Secure Shell能做的其他事情。现在你已经了解了SSH的基本知识，你可以学习利用SSH来做一些很酷的事。如你可以转发不同类型的TCP应用，包括X、POP、FTP、Telnet、DNS和其他一些基于TCP的应用。你可以学会如何使SSH和TCP包装(TCP wrappers)协同增强网络的安全性。另外还有远程备份和其他非SSH默认的身份认证方法。

第10章：排除Secure Shell中的错误。你一次又一次地想使SSH运行起来，但一次次地都失败了。本章将向你介绍如何使SSH顺利地工作起来，给你解释一些奇怪的现象，并帮助你排除一些可能遇到的问题。

第五部分：附录

附录将向你提供一些有关加密的背景知识，包括一些基础知识、术语和你可能会碰到的法律问题、当然得看你在哪个国家了。而且，你还会看到有一部分是关于获取其他版本的SSH的方法，这些版本在本书所附带的光盘中没有提供，因为那涉及美国有关RSA的专利法规。此外，光盘中还有SSH1、SSH2和其他一些商业软件的注册信息。

附录A：加密技术基础。解释加密技术的一些基础知识。

附录B：国际加密技术法律。围绕加密技术的出口问题，涵盖了当今与加密有关的法律问题。

附录C：加密技术术语一览。定义解释了你所不熟悉的烦人的加密术语。

附录D：光盘内容介绍。告诉你在光盘上可以找到什么。

如何与作者联系

我非常乐于听取有关本书的反馈意见，我希望下一版编得更好。就我所能提供的帮助而言，有关技术支持请不要找我联系——恕我没有足够的时间来回答那么多的email。请访问站点comp.unix.ssh或利用SSH的技术支持地址表，该列表上有许多优秀的人士会解答你所遇到的问题。如果你有兴趣同我联系的话，可以采用传统的信函方式由McGraw-Hill出版社转交。

或者，如果你更喜欢利用计算机的话，可以通过以下email地址和我联系：stripes@tigerlair .com。

目　录

第四部分 Secure Shell的高级使用

第五部分 附 录

第一部分　获得并安装SSH

第1章　什么是Secure Shell

本章内容如下：

- 为什么使用Secure Shell?
- Secure Shell的安全保护功能是如何实现的?
- Secure Shell不能保护什么?
- s命令与r命令的比较。

通过本章，你将看到：使用SSH的好处并对它的工作过程有一个总体的认识，伯克利的r命令和SSH的s命令的比较，以及通过SSH可以提高系统的安全性。你还会看到一些基于UNIX的例子，包括网络和系统命令。如果你感到有必要复习加密的有关知识，可以参阅附录A“加密技术基础”。

1.1　为什么使用Secure Shell

既然你已经购买了本书，你一定很想知道SSH的高明之处。Secure Shell，又可记为SSH，最初是UNIX系统上的一个程序，后来又迅速扩展到其他操作平台。本章将说明SSH是一个多么好的应用程序，以及在正确使用时，它是如何弥补网络中的漏洞的。除此以外，SSH之所以酷，还有以下原因：

SSH客户端适用于多种平台。几乎所有的UNIX平台——包括HP-UX、Linux、AIX、Solaris、Digital UNIX、Irix、SCO，以及其他平台——都可以运行SSH。而且，已经有一些客户端(其中有些为测试版)可以运行于UNIX操作平台以外，包括OS/2、VMS、BeOS、Java、Windows95/98和Windows NT。这样，你就可以在几乎所有的平台上运行SSH客户端程序了。

对非商业用途它是免费的。许多SSH版本可以获得源代码，并且只要不用于商业目的，都可以免费得到。而且，UNIX版本也提供了源代码，这就意味着任何人都可以对它进行修改。但是，如果你选择它用于商业目的，那么无论使用何种版本的SSH，你都得确认已经注册并获得了相应权限。绝大多数SSH的客户端和守护进程都有一些注册限制。惟一的SSH通用公共注册(General Public License，GPL)版本是lsh，它目前还是测试版。

通过Internet传送密码安全可靠。这是SSH被认可的优点之一。如果你考察一下接入ISP(Internet Service Provider，Internet服务供应商)或大学的方法，一般都是采用Telnet或POP邮件客户进程。因此，每当要进入自己的账号时，你输入的密码将会以明码方式发送(即没有保护，直接可读)，这就给攻击者一个盗用你账号的机会——最终你将为他的行为负责。

对应用的支持。由于SSH的源代码是公开的，所以在UNIX世界里它获得了广泛的认可。Linux，其源代码也是公开的，大众可以免费获得，并同时获得了类似的认可。这就使得所有开发者(或任何人)都可以通过补丁程序或bug修补来提高其性能，甚至还可以增加功能。这也

意味着其性能可以不断得到提高而无须得到来自原始创作者的直接技术支持。

SSH替代了不安全的远程应用程序。SSH是设计用来替代伯克利版本的r命令集的；它同时继承了类似的语法。其结果是，使用者注意不到使用SSH和r命令集的区别。

利用它，你还可以干一些很酷的事。通过使用SSH，你在不安全的网络中发送信息时不必担心会被监听。你也可以使用POP通道和Telnet方式，通过SSH可以利用PPP通道创建一个虚拟个人网络(Virtual Private Network, VPN)。SSH也支持一些其他的身份认证方法，如Kerberos和安全ID卡等。在第9章“Secure Shell能做的其他事情”中，我们会探讨更多的细节。

1.1.1 SSH能保护什么

SSH可以防止IP地址欺骗、DNS欺骗和源路径攻击。SSH提供给用户身份认证的主要方法就是使用公共密钥加密法。根据所用SSH版本的不同，可以采用RSA或者Diffie-Helman和数字签名标准来实现。也可以选择使用各种不同的身份认证方法，包括公共密钥法、rhosts/shosts认证法和密码认证，这些方法都很简单安全。的确，利用SSH即便是使用.rhosts认证方式也能确保安全性。

SSH所提供的是通过网络进入某个特定账号的安全方法。每个用户都拥有自己的RSA密钥。通过严格的主机密钥检查，用户可以核对来自服务器的公共密钥同先前所定义的是否一致。这样就防止了某个用户访问一个他没有相应公共密钥的主机。

注意　如果你想了解更多有关RSA、公共密钥加密和身份认证的知识，可以参考附录A“加密技术基础”。

只需进行很小的修补，SSH就能保护一些不安全的连接，如X或POP。这将帮助你提高所管理的网络连接的安全性。

由于SSH提供了主机身份认证，利用公共密钥而不是IP地址，所以它使网络更加安全可靠，并且不容易受到IP地址欺骗的攻击。这有助于辨认连接到你系统上的访问者身份，从而防止非法访问者登录到你的系统中。

如果用户或系统打算采用rhosts/shosts的身份认证方式，主机就面临着公共密钥和私人密钥信息交换的挑战。否则，就得使用其他认证方式。在认证发生之前，会话已经通过对称密钥技术进行了加密，如DES、三重DES、IDEA、Twofish或Blowfish。这就使得会话自身被加密，从而防止了别人在你输入或同别人聊天时截取你的信息。同时也意味着你所输入的密码不会被他人读取，因为它也被加密了。加密技术基本上可以防止有人监听你的数据，同时也确保了数据的完整性，即防止有人肆意篡改你的信息和数据。表1-1列出了SSH所能保护的网络攻击。

表1-1　SSH保护的网络攻击类型

网络攻击类型	内　容
包欺骗	某IP包并不是你的，但被伪造成了你的
IP/主机欺骗	IP或主机名被别人使用了
密码截获	有人从网上读到了含有你密码的包
侦听	有人从网上读取你的包，分析其内容

在各种类型的加密技术当中，IDEA是一种运算速度较快的密钥，并为SSH所采纳。由于

注册问题，IDEA的应用在欧洲受到了限制。如果你不能使用IDEA，那么Blowfish和Twofish也可作为快速密钥来使用。此外，DES的应用比IDEA、Blowfish和Twofish都更为普遍。即使是存在可以在数小时内攻破DES的最新解密技术，也不用担心，因为这种解密技术需要价值25万美金的昂贵的并且是专门设计的计算机。

正如前面所讲，SSH使用公共密钥加密技术来执行身份认证，它有两种形式：DSA和RSA。RSA用在SSH 1.5协议中，规定密钥交换和公共密钥身份认证。在SSH 2.0协议中，DSA用于公共密钥身份认证，Diffe_Helman用于公共密钥交换。如果你所用的是SSH 2.0协议的商业版，也可以使用RSA来进行身份认证。

现在你已明白了SSH能够做什么以及它是如何工作的，那么它所不能做的又是什么呢？

1.1.2 SSH所不能保护的

尽管SSH提供了大量的安全措施，但它仍不能为你的系统提供完全的在线保护。SSH并不能堵住所有其他端口上的全部漏洞。如果有人通过Telnet攻击你的网络，端口号为23，SSH就不能提供安全保护，因为SSH运行在另外一个端口。另外一个例子是NFS(Network File System，网络文件系统)，其安全性已经声名狼藉了。如果有人借助NFS安装了根目录，那么你的计算机就会很危险。

为表明如何使用SSH，让我们来建立一个小型网络。有一个名为tigerlair.com的网络，其中包括sherekhan、tigger、litterbox和hobbes，并且sherekhan为防火墙，litterbox用于测试。在此受托网络之外，Internet中另有isp.com、work.com和purdue.edu等网络，如图1-1所示。

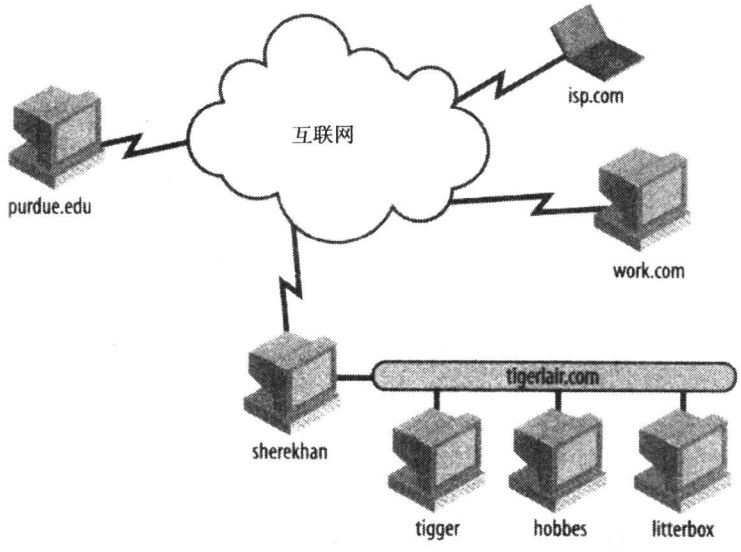

图1-1 我们的网络

分析一个来自网络的攻击：我们假设攻击者通过自己的ISP账号试图进入名为tigger.tigerlair .com的主机，即我们的邮件服务器。如果防火墙sherekhan.tigerlair.com没有正常配置或允许Telnet通过，那么攻击者就可以强行进入tigger。现在我们有麻烦了，因为有人能够进入我们的邮件服务器，并使用它做非法的email广告。

现在，我们需要消除这种危害。假设希望某些人能够通过Internet访问我们的系统，那么可以使用SSH把他们加入进来。如果允许通过某种协议来访问我们的系统，那么当有人使用其他方式来访问根目录时，我们就能够发现。

如果有人可以进入你的UNIX系统根目录，SSH就不能为你提供保护，因为入侵者可以使用他自己的版本的SSH来替代你的SSH，这样他就可以获取你所有的文件，而SSH的执行和密码就会被绕过或替换。在完全信任任何应用之前，一定要确认你已经封住了系统中易于遭受攻击的漏洞。而且，SSH不能制止特洛伊木马或拒绝服务(denial-of-service，DoS)类型的攻击。

表1-2列出了SSH不能保护的攻击类型。

表1-2　SSH不能保护的攻击类型

攻　击	描　述	攻　击	描　述
NFS安装	通过网络安装文件系统	Internet攻击	危害主机
本地攻击	危害主机	拒绝服务	阻止服务和访问

1.1.3　SSH的工作机制

SSH有两部分：客户端和服务器程序。服务器程序是一个守护进程，它在后台运行且无须任何类型的常规管理，并响应来自客户端的连接请求。客户端提供了用户界面。

服务器端　服务器端包含一个文件，即sshd程序。它通常被放在目录/usr/local/sbin下。服务器端提供了对远程连接的处理，包括公共密钥认证、密钥交换、对称密钥加密和非安全连接本身。对SSH2来讲，用sftp-server来管理安全文件传输的连接。

客户端　客户端包括几个不同的文件。这些文件包括ssh(该文件允许不用登录就可以在一

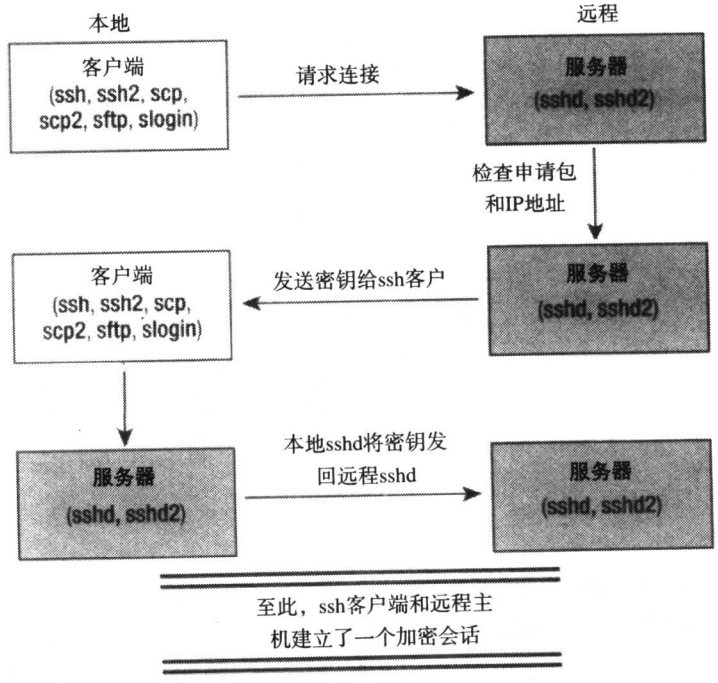

图1-2　SSH服务器和客户端的工作机制

个远程机器上运行你的程序)、远程拷贝(scp)、远程登录(slogin)。SSH2有一个安全文件传输客户端(sftp)，它使用安全文件传输来替代文件传输协议(File Transfer Protocol，FTP)。因为FTP不安全，所以SSH使用自己的客户端替代它。当然，你得在服务器端运行sftp-server。图1-2说明了客户端/服务器连接工作的过程。

1.2 s命令与r命令的比较

现在举例来说明如何使用SSH提供所需的安全策略，以替代其不安全的前身——伯克利版本的 r 命令集。伯克利版本的 r 命令和SSH的s 命令集具有相同功能；然而，SSH比 r 命令提高了安全性。

1.2.1 伯克利版本的r命令集

伯克利版本的r 命令集是UNIX的一个完整的部分。因为UNIX是一个开放的系统，许多人都感到有必要增强系统的安全性。然而，随着越来越多的偏执狂对网络安全漏洞感兴趣，管理人员和使用者渐渐认识到了伯克利版本的r 命令集的问题。

最初，伯克利版本的r 命令集是为了提高Telnet的安全性而开发的，使用时不必在网上以明码方式输入密码(那时它是非常成功的)。r服务也提供了主机名或IP地址认证，Telnet却不能做到这些。r命令的主机名和用户名认证标志着伯克利服务是在网络安全连接方面有着重大影响的一步。

遗憾的是，通过主机名和IP地址认证方式来提高连接的安全性是不可靠的。攻击者开始使用一些已经公开的能够绕过r命令认证机制的IP地址，这就使得攻击者可以从他们自己的主机上发送数据包，并假装是你，而实际上你的系统根本就没有发送这些包，这就是所谓的IP欺骗技术。或者，攻击者可以使用那些有效的IP地址或用户名，从而可以不用密码就进入你的系统。所要做的仅仅是用你的主机名或IP地址重新配置他们的计算机。图1-3表明IP欺骗是如何工作的。

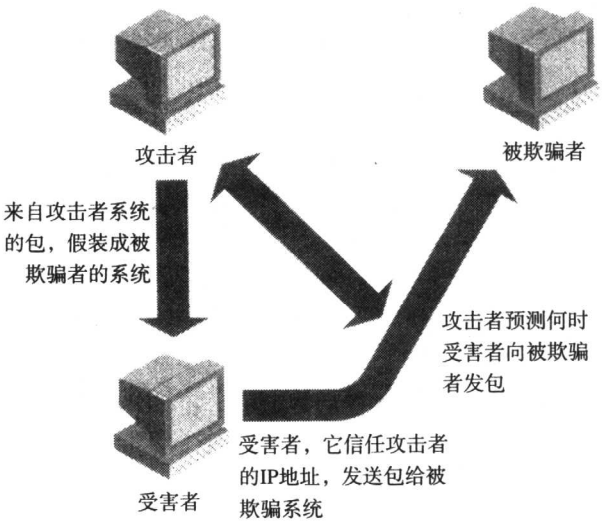

图1-3 IP欺骗

攻击者也可以使用你的DNS，并用他们的DNS服务器冒充你的DNS服务器给你发错误的信息。这就是所谓的DNS欺骗，它可以影响 r 服务的认证。SSH构建在r 命令基础之上，却有着更强大的认证手段。

伯克利版本的r命令引用了一系列的文件，允许与另一个主机建立一种无缝连接。这些命令包括远程登录(rlogin)、远程shell(rsh)和远程拷贝(rcp)。表1-3列出了目前可利用的伯克利服务。