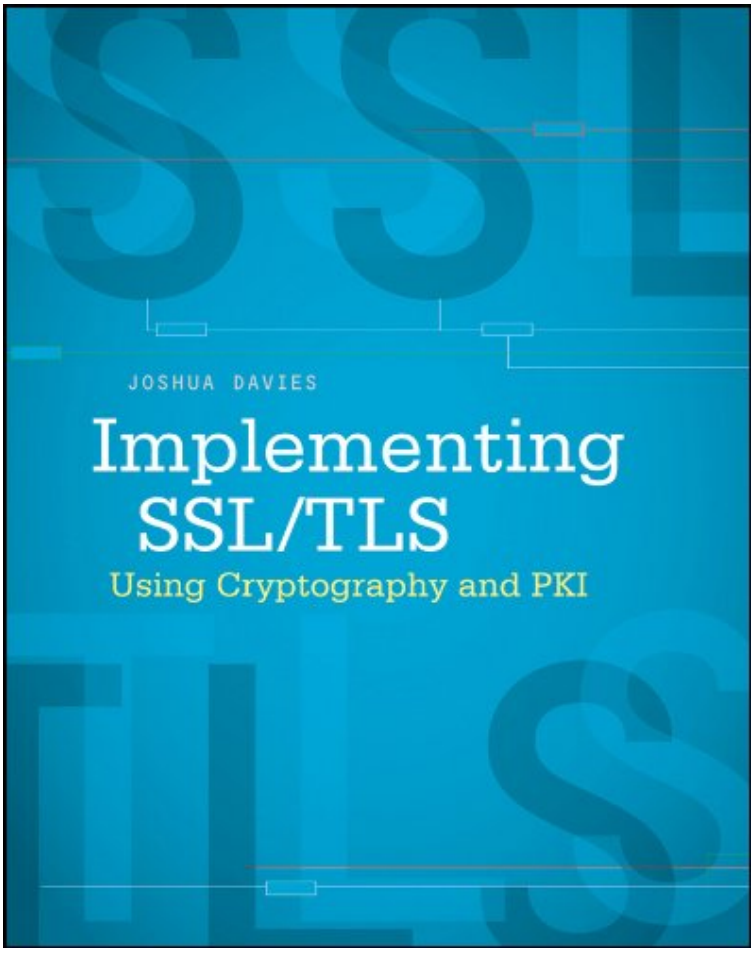
Implementing SSL / TLS Using Cryptography and PKI

Von Joshua Davies
*DOC | *audiobook | ebooks | Download PDF | ePub*



Produktinformation -Verkaufsrang: #419952 in eBooksVerffentlicht am: 2011-01-07Erscheinungsdatum: 2011-01-07File Name: B004IK9TVO | File size: 22.Mb

Von Joshua Davies : Implementing SSL / TLS Using Cryptography and PKI before purchasing it in order to gage whether or not it would be worth my time, and all praised Implementing SSL / TLS Using Cryptography and PKI:

KundenrezensionenHilfreichste Kundenrezensionen2 von 2 Kunden fanden die folgende Rezension hilfreich. A must for any professional TLS related developerVon Victor C.This book is not only an excellent template for developing your own system for secured communication but also the incredible introduction into the basics of the cryptography in the volume minimally sufficient for understanding SSL and TLS.If your challenge is one of the following this is the book for you:1. Deep understanding in the shortest possible time how the secured communication and networks if trust work2. Development of your own or extending an existing implementation of SSL/TLS e.g. for an embedded system or any other where you cannot, don't want or may not use existing open source and commercial solutions3. Development of the protocol network or similar analyzers4. Security audits of the network traffic5. Development of the test software which should emulate a "controlled incorrect" behavior of one of the communication partnerThis list

is of course not complete and can be continuedThe only small weakness which should be fixed by the author is the matter that the proposed TLS 1.2 has intentionally adopted some bugs of the current for the publication time version of the GnuTLS. This was one of the very few, when not the only publicly available implementation of the TLS 1.2. This was done to make the sources in the book testable against those of the reader utilizing the TLS 1.2 in GnuTLS. The latter are fixed a long time ago but the downloadable sources for the book are not modified. So the implementation of the PRF for the TLS 1.2 in the book must be double checked before using.

KurzbeschreibungHands-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. Coverage includes: Understanding Internet Security Protecting against Eavesdroppers with Symmetric Cryptography Secure Key Exchange over an Insecure Medium with Public Key Cryptography Authenticating Communications Using Digital Signatures Creating a Network of Trust Using X.509 Certificates A Usable, Secure Communications Protocol: Client-Side TLS Adding Server-Side TLS 1.0 Support Advanced SSL Topics Adding TLS 1.2 Support to Your TLS Library Other Applications of SSL A Binary Representation of Integers: A Primer Installing TCPDump and OpenSSL Understanding the Pitfalls of SSLv2 Set up and launch a working implementation of SSL with this practical guide.KurzbeschreibungHands-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. Coverage includes: Understanding Internet Security Protecting against Eavesdroppers with Symmetric Cryptography Secure Key Exchange over an Insecure Medium with Public Key Cryptography Authenticating Communications Using Digital Signatures Creating a Network of Trust Using X.509 Certificates A Usable, Secure Communications Protocol: Client-Side TLS Adding Server-Side TLS 1.0 Support Advanced SSL Topics Adding TLS 1.2 Support to Your TLS Library Other Applications of SSL A Binary Representation of Integers: A Primer Installing TCPDump and OpenSSL Understanding the Pitfalls of SSLv2 Set up and launch a working implementation of SSL with this practical guide.BuchrckseiteLet's get down to a practical implementation of SSL and TLSSSL/TLS is a standardized, widely implemented, peer-reviewed protocol for applying cryptographic primitives to arbitrary networked communications. It provides privacy, integrity, and a measure of authenticity to otherwise inherently untrustworthy network connections.While most books detail the protocol, this one is intended to provide you with a nearly complete SSL/TLS library, developed incrementally using C code. Whether or not you have a working knowledgeof cryptography, you'll find this practical guide helps you understand the internals of these libraries so that, when it comes time to use one, you will have a firm understanding of what takes place at each stage.* Understand secure sockets and the HTTP protocol* Learn to protect against eavesdroppers with symmetric cryptography* Secure key exchanges over an insecure medium with public key cryptography and boost security with elliptic curve cryptography* Examine the use of digital signatures and X.509 certificates* Develop a usable, secure communications protocol with client-side TLS* Add server-side TLS 1.0 support* Use SSL in advanced situations, including safely reusing key material with sessionresumption and verifying identity with client authenticationGo to www.wiley.com/go/implementingssl to find code and other features related to this book