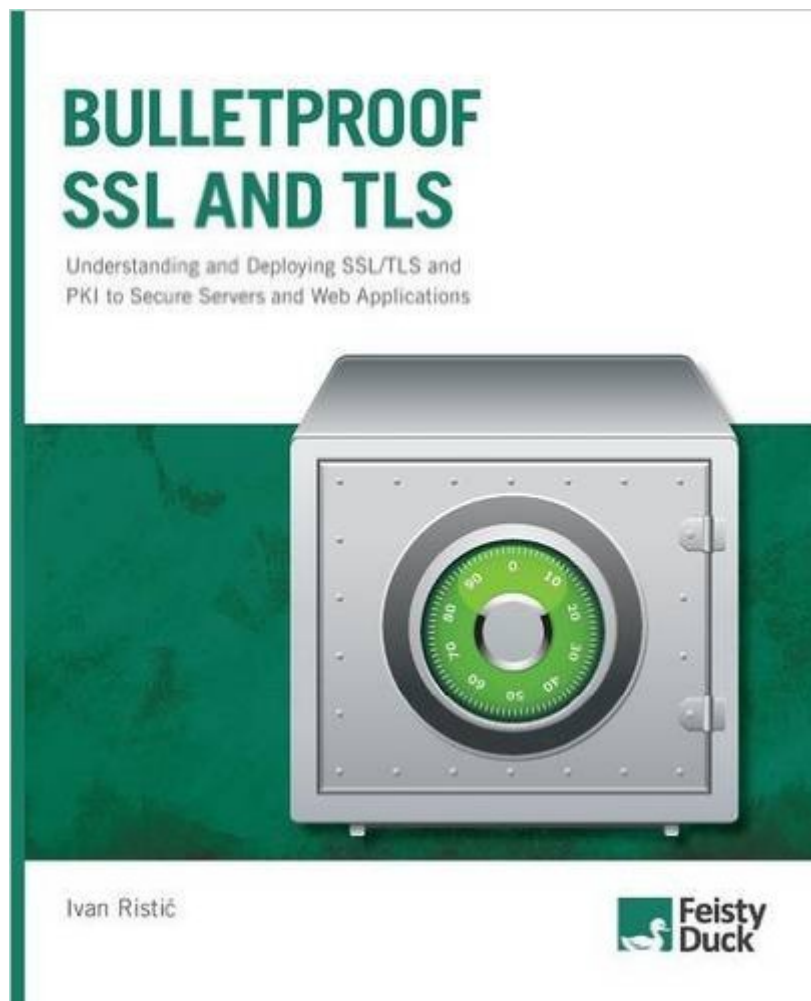# Bulletproof SSL And TLS: Understanding And Deploying SSL/TLS And PKI To Secure Servers And Web Applications

Synopsis

FULLY REVISED IN AUGUST 2015. Bulletproof SSL and TLS is a complete guide to using SSL and TLS encryption to deploy secure servers and web applications. Written by Ivan Ristic, the author of the popular SSL Labs web site, this book will teach you everything you need to know to protect your systems from eavesdropping and impersonation attacks.In this book, you'll find just the right mix of theory, protocol detail, vulnerability and weakness information, and deployment advice to get your job done:Comprehensive coverage of the ever-changing field of SSL/TLS and Internet PKI, with updates to the digital versionFor IT security professionals, help to understand the risksFor system administrators, help to deploy systems securelyFor developers, help to design and implement secure web applicationsPractical and concise, with added depth when details are relevantIntroduction to cryptography and the latest TLS protocol versionDiscussion of weaknesses at every level, covering implementation issues, HTTP and browser problems, and protocol vulnerabilitiesCoverage of the latest attacks, such as BEAST, CRIME, BREACH, Lucky 13, RC4 biases, Triple Handshake Attack, and HeartbleedThorough deployment advice, including advanced technologies, such as Strict Transport Security, Content Security Policy, and pinningGuide to using OpenSSL to generate keys and certificates and to create and run a private certification authorityGuide to using OpenSSL to test servers for vulnerabilitiesPractical advice for secure server configuration using Apache httpd, IIS, Java, Nginx, Microsoft Windows, and TomcatThis book is available in paperback and a variety of digital formats without DRM. Digital version of Bulletproof SSL and TLS can be obtained directly from the author, at feistyduck.com.

Book Information

Paperback: 530 pages

Publisher: Feisty Duck (August 1, 2014)

Language: English

ISBN-10: 1907117040

ISBN-13: 978-1907117046

Product Dimensions: 7.5 x 1.1 x 9.2 inches

Shipping Weight: 2.1 pounds (View shipping rates and policies)

Average Customer Review: 4.8 out of 5 stars See all reviews (34 customer reviews)

Best Sellers Rank: #34,270 in Books (See Top 100 in Books)   #12 in Books > Computers & Technology > Security & Encryption > Encryption   #13 in Books > Computers & Technology > Security & Encryption > Cryptography   #30 in Books > Computers & Technology > Security &

Customer Reviews

This is *the* HTTPS book to buy, whether you're a web developer, IT administrator, security researcher, or computer science student.Author Ivan Ristic's meticulously-researched book covers every important aspect of HTTPS, from cryptography, to public key infrastructure, to deployment and operations. Weighing in at a hefty 506 pages, it's unlikely that you'll read this book as I did, from cover-to-cover, so the author thoughtfully crafted the book with distinct sections so you can easily start with the content most important to your needs before (or instead of) reading anything else.For security enthusiasts, there's excellent coverage of all of the major attacks against TLS and PKI over the last decade or so, from CA compromise to TLS protocol attacks like BEAST, CRIME, Lucky 13, and more. This book serves as an excellent resource on each of these attacks-- how they operate, and how to mitigate against them.Web developers charged with keeping their sites fast as they move to HTTPS will appreciate nearly 30 pages of content on optimizing HTTPS for both the network and CPU, and fantastic coverage of OpenSSL will help you navigate the many functions of that powerful toolchain, even if your servers are running on other technologies. Thoughtful coverage on the tradeoffs between high security and interoperability problems is found in every chapter, to help you make the right decisions for your site's needs.One of the best features about this book is its breadth of platform coverage; unlike many guides that cover only one particular implementation, Bulletproof SSL and TLS covers all of the major platforms including thorough sections on OpenSSL, Apache, Java/Tomcat, IIS, and Nginx, with comments and footnotes about more obscure platforms as appropriate.

Download to continue reading...

Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications Handcrafted CSS: More Bulletproof Web Design, Video Edition (includes Handcrafted CSS book and Handcrafted CSS: Bulletproof Essentials DVD) Safe & Secure: Secure Your Home Network, and Protect Your Privacy Online Understanding and Deploying LDAP Directory Services (MacMillan Network Architecture & Development) Bulletproof Web Design: Improving flexibility and protecting against worst-case scenarios with XHTML and CSS (2nd Edition) Bulletproof Web Design: Improving flexibility and protecting against worst-case scenarios with HTML5 and CSS3 (3rd Edition) (Voices That Matter) Bulletproof Web Design: Improving flexibility and protecting against worst-case scenarios with XHTML and CSS Sap R/3 on DB2 for Os/390: Implementing With Aix or Windows Nt Applications Servers Focus and Leverage: The Critical

Methodology for Theory of Constraints, Lean, and Six Sigma (TLS) Building Web Applications with ADO.NET and XML Web Services (Gearhead Press) The Tangled Web: A Guide to Securing Modern Web Applications Solaris and LDAP Naming Services: Deploying LDAP in the Enterprise Enterprise Integration Patterns: Designing, Building, and Deploying Messaging Solutions Deploying License-Free Wireless Wide-Area Networks Deployment Fundamentals, Vol. 6: Deploying Windows 10 Using Microsoft Deployment Toolkit Innovating Lean Six Sigma: A Strategic Guide to Deploying the World's Most Effective Business Improvement Process Embedded Linux Porting on ARM & RFID Implementation Using ARM SoC: Developing a flexible and agile Board Secure Package Linux with multiple applications Wired for Love: How Understanding Your Partner's Brain and Attachment Style Can Help You Defuse Conflict and Build a Secure Relationship Stronger Than Steel: Spider Silk DNA and the Quest for Better Bulletproof Vests, Sutures, and Parachute Rope (Scientists in the Field Series) The Bulletproof Diet: Lose Up to a Pound a Day, Reclaim Your Energy and Focus, and Upgrade Your Life

Dmca