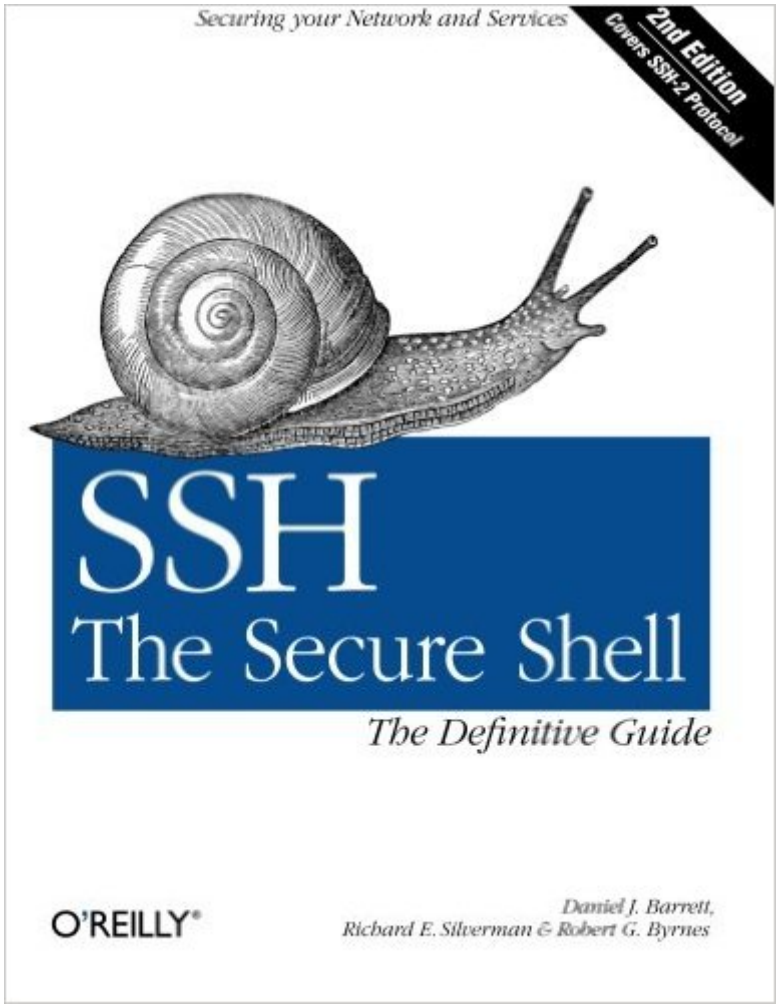
SSH, The Secure Shell: The Definitive Guide



Synopsis

Are you serious about network security? Then check out SSH, the Secure Shell, which provides key-based authentication and transparent encryption for your network connections. It’s reliable, robust, and reasonably easy to use, and both free and commercial implementations are widely available for most operating systems. While it doesn’t solve every privacy and security problem, SSH eliminates several of them very effectively.Everything you want to know about SSH is in our second edition of SSH, The Secure Shell: The Definitive Guide. This updated book thoroughly covers the latest SSH-2 protocol for system administrators and end users interested in using this increasingly popular TCP/IP-based solution.How does it work? Whenever data is sent to the network, SSH automatically encrypts it. When data reaches its intended recipient, SSH decrypts it. The result is "transparent" encryption-users can work normally, unaware that their communications are already encrypted. SSH supports secure file transfer between computers, secure remote logins, and a unique "tunneling" capability that adds encryption to otherwise insecure network applications. With SSH, users can freely navigate the Internet, and system administrators can secure their networks or perform remote administration.Written for a wide, technical audience, SSH, The Secure Shell: The Definitive Guide covers several implementations of SSH for different operating systems and computing environments. Whether you’re an individual running Linux machines at home, a corporate network administrator with thousands of users, or a PC/Mac owner who just wants a secure way to telnet or transfer files between machines, our indispensable guide has you covered. It starts with simple installation and use of SSH, and works its way to in-depth case studies on large, sensitive computer networks.No matter where or how you’re shipping information, SSH, The Secure Shell: The Definitive Guide will show you how to do it securely.

Book Information

Paperback: 670 pages
Publisher: O’Reilly Media; 2 edition (May 20, 2005)
Language: English
ISBN-10: 0596008953
ISBN-13: 978-0596008956
Product Dimensions: 7 x 1.5 x 9.2 inches
Shipping Weight: 2.8 pounds (View shipping rates and policies)
Average Customer Review: 4.1 out of 5 starsÂ Â See all reviewsÂ (40 customer reviews)
Best Sellers Rank: #71,919 in Books (See Top 100 in Books) #4 inÂ Books > Computers &

Technology > Operating Systems > Unix > Shell #10 inÂ Books > Computers & Technology > Networking & Cloud Computing > Intranets & Extranets #60 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security

Customer Reviews

There is a good reason why people write superficial messages on post cards: post cards afford no confidentiality and there is no expectation of privacy. The Internet can be compared to a post card; it is one large system where data is freely interchanged. While common sense tells us that post cards are open to the public, there is a misperception among non-technical Internet users that Internet data is kept private. However, nothing could be further from the truth; on the Wild West net,all data is inherently open and unregulated.There are solutions to this predicament. One solution is called SSH (Secure Shell). SSH provides a way to take that "postcard" and have it securely delivered by a courier.In a nutshell, the book SSH, the Secure Shell: The Definitive Guide expands on two basic ideas: - Privacy is a basic human right, but on today's computer networks, privacy isn't guaranteed. - SSH is a simple idea, but it has many complex parts.But the truth is that the need for privacy and security on today's networks is far too important to be encapsulated in two bullets. This book is so loaded with valuable and important information that anyone using or administering SSH should read it thoroughly.As an introduction, SSH is a protocol that enables secure communications between computer systems that are communicating over insecure channels. SSH is more than simply a point-to-point encryption process such as a VPN. SSH allows users to authenticate themselves to remote hosts. After authentication, users can securely execute commands on a remote machine. SSH fills in for the security deficiencies that are inherent in applications such as telnet, ftp, rlogin, rsh, and rcp.

SSH has quickly become the tool of choice for remotely administering a Unix (or for that matter) Linux computer, replacing telnet, rsh and ftp. This is for good reason, these tools can easily become security holes and it is much easier to keep one tool well maintinaed and secure than a number.SSH gives improved security, both at login and of the data transmitted between computers. SSH offers both security and privacy, rare things online today. It allows secure communications between computers. SSH allows users to authenticate themselves to remote hosts. After authentication, users can securely execute commands on a remote machine. SSH fills in for the security deficiencies that are inherent in earlier methods.SSH was developed in response to the vulnerability to attack in earlier remote login and control methods. Some of these vulnerabilities

include password and protocol sniffing, spoofing, eavesdropping and connection hijacking. Simply, it is the protocol of choice for secure communications between two computers across internet connections.Administering and running SSH can be a pain. As the book points out it is a simple concept with complex parts. It took me a good three or four hours for my first connection to a remote computer and another two to get SSH logins working on my computer. This book was an excellent assist throughout.It covers the three varieties of SSH (SSH 1, SSH2 and Open SSH), giving the differences and benefits of the versions. The book also shows how SSH can be used to secure other protocols, such as POP, SMTP, IMAP, and others.It also gives detailed explanations of what SSH secures against and, perhaps more importantly, what it doesn't secure against.