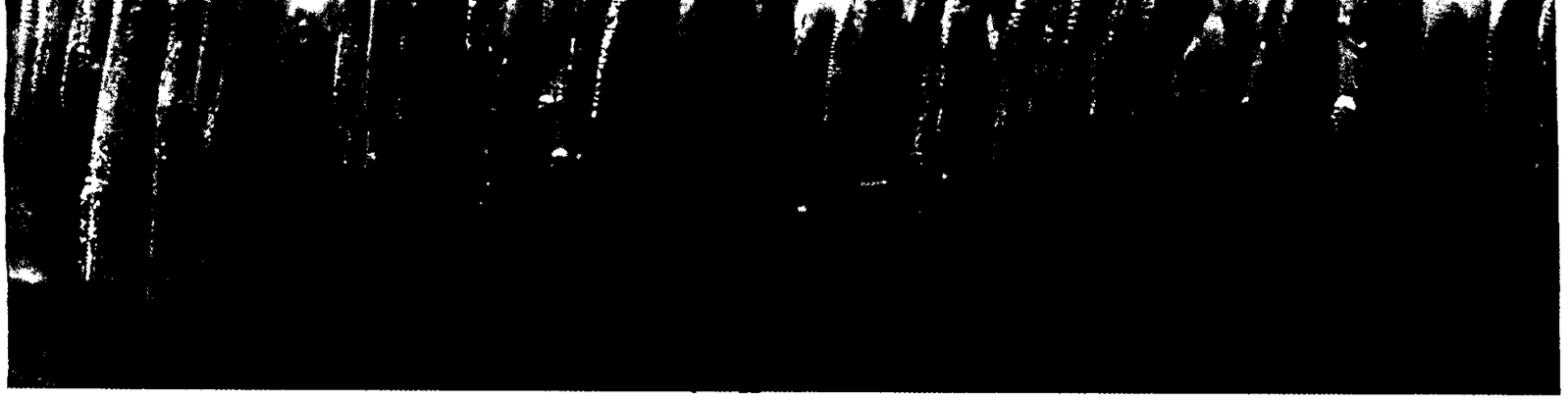
SSL 与 TLS

Designing and Building Secure Systems

Eric Rescorla 著
崔 凯 译

Addison-Wesley

中国电力出版社
www.infopower.com.cn



SSL 与 TLS

Designing and Building Secure Systems

Eric Rescorla 著
崔 凯 译

中国电力出版社

内 容 提 要

SSL(Security Socket Layer) 加密套接字协议层是世界上部署最为广泛的安全协议，每种商业浏览器和服务器都在其内部使用 SSL 来支持安全的 Web 交易，TLS(Transport Layer Security) 是 SSL 的后继。

本书的前半部分主要讲述 SSL 和 TLS 工作的技术细节，分别讨论了它们的安全与性能属性。后半部分讲述了如何使用 SSL/TLS 来安全地应用协议和系统实现。首先讲述使用 SSL/TLS 的一般性指导，然后又介绍几种已经使用 SSL/TLS 来保障安全的协议。

本书适用于那些对 TCP/IP 协议有一定了解，且对网络传输安全感兴趣的读者阅读。

图书在版编目（CIP）数据

SSL 与 TLS/（美）雷斯克拉著；崔凯译. —北京：中国电力出版社，2002.7
ISBN 7-5083-1093-4

Ⅰ.S… Ⅱ.①雷…②崔… Ⅲ. 计算机通信网—安全技术
Ⅳ. TN915.08

中国版本图书馆 CIP 数据核字（2002）第 037076 号

著作权合同登记号 图字：01-2002-0714 号
本书英文版原名：SSL and TLS Designing and Building Secure Systems
Published by arrangement with Addison Wesley Longman, Inc.

中国电力出版社出版、发行
（北京三里河路 6 号 100044 http://www.infopower.com.cn）
汇鑫印务有限公司印刷
各地新华书店经售
*
2002 年 10 月第一版 2002 年 10 月北京第一次印刷
787 毫米×1092 毫米 16 开本 25 印张 556 千字
定价 40.00 元

序　言

安全套接层协议SSL（Secure Socket Layer）是世界上部署最为广泛的安全协议。每一种商业浏览器和服务器都在其内部使用SSL来支持安全的Web交易。当你使用“安全的”Web页面进行联机采购（2000年此类交易的价值大概有200亿美圆）时，几乎可以肯定，你是在使用SSL。

尽管SSL最常见的用途是保证Web通信的安全，但实际上它也是一种相当通用的协议，适用于保护种类繁多的各种通信数据的安全。其中的一些，如文件传输（FTP）、远程对象存取（RMI、CORBA、IIOP）、E-mail传输（SMTP）、远程终端服务（Telnet）以及目录存取（LDAP）业已成为使用SSL或其后继TLS（Transport Layer Security）来保障安全的一部分应用。

保证所有这些协议安全所耗费的精力使我们吸取了许多重要的教训。首先，要想很好地使用SSL/TLS保证一种协议的安全，就要求对SSL/TLS的工作原理有着相当扎实的理解。我们不可能简单的将SSL/TLS当作黑箱对待，指望它能够在使用时神奇地提供所需要的安全。

其次，尽管每种应用稍有不同，但似乎对每种想保证其安全的应用来说都有一组共同的安全问题。例如，我们通常要设法找出某种让一种应用协议中不安全与安全版本和平共处的方法。尽管对这些问题来说没有一致的解决方案，但是专门研究安全的团体还是正在着手开发一组使用SSL/TLS来解决此类问题的公共技术。

我们常常可以稍加修改就能将这些技术应用于一种新的应用协议中。从本质上讲，我们已开发了一套用于保证协议安全的设计模式（design pattern）。保证系统安全的很大一部分工作就是识别出与正在使用的系统最为匹配的模式，然后再采用相应的技术。

本书的意图就是针对这两方面的需求进行讲解。在读完这本书之后，你应当了解即便不是所有也是绝大多数使用SSL/TLS设计安全系统所需的知识。你将会了解足以理解SSL/TLS所能提供以及所不能提供的各种安全特性的知识。此外，还会熟悉使用SSL/TLS的常见设计模式，并随时可以在新的情况下应用这些模式。

本书所提供的内容

本书适用于任何想要理解和使用SSL/TLS的读者。

对设计者来说，本书不但提供了已经付诸使用的技术库，还提供了使用SSL/TLS来设计系统的有关信息。

对于使用SSL/TLS编程的程序员来说，本书提供了有关函数库底层的工作机理，以及你所调用的函数实际完成的工作内容。理解这些细节对于获得可接受及可预料的应用性能非常关键。

对于SSL/TLS的实现者来说，本书可以作为标准之外的辅助资料，起到解疑释惑的作用。

面向的读者群

本书假定你对TCP/IP协议的工作原理有着基本的了解。那些对TCP/IP不熟的读者最好还是能够参考一本讲解TCP/IP的好书。TCP/IP Illustrated, 第一卷[Stevens 1994]是一本不错的选择。RFC791[Postel1991a]、RFC792[Postel1991b]，以及RFC793[Postel1991c]提供了有关TCP/IP的终极参考。尽管无须深刻理解TCP/IP也能理解本书中的一些内容，但是不理解TCP的行为就很难明白大量与性能有关的讨论。

由于SSL/TLS是一种密码协议（cryptographic protocol），所以要想正确地理解有关内容则需要熟悉密码学算法（cryptographic algorithm），其中包括公用密钥加密算法（public key cryptography）、对称加密算法（symmetric cryptography）以及摘要（digest）算法。第一章将介绍密码学与通信，但由于篇幅的限制，无法提供完整的描述。我们试图含盖理解SSL/TLS所必需的所有加密算法细节。不过，有兴趣从更广的层面上理解加密算法知识的读者应当参阅一本有关密码学的教程，如 [Schneier1996a] 或 [Kaufman1995]。

本书的结构

本书是分成两个部分来写的，这与我们前面所描述的两个目标：理解协议以及如何使用是一致的。前半部分，从第1到第6章主要讲述SSL和TLS。我们主要关心的是SSL和TLS工作的技术细节，并分开讨论它们的安全与性能属性。

而在本书的后半部分，从第7章到第11章，讲述了如何使用SSL/TLS来保证安全地应用协议和系统实现。首先讲述使用SSL/TLS的一般性指导，然后讨论几种已经使用SSL/TLS来保障安全的协议。

第1章——与安全有关的概念，提供了对密码学与通信安全的介绍，并着眼于它在SSL/TLS中的应用。如果你已经熟悉通信安全的相关知识，那么就可以跳过这一章。反之，就应当仔细阅读本章，以免到后边不知所云。

第2章——SSL介绍，粗略概括了SSL/TLS的历史以及它所提供的各种安全特性。此外，还提供了在编写本书时使用SSL/TLS来保证安全的各种协议的现况。

第3章——SSL基础，讲述了最常用的SSL/TLS操作模式（operational mode）。我们从头到尾描述了整个SSL/TLS的连接过程。本章可以让你很好地理解SSL/TLS的实际工作原理。一旦理解了本章的内容，你就能够轻而易举地理解其他操作模式。

第4章——高级SSL，讲述了其余主要的操作模式。讲解了会话恢复（session resumption）、客户端认证（client authentication），以及几种当前只在SSL/TLS中才被采用的算法，如DH/DSS和Kerberos。

第5章——SSL的安全，描述了SSL所提供的安全裨益，以及所不能提供的一些个好处（这些内容甚至更为重要）。前面的章节主要将重点放在工作原理上，而本章则将重点放在为保证使用SSL/TLS的系统安全所要完成的工作上。

第6章——SSL的性能，描述了基于TLS系统的性能剖析。众所周知，安全措施对系统提出了很高的性能要求，但是理解这种影响仅限于协议特定部分的人却不多。我们将讨论这些

问题，并着眼于在获得更高性能的同时维持良好的安全性。

第7章——使用SSL进行设计，是有关使用SSL/TLS来保证应用协议安全的指南。我们将重点放在识别所需的安全属性上，并深刻理解满足这些属性的设计技术。

第8章——进行SSL编程，讨论了编写使用SSL/TLS的软件所需的常见编程套路（programming idiom）。我们提供了完整的采用OpenSSL和PureTLS工具箱，用C和Java语言编写了的范例程序。

第9章——SSL上的HTTP，讲述了开创SSL的应用。SSL起先是由Netscape设计用来与HTTP一起工作的，我们在这里讲述了完成此类工作的传统方式，同时也讲解了当前建议的替代方式。

第10章——TLS上的SMTP，讲述了使用TLS来保证简单邮件传输协议（SMTP）安全的内容，SMTP是用来传输E-mail的协议。SMTP与TLS并不相称，而本章举例说明了SSL与TLS的一些限制。

第11章——各种方案的对比，描述了其他保证应用安全的方案。SSL/TLS并不总是最好的解决方案，了解何时不去使用它也是了解如何使用某种协议所需的。本章试图带你领略一下其他的选择。我们讨论了除SSL/TLS之外的其他方案：IPSEC、S-HTTP和S/MIME。

如何阅读本书

本书适合各种具有不同技术能力和需求的读者。你可以阅读任何自己感兴趣的章节，也可以根据自己的需要，将重点放在特定的章节上。

协议设计人员

如果你是在设计一种新的应用层协议或是使用SSL/TLS来保证一种现有协议的安全，就应当阅读头一部分第1~6章的内容，以便对SSL/TLS的工作原理有个大致了解。然后再仔细阅读第7章有关SSL/TLS设计原则的指南。如果你不打算实现自己的设计，就可以跳过第8章，但是一定要阅读第9章和第10章。从中你能看到现实世界中的一些例子，了解在实际运用中应当怎样和不应当怎样使用SSL/TLS。在开始设计之前，还应该阅读第11章的内容以确信SSL/TLS适合你的设计，以及有没有其他更好的安全协议可供使用。

应用程序员

如果你使用现有的SSL/TLS工具箱编写应用，就可以放心读完第一部分1至6章的内容。你还应当阅读每章之后的总结，这些章节概括性地讨论了SSL/TLS及其实现技术。这些内容将会提供理解SSL/TLS完成各项工作的足够信息。你应当仔细阅读第7章和第8章，要特别注意第8章所讨论的编程技术。如果你是在SSL上实现HTTP或SMTP的话，还应当阅读与这些协议有关的章节。

SSL/TLS实现者

如果你是在从头实现SSL/TLS，就应当阅读整本书的内容。如果你已经熟悉密码学的话，

就可以跳过第1章。然而，如果对密码学没有具体的了解，则应当通读整章的内容。你应当特别注意第2到第6章的内容，这些章节提供了对SSL/TLS的具体描述，以及创建快速而安全的实现所需要的各种实现技术。

仅仅出于好奇

如果你只是想对SSL/TLS有所了解，则可以随意挑选书中的章节阅读。但如果事先不了解有关密码学的知识，就应该阅读第1章的全部内容。然后再阅读第2到第6章以了解SSL/TLS的工作原理。接着就可以或多或少地阅读其余自己感兴趣的章节。要想了解SSL/TLS与其他安全协议之间的比较的话，第11章或许值得一读。

SSL/TLS的版本

至此，你可能已经厌倦了看到SSL/TLS这个字眼。我们一直使用它来避免谈及我们所意指的确切版本。当前有两个版本的SSL被广泛部署：SSL版本2（SSLv2）和SSL版本3（SSLv3）。TLS是SSLv3的一种变体，由因特网工程任务组（IETF）在1999年加以标准化。除了从名字可以想到的内容之外，SSLv2与SSLv3是两种截然不同的协议，而TLS与SSLv3极其相似。SSLv2实质上已经过时，而在编写这本书的当刻，还没有真正地广泛部署TLS。总而言之，我们将使用SSL这个字眼来互换的指代SSLv3/TLS。当意指某种协议时，我们会具体指明。在个别谈论SSL版本2的实例中，我们将会使用SSLv2。

排版约定

本书包含许多真实SSL或TLS会话的网络跟踪信息。在展示此类跟踪信息时，我们使用等宽字体来显示程序输出（CONSTRUCTED），使用斜体表示之后插入的注释（Comment）。在网络跟踪信息中显示以十六进制表达协议数据的地方，我们使用等宽粗体（01 02 03）来显示。在以明文来显示加密数据的地方，我们将使用等宽斜体来显示（data）。

正文中，从各项标准（如，因特网RFC）和协议结构定义节选的内容以sans serif字体来显示（helvetica），而图示中使用可读性好的Times字体。代码片段以等宽字体（int）来显示。在个别特殊情况下，需要折行显示较长的行，这种情况下，我们将在折行的行尾使用符号↵来表示下面是该行的接续文本。

历史文献注解和旁白将会用这种较小的字体缩进来显示。

网络跟踪信息

本书中的网络跟踪信息全都源于真实的会话（session），大部分都是在作者家里的以太网上捕获的。使用了各种各样的客户端和服务器程序，其中包括OpenSSL、Netscape Navigator、Internet Explorer和qmail。这些跟踪信息是用tcpdump程序捕获，并存储在磁盘上的。文中显示的跟踪信息是用作者编写的SSL解码软件包ssldump产生的。你可以从http://www.tcpdump.org/获得tcpdump，从http://www.rtfm.com/ssldump/处获得ssldump。

源代码

本书包含了许多源代码片段。第8章和第9章的源代码是由作者编写的，©1999-2000。不管出于什么目的，你都可以免费使用和拷贝，但是并不提供任何种类的担保。你可以从作者的Web站点http://www.rtfm.com/ssldump/获得机器可读的版本。

第5章中的Java源代码是PureTLS Java SSL/TLS实现的一部分。你可以从http://www.rtfm.com/puretls得到。该源代码具有下列版权。

```
Copyright (C) 1999, Claymore Systems, Inc.
All Rights Reserved.

ekr@rtfm.com Tue May 18 09:43:47 1999

This package is a SSLv3/TLS implementation written by Eric Rescorla
<ekr@rtfm.com> and licensed by Claymore Systems, Inc.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1.Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2.Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
3.All advertising materials mentioning features or use of this software
  must display the following acknowledgement:
  This product includes software developed by Claymore Systems, Inc.
4.Neither the name of Claymore Systems, Inc. nor the name of Eric
Rescorla may be used to endorse or promote products derived from this
  software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ''AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.
```

附录A中SSL会话缓存的例子出自Ralf S. Engelschall（rse's）的mod_ssl软件包，你可以从http://www.modssl.org/获得该软件包，这里使用的版本是2.6.1-1.3.12。它受下列版权限制。

```
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
OF THE POSSIBILITY OF SUCH DAMAGE.
    ================================================================
```

致谢

没有许多人的协助是不可能编写图书的，更不要说是一本技术书籍。作为一种惯例，我想在此感谢其中的一些个人。

我的技术审阅人员不但使我诚实，而且使我的写作尽可能的清晰。Josha Ball、Joe Balsama、Douglas Barnes、DebasishBiswas、Andrew Brown、Robert Bruen、Megan Conklin、Russ Housley、Paul Kocher、Brian Korver、Chris Kostick、Marcus Leech、Robert Lynch、Joerg Meyer、D.Jay Newman、Tim Newsham、Stacey O'Rourke、Radia Perlman、Mark Schertler、Win Treese、Tom Weinstein和Tom Woo，这些人都参加了对手稿的各个章节审阅的工作。

许多人时常、甚至在不知道的情况下，慷慨地解答了我在写作中遇到的技术问题。我要特别感谢John Banes、Steve Bellovin、Burt Kaliski、Paul Kocher、Bodo Moeller、Dan Simon和Robert Zuccherato，感谢你们填补了我的知识空白。尤其要感谢Terence Spies，是他就整个手稿提出了宝贵的批评，并解答了大量有关微软SSL实现的技术问题。

本书大量使用OpenSSL来产生SSL通信演示。如果没有Eric Young和Tim Hudson在创建SSLeay中的艰苦工作，以及OpenSSL团队在Eric Young为寻求更好的发展而离开后对OpenSSL进行的维护和改进，OpenSSL就不会存在。

来自Alchemy/Nokia的Brian Korver和Stacey O'Rourke在收集第6章的一些性能数据时提供了大量帮助。他们不但允许我使用他们的机器和网络，还亲切地以各种晦涩的方式重新对环境进行配置，以便我能够特定应用情景。

尽管从未谋面，现已去世的W.Richard Stevens仍然对本书有着巨大的贡献。使用网络跟踪信息来演示协议的思想就是从Stevens的那套优秀的TCP/IP Illustrated中汲取的。贯穿本书，我努力模仿他清晰易读的风格（只获得了有限的成功）。当然，没有出版社就不可能出版任何东西，而我非常高兴能够与Addison-Wesley一起工作。我特别要感谢Mary Hart，是她提议这个项目，并忍受着漫无天日的拖延，而本书也从薄薄的200页激增并突破400页大关。我还要感谢我的出品经理Kathy Glidden，是她在耐心地回答我无休止的排版问题。

尽管这些人没有直接对本书的写作做出贡献，但我还是要感谢Allan Schiffman、Marty Tenenbaum和Jay Weber。是Jay和Marty在我只有天分而没有经验时给了我机会。从我认识他的八年来，Allan传授给了我不可估量的计算机科学知识。同样，假如没有我的父母教育我如何思考，我也根本不会取得这些成绩。

写书是一项艰苦的任务，在此过程中，是Jennifer Gates扮演了保证我头脑清醒的主要角色。在过去的几年中，她和她的丈夫Lee许多次提供了超出义务之外的友善和友谊。

另一种使自己持续保持头脑清晰的因素就是三项全能。Kevin Joyce和Kyle Welch提供了宝贵的保持我这种习惯的建议和动力。

最后我还要感谢Lisa Dusseault和Kevin Dick。Lisa和Kevin他们两个阅读整个手稿，并帮我将初稿转变成易读的篇章。没有他们，我极有可能根本无法完成这些工作，而且文章也要比现在糟糕的多。

照排版是由笔者使用James Clark的Groff软件包制作而成的。欢迎读者给我电子邮件提出批评和建议。

Mountain View, CA　　Eric Rescorla
September 2000　　ekr@rtfm.com

目　录