DESCRIPTION

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.

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 TCDDump and OpenSSL

• Understanding the Pitfalls of SSLv2

Set up and launch a working implementation of SSL with this practical guide.

---

About the Author

Joshua Davies is a principal architect for Travelocity.com, responsible for the architecture of the main Web site with a focus on networking and security. Previously, he designed distributed systems for AT&T, Digex, and the Mexican telecommunications giant Pegaso.

---

For additional product details, please visit https://www.wiley.com/en-us