

Bulletproof Ssl And Tls

This completely revised and expanded second edition of SSL and TLS: Theory and Practice provides an overview and a comprehensive discussion of the Secure Sockets Layer (SSL), Transport Layer Security (TLS), and Datagram TLS (DTLS) protocols that are omnipresent in today's e-commerce and e-business applications and respective security solutions. It provides complete details on the theory and practice of the protocols, offering readers a solid understanding of their design principles and modes of operation. Updates to this edition include coverage of the recent attacks against the protocols, newly specified extensions and firewall traversal, as well as recent developments related to public key certificates and respective infrastructures. This book targets software developers, security professionals, consultants, protocol designers, and chief security officers who will gain insight and perspective on the many details of the SSL, TLS, and DTLS protocols, such as cipher suites, certificate management, and alert messages. The book also comprehensively discusses the advantages and disadvantages of the protocols compared to other Internet security protocols and provides the details necessary to correctly implement the protocols while saving time on the security practitioner's side.

ModSecurity Handbook is the definitive guide to ModSecurity, the popular open source web application firewall. Written by Christian Folini and ModSecurity's original developer, Ivan Ristic, this book will teach you how to monitor activity on your web sites and protect them from attack. Situated between your web sites and the world, web application firewalls provide an additional security layer, monitoring everything that comes in and everything that goes out in real time. They enable you to perform many advanced activities, such as access control, virtual patching, HTTP traffic logging, continuous passive security assessment, and web application hardening. Web application firewalls can be very effective in preventing application security attacks, such as SQL injection, cross-site scripting, remote file inclusion, and others that plague most web sites today. ModSecurity Handbook covers the following topics, which will help anyone with a web site to run: Installation and configuration of ModSecurity Detailed guide to writing rules IP address, session, and user tracking Session management hardening Whitelisting, blacklisting, and IP reputation management Anomaly scoring and advanced blocking strategies Integration with other Apache modules Working with predefined rule sets Virtual patching and content injection Performance considerations Writing rules in Lua and extending ModSecurity in C Detailed coverage of ModSecurity's numerous directives, variables, transformations, and operators The book is suitable for all reader levels: It takes newcomers by the hand to turn them into seasoned users, while seasoned users will learn advanced techniques from the top experts on the subject and find hidden clues to master the rule language. An updated ModSecurity Reference Manual is included in the second part of the book.

ABOUT THE AUTHORS Dr. Christian Folini is a twelve-year veteran of ModSecurity. He is a renowned speaker, teacher, and system engineer who has specialized in securing high-profile web servers. Christian is one of the leaders of the OWASP ModSecurity Core Rule Set project, a key member of the ModSecurity community, program chair of the Swiss Cyber Storm conference, and vice president of Swiss Cyber Experts (a public-private partnership). Ivan Ristic is a security researcher, engineer, and author, known especially for his contributions to the web application firewall field and development of ModSecurity, an open source web application firewall, and for his SSL/TLS and PKI research, tools and guides published on the SSL Labs web site. His latest project, Hardenize, is a security posture analysis service that makes security fun again. He is the author of three books, Apache Security, ModSecurity Handbook, and Bulletproof SSL and TLS.

Rigorous in its definitions yet easy to read, Crypto Dictionary covers the field of cryptography in an approachable, and sometimes humorous way. Expand your mind and your crypto knowledge with the ultimate desktop dictionary for all things cryptography. Written by a renowned cryptographer for experts and novices alike, Crypto Dictionary is rigorous in its definitions, yet easy to read and laced with humor. Flip to any random page to find something new, interesting, or mind-boggling, such as:

- A survey of crypto algorithms both widespread and niche, from RSA and DES to the USSR's GOST cipher
- Trivia from the history of cryptography, such as the MINERVA backdoor in Crypto AG's encryption algorithms
- An explanation of why the reference to the Blowfish cipher in the TV show 24 makes absolutely no sense
- Types of cryptographic protocols like zero-knowledge; security; and proofs of work, stake, and resource
- A polemic against referring to cryptocurrency as "crypto"
- Discussions of numerous cryptographic attacks, including slide and biclique

The book also looks toward the future of cryptography, with discussions of the threat quantum computing poses to current cryptosystems and a nod to post-quantum algorithms, such as lattice-based cryptographic schemes. With hundreds of incisive entries organized alphabetically, Crypto Dictionary is the crypto go-to guide you'll always want within reach.

Get in-depth guidance for designing and implementing certificate-based security solutions—straight from PKI expert Brian Komar. No need to buy or outsource costly PKI services when you can use the robust PKI and certificate-based security services already built into Windows Server 2008! This in-depth reference teaches you how to design and implement even the most demanding certificate-based security solutions for wireless networking, smart card authentication, VPNs, secure email, Web SSL, EFS, and code-signing applications using Windows Server PKI and certificate services. A principal PKI consultant to Microsoft, Brian shows you how to incorporate best practices, avoid common design and implementation mistakes, help minimize risk, and optimize security administration.

SSL & TLS Essentials

GSM, UMTS, 802.11, and Ad Hoc Security

Analyzing Computer Security

A Guide to PKI Operations

A Threat/vulnerability/countermeasure Approach

Android Hacker's Handbook

Security in Computing and Communications

The bash shell is a complete programming language, not merely a glue to combine external Linux commands. By taking full advantage of shell internals, shell programs can perform as snappily as utilities written in C or other compiled languages. And you will see how, without assuming Unix lore, you can write professional bash 4.0 programs through standard programming

techniques. Complete bash coverage Teaches bash as a programming language Helps you master bash 4.0 features Introduces the concepts of public key infrastructure design and policy and discusses use of the technology for computer network security in the business environment.

Bulletproof SSL and TLS Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications Feisty Duck CD-ROM contains: text in a searchable Adobe Acrobat file ([http.pdf](http://pdf)); Adobe Acrobat Reader 4.0 for Windows and MacOS.

Understanding PKI

Governance, Risk, and Compliance for PKI Operations

Bulletproof Wireless Security

Advances in Security, Networks, and Internet of Things

What Every Programmer Needs to Know

SSL and TLS

Recipe-based guide for security, networking and PKI in Windows Server 2016

The perimeter defenses guarding your network perhaps are not as secure as you think. Hosts behind the firewall have no defenses of their own, so when a host in the "trusted" zone is breached, access to your data center is not far behind. That's an all-too-familiar scenario today. With this practical book, you'll learn the principles behind zero trust architecture, along with details necessary to implement it. The Zero Trust Model treats all hosts as if they're internet-facing, and considers the entire network to be compromised and hostile. By taking this approach, you'll focus on building strong authentication, authorization, and encryption throughout, while providing compartmentalized access and better operational agility. Understand how perimeter-based defenses have evolved to become the broken model we use today Explore two case studies of zero trust in production networks on the client side (Google) and on the server side (PagerDuty) Get example configuration for open source tools that you can use to build a zero trust network Learn how to migrate from a perimeter-based network to a zero trust network in production

*Updated for Docker Community Edition v18.09! Docker book designed for SysAdmins, SREs, Operations staff, Developers and DevOps who are interested in deploying the open source container service Docker. In this book, we'll walk you through installing, deploying, managing, and extending Docker. We're going to do that by first introducing you to the basics of Docker and its components. Then we'll start to use Docker to build containers and services to perform a variety of tasks. We're going to take you through the development lifecycle, from testing to production, and see where Docker fits in and how it can make your life easier. We'll make use of Docker to build test environments for new projects, demonstrate how to integrate Docker with continuous integration workflow, and then how to build application services and platforms. Finally, we'll show you how to use Docker's API and how to extend Docker yourself. We'll teach you how to: * Install Docker. * Take your first steps with a Docker container. * Build Docker images. * Manage and share Docker images. * Run and manage more complex Docker containers. * Deploy Docker containers as part of your testing pipeline. * Build multi-container applications and environments. * Learn about orchestration using Compose and Swarm for the orchestration of Docker containers and Consul for service discovery. * Explore the Docker API. * Getting Help and Extending Docker.*

This publication seeks to assist organizations in mitigating the risks associated with the transmission of sensitive information across networks by providing practical guidance on implementing security services based on Internet Protocol Security (IPsec).

PRODUCT DESCRIPTION ModSecurity Handbook is the definitive guide to ModSecurity, a popular open source web application firewall. Written by Ivan Ristic, who designed and wrote much of ModSecurity, this book will teach you everything you need to know to monitor the activity on your web sites and protect them from attack. Situated between your web sites and the world, web application firewalls provide an additional security layer, monitoring everything that comes in and everything that goes out. They enable you to perform many advanced activities, such as real-time application security monitoring, access control, virtual patching, HTTP traffic logging, continuous passive security assessment, and web application hardening. They can be very effective in preventing application security attacks, such as cross-site scripting, SQL injection, remote file inclusion, and others. Considering that most web sites today suffer from one problem or another, ModSecurity Handbook will help anyone who has a web site to run. The topics covered include: - Installation and configuration of ModSecurity - Logging of complete HTTP traffic - Rule writing, in detail - IP address, session, and user tracking - Session management hardening - Whitelisting, blacklisting, and IP reputation management - Advanced blocking strategies - Integration with other Apache modules - Working with rule sets - Virtual patching - Performance considerations - Content injection - XML inspection - Writing rules in Lua - Extending ModSecurity in C The book is suitable for all reader levels: it contains step-by-step installation and configuration instructions for those just starting out, as well as detailed explanations of the internals and discussion of advanced techniques for seasoned users. The official ModSecurity Reference Manual is included in the second part of the book. A digital version is available. For more information and to access the online companion, go to www.modsecurityhandbook.com ABOUT THE AUTHOR Ivan Ristic is a respected security expert and author, known especially for his contribution to the web application firewall field and the development of ModSecurity, the open source web application firewall. He is also the author of Apache Security, a comprehensive security guide for the Apache web server. A frequent speaker at computer security conferences, Ivan is an active participant in the application security community, a member of the Open Web Application Security Project, and an officer of the Web Application Security Consortium.

The Antivirus Hacker's Handbook

Pro Bash Programming

500 Tasty Tidbits for the Curious Cryptographer

Securing the Web

Windows Server 2016 Security, Certificates, and Remote Access Cookbook

SSL and TLS: Theory and Practice, Second Edition

Server Security from TLS to Tor

""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

Hack your antivirus software to stamp out future vulnerabilities The Antivirus Hacker's Handbook guides you through the process of reverse engineering antivirus software. You explore how to detect and exploit vulnerabilities that can be leveraged to improve future software design, protect your network, and anticipate attacks that may sneak through your antivirus' line of defense. You'll begin building your knowledge by diving into the reverse engineering process, which details how to start from a finished antivirus software program and work your way back through its development using the functions and other key elements of the software. Next, you leverage your new knowledge about software development to evade, attack, and exploit antivirus software—all of which can help you strengthen your network and protect your data. While not all viruses are damaging, understanding how to better protect your computer against them can help you maintain the integrity of your network. Discover how to reverse engineer your antivirus software Explore methods of antivirus software evasion Consider different ways to attack and exploit antivirus software Understand the current state of the antivirus software market, and get recommendations for users and vendors who are leveraging this software The Antivirus Hacker's Handbook is the essential reference for software reverse engineers, penetration testers, security researchers, exploit writers, antivirus vendors, and software engineers who want to understand how to leverage current antivirus software to improve future applications. Finally--a single volume guide to really effective security for both voice and data wireless networks! More and more data and voice communications are going via wireless at some point between the sender and intended recipient. As a result, truly "bulletproof" wireless security is now more than a desirable feature--instead, it's a necessity to protect essential personal and business data from hackers and eavesdroppers. In this handy reference, Praphul Chandra gives you the conceptual and practical tools every RF, wireless, and network engineer needs for high-security wireless applications. Inside this book you'll find coverage of these essential topics: + Cryptographic protocols used in wireless networks. + Key-based protocols, including key exchange and authentication techniques + Various types of wireless network attacks, including reflection, session hijacks, and Fluhrer-Mantin-Shamir (FMS) attacks. + Encryption/decryption standards and methods. + Multi-layered security architectures. + Secure sockets layer (SSL) and transport layer security (TLS) protocols. + Cellular telephone network architectures and their vulnerabilities. + Modulation techniques, such as direct-sequence spread spectrum (DSSS) and orthogonal frequency division multiplexing (OFDM) And you'll also find coverage on such cutting-edge topics as security techniques for ad hoc networks and protecting Bluetooth networks. If you're serious about wireless security, then this title belongs on your reference bookshelf!

This book constitutes the refereed proceedings of the 4th International Symposium on Security in Computing and Communications, SSCC 2016, held in Jaipur, India, in September 2016. The 23 revised full papers presented together with 16 short papers and an invited paper were carefully reviewed and selected from 136 submissions. The papers are organized in topical sections on cryptosystems, algorithms, primitives; security and privacy in networked systems; system and network security; steganography, visual cryptography, image forensics; applications security.

Scripting the Linux Shell

The Colony of New Netherland

A Dutch Settlement in Seventeenth-century America

Windows Server 2008 PKI and Certificate Security

Security Engineering

Applied Computing and Information Technology

Network Security with OpenSSL

In this book, the authors of the 20-year best-selling classic Security in Computing take a fresh, contemporary, and powerfully relevant new approach to introducing computer security. Organised around attacks and mitigations, the Pfleegers' new Analyzing Computer Security will attract students' attention by building on the high-profile security failures they may have already encountered in the popular media. Each section starts with an attack description. Next, the authors explain the vulnerabilities that have allowed this attack to occur. With this foundation in place, they systematically present today's most effective countermeasures for blocking or weakening the attack. One step at a time, students progress from attack/problem/harm to solution/protection/mitigation, building the powerful real-world problem solving skills they need to succeed as information security professionals. Analyzing Computer Security addresses crucial contemporary computer security themes throughout, including effective security management and risk analysis; economics and quantitative study; privacy, ethics, and laws; and the use of overlapping controls. The authors also present significant new material on computer forensics, insiders, human factors, and trust.

The IBM® i operation system (formerly IBM i5/OS®) is considered one of the most secure systems in the industry. From the beginning, security was designed as an integral part of the system. The System i® platform provides a rich set of security features and services that pertain to the goals of authentication, authorization, integrity, confidentiality, and auditing. However, if an IBM Client does not know that a service, such as a virtual private network (VPN) or hardware cryptographic support, exists on the system, it will not use it. In addition, there are more and more security auditors and consultants who are in charge of implementing corporate security policies in an organization. In many cases, they are not familiar with the IBM i operating system, but must understand the security services that are available. This IBM Redbooks® publication guides you through the broad range of native security features that are available within IBM i Version and release level 6.1. This book is intended for security auditors and consultants, IBM System Specialists, Business Partners, and clients to help you answer first-level questions concerning the security features that are available under IBM.

The focus in this publication is the integration of IBM 6.1 enhancements into the range of security facilities available within IBM i up through Version release level 6.1. IBM i 6.1 security enhancements include: - Extended IBM i password rules and closer affinity between normal user IBM i operating system user profiles and IBM service tools user profiles - Encrypted disk data within a user Auxiliary Storage Pool (ASP) - Tape data save and restore encryption under control of the Backup Recovery and Media Services for i5/OS (BRMS) product, 5761-BR1 - Networking security enhancements including additional control of Secure Sockets Layer (SSL) encryption rules and greatly expanded IP intrusion detection protection and actions. DB2® for i5/OS built-in column encryption expanded to include support of the Advanced Encryption Standard (AES) encryption algorithm to the already available Rivest Cipher 2 (RC2) and Triple DES (Data Encryption Standard) (TDES) encryption algorithms. The IBM i V5R4 level IBM Redbooks publication IBM System i Security Guide for IBM i5/OS Version 5 Release 4, SG24-6668, remains available.

Set up a secure network at home or the office Fully revised to cover Windows 10 and Windows Server 2019, this new edition of the trusted Networking For Dummies helps both beginning network administrators and home users to set up and maintain a network. Updated coverage of broadband and wireless technologies, as well as storage and back-up procedures, ensures that you'll learn how to build a wired or wireless network, secure and optimize it, troubleshoot problems, and much more. From connecting to the Internet and setting up a wireless network to solving networking problems and backing up your data—this #1 bestselling guide covers it all. Build a wired or wireless network Secure and optimize your network Set up a server and manage Windows user accounts Use the cloud—safely Written by a seasoned technology author—and jam-packed with tons of helpful step-by-step instructions—this is the book network administrators and everyday computer users will turn to again and again.

This book contains more than 25 hands-on recipes that will equip you to build a PKI and roll out remote access capabilities via Microsoft DirectAccess and VPN. This book also contains tips and tricks for increasing the security footprint of your Windows Server infrastructure. Key Features Identify and mitigate security risks in your Windows Server 2016 infrastructure Learn how to build a PKI and use it to issue certificates within your network In-depth information for setting up Microsoft DirectAccess Book Description Windows Server 2016 is an operating system designed to run on today's highly performant servers, both on-premise and in the cloud. It supports enterprise-level data storage, communications, management, and applications. This book builds off a basic knowledge of the Windows Server operating system, and assists administrators with taking the security of their systems one step further. You will learn tips for configuring proper networking, especially on multi-homed systems, and tricks for locking down access to your servers. Then you will move onto one of the hottest security topics of the year – certificates. You will learn how to build your own PKI, or how to better administer one that you already have. You will publish templates, issue certificates, and even configure autoenrollment in your network. When we say “networking” we don't only mean inside the LAN. To deal safely with mobile devices, you will learn about the capabilities of Windows Server 2016 for connecting these assets securely back into the corporate network, with information about DirectAccess and VPN. The material in the book has been selected from the content of Packt's Windows Server 2016 Cookbook by Jordan Krause to provide a specific focus on these key Windows Server tasks. What you will learn Implement solid networking and security practices into your Windows Server environment Design your own PKI and start issuing certificates today Connect your remote laptops back to the corporate network using Microsoft's own remote access technologies, including DirectAccess Learn to use commands that will help you with monitoring network traffic. Build and explore your first Server Core instance today! Who this book is for If you are a Windows Server administrator interested in learning the key security and networking functions available in Windows Server 2016, keep this book close at hand. If you are a server administrator setting up certificate services for the first time you will also benefit from the step-by-step instructions on implementation of a PKI.

Modsecurity Handbook, Second Edition

4th International Symposium, SSCC 2016, Jaipur, India, September 21-24, 2016, Proceedings

Nginx HTTP Server

Modsecurity Handbook

Protocols for Secure, Scalable Web Sites

Network Security Hacks

Security Guide for IBM i V6.1

Pragmatically, a PKI is an operational system that employs asymmetric cryptography, information technology, operating rules, physical and logical security, and legal matters. Much like any technology, cryptography in general undergoes changes: sometimes evolutionary, sometimes dramatically, and sometimes unknowingly. This book discusses what not to do in PKI operations. Providing a no-nonsense approach and multiple case studies, the book is a straightforward, real-world guide to how to successfully operate a PKI system. Make the most of your infrastructure and serve pages faster than ever with Nginx. Key Features Discover possible interactions between Nginx and Apache to get the best of both worlds Learn to exploit the features offered by Nginx for your web applications Get your hands on the most updated version of Nginx (1.13.2) to support all your web administration requirements Book Description Nginx is a lightweight HTTP server designed for high-traffic websites, with network scalability as the primary objective. With the advent of high-speed internet access, short loading times and fast transfer rates have become a necessity. This book is a detailed guide to setting up Nginx in ways that correspond to actual production situations: as a standalone server, as a reverse proxy, interacting with applications via FastCGI, and more. In addition, this complete direct reference will be indispensable at all stages of the configuration and maintenance processes. This book mainly targets the most recent version of Nginx (1.13.2) and focuses on all the new additions and improvements, such as support for HTTP/2, improved dynamic modules, security enhancements, and support for multiple SSL certificates. This book is the perfect companion for both Nginx beginners and experienced administrators. For beginners, it will take you through the complete process of setting up this lightweight HTTP server on your system and configuring its various modules so that it does exactly what you need quickly and securely. For more experienced administrators, this book provides different approaches that can help you make the most of your current infrastructure. Nginx can be employed in many situations, whether you are looking to construct an entirely new web-serving architecture or simply want to integrate an efficient tool to optimize your site loading speeds. What you will learn Download and install Nginx on your system Prepare a basic configuration and test your initial setup Discover the core functionality of the HTTP module Make the most of first- and third-party Nginx modules Set up Nginx to work with PHP, Python, and other applications Learn how to set up Nginx to work with Apache Fully replace Apache with Nginx Optimize your architecture with threads or load balancing Identify errors in configuration and learn basic troubleshooting techniques Consult the exhaustive directive and module index for reference Who this book is for This book is a perfect match to web administrators who are interested in solutions to optimize their infrastructure. Whether you are looking into replacing your existing web server software or integrating a new tool to cooperate with applications that are already up and running, this book is your ideal resource.

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 version - For IT security professionals, help to understand the risks - For system administrators, help to deploy systems securely - For developers, help to design and implement secure web applications - Practical and concise, with added depth when details are relevant - Introduction to cryptography and the latest TLS protocol version - Discussion of weaknesses at every level, covering implementation issues, HTTP and browser problems, and protocol vulnerabilities -

Coverage of the latest attacks, such as BEAST, CRIME, BREACH, Lucky 13, RC4 biases, Triple Handshake Attack, and Heartbleed - Thorough deployment advice, including advanced technologies, such as Strict Transport Security, Content Security Policy, and pinning - Guide to using OpenSSL to generate keys and certificates and to create and run a private certification authority - Guide to using OpenSSL to test servers for vulnerabilities - Practical advice for secure server configuration using Apache httpd, IIS, Java, Nginx, Microsoft Windows, and Tomcat This book is available in paperback and a variety of digital formats without DRM.

Implement Industrial-Strength Security on Any Linux Server In an age of mass surveillance, when advanced cyberwarfare weapons rapidly migrate into every hacker's toolkit, you can't rely on outdated security methods—especially if you're responsible for Internet-facing services. In *Linux® Hardening in Hostile Networks*, Kyle Rankin helps you to implement modern safeguards that provide maximum impact with minimum effort and to strip away old techniques that are no longer worth your time. Rankin provides clear, concise guidance on modern workstation, server, and network hardening, and explains how to harden specific services, such as web servers, email, DNS, and databases. Along the way, he demystifies technologies once viewed as too complex or mysterious but now essential to mainstream Linux security. He also includes a full chapter on effective incident response that both DevOps and SecOps can use to write their own incident response plan. Each chapter begins with techniques any sysadmin can use quickly to protect against entry-level hackers and presents intermediate and advanced techniques to safeguard against sophisticated and knowledgeable attackers, perhaps even state actors. Throughout, you learn what each technique does, how it works, what it does and doesn't protect against, and whether it would be useful in your environment. Apply core security techniques including 2FA and strong passwords Protect admin workstations via lock screens, disk encryption, BIOS passwords, and other methods Use the security-focused Tails distribution as a quick path to a hardened workstation Compartmentalize workstation tasks into VMs with varying levels of trust Harden servers with SSH, use apparmor and sudo to limit the damage attackers can do, and set up remote syslog servers to track their actions Establish secure VPNs with OpenVPN, and leverage SSH to tunnel traffic when VPNs can't be used Configure a software load balancer to terminate SSL/TLS connections and initiate new ones downstream Set up standalone Tor services and hidden Tor services and relays Secure Apache and Nginx web servers, and take full advantage of HTTPS Perform advanced web server hardening with HTTPS forward secrecy and ModSecurity web application firewalls Strengthen email security with SMTP relay authentication, SMTPS, SPF records, DKIM, and DMARC Harden DNS servers, deter their use in DDoS attacks, and fully implement DNSSEC Systematically protect databases via network access control, TLS traffic encryption, and encrypted data storage Respond to a compromised server, collect evidence, and prevent future attacks Register your product at informit.com/register for convenient access to downloads, updates, and corrections as they become available.

Cryptography for Secure Communications

Zero Trust Networks

Networking For Dummies

A Guide to Building Dependable Distributed Systems

OpenSSL Cookbook

Linux Hardening in Hostile Networks

Building Secure Systems in Untrusted Networks

Introduces more than one hundred effective ways to ensure security in a Linux, UNIX, or Windows network, covering both TCP/IP-based services and host-based security techniques, with examples of applied encryption, intrusion detections, and logging.

Most applications these days are at least somewhat network aware, but how do you protect those applications against common network security threats? Many developers are turning to OpenSSL, an open source version of SSL/TLS, which is the most widely used protocol for secure network communications. The OpenSSL library is seeing widespread adoption for web sites that require cryptographic functions to protect a broad range of sensitive information, such as credit card numbers and other financial transactions. The library is the only free, full-featured SSL implementation for C and C++, and it can be used programmatically or from the command line to secure most TCP-based network protocols. Network Security with OpenSSL enables developers to use this protocol much more effectively. Traditionally, getting something simple done in OpenSSL could easily take weeks. This concise book gives you the guidance you need to avoid pitfalls, while allowing you to take advantage of the library's advanced features. And, instead of bogging you down in the technical details of how SSL works under the hood, this book provides only the information that is necessary to use OpenSSL safely and effectively. In step-by-step fashion, the book details the challenges in securing network communications, and shows you how to use OpenSSL tools to best meet those challenges. As a system or network administrator, you will benefit from the thorough treatment of the OpenSSL command-line interface, as well as from step-by-step directions for obtaining certificates and setting up your own certification authority. As a developer, you will further benefit from the in-depth discussions and examples of how to use OpenSSL in your own programs. Although OpenSSL is written in C, information on how to use OpenSSL with Perl, Python and PHP is also included. OpenSSL may well answer your need to protect sensitive data. If that's the case, Network Security with OpenSSL is the only guide available on the subject.

Software developers need to worry about security as never before. They need clear guidance on safe coding practices, and that's exactly what this book delivers. The book does not delve deep into theory, or rant about the politics of security. Instead, it clearly and simply lays out the most common threats that programmers need to defend against. It then shows programmers how to make their defense. The book takes a broad focus, ranging over SQL injection, worms and buffer overflows, password security, and more. It sets programmers on the path towards successfully defending against the entire gamut of security threats that they might face.

This book presents the selected results of the 1st International Symposium on Applied Computers and Information Technology (ACIT 2013) held on August 31 – September 4, 2013 in Matsue City, Japan, which brought together researchers, scientists, engineers, industry practitioners and students to discuss all aspects of Applied Computers & Information Technology and its practical challenges. This book includes the best 12 papers presented at the conference, which were chosen based on review scores submitted by members of the program committee and underwent further rigorous rounds of review.

What every web developer should know about networking and web performance

Apache Security

Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications

Security in Computing

BULLETPROOF SSL AND TLS.

Security without Obscurity

Foundations of Security

"The complete guide to securing your Apache web server"--Cover.

The book presents the proceedings of four conferences: The 19th International Conference on Security & Management (SAM'20), The 19th International Conference on Wireless Networks (ICWN'20), The 21st International Conference on

Computing & Internet of Things (ICOMP'20), and The 18th International Conference on Embedded Systems, Cyber-ph Systems (ESCS'20). The conferences took place in Las Vegas, NV, USA, July 27-30, 2020. The conferences are part of the 2020 World Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE'20), which features 2 tracks. Authors include academics, researchers, professionals, and students. Presents the proceedings of four conferences of the 2020 World Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE'20); Includes topics on security & management, wireless networks, internet computing and IoT, and embedded systems as well as cyber systems; Features papers from SAM'20, ICWN'20, ICOMP'20 and ESCS'20.

A guide to the most frequently used OpenSSL features and commands, written by Ivan Ristic. Comprehensive coverage of OpenSSL installation, configuration, and key and certificate management Includes SSL/TLS Deployment Best Practices and deployment guide Written by a well-known practitioner in the field and the author of SSL Labs and the SSL/TLS configuration assessment tool Available in a variety of digital formats (PDF, EPUB, Mobi/Kindle); no DRM Continuously updated OpenSSL Cookbook is built around one chapter from Bulletproof SSL/TLS and PKI, a larger work that provides complete coverage of SSL/TLS and PKI topics. To download your free copy in various formats, visit feistyduck.com/bulletproof-cookbook/

How prepared are you to build fast and efficient web applications? This eloquent book provides what every web developer knows about the network, from fundamental limitations that affect performance to major innovations for building even more powerful browser applications—including HTTP 2.0 and XHR improvements, Server-Sent Events (SSE), WebSocket, and WebRTC. Author Ilya Grigorik, a web performance engineer at Google, demonstrates performance optimization best practices for TCP, UDP, and TLS protocols, and explains unique wireless and mobile network optimization requirements. You'll then explore performance characteristics of technologies such as HTTP 2.0, client-side network scripting with XHR, real-time streaming with SSE and WebSocket, and P2P communication with WebRTC. Deliver superlative TCP, UDP, and TLS performance Speed up network performance over 3G/4G mobile networks Develop fast and energy-efficient mobile applications Address bottlenecks in HTTP 1.x and other browser protocols Plan for and deliver the best HTTP 2.0 performance Enable efficient real-time communication in the browser Create efficient peer-to-peer videoconferencing and low-latency applications with real-time WebRTC Harness the power of Nginx to make the most of your infrastructure and serve pages faster than ever before, 4th Edition Containerization Is the New Virtualization

A Guide to the Most Frequently Used OpenSSL Features and Commands

HTTP Essentials

Designing and Building Secure Systems

Trust Me

Proceedings from SAM'20, ICWN'20, ICOMP'20, and ESCS'20

The Dutch involvement in North America started after Henry Hudson, sailing under a Dutch flag in 1609, traveled up the river that would later bear his name. The Dutch control of the region was short-lived, but had profound effects on the Hudson Valley region. In *The Colony of New Netherland*, Jaap Jacobs offers a comprehensive history of the Dutch colony on the Hudson from the first trading voyages in the 1610s to 1674, when the Dutch ceded the colony to the English. As Jacobs shows, New Netherland offers a distinctive example of economic colonization and in its social and religious profile represents a noteworthy divergence from the English colonization in North America. Centered around New Amsterdam on the island of Manhattan, the colony extended north to present-day Schenectady, New York, east to central Connecticut, and south to the border shared by Delaware, New Jersey, and Pennsylvania, leaving an indelible imprint on the culture, political geography, and language of the early modern mid-Atlantic region. Dutch colonists' vivid accounts of the land and people of the area shaped European perceptions of this bountiful land; their own activities had a lasting effect on land use and the flora and fauna of New York State, in particular, as well as on relations with the Native people with whom they traded. Sure to become readers' first reference to this crucial phase of American early colonial history, *The Colony of New Netherland* is a multifaceted and detailed depiction of life in the colony, from exploration and settlement through governance, trade, and agriculture. Jacobs gives a keen sense of the built environment and social relations of the Dutch colonists and closely examines the influence of the church and the social system adapted from that of the Dutch Republic. Although Jacobs focuses his narrative on the realities of quotidian existence in the colony, he considers that way of life in the broader context of the Dutch Atlantic and in comparison to other European settlements in North America.

Now that there's software in everything, how can you make anything secure? Understand how to engineer dependable systems with this newly updated classic *In Security Engineering: A Guide to Building Dependable Distributed Systems*, Third Edition Cambridge University professor Ross Anderson updates his classic textbook and teaches readers how to design, implement, and test systems to withstand both error and attack. This book became a best-seller in 2001 and helped establish the discipline of security engineering. By the second edition in 2008, underground dark markets had let the bad guys specialize and scale up; attacks were increasingly on users rather than on technology. The book repeated its success by showing how security engineers can focus on usability. Now the third edition brings it up to date for 2020. As people now go online from phones more than laptops, most servers are in the cloud, online advertising drives the Internet and social networks have taken over much human interaction, many patterns of crime and abuse are the same, but the methods have evolved. Ross Anderson explores what security engineering means in 2020, including: How the basic elements of cryptography, protocols, and access control translate to the new world of phones, cloud services, social media and the Internet of Things Who the attackers are - from nation states and business competitors through criminal gangs to stalkers and playground bullies What they do - from phishing and carding through SIM swapping and software exploits to DDoS and fake news Security psychology, from privacy through ease-of-use to deception The economics of

security and dependability – why companies build vulnerable systems and governments look the other way How dozens of industries went online – well or badly How to manage security and safety engineering in a world of agile development – from reliability engineering to DevSecOps The third edition of Security Engineering ends with a grand challenge: sustainable security. As we build ever more software and connectivity into safety-critical durable goods like cars and medical devices, how do we design systems we can maintain and defend for decades? Or will everything in the world need monthly software upgrades, and become unsafe once they stop?

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 TCPDump and OpenSSL Understanding the Pitfalls of SSLv2 Set up and launch a working implementation of SSL with this practical guide.

The first comprehensive guide to discovering and preventing attacks on the Android OS As the Android operating system continues to increase its share of the smartphone market, smartphone hacking remains a growing threat. Written by experts who rank among the world's foremost Android security researchers, this book presents vulnerability discovery, analysis, and exploitation tools for the good guys. Following a detailed explanation of how the Android OS works and its overall security architecture, the authors examine how vulnerabilities can be discovered and exploits developed for various system components, preparing you to defend against them. If you are a mobile device administrator, security researcher, Android app developer, or consultant responsible for evaluating Android security, you will find this guide is essential to your toolbox. A crack team of leading Android security researchers explain Android security risks, security design and architecture, rooting, fuzz testing, and vulnerability analysis Covers Android application building blocks and security as well as debugging and auditing Android apps Prepares mobile device administrators, security researchers, Android app developers, and security consultants to defend Android systems against attack Android Hacker's Handbook is the first comprehensive resource for IT professionals charged with smartphone security. Concepts, Standards, and Deployment Considerations

Guide to Ipsec Vpns

High Performance Browser Networking

The Docker Book

Bulletproof SSL and TLS

Recommendations of the National Institute of Standards and Technology

CD-ROM includes: Full-text, electronic edition of text.

Most books on public key infrastructure (PKI) seem to focus on asymmetric cryptography, X.509 certificates, certificate authority (CA) hierarchies, or certificate policy (CP), and certificate practice statements. While algorithms, certificates, and theoretical policy are all excellent discussions, the real-world issues for operating a commercial or
Trust Me by Brenda Novak The Last Stand (Book 1) This classic story of romantic suspense by New York Times bestselling author Brenda Novak “generates genuine thrills.” (Publishers Weekly) Four years ago, Skye Kellerman was attacked in her own bed. She managed to fend off her knife-wielding assailant, but the trauma changed everything about her life. As a result of that night, she joined two friends—also survivors—in starting The Last Stand, an organization to help victims of crime. But now, her would-be rapist is getting out of prison. Skye knows that Dr. Oliver Burke hasn't forgotten that her testimony cost him his reputation—and his freedom. Sacramento detective David Willis, who investigated her case, believes Burke is a clear and present danger—and guilty of at least two unsolved murders. And now Burke is free to terrorize Skye again. Unless David can stop him. Unless Skye can fight back. Because Oliver Burke has every intention of finishing what he started. And that's a promise. Trust me. Originally published in 2008

Implementing SSL / TLS Using Cryptography and PKI

Crypto Dictionary