Price List Viega

Although most people don't give security much attention until their personal or business systems are attacked, this thought-provoking anthology demonstrates that digital security is not only worth thinking about, it's also a fascinating topic. Criminals succeed by exercising enormous creativity, and those defending against them must do the same. Beautiful Security explores this challenging subject with insightful essays and analysis on topics that include: The underground economy for personal information: how it works, the relationships among criminals, and some of the new ways they pounce on their prey How social networking, cloud computing, and other popular trends help or hurt our online security How metrics, requirements gathering, design, and law can take security to a higher level The real, little-publicized history of PGP This book includes contributions from: Peiter "Mudge" Zatko Jim Stickley Elizabeth Nichols Chenxi Wang Ed Bellis Ben Edelman Phil Zimmermann and Jon Callas Kathy Wang Mark Curphey John McManus James Routh Randy V. Sabett Anton Chuvakin Grant Geyer and Brian Dunphy Peter Wayner Michael Wood and Fernando Francisco All royalties will be donated to the Internet Engineering Task Force (IETF).

Compares the architecture, management responsibilities, storage procedures, size, and reliability of the information storage and retrieval technologies.

Password sniffing, spoofing, buffer overflows, and denial of service: these are only a few of the attacks on today's computer systems and networks. At the root of this epidemic is poorly written, poorly tested, and insecure code that puts everyone at risk. Clearly, today's developers need help figuring out how to write code that attackers won't be able to exploit. But writing such code is surprisingly difficult. Secure Programming Cookbook for C and C++ is an important new resource for developers serious about writing secure code. It contains a wealth of solutions to problems faced by those who care about the security of their applications. It covers a wide range of topics, including safe initialization, access control, input validation, symmetric and public key cryptography, cryptographic hashes and MACs, authentication and key exchange, PKI, random numbers, and anti-tampering. The rich set of code samples provided in the book's more than 200 recipes will help programmers secure the C and C++ programs they write for both Unix® (including Linux®) and Windows® environments. Readers will learn: How to avoid common programming errors, such as buffer overflows, race conditions, and format string problems How to properly SSL-enable applications How to create secure channels for client-server communication without SSL How to integrate Public Key Infrastructure (PKI) into applications Best practices for using cryptography properly Techniques and strategies for properly validating input to programs How to launch programs securely How to use file access mechanisms properly Techniques for protecting applications from reverse engineering The book's web site supplements the book by providing a place to post new recipes, including those written in additional languages like Perl, Java, and Python. Monthly prizes will reward the best recipes submitted by readers. Secure Programming Cookbook for C and C++ is destined to become an essential part of any developer's library, a code companion developers will turn to again and again as they seek to protect their systems from attackers and reduce the risks they face in today's dangerous world.

For 10 years (and counting), The Naked Roommate has been the #1 go-to guide for your very best college experience! From sharing a bathroom with 40 strangers to sharing lecture notes, The Naked Roommate is your behind-the-scenes look at EVERYTHING you need to know about college (but never knew you needed to know). This essential, fully updated edition is packed with real-life advice on everything from making friends to managing stress. Hilarious, outrageous, and telling stories from students on over 100 college campuses cover the basics, and then some, including topics on College Living •Dorm dos, don'ts, and dramas •Lying, noisy, nasty roommates Finding People, Places, & Patience •Social network dos and don'ts •Friend today, gone tomorrow Classes •To go or not to go? •How to get an A, C, or F Dating •17 kinds of college hookups •Long distance = BIG concerns The Party Scene •The punch in the "fruit punch" •Sex, drugs, and safety first Money •Grants, loans, and loose change •Credit cards and campus jobs In college, there's a surprise around every corner. Luckily, The Naked Roommate has you covered!

Role Of The Churches

Introduces the concepts of public key infrastructure design and policy and discusses use of the technology for computer network security in the business environment.

"What makes this book so important is that it reflects the experiences of two of the industry's most experienced hands at getting real-world engineers to understand just what they're being asked for when they're asked to write secure code. The book reflects Michael Howard's and David LeBlanc's experience in the trenches working with developers years after code was long since shipped, informing them of problems." --From the Foreword by Dan Kaminsky, Director of Penetration Testing, IOActive Eradicate the Most Notorious Insecure Designs and Coding Vulnerabilities Fully updated to cover the latest security issues, 24 Deadly Sins of Software Security reveals the most common design and coding errors and explains how to fix each one-or better yet, avoid them from the start. Michael Howard and David LeBlanc, who teach Microsoft employees and the world how to secure code, have partnered again with John Viega, who uncovered the original 19 deadly programming sins. They have completely revised the book to address the most recent vulnerabilities and have added five brand-new sins. This practical guide covers all platforms, languages, and types of applications. Eliminate these security flaws from your code: SQL injection Web server- and client-related vulnerabilities Use of magic URLs, predictable cookies, and hidden form fields Buffer overruns Format string problems Integer overflows C++ catastrophes Insecure exception handling Command injection Failure to handle errors Information leakage Race conditions Poor usability Not updating easily Executing code with too much privilege Failure to protect stored data Insecure mobile code Use of weak password-based systems Weak random numbers Using cryptography incorrectly Failing to protect network traffic Improper use of PKI Trusting network name resolution

Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.

This professional guide presents an extensive overview of the German family enterprise landscape, with a special focus on its structure and diversity. Drawing on several scientific studies conducted by the authors, its goal is to provide a detailed assessment of the development of German family enterprises. Analyzing data from over 500 family firms, it offers a valuable reference guide for market research and academic research on family-owned enterprises. A unique factor: the authors’ revealing insights into the decline of family firms.

"This is a rich and learned volume that has a story to tell to those seeking to understand contemporary Southern California."—David Johnson, managing editor of the Pacific Historical Review "Engagingly written and well researched, California Vieja is an intriguing, persuasive examination of the politics of memory and the built environment in southern California."—Vicki Ruiz, author of From Out of the Shadows: Mexican Women in Twentieth-Century America

Health Canada's Pest Management Regulatory Agency (PMRA), under the authority of the Pest Control Products Act and Regulations, is proposing full registration for the sale and use of Prohexadione Calcium Technical Plant Growth Regulator and Apogee Plant Growth Regulator, containing the technical grade active ingredient prohexadione calcium, for use in apple orchards to reduce vegetative growth and to allow a balance between canopy development and fruit production. An evaluation of available scientific information found that, under the approved conditions of use, the product has value and does not present an unacceptable risk to human health or the environment. This document describes the key points of the evaluation and provides detailed technical information on the human health, environmental and value assessments of Prohexadione Calcium Technical Plant Growth Regulator and Apogee Plant Growth Regulator.--Includes text from document.

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.

Provides practical information about the design and installation of ductile iron pressure piping systems for water utilities. The 12 chapters outlines the procedure for calculating pipe wall thickness and class, and describes the types of joints, fittings, valves, linings, and corrosion protection a

This is the eagerly-anticipated revision to one of the seminal books in the field of software architecture which clearly defines and explains the topic.

""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

New articles from recent issues of the popular magazine have been added to "Remodeling a Bathroom" to provide readers with the very best current information on this ever-popular home improvement topic.

In its 114th year, Billboard remains the world's premier weekly music publication and a diverse digital, events, brand, content and data licensing platform. Billboard publishes the most trusted charts and offers unrivaled reporting about the latest music, video, gaming, media, digital and mobile entertainment issues and trends.

A collection of stories by Sandra Cisneros, the winner of the 2019 PEN/Nabokov Award for Achievement in International Literature. The lovingly drawn characters of these stories give voice to the vibrant and varied life on both sides of the Mexican border with tales of pure discovery, filled with moments of infinite and intimate wisdom.

Describes how to put software security into practice, covering such topics as risk analysis, coding policies, Agile Methods, cryptographic standards, and threat tree patterns.

This book describes new approaches to wireless security enabled by the recent development of new core technologies for Wi-Fi/802.11. It shows how the new approaches work and how they should be applied for maximum effect. For system administrators, product designers, or advanced home users.

In recent years, air pollution has become a major worldwide concern. Air pollutants can affect metabolic activity, impede healthy development, and exhibit carcinogenic and toxic properties in humans. Over the past two decades, the use of microbes to remove pollutants from contaminated air streams has become a widely accepted and efficient alternative to the classical physical and chemical treatment technologies. Air Pollution Prevention and Control: Bioreactors and Bioenergy focusses on these biotechnological alternatives looking at both the optimization of bioreactors and the development of cleaner biofuels. Structured in five parts, the book covers: Fundamentals and microbiological aspects Biofilters, bioscrubbers and other end-of-pipe treatment technologies Specific applications of bioreactors Biofuels production from pollutants and renewable resources (including biogas, biohydrogen, biodiesel and bioethanol) and its environmental impacts Case studies of applications including biotrickling filtration of waste gases, industrial bioscrubbers applied in different industries and biogas upgrading Air Pollution Prevention and Control: Bioreactors and Bioenergy is the first reference work to give a broad overview of bioprocesses for the mitigation of air pollution. Primarily intended for researchers and students in environmental engineering, biotechnology and applied microbiology, the book will also be of interest to industrial and governmental researchers.

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.

A guide to computer software security covers such topics as format string problems, command injection, cross-site scripting, SSL, information leakage, and key exchange.

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.

Introduces meditation and relaxation by presenting such imaginary situations as riding a unicorn, climbing a mountain, or being a king, with each exercise ending with an affirmation; and provides instructions to caregivers.

Publisher Description

In a rapidly changing world, there is an ever-increasing need to monitor the Earth’s resources and manage it sustainably for future generations. Earth observation from satellites is critical to provide information required for informed and timely decision making in this regard. Satellite-based earth observation has advanced rapidly over the last 50 years, and there is a plethora of satellite sensors imaging the Earth at finer spatial and spectral resolutions as well as high temporal resolutions. The amount of data available for any single location on the Earth is now at the petabyte-scale. An ever-increasing capacity and computing power is needed to handle such large datasets. The Google Earth Engine (GEE) is a cloud-based computing platform that was established by Google to support such data processing. This facility allows for the storage, processing and analysis of spatial data using centralized high-power computing resources, allowing scientists, researchers, hobbyists and anyone else interested in such fields to mine this data and understand the changes occurring on the Earth’s surface. This book presents research that applies the Google Earth Engine in mining, storing, retrieving and processing spatial data for a variety of applications that include vegetation monitoring, cropland mapping, ecosystem assessment, and gross primary productivity, among others. Datasets used range from coarse spatial resolution data, such as MODIS, to medium resolution datasets (Worldview -2), and the studies cover the entire globe at varying spatial and temporal scales.

Stellar author team of Microsoft MVPs helps developers and administrators get the most out of Windows IIS 8 If you're a developer or administrator, you'll want to get thoroughly up to speed on Microsoft's new IIS 8 platform with this complete, in-depth reference. Prepare yourself to administer IIS 8 in not only commercial websites and corporate intranets, but also the mass web hosting market with this expert content. The book covers common administrative tasks associated with monitoring and managing an IIS environment--and then moves well beyond, into extensibility, scripted admin, and other complex topics. The book highlights automated options outside the GUI, options that include the PowerShell provider and AppCmd tool. It explores extensibility options for developers, including ISAPI and HTTPModules. And, it delves into security protocols and high availability/load balancing at a level of detail that is not often found in IIS books. Author team includes Microsoft MVPs and an IIS team member Covers the management and monitoring of Microsoft Internet Information Services (IIS) 8 for administrators and developers, including MOF and MOM Delves into topics not often included in IIS books, including using the PowerShell provider and AppCmd tool and other automated options, and extending IIS 8 with ISAPI or HTTPModules Explores security issues in depth, including high availability/load balancing, and the Kerberos, NTLM, and PKI/SSL protocols Explains how to debug and troubleshoot IIS Professional Microsoft IIS 8 features a wealth of information gathered from individuals running major intranets and web hosting facilities today, making this an indispensible and real-world reference to keep on hand.

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.

In a brutal world where everyone is born an Alpha, beta, or omega, is it possible to be one birth nature but still lead a full life while pretending to be another? Tobias Hanson is a cop, specifically a homicide detective. The cases he investigates? Murdered omegas. Except in Tobias' world, an Alpha killing his omega is perfectly acceptable. After all, omegas are nothing more than easily replaced, purchased property. With his family long since gone, Tobias spends his days with dead omegas, and his nights in self-imposed solitary loneliness. Abundio Chale is an enigma. Like most alphas, he is highly educated, attractive, and possesses the same self-confidence all of his birth nature do. Yet, despite his schooling and his alpha privilege, he hops from job to job as if searching for something. And, like Tobias, he spends most evenings alone, longing for the one thing he doesn't have. A chance meeting puts both men on a path neither saw coming. Lives will change, love will be found, and both men may get exactly what they want. But, like most things, there will be a price to pay. Will it be worth it? Tags: GAY, EROTICA, DEGRADATION, HUMILIATION, SPH, SEXUAL SLAVERY, BRUTAL, DUB-CON, NON-CON

"The security of information systems has not improved at a rate consistent with the growth and sophistication of the attacks being made against them. To address this problem, we must improve the underlying strategies and techniques used to create our systems. Specifically, we must build security in from the start, rather than append it as an afterthought. That's the point of Secure Coding in C and C++. In careful detail, this book shows software developers how to build high-quality systems that are less vulnerable to costly and even catastrophic attack. It's a book that every developer should read before the start of any serious project." --Frank Abagnale, author, lecturer, and leading consultant on fraud prevention and secure documents Learn the Root Causes of Software Vulnerabilities and How to Avoid Them Commonly exploited software vulnerabilities are usually caused by avoidable software defects. Having analyzed nearly 18,000 vulnerability reports over the past ten years, the CERT/Coordination Center (CERT/CC) has determined that a relatively small number of root causes account for most of them. This book identifies and explains these causes and shows the steps that can be taken to prevent exploitation. Moreover, this book encourages programmers to adopt security best practices and develop a security mindset that can help protect software from tomorrow's attacks, not just today's. Drawing on the CERT/CC's reports and conclusions, Robert Seacord systematically identifies the program errors most likely to lead to security breaches, shows how they can be exploited, reviews the potential consequences, and presents secure alternatives. Coverage includes technical detail on how to Improve the overall security of any C/C++ application Thwart buffer overflows and stack-smashing attacks that exploit insecure string manipulation logic Avoid vulnerabilities and security flaws resulting from the incorrect use of dynamic memory management functions Eliminate integer-related problems: integer overflows, sign errors, and truncation errors Correctly use formatted output functions without introducing format-string vulnerabilities Avoid I/O vulnerabilities, including race conditions Secure Coding in C and C++ presents hundreds of examples of secure code, insecure code, and exploits, implemented for Windows and Linux. If you're responsible for creating secure C or C++ software--or for keeping it safe--no other book offers you this much detailed, expert assistance.