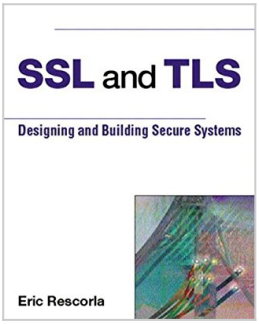

SSL and TLS: Designing and Building Secure Systems

By Eric Rescorla

SSL and TLS: Designing and Building Secure Systems By Eric Rescorla

This is the best book on SSL/TLS. Rescorla knows SSL/TLS as well as anyone and presents it both clearly and completely.... At times, I felt like hes been looking over my shoulder when I designed SSL v3. If network security matters to you, buy this book. Paul Kocher, Cryptography Research, Inc. Co-Designer of SSL v3 Having the right crypto is necessary but not sufficient to having secure communications. If youre using SSL/TLS, you should have SSL and TLS sitting on your shelf right next to Applied Cryptography. Bruce Schneier, Counterpane Internet Security, Inc. Author of Applied Cryptography Everything you wanted to know about SSL/TLS in one place. It covers the protocols down to the level of packet traces. It covers how to write software that uses SSL/TLS. And it contrasts SSL with other approaches. All this while being technically sound and readable! Radia Perlman, Sun Microsystems, Inc. Author of Interconnections Secure Sockets Layer (SSL) and its IETF successor, Transport Layer Security (TLS), are the leading Internet security protocols, providing security for e-commerce, web services, and many other network functions. Using SSL/TLS effectively requires a firm grasp of it

SSL and TLS: Designing and Building Secure Systems

By Eric Rescorla

SSL and TLS: Designing and Building Secure Systems By Eric Rescorla

This is the best book on SSL/TLS. Rescorla knows SSL/TLS as well as anyone and presents it both clearly and completely.... At times, I felt like hes been looking over my shoulder when I designed SSL v3. If network security matters to you, buy this book. Paul Kocher, Cryptography Research, Inc. Co-Designer of SSL v3 Having the right crypto is necessary but not sufficient to having secure communications. If youre using SSL/TLS, you should have SSL and TLS sitting on your shelf right next to Applied Cryptography. Bruce Schneier, Counterpane Internet Security, Inc. Author of Applied Cryptography Everything you wanted to know about SSL/TLS in one place. It covers the protocols down to the level of packet traces. It covers how to write software that uses SSL/TLS. And it contrasts SSL with other approaches. All this while being technically sound and readable! Radia Perlman, Sun Microsystems, Inc. Author of Interconnections Secure Sockets Layer (SSL) and its IETF successor, Transport Layer Security (TLS), are the leading Internet security protocols, providing security for e-commerce, web services, and many other network functions. Using SSL/TLS effectively requires a firm grasp of it

SSL and TLS: Designing and Building Secure Systems By Eric Rescorla Bibliography

- Sales Rank: #466274 in Books
- Published on: 2000-10-27
- Original language: English
- Number of items: 1
- Dimensions: 9.00" h x 1.20" w x 7.40" l, 1.65 pounds
- Binding: Paperback
- 528 pages

Editorial Review

From the Inside Flap

The Secure Sockets Layer (SSL) is by far the most widely deployed security protocol in the world. Essentially every commercial Web browser and server supports secure Web transactions using SSL. When you buy online using "secure" Web pages an estimated 20 billion dollars' worth of such transactions will occur in 2000), you're almost certainly using SSL.

Although its most common use is for securing Web traffic, SSL is actually quite a general protocol suitable for securing a wide variety of kinds of traffic. File transfer (FTP), remote object access (RMI, CORBA IIOP), e-mail transmission (SMTP), remote terminal service (Telnet) and directory access (LDAP) are just some of the applications that have already been secured with SSL or its successor, Transport Layer Security (TLS).

The effort to secure all these protocols has taught us a number of significant lessons. First, doing a good job of using SSL/TLS to secure a protocol requires having a fairly deep knowledge of how it works. It is not possible to simply treat SSL/TLS as a black box that somehow magically provides security when used.

Second, although each application is slightly different, there seems to be a set of security problems that are common to every application you wish to secure. For instance, we usually need to figure out some way for the insecure and secure versions of an application protocol to coexist. Although there aren't cookie-cutter solutions to these problems, the security community is starting to develop a common set of techniques for solving these problems using SSL/TLS.

These techniques can often be applied to a new application protocol with minimal modification. In essence, we've developed a set of design patterns for securing protocols. Much of the work of securing a system is in recognizing which pattern most closely matches the system you're working with and then using the appropriate techniques.

The purpose of this book, then, is to address both of these needs. After reading this book, you should know most if not all of what you need to know in order to design secure systems using SSL/TLS. You'll know enough about SSL/TLS to understand what security features it can deliver and what it can't deliver. Further, you'll be familiar with the common design patterns for using SSL/TLS and be ready to apply them to new situations.

What This Book Provides This book is intended for anyone who wants to understand and use SSL/TLS.

For designers, it provides information on designing systems that use SSL/TLS as well as a library of the techniques that have already been used. For programmers who program with SSL/TLS, it provides information on what your libraries are doing under the covers and what those functions you're calling are really doing. Understanding these details is critical for obtaining acceptable and predictable application performance. For SSL/TLS implementors it acts as an adjunct to the standard, explaining obscure sections and describing both common practice and why things are the way they are.

Intended Audience

This book assumes a basic familiarity with how the TCP/IP protocols work. Readers who are unfamiliar with TCP/IP would be best served to consult one of the many fine books describing TCP/IP. TCP/IP Illustrated, Volume 1 Stevens1994a is a good choice. Postel1991a, Postel1991b, and Postel1991c provide the definitive reference for TCP/IP. Although some of this book will be understandable without a deep understanding of TCP/IP, much of the discussion of performance will be difficult to follow without an understanding of TCP behavior.

Because SSL/TLS is a cryptographic protocol, properly understanding it requires at least basic familiarity with cryptographic algorithms, including public key cryptography, symmetric cryptography, and digest algorithms. Chapter 1 provides an introduction to cryptography and communications, but space is too limited to do a complete job. We attempt to cover the requisite cryptographic details for understanding SSL/TLS; however, readers interested in a broader understanding of the cryptographic issues should consult a cryptography text such as Schneier1996a or Kaufman1995a

Organization of the Book

This book is written in two halves, matching the two primary goals described previously: understanding the protocol and understanding how to use it. The first half, Chapters 1-6, is devoted to describing SSL and TLS. We concern ourselves with the technical details of how they work and their security and performance properties in isolation.

The second half of the book, Chapters 7-11, covers the design of application protocols and systems that use SSL/TLS for security. First we describe general guidelines for using SSL/TLS and then we discuss several protocols that have already been secured using SSL/TLS.

Chapter 1 - Security Concepts provides an introduction to cryptography and communications security, with an eye towards its use in SSL/TLS. If you're already familiar with communications security, you may want to skip this chapter. If, on the other hand, you're not familiar with security, you'll want to read this chapter carefully so you don't get lost later.

Chapter 2 - Introduction to SSL is a broad overview of the history of SSL/TLS and what sorts of security features it provides. We also provide a snapshot of the status of SSL/TLS-secured protocols as of the time of this writing.

Chapter 3 - Basic SSL covers the most common SSL/TLS operational mode. We describe an entire SSL/TLS connection from start to finish. This chapter should give you a very good idea of how SSL/TLS works in practice. All the other operational modes can be easily understood once you understand this chapter.

Chapter 4 - Advanced SSL covers the rest of the major operational modes. We cover session resumption, client authentication, and a number of algorithms that are only now seeing deployment with SSL/TLS, such as DH/DSS and Kerberos.

Chapter 5 - SSL Security describes the security benefits that SSL offers as well as (even more important) those it doesn't offer. Whereas previous chapters mostly focused on describing how things work, this chapter focuses on what you need to do to make a system that uses SSL/TLS secure.

Chapter 6 - SSL Performance describes the performance profile of TLS-based systems. It's been widely observed that security imposes significant performance demands on systems, but it's not widely understood that this impact is limited to certain parts of the protocol. We'll discuss these issues with an eye to getting better performance while preserving good security.

Chapter 7 - Designing with SSL is a guide to using SSL/TLS to secure application layer protocols. We focus on identifying the required security properties and on well-understood design techniques for satisfying these properties.

Chapter 8 - Coding with SSL discusses the common program- ming idioms required to write software that uses SSL/TLS. We provide complete sample programs in C and Java using the OpenSSL and PureTLS toolkits.

Chapter 9 - HTTP over SSL describes the application that started it all. SSL was originally designed by Netscape to work with HTTP and we cover both the traditional way of doing things and the replacement that's currently being proposed.

Chapter 10 - SMTP over TLS describes the use of TLS to secure the Simple Mail Transport Protocol (SMTP) which is used for transporting email. SMTP is a bad match for TLS and this chapter illustrates some of the limitations of SSL and TLS.

Chapter 11 - Contrasting Approaches is devoted to describing other alternatives to securing your applications. SSL/TLS isn't always the best solution and part of knowing how to use a protocol is knowing when not to. This chapter tries to give you a perspective on your other choices. We discuss IPSEC, S-HTTP, and S/MIME as alternatives to SSL/TLS.

How to Read This Book

This book is suitable for a number of audiences of different technical abilities and requirements. You should read any section that interests you, but depending on your needs you may want to focus on specific sections.

Protocol Designers If you're designing a new application-level protocol or securing an existing protocol with SSL, you should read the first parts of Chapters 1-6 so that you have a good general understanding of how SSL works. Then carefully read Chapter 7 for a guide to SSL design principles. You can skip Chapter 8 unless you intend to implement your design, but be sure to read Chapters 9 and 10 so you can see real-world examples of how SSL should and should not be used in practice. Finally, before you start to design, read Chapter 11 to make sure that SSL is appropriate for your design and that you wouldn't be better served by using another security protocol.

Application Programmers

If you're writing an application that uses a preexisting SSL toolkit you can safely read only the first parts of Chapters 1-6. You should also read the summaries at the end of each chapter. These sections discuss SSL and SSL implementation techniques in overview form. This will provide enough information to understand what your SSL toolkit is doing. You should carefully read Chapters 7 and 8, paying special attention to the programming techniques discussed in Chapter 8. If you are implementing HTTP or SMTP over SSL, you should also read the chapters that deal with those protocols.

SSL/TLS Implementors

If you're implementing SSL from scratch, you should read the entire book. If you're already familiar with cryptography you can skip Chapter 1; however, if you don't have a detailed knowledge of cryptography you should read the entire chapter. You should pay particular attention to Chapters 2-6, which provide a detailed description of SSL and of the various implementation techniques required to produce a fast and secure implementation.

Just Curious If you just want to learn about SSL you can skip around in the book. If you don't already know about cryptography, read all of Chapter 1. Then read Chapters 2-6 so you know how SSL works. Then you can read as much or as little of the rest of the book as interests you. It's probably worth reading Chapter 11 to get some perspective on how SSL compares to other security protocols. SSL/TLS Versions

By now you've no doubt gotten tired of seeing the name SSL/TLS. We've been using it to avoid being specific about exactly which version we mean. There are currently two versions of SSL in wide deployment: SSL version 2 (SSLv2) and SSL version 3 (SSLv3). TLS, a modification of SSLv3, was standardized by the Interenet Engineering Task Force (IETF) in 1999. Despite what you might think from the names, SSLv2 and SSLv3 are completely different protocols, and TLS is extremely similar to SSLv3. SSLv2 is essentially obsolete, and TLS isn't really in wide deployment as of this writing. In general, we'll use the term SSL to refer to SSLv3/TLS interchangeably. When we mean one or the other, we'll specify it explicitly. In the few instances when we're talking about SSL version 2, we'll use SSLv2. 0201615983P04062001

From the Back Cover

"This is the best book on SSL/TLS. Rescorla knows SSL/TLS as well as anyone and presents it both clearly and completely.... At times, I felt like he's been looking over my shoulder when I designed SSL v3. If network security matters to you, buy this book."
Paul Kocher, Cryptography Research, Inc.
Co-Designer of SSL v3

"Having the right crypto is necessary but not sufficient to having secure communications. If you're using SSL/TLS, you should have **SSL and TLS** *sitting on your shelf right next to* Applied Cryptography."
Bruce Schneier, Counterpane Internet Security, Inc.
Author of *Applied Cryptography*

"Everything you wanted to know about SSL/TLS in one place. It covers the protocols down to the level of packet traces. It covers how to write software that uses SSL/TLS. And it contrasts SSL with other approaches. All this while being technically sound and readable!"
Radia Perlman, Sun Microsystems, Inc.
Author of *Interconnections*

Secure Sockets Layer (SSL) and its IETF successor, Transport Layer Security (TLS), are the leading Internet security protocols, providing security for e-commerce, web services, and many other network functions. Using SSL/TLS effectively requires a firm grasp of its role in network communications, its security properties, and its performance characteristics. ***SSL and TLS*** provides total coverage of the protocols from the bits on the wire up to application programming.

This comprehensive book not only describes how SSL/TLS is supposed to behave but also uses the author's free ssldump diagnostic tool to show the protocols in action. The author covers each protocol feature, first explaining how it works and then illustrating it in a live implementation. This unique presentation bridges the difficult gap between specification and implementation that is a common source of confusion and incompatibility.

In addition to describing the protocols, ***SSL and TLS*** delivers the essential details required by security architects, application designers, and software engineers. Use the practical design rules in this book to quickly design fast and secure systems using SSL/TLS. These design rules are illustrated with chapters covering the new IETF standards for HTTP and SMTP over TLS.

Written by an experienced SSL implementor, ***SSL and TLS*** contains detailed information on programming SSL applications. The author discusses the common problems faced by implementors and provides complete sample programs illustrating the solutions in both C and Java. The sample programs use the free OpenSSL and PureTLS toolkits so the reader can immediately run the examples.

0201615983B04062001

About the Author

Eric Rescorla is an Internet security consultant and author of several commercial SSL implementations, including the freely available Java PureTLS toolkit. He is also the author of *HTTP over TLS* and *Secure HTTP IETF* RFCs.

0201615983AB04062001

Users Review

From reader reviews:

Marina Rutt:

The ability that you get from SSL and TLS: Designing and Building Secure Systems is a more deep you digging the information that hide inside the words the more you get serious about reading it. It does not mean that this book is hard to know but SSL and TLS: Designing and Building Secure Systems giving you enjoyment feeling of reading. The author conveys their point in specific way that can be understood by means of anyone who read the idea because the author of this publication is well-known enough. That book also makes your personal vocabulary increase well. It is therefore easy to understand then can go along with you, both in printed or e-book style are available. We highly recommend you for having this SSL and TLS: Designing and Building Secure Systems instantly.

James Fletcher:

This book untitled SSL and TLS: Designing and Building Secure Systems to be one of several books that will best seller in this year, that's because when you read this publication you can get a lot of benefit into it. You will easily to buy this book in the book retailer or you can order it by means of online. The publisher on this book sells the e-book too. It makes you easier to read this book, since you can read this book in your Mobile phone. So there is no reason to you personally to past this reserve from your list.

Shannon Blackshear:

The publication with title SSL and TLS: Designing and Building Secure Systems contains a lot of information that you can study it. You can get a lot of benefit after read this book. This particular book exist new expertise the information that exist in this reserve represented the condition of the world today. That is important to yo7u to be aware of how the improvement of the world. That book will bring you in new era of the globalization. You can read the e-book on your own smart phone, so you can read the item anywhere you

want.

Kaci Carter:

Reading a book to be new life style in this calendar year; every people loves to go through a book. When you read a book you can get a lot of benefit. When you read ebooks, you can improve your knowledge, due to the fact book has a lot of information into it. The information that you will get depend on what sorts of book that you have read. In order to get information about your examine, you can read education books, but if you act like you want to entertain yourself you can read a fiction books, these kinds of us novel, comics, along with soon. The SSL and TLS: Designing and Building Secure Systems will give you new experience in reading through a book.

Read SSL and TLS: Designing and Building Secure Systems By Eric Rescorla for online ebook

SSL and TLS: Designing and Building Secure Systems By Eric Rescorla Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read SSL and TLS: Designing and Building Secure Systems By Eric Rescorla books to read online.

Online SSL and TLS: Designing and Building Secure Systems By Eric Rescorla ebook PDF download

SSL and TLS: Designing and Building Secure Systems By Eric Rescorla Doc

SSL and TLS: Designing and Building Secure Systems By Eric Rescorla Mobipocket

SSL and TLS: Designing and Building Secure Systems By Eric Rescorla EPub

YXZVJEDSQ60: SSL and TLS: Designing and Building Secure Systems By Eric Rescorla