

Geekonomics The Real Cost Of Insecure Software

The Pompeii Syndrome Botnets Fuzzing for Software Security Testing and Quality Assurance, Second Edition Emotional Intelligence Geekonomics Sources for the Study of Greek Religion Cyber Security Policy Guidebook Ethical Hacking Developing Real World Software Open Source Practicing Organization Development International Security Studies Cyber Insecurity Digital Democracy and the Impact of Technology on Governance and Politics: New Globalized Practices Give the Pig a Chance & Other Stories Managing Risk and Information Security Heart-shaped Cookies The Dot Crime Manifesto Engineering Emergence Lucifer's Quest Your Brain: The Missing Manual Writing Secure Code Programming C# 8.0 Modern Programming: Object Oriented Programming and Best Practices Math Refresher for Scientists and Engineers Official (ISC)2 Guide to the CSSLP Song of Tiananmen Square Remote Workforce Training: Effective Technologies and Strategies Software Engineering Best Practices The 7 Qualities of Highly Secure Software Moebius Noodles Roadway Design With InRoads Information Technology Law The New School of Information Security Crazy Loco Computerworld Dr. Dobb's Journal Shattered Vows A Human Capital Crisis in Cybersecurity Cisco Software-Defined Access

The Pompeii Syndrome

Botnets

The fifth edition of Information Technology Law continues to be dedicated to a detailed analysis of and commentary on the latest developments within this burgeoning field of law. It provides an essential read for all those interested in the interface between law and technology and the effect of new technological developments on the law. The contents have been restructured and the reordering of the chapters provides a coherent flow to the subject matter. Criminal law issues are now dealt with in two separate chapters to enable a more focused approach to content crime. The new edition contains both a significant amount of incremental change as well as substantial new material and, where possible, case studies have been used to illustrate significant issues. In particular, new additions include: • Social media and the criminal law; • The impact of the decision in Google Spain and the 'right to be forgotten'; • The Schrems case and the demise of the Safe Harbour agreement; • The judicial reassessment of the proportionality of ICT surveillance powers within the UK and EU post the Madrid bombings; • The expansion of the ICANN gTLDs and the redesigned domain name registration and dispute resolution processes.

Fuzzing for Software Security Testing and Quality Assurance, Second Edition

#1 BESTSELLER • The groundbreaking book that redefines what it means to be smart, with a new introduction by the author "A thoughtfully written, persuasive account explaining emotional intelligence and why it can be crucial."—USA Today Everyone knows that high IQ is no guarantee of success, happiness, or virtue, but until Emotional Intelligence, we could only guess why. Daniel Goleman's brilliant

report from the frontiers of psychology and neuroscience offers startling new insight into our “two minds”—the rational and the emotional—and how they together shape our destiny. Drawing on groundbreaking brain and behavioral research, Goleman shows the factors at work when people of high IQ flounder and those of modest IQ do surprisingly well. These factors, which include self-awareness, self-discipline, and empathy, add up to a different way of being smart—and they aren’t fixed at birth. Although shaped by childhood experiences, emotional intelligence can be nurtured and strengthened throughout our adulthood—with immediate benefits to our health, our relationships, and our work. The twenty-fifth-anniversary edition of Emotional Intelligence could not come at a better time—we spend so much of our time online, more and more jobs are becoming automated and digitized, and our children are picking up new technology faster than we ever imagined. With a new introduction from the author, the twenty-fifth-anniversary edition prepares readers, now more than ever, to reach their fullest potential and stand out from the pack with the help of EI.

Emotional Intelligence

The Real Cost of Insecure Software • In 1996, software defects in a Boeing 757 caused a crash that killed 70 people... • In 2003, a software vulnerability helped cause the largest U.S. power outage in decades... • In 2004, known software weaknesses let a hacker invade T-Mobile, capturing everything from passwords to Paris Hilton’s photos... • In 2005, 23,900 Toyota Priuses were recalled for software errors that could cause the cars to shut down at highway speeds... • In 2006 dubbed “The Year of Cybercrime,” 7,000 software vulnerabilities were discovered that hackers could use to access private information... • In 2007, operatives in two nations brazenly exploited software vulnerabilities to cripple the infrastructure and steal trade secrets from other sovereign nations... Software has become crucial to the very survival of civilization. But badly written, insecure software is hurting people—and costing businesses and individuals billions of dollars every year. This must change. In Geekonomics, David Rice shows how we can change it. Rice reveals why the software industry is rewarded for carelessness, and how we can revamp the industry’s incentives to get the reliability and security we desperately need and deserve. You’ll discover why the software industry still has shockingly little accountability—and what we must do to fix that. Brilliantly written, utterly compelling, and thoroughly realistic, Geekonomics is a long-overdue call to arms. Whether you’re software user, decision maker, employee, or business owner this book will change your life...or even save it.

Geekonomics

Could it be that first in the foundation of the United States, and now the New World Order, Satan has been working to undo that which God accomplished at the Tower of Babel? In this book, David Rice presents the thesis that other than the cross of Christ, the separation of mankind into tribes and tongues and nations was the most devastating blow ever dealt to the enemy of our souls. Genesis 11:6 reads, "The Lord said, "If as one people speaking the same language they have begun to do this, then nothing they plan to do will be impossible for them." David maintains that Satan has never forgotten that statement and that he has worked tirelessly to undo that separation and reunite mankind. If he succeeds, and Scripture tells us

that he will, the Devil believes or pretends to believe that he, his angels and a united people can defeat Jehovah God. How has this played out in history and how is it being worked out today? Can we see, in today's push for global governance, the continued efforts of Satan to undo Babel? David writes, "That which God has cast asunder, let no man reassemble!" This is an exciting book that may lead you to think in ways you have never thought before and to understand that which has been hidden from you. Join in as we travel from Babel to Egypt, to Greece through Rome, England, the United States, and the coming New World Order. We will follow the works of the enemy as he seeks to undo that which God has done at Babel, reunite mankind and defeat Jehovah at Armageddon.

Sources for the Study of Greek Religion

Discover the untapped features of object-oriented programming and use it with other software tools to code fast, efficient applications. Key Features Explore the complexities of object-oriented programming (OOP) Discover what OOP can do for you Learn to use the key tools and software engineering practices to support your own programming needs Book Description Your experience and knowledge always influence the approach you take and the tools you use to write your programs. With a sound understanding of how to approach your goal and what software paradigms to use, you can create high-performing applications quickly and efficiently. In this two-part book, you'll discover the untapped features of object-oriented programming and use it with other software tools to code fast and efficient applications. The first part of the book begins with a discussion on how OOP is used today and moves on to analyze the ideas and problems that OOP doesn't address. It continues by deconstructing the complexity of OOP, showing you its fundamentally simple core. You'll see that, by using the distinctive elements of OOP, you can learn to build your applications more easily. The next part of this book talks about acquiring the skills to become a better programmer. You'll get an overview of how various tools, such as version control and build management, help make your life easier. This book also discusses the pros and cons of other programming paradigms, such as aspect-oriented programming and functional programming, and helps to select the correct approach for your projects. It ends by talking about the philosophy behind designing software and what it means to be a "good" developer. By the end of this two-part book, you will have learned that OOP is not always complex, and you will know how you can evolve into a better programmer by learning about ethics, teamwork, and documentation. What you will learn Untangle the complexity of object-oriented programming by breaking it down to its essential building blocks Realize the full potential of OOP to design efficient, maintainable programs Utilize coding best practices, including TDD, pair programming and code reviews, to improve your work Use tools, such as source control and IDEs, to work more efficiently Learn how to most productively work with other developers Build your own software development philosophy Who this book is for This book is ideal for programmers who want to understand the philosophy behind creating software and what it means to be "good" at designing software. Programmers who want to deconstruct the OOP paradigm and see how it can be reconstructed in a clear, straightforward way will also find this book useful. To understand the ideas expressed in this book, you must be an experienced programmer who wants to evolve their practice.

Cyber Security Policy Guidebook

Proven techniques for software engineering success This in-depth volume examines software engineering topics that are not covered elsewhere: the question of why software engineering has developed more than 2,500 programming languages; problems with traditional definitions of software quality; and problems with common metrics, "lines of code," and "cost per defect" that violate standard economic assumptions. The book notes that a majority of "new" projects are actually replacements for legacy applications, illustrating that data mining for lost requirements should be a standard practice. Difficult social engineering issues are also covered, such as how to minimize harm from layoffs and downsizing. Software Engineering Best Practices explains how to effectively plan, size, schedule, and manage software projects of all types, using solid engineering procedures. It details proven methods, from initial requirements through 20 years of maintenance. Portions of the book have been extensively reviewed by key engineers from top companies, including IBM, Microsoft, Unisys, and Sony. Manage Agile, hierarchical, matrix, and virtual software development teams Optimize software quality using JAD, OFD, TSP, static analysis, inspections, and other methods with proven success records Use high-speed functional metrics to assess productivity and quality levels Plan optimal organization, from small teams through more than 1,000 personnel

Ethical Hacking

"How do you want your child to feel about math? Confident, curious and deeply connected? Then Moebius Noodles is for you. It offers advanced math activities to fit your child's personality, interests, and needs. Can you enjoy playful math with your child? Yes! The book shows you how to go beyond your own math limits and anxieties to do so. It opens the door to a supportive online community that will answer your questions and give you ideas along the way. Learn how you can create an immersive rich math environment for your baby. Find out ways to help your toddler discover deep math in everyday experiences. Play games that will develop your child's sense of happy familiarity with mathematics. A five-year-old once asked us, "Who makes math?" and jumped for joy at the answer, "You!" Moebius Noodles helps you take small, immediate steps toward the sense of mathematical power. You and your child can make math your own. Together, make your own math!"--Publisher's website.

Developing Real World Software

Internet crime keeps getting worsebut it doesn't have to be that way. In this book, Internet security pioneer Phillip Hallam-Baker shows how we can make the Internet far friendlier for honest people--and far less friendly to criminals. The dotCrime Manifestobegins with a revealing new look at the challenge of Internet crime--and a surprising look at today's Internet criminals. You'll discover why the Internet's lack of accountability makes it so vulnerable, and how this can be fixed --technically, politically, and culturally. Hallam-Baker introduces tactical, short-term measures for countering phishing, botnets, spam, and other forms of Internet crime. Even more important, he presents a comprehensive plan for implementing

accountability-driven security infrastructure: a plan that draws on tools that are already available, and rapidly emerging standards and products. The result: a safer Internet that doesn't sacrifice what people value most: power, ubiquity, simplicity, flexibility, or privacy. Tactics and strategy: protecting Internet infrastructure from top to bottom Building more secure transport, messaging, identities, networks, platforms, and more Gaining safety without sacrificing the Internet's unique power and value Making the Internet safer for honest people without sacrificing ubiquity, simplicity, or privacy Spam: draining the swamp, once and for all Why spam contributes to virtually every form of Internet crime--and what we can do about it Design for deployment: how to really make it happen Defining security objectives, architecture, strategy, and design--and evangelizing them How to Build a Safer, Better Internet You'll find yourself deeply concerned, then fascinated, then hopeful as you read about " Building an Internet that resists online crime " Phishing, botnets, and spam: tactical, workable, immediate countermeasures " Establishing the "Accountable Web": a strategic, long-term solution to Internet crime " Improving security without sacrificing what people love about the Internet The Internet is today's Wild West: too much lawlessness, too little accountability. Now, one of the Internet's leading pioneers shows how we can build a more trustworthy Internet: one that resists crime without frustrating honest people or compromising privacy and civil liberties. Drawing on years at the cutting edge of Internet and security research, Phillip Hallam-Baker offers a complete plan for reinventing the Internet: a plan that addresses everything from technology to politics and culture. Whether you're a technology professional, policymaker, or citizen, this book will show you how we can make the Internet better, smarter, and above all, safer. informit.com/aw Preface xix Acknowledgments xxiv About the Author xxviii Chapter 1: Motive 1 Chapter 2: Famous for Fifteen Minutes 37 Chapter 3: Learning from Mistakes 51 Chapter 4: Making Change Happen 81 Chapter 5: Design for Deployment 107 Chapter 6: Spam Whack-a-Mole 119 Chapter 7: Stopping Spam 135 Chapter 8: Stopping Phishing 155 Chapter 9: Stopping Botnets 175 Chapter 10: Cryptography 199 Chapter 11: Establishing Trust 215 Chapter 12: Secure Transport 227 Chapter 13: Secure Messaging 251 Chapter 14: Secure Identity 277 Chapter 15: Secure Names 311 Chapter 16: Secure Networks 323 Chapter 17: Secure Platforms 343 Chapter 18: Law 355 Chapter 19: The dotCrime Manifesto 377 Further Reading 383 References 387 Index 395

Open Source

Puzzles and brain twisters to keep your mind sharp and your memory intact are all the rage today. More and more people -- Baby Boomers and information workers in particular -- are becoming concerned about their gray matter's ability to function, and with good reason. As this sensible and entertaining guide points out, your brain is easily your most important possession. It deserves proper upkeep. Your Brain: The Missing Manual is a practical look at how to get the most out of your brain -- not just how the brain works, but how you can use it more effectively. What makes this book different than the average self-help guide is that it's grounded in current neuroscience. You get a quick tour of several aspects of the brain, complete with useful advice about: Brain Food: The right fuel for the brain and how the brain commands hunger (including an explanation of the different chemicals that control appetite and cravings) Sleep: The sleep cycle and circadian rhythm, and how to get a good night's sleep (or do the best you can without it) Memory:

Techniques for improving your recall Reason: Learning to defeat common sense; logical fallacies (including tactics for winning arguments); and good reasons for bad prejudices Creativity and Problem-Solving: Brainstorming tips and thinking not outside the box, but about the box -- in other words, find the assumptions that limit your ideas so you can break through them Understanding Other People's Brains: The battle of the sexes and babies developing brains Learn about the built-in circuitry that makes office politics seem like a life-or-death struggle, causes you to toss important facts out of your memory if they're not emotionally charged, and encourages you to eat huge amounts of high-calorie snacks. With Your Brain: The Missing Manual you'll discover that, sometimes, you can learn to compensate for your brain or work around its limitations -- or at least to accept its eccentricities. Exploring your brain is the greatest adventure and biggest mystery you'll ever face. This guide has exactly the advice you need.

Practicing Organization Development

A collection of nine stories about Mexican American kids growing up in the Rio Grande Valley of southern Texas.

International Security Studies

As the global leader in information security education and certification, (ISC)² has a proven track record of educating and certifying information security professionals. Its newest certification, the Certified Secure Software Lifecycle Professional (CSSLP) is a testament to the organization's ongoing commitment to information and software security

Cyber Insecurity

Evidence continues to build showing our information infrastructure is vulnerable to threats not just from nation states but also from individuals and small groups who seek to do us harm or who wish to exploit our weaknesses for personal gain. A critical element of a robust cybersecurity strategy is having the right people at every level to identify, build and staff the defenses and responses. And that is, by many accounts, the area where we are the weakest.

Digital Democracy and the Impact of Technology on Governance and Politics: New Globalized Practices

Direct from Cisco, this comprehensive book guides networking professionals through all aspects of planning, implementing, and operating Cisco Software Defined Access, helping them use intent-based networking, SD-Access, Cisco ISE, and Cisco DNA Center to harden campus network security and simplify its management. Drawing on their unsurpassed experience architecting SD-Access solutions and training technical professionals inside and outside Cisco, the authors cover all facets of the product: its relevance, value, and use cases; its components and inner workings; planning and deployment; and day-to-day administration, support, and troubleshooting. Case studies demonstrate the use of Cisco SD-Access components to address Secure Segmentation, Plug and Play, Software

Image Management (SWIM), Host Mobility, and more. Building on core concepts and techniques, the authors present full chapters on advanced SD-Access and Cisco DNA Center topics, as well as detailed coverage of fabric assurance.

Give the Pig a Chance & Other Stories

Growing dependence on cyberspace for commerce, communication, governance, and military operations has left society vulnerable to a multitude of security threats. Mitigating the inherent risks associated with the use of cyberspace poses a series of thorny public policy problems. In this volume, academics, practitioners from both private sector and government, along with former service members come together to highlight sixteen of the most pressing contemporary challenges in cybersecurity, and to offer recommendations for the future. As internet connectivity continues to spread, this book will offer readers greater awareness of the threats of tomorrow—and serve to inform public debate into the next information age. Contributions by Adrienne Allen, Aaron Brantly, Lauren Boas Hayes, Jane Chong, Joshua Corman, Honorable Richard J. Danzig, Kat Dransfield, Ryan Ellis, Maily Fidler, Allan Friedman, Taylor Grossman, Richard M. Harrison, Trey Herr, Drew Herrick, Jonah F. Hill, Robert M. Lee, Herbert S. Lin, Anastasia Mark, Robert Morgus, Paul Ohm, Eric Ormes, Jason Rivera, Sasha Romanosky, Paul Rosenzweig, Matthew Russell, Nathaniel Tisa, Abraham Wagner, Rand Waltzman, David Weinstein, Heather West, and Beau Woods.

Managing Risk and Information Security

How will governments and courts protect civil liberties in this new era of hacktivism? Ethical Hacking discusses the attendant moral and legal issues. The first part of the 21st century will likely go down in history as the era when ethical hackers opened governments and the line of transparency moved by force. One need only read the motto “we open governments” on the Twitter page for Wikileaks to gain a sense of the sea change that has occurred. Ethical hacking is the non-violent use of a technology in pursuit of a cause—political or otherwise—which is often legally and morally ambiguous. Hacktivists believe in two general but spirited principles: respect for human rights and fundamental freedoms, including freedom of expression and personal privacy; and the responsibility of government to be open, transparent and fully accountable to the public. How courts and governments will deal with hacking attempts which operate in a grey zone of the law and where different ethical views collide remains to be seen. What is undisputed is that Ethical Hacking presents a fundamental discussion of key societal questions. A fundamental discussion of key societal questions. This book is published in English. - La première moitié du XXIe siècle sera sans doute reconnue comme l'époque où le piratage éthique a ouvert de force les gouvernements, déplaçant les limites de la transparence. La page twitter de Wikileaks enchâsse cet ethos à même sa devise, « we open governments », et sa volonté d'être omniprésent. En parallèle, les grandes sociétés de technologie comme Apple se font compétition pour produire des produits de plus en plus sécuritaires et à protéger les données de leurs clients, alors même que les gouvernements tentent de limiter et de décrypter ces nouvelles technologies d'encryption. Entre-temps, le marché des vulnérabilités en matière de sécurité augmente à mesure que les experts en sécurité informatique vendent des

vulnérabilités de logiciels des grandes technologies, dont Apple et Google, contre des sommes allant de 10 000 à 1,5 million de dollars. L'activisme en sécurité est à la hausse. Le piratage éthique est l'utilisation non-violence d'une technologie quelconque en soutien d'une cause politique ou autre qui est souvent ambiguë d'un point de vue juridique et moral. Le hacking éthique peut désigner les actes de vérification de pénétration professionnelle ou d'experts en sécurité informatique, de même que d'autres formes d'actions émergentes, comme l'hacktivism et la désobéissance civile en ligne. L'hacktivism est une forme de piratage éthique, mais également une forme de militantisme des droits civils à l'ère numérique. En principe, les adeptes du hacktivism croient en deux grands principes : le respect des droits de la personne et les libertés fondamentales, y compris la liberté d'expression et à la vie privée, et la responsabilité des gouvernements d'être ouverts, transparents et pleinement redevables au public. En pratique, toutefois, les antécédents comme les agendas des hacktivismes sont fort diversifiés. Il n'est pas clair de quelle façon les tribunaux et les gouvernements traiteront des tentatives de piratage eu égard aux zones grises juridiques, aux approches éthiques conflictuelles, et compte tenu du fait qu'il n'existe actuellement, dans le monde, presque aucune exception aux provisions, en matière de cybercrime et de crime informatique, liées à la recherche sur la sécurité ou l'intérêt public. Il sera également difficile de déterminer le lien entre hacktivism et droits civils. Ce livre est publié en anglais.

Heart-shaped Cookies

This newly revised and expanded second edition of the popular Artech House title, *Fuzzing for Software Security Testing and Quality Assurance*, provides practical and professional guidance on how and why to integrate fuzzing into the software development lifecycle. This edition introduces fuzzing as a process, goes through commercial tools, and explains what the customer requirements are for fuzzing. The advancement of evolutionary fuzzing tools, including American Fuzzy Lop (AFL) and the emerging full fuzz test automation systems are explored in this edition. Traditional software programmers and testers will learn how to make fuzzing a standard practice that integrates seamlessly with all development activities. It surveys all popular commercial fuzzing tools and explains how to select the right one for software development projects. This book is a powerful new tool to build secure, high-quality software taking a weapon from the malicious hacker's arsenal. This practical resource helps engineers find and patch flaws in software before harmful viruses, worms, and Trojans can use these vulnerabilities to rampage systems. The book shows how to make fuzzing a standard practice that integrates seamlessly with all development activities.

The DotCrime Manifesto

Based on a real world roadway design project, *ROADWAY DESIGN WITH INROADS V8I* provides information on not only the use of InRoads™, but also AASHTO and State roadway design guidelines. Readers are able to take a design from inception to design modification, and to the development of a contract plan set. This comprehensive text provides information, references, guidelines, step-by-step instructions, and exercises for individuals of varying skill levels, and is designed for individual study, for the university environment including the senior transportation

capstone course, and for in-house training for roadway and design agencies.
Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Engineering Emergence

Chinese student Song Lan is at first reluctant to join the protest movement in Beijing but as the demonstrations increase starts to join the protests. She soon finds herself in Tiananmen Square where she meets the journalist P J O'Connor. When the soldiers move in, using machine guns and tanks against the young people, Song and O'Connor are separated and in the chaos of events around the massacre O'Connor searches for Song but to no avail. He is arrested and expelled from China but just before his expulsion there is one last surprise.

Lucifer's Quest

Computer Architecture/Software Engineering

Your Brain: The Missing Manual

A collection of ten short stories reprinted from "Give the pig a chance" and other anthologies, nine new stories, and a play by Mike D. Garcia based on Rice's short story, "She flies."

Writing Secure Code

This book provides solid, state-of-the-art contributions from both scientists and practitioners working on botnet detection and analysis, including botnet economics. It presents original theoretical and empirical chapters dealing with both offensive and defensive aspects in this field. Chapters address fundamental theory, current trends and techniques for evading detection, as well as practical experiences concerning detection and defensive strategies for the botnet ecosystem, and include surveys, simulations, practical results, and case studies.

Programming C# 8.0

Covers topics such as the importance of secure systems, threat modeling, canonical representation issues, solving database input, denial-of-service attacks, and security code reviews and checklists.

Modern Programming: Object Oriented Programming and Best Practices

This book examines the nature of emergence in context of man-made (i.e. engineered) systems, in general, and system of systems engineering applications, specifically. It investigates emergence to interrogate or explore the domain space from a modeling and simulation perspective to facilitate understanding, detection, classification, prediction, control, and visualization of the phenomenon. Written by leading international experts, the text is the first to address emergence from an

engineering perspective. "System engineering has a long and proud tradition of establishing the integrative view of systems. The field, however, has not always embraced and assimilated well the lessons and implications from research on complex adaptive systems. As the editors' note, there have been no texts on Engineering Emergence: Principles and Applications. It is therefore especially useful to have this new, edited book that pulls together so many of the key elements, ranging from the theoretical to the practical, and tapping into advances in methods, tools, and ways to study system complexity. Drs. Rainey and Jamshidi are to be congratulated both for their vision of the book and their success in recruiting contributors with so much to say. Most notable, however, is that this is a book with engineering at its core. It uses modeling and simulation as the language in which to express principles and insights in ways that include tight thinking and rigor despite dealing with notably untidy and often surprising phenomena." — Paul K. Davis, RAND and Frederick S. Pardee RAND Graduate School The first chapter is an introduction and overview to the text. The book provides 12 chapters that have a theoretical foundation for this subject. Includes 7 specific example chapters of how various modeling and simulation paradigms/techniques can be used to investigate emergence in an engineering context to facilitate understanding, detection, classification, prediction, control and visualization of emergent behavior. The final chapter offers lessons learned and the proposed way-ahead for this discipline.

Math Refresher for Scientists and Engineers

Expanded coverage of essential math, including integral equations, calculus of variations, tensor analysis, and special integrals Math Refresher for Scientists and Engineers, Third Edition is specifically designed as a self-study guide to help busy professionals and students in science and engineering quickly refresh and improve the math skills needed to perform their jobs and advance their careers. The book focuses on practical applications and exercises that readers are likely to face in their professional environments. All the basic math skills needed to manage contemporary technology problems are addressed and presented in a clear, lucid style that readers familiar with previous editions have come to appreciate and value. The book begins with basic concepts in college algebra and trigonometry, and then moves on to explore more advanced concepts in calculus, linear algebra (including matrices), differential equations, probability, and statistics. This Third Edition has been greatly expanded to reflect the needs of today's professionals. New material includes: * A chapter on integral equations * A chapter on calculus of variations * A chapter on tensor analysis * A section on time series * A section on partial fractions * Many new exercises and solutions Collectively, the chapters teach most of the basic math skills needed by scientists and engineers. The wide range of topics covered in one title is unique. All chapters provide a review of important principles and methods. Examples, exercises, and applications are used liberally throughout to engage the readers and assist them in applying their new math skills to actual problems. Solutions to exercises are provided in an appendix. Whether to brush up on professional skills or prepare for exams, readers will find this self-study guide enables them to quickly master the math they need. It can additionally be used as a textbook for advanced-level undergraduates in physics and engineering.

Official (ISC)2 Guide to the CSSLP

"Drawing upon a wealth of experience from academia, industry, and government service, this book details and dissects current organizational cybersecurity policy issues on a global scale. Using simple language, it includes a thorough description of each issue, lists pros and cons, documents policy alternatives for the sake of clarity with respect to policy alone, and dives into organizational implementation issues. It also equips the reader with descriptions of the impact of specific policy choices, both positive and negative. This book gives students, scholars, and technical decision-makers the necessary knowledge of cybersecurity policy in order to make more informed decisions"--Provided by publisher.

Song of Tiananmen Square

Since its initial publication in 1979, Sources for the Study of Greek Religion has become an essential classroom resource in the field of classical studies. The Society of Biblical Literature is pleased to present a corrected edition—in a new, attractive, and electronic-friendly format—with hopes that it will inspire a new generation of classicists and religious historians.

Remote Workforce Training: Effective Technologies and Strategies

C# is undeniably one of the most versatile programming languages available to engineers today. With this comprehensive guide, you'll learn just how powerful the combination of C# and .NET can be. Author Ian Griffiths guides you through C# 8.0 fundamentals and techniques for building cloud, web, and desktop applications. Designed for experienced programmers, this book provides many code examples to help you work with the nuts and bolts of C#, such as generics, LINQ, and asynchronous programming features. You'll get up to speed on .NET Core and the latest C# 8.0 additions, including asynchronous streams, nullable references, pattern matching, default interface implementation, ranges and new indexing syntax, and changes in the .NET tool chain. Discover how C# supports fundamental coding features, such as classes, other custom types, collections, and error handling Learn how to write high-performance memory-efficient code with .NET Core's Span and Memory types Query and process diverse data sources, such as in-memory object models, databases, data streams, and XML documents with LINQ Use .NET's multithreading features to exploit your computer's parallel processing capabilities Learn how asynchronous language features can help improve application responsiveness and scalability

Software Engineering Best Practices

A vision For The future of the security industry, focusing on what threats companies now face and how they can best face them.

The 7 Qualities of Highly Secure Software

"In the title story, two cousins fight over the death of a potbellied pig but come to a

sincere reconciliation in the end. In "Tina La Tinaca," a woman grieving over the death of her son grows so obese that when she dies, an emergency crew must widen the doorway of her home so that her body can be removed. Culture and place figure prominently in Rice's work; most of the stories are set in the lower Rio Grande Valley of Texas and explore issues surrounding contemporary Mexican American life near the border. These stories ring with the author's distinctive voice and will certainly establish him as one of the most important young Chicano writers today."--BOOK JACKET.Title Summary field provided by Blackwell North America, Inc. All Rights Reserved

Moebius Noodles

Roadway Design With InRoads

This new textbook provides students with a comprehensive and accessible introduction to the subject of security studies, with a strong emphasis on the use of case studies. In addition to presenting the major theoretical perspectives, the book examines a range of important and controversial topics in modern debates, covering both traditional military and non-military security issues, such as proliferation, humanitarian intervention, food security and environmental security. Unlike most standard textbooks, the volume also offers a wide range of case studies - including chapters on the USA, China, the Middle East, Russia, Africa, the Arctic, the Middle East, Europe and Latin America - providing detailed analyses of important global security issues. The 34 chapters contain pedagogical features such as textboxes, summary points and recommended further reading and are divided into five thematic sections: Conceptual and Theoretical Military Security Non-Military Security Institutions and Security Case Studies This textbook will be essential reading for all students of security studies and highly recommended for students of critical security studies, human security, peace and conflict studies, foreign policy and International Relations in general.

Information Technology Law

The New School of Information Security

The evolution of modern technology has allowed digital democracy and e-governance to transform traditional ideas on political dialogue and accountability. Digital Democracy and the Impact of Technology on Governance and Politics: New Globalized Practices brings together a detailed examination of the new ideas on electronic citizenship, electronic democracy, e-governance, and digital legitimacy. By combining theory with the study of law and of matters of public policy, this book is essential for both academic and legal scholars, researchers, and practitioners.

Crazy Loco

Managing Risk and Information Security: Protect to Enable, an ApressOpen title, describes the changing risk environment and why a fresh approach to information

security is needed. Because almost every aspect of an enterprise is now dependent on technology, the focus of IT security must shift from locking down assets to enabling the business while managing and surviving risk. This compact book discusses business risk from a broader perspective, including privacy and regulatory considerations. It describes the increasing number of threats and vulnerabilities, but also offers strategies for developing solutions. These include discussions of how enterprises can take advantage of new and emerging technologies—such as social media and the huge proliferation of Internet-enabled devices—while minimizing risk. With ApressOpen, content is freely available through multiple online distribution channels and electronic formats with the goal of disseminating professionally edited and technically reviewed content to the worldwide community. Here are some of the responses from reviewers of this exceptional work: “Managing Risk and Information Security is a perceptive, balanced, and often thought-provoking exploration of evolving information risk and security challenges within a business context. Harkins clearly connects the needed, but often-overlooked linkage and dialog between the business and technical worlds and offers actionable strategies. The book contains eye-opening security insights that are easily understood, even by the curious layman.” Fred Wettling, Bechtel Fellow, IS&T Ethics & Compliance Officer, Bechtel “As disruptive technology innovations and escalating cyber threats continue to create enormous information security challenges, *Managing Risk and Information Security: Protect to Enable* provides a much-needed perspective. This book compels information security professionals to think differently about concepts of risk management in order to be more effective. The specific and practical guidance offers a fast-track formula for developing information security strategies which are lock-step with business priorities.” Laura Robinson, Principal, Robinson Insight Chair, Security for Business Innovation Council (SBIC) Program Director, Executive Security Action Forum (ESAF) “The mandate of the information security function is being completely rewritten. Unfortunately most heads of security haven’t picked up on the change, impeding their companies’ agility and ability to innovate. This book makes the case for why security needs to change, and shows how to get started. It will be regarded as marking the turning point in information security for years to come.” Dr. Jeremy Bergsman, Practice Manager, CEB “The world we are responsible to protect is changing dramatically and at an accelerating pace. Technology is pervasive in virtually every aspect of our lives. Clouds, virtualization and mobile are redefining computing – and they are just the beginning of what is to come. Your security perimeter is defined by wherever your information and people happen to be. We are attacked by professional adversaries who are better funded than we will ever be. We in the information security profession must change as dramatically as the environment we protect. We need new skills and new strategies to do our jobs effectively. We literally need to change the way we think. Written by one of the best in the business, *Managing Risk and Information Security* challenges traditional security theory with clear examples of the need for change. It also provides expert advice on how to dramatically increase the success of your security strategy and methods – from dealing with the misperception of risk to how to become a Z-shaped CISO. *Managing Risk and Information Security* is the ultimate treatise on how to deliver effective security to the world we live in for the next 10 years. It is absolute must reading for anyone in our profession – and should be on the desk of every CISO in the world.” Dave Cullinane, CISSP CEO Security Starfish, LLC “In this overview, Malcolm Harkins delivers an insightful survey of the trends, threats, and

tactics shaping information risk and security. From regulatory compliance to psychology to the changing threat context, this work provides a compelling introduction to an important topic and trains helpful attention on the effects of changing technology and management practices." Dr. Mariano-Florentino Cuéllar Professor, Stanford Law School Co-Director, Stanford Center for International Security and Cooperation (CISAC), Stanford University "Malcolm Harkins gets it. In his new book Malcolm outlines the major forces changing the information security risk landscape from a big picture perspective, and then goes on to offer effective methods of managing that risk from a practitioner's viewpoint. The combination makes this book unique and a must read for anyone interested in IT risk." Dennis Devlin AVP, Information Security and Compliance, The George Washington University "Managing Risk and Information Security is the first-to-read, must-read book on information security for C-Suite executives. It is accessible, understandable and actionable. No sky-is-falling scare tactics, no techno-babble - just straight talk about a critically important subject. There is no better primer on the economics, ergonomics and psycho-behaviourals of security than this." Thornton May, Futurist, Executive Director & Dean, IT Leadership Academy "Managing Risk and Information Security is a wake-up call for information security executives and a ray of light for business leaders. It equips organizations with the knowledge required to transform their security programs from a "culture of no" to one focused on agility, value and competitiveness. Unlike other publications, Malcolm provides clear and immediately applicable solutions to optimally balance the frequently opposing needs of risk reduction and business growth. This book should be required reading for anyone currently serving in, or seeking to achieve, the role of Chief Information Security Officer." Jamil Farshchi, Senior Business Leader of Strategic Planning and Initiatives, VISA "For too many years, business and security - either real or imagined - were at odds. In Managing Risk and Information Security: Protect to Enable, you get what you expect - real life practical ways to break logjams, have security actually enable business, and marries security architecture and business architecture. Why this book? It's written by a practitioner, and not just any practitioner, one of the leading minds in Security today." John Stewart, Chief Security Officer, Cisco "This book is an invaluable guide to help security professionals address risk in new ways in this alarmingly fast changing environment. Packed with examples which makes it a pleasure to read, the book captures practical ways a forward thinking CISO can turn information security into a competitive advantage for their business. This book provides a new framework for managing risk in an entertaining and thought provoking way. This will change the way security professionals work with their business leaders, and help get products to market faster. The 6 irrefutable laws of information security should be on a stone plaque on the desk of every security professional." Steven Proctor, VP, Audit & Risk Management, Flextronics

Computerworld

A routine investigation into security at a British nuclear facility leads to a series of terrifying discoveries that could have a devastating impact on all of Europe.

Dr. Dobb's Journal

Lifelong learning can occur both in and out of the classroom, but the most valuable

instruction takes place on the job. *Remote Workforce Training: Effective Technologies and Strategies* investigates methods, techniques, and systems used in employee training programs. The tools and technologies surveyed within these pages will help employers take their workers beyond the transient skill sets offered by university degrees and into a constant state of learning and practice that will enhance both their productivity and technical abilities on a regular basis. In particular, the knowledge offered by this reference book will be of use to educators and students as well as managers, leaders, administrators, and personnel.

Shattered Vows

The 7 Qualities of Highly Secure Software provides a framework for designing, developing, and deploying hacker-resilient software. It uses engaging anecdotes and analogies-ranging from Aesop's fables, athletics, architecture, biology, nursery rhymes, and video games-to illustrate the qualities that are essential for the development of highly secure

A Human Capital Crisis in Cybersecurity

Completely revised, this new edition of the classic book offers contributions from experts in the field (Warner Burke, David Campbell, Chris Worley, David Jamieson, Kim Cameron, Michael Beer, Edgar Schein, Gibb Dyer, and Margaret Wheatley) and provides a road map through each episode of change facilitation. This updated edition features new chapters on positive change, leadership transformation, sustainability, and globalization. In addition, it includes exhibits, activities, instruments, and case studies, supplemental materials on accompanying Website. This resource is written for OD practitioners, consultants, and scholars.

Cisco Software-Defined Access

From the Internet's infrastructure to operating systems like GNU/Linux, the open source movement comprises some of the greatest accomplishments in computing over the past quarter century. Its story embraces technological advances, unprecedented global collaboration, and remarkable tools for facilitating distributed development. The evolution of the Internet enabled an enormous expansion of open development, allowing developers to exchange information and ideas without regard to constraints of space, time, or national boundary. The movement has had widespread impact on education and government, as well as historic cultural and commercial repercussions. Part I discusses key open source applications, platforms, and technologies used in open development. Part II explores social issues ranging from demographics and psychology to legal and economic matters. Part III discusses the Free Software Foundation, open source in the public sector (government and education), and future prospects.

[ROMANCE](#) [ACTION & ADVENTURE](#) [MYSTERY & THRILLER](#) [BIOGRAPHIES & HISTORY](#) [CHILDREN'S](#) [YOUNG ADULT](#) [FANTASY](#) [HISTORICAL FICTION](#) [HORROR](#) [LITERARY FICTION](#) [NON-FICTION](#) [SCIENCE FICTION](#)