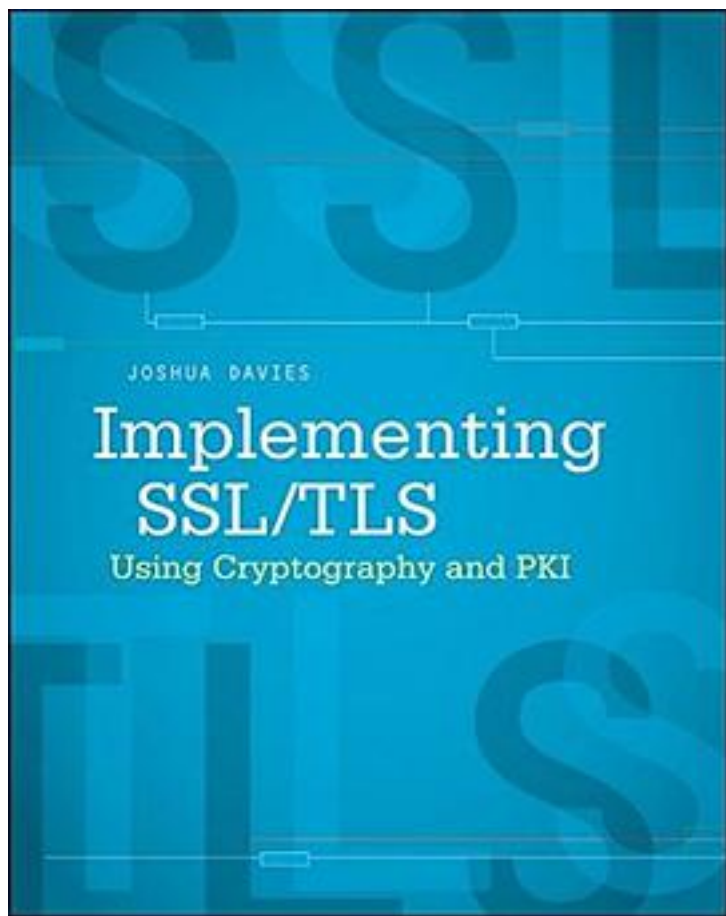


Implementing SSL/TLS



[Implementing SSL/TLS 下载链接1](#)

著者:Joshua Davies

出版者:Wiley

出版时间:2010-12-23

装帧:Paperback

isbn:9780470920411

Hands-on, practical guide to implementing SSL and TLS protocols for Internet security
If you are a network professional who knows C programming, this practical book is for you. Focused on how to implement Secure Socket Layer (SSL) and Transport Layer Security (TLS), this book guides you through all necessary steps, whether or not you

have a working knowledge of cryptography. The book covers SSLv2, TLS 1.0, and TLS 1.2, including implementations of the relevant cryptographic protocols, secure hashing, certificate parsing, certificate generation, and more. Shows network professionals how to implement SSL and TLS using cryptography and PKI Provides specific techniques and strategies, even if you have no prior knowledge of cryptography Covers HTTP, HTTPS, and HTTP proxy support (including how HTTP proxies interact with SSL); symmetric cryptography, including DES, 3DES, AES and RC4, along with CBC, OFB, COUNTER and AEAD Delves into public-key cryptography including RSA, Diffie-Hellman key exchange, and Elliptic-curve cryptography Takes you through digital signature algorithms including RSA, DSA, ECDSA, SHA-1, MD5, and HMAC Includes additional topics, such as X.509 certificates, ASN.1, and more Set up and launch a working implementation of SSL with this practical guide.

作者介绍:

目录:

[Implementing SSL/TLS_下载链接1](#)

标签

TLS

Security

阿男

ssl

阿男推荐

程序世界

安全

programming

评论

[Implementing SSL/TLS 下载链接1](#)

书评

[Implementing SSL/TLS 下载链接1](#)