

Corporate Computer Security 4th Edition

For MBA/graduate students taking a course in corporate finance. Using the unifying valuation framework based on the Law of One Price, top researchers Jonathan Berk and Peter DeMarzo set the new standard for corporate finance textbooks. Corporate Finance blends coverage of time-tested principles and the latest advancements with the practical perspective of the financial manager. With this ideal melding of the core with modern topics, innovation with proven pedagogy, Berk and DeMarzo establish the new canon in finance. The second edition reflects the constantly changing world of finance, including information on the recent financial crisis, new behavioral finance research, and updated practitioner interviews.

Presents the fundamentals of hardware technologies, assembly languages, computer arithmetic, pipelining, memory hierarchies and I/O-

Introduction to Computer Security draws upon Bishop's widely praised Computer Security: Art and Science, without the highly complex and mathematical coverage that most undergraduate students would find difficult or unnecessary. The result: the field's most concise, accessible, and useful introduction. Matt Bishop thoroughly introduces fundamental techniques and principles for modeling and analyzing security. Readers learn how to express security requirements, translate requirements into policies, implement mechanisms that enforce policy, and ensure that policies are effective. Along the way, the author explains how failures may be exploited by attackers--and how attacks may be discovered, understood, and countered. Supplements available including slides and solutions.

A strong managerial focus along with a solid technical presentation of security tools. Guided by discussions with IT security professionals, Corporate Computer and Network Security covers the specific material that all IT majors and future IT security specialists need to learn from an introductory network security course. This text has been entirely rewritten in its second edition to reflect the latest trends and cutting-edge technology that students will work with in their future careers.

Introduction to Computer Security

Computer Security and the Internet

Guide to Computer Network Security

Principles and Practice

Principles of Computer Security: CompTIA Security+ and Beyond, Sixth Edition (Exam SY0-601)

Contemporary Security Management

PART OF THE JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Revised and updated with the latest information from this fast-paced field, **Fundamentals of Information System Security, Second Edition** provides a comprehensive overview of the essential concepts readers must know as they pursue careers in information systems security. The text opens with a discussion of the new risks, threats, and vulnerabilities associated with the transformation to a digital world, including a look at how business, government, and individuals operate today. Part 2 is adapted from the Official (ISC)² SSCP Certified Body of Knowledge and presents a high-level overview of each of the seven domains within the System Security Certified Practitioner certification. The book closes with a resource for readers who desire additional material on information security standards, education, professional certifications, and compliance laws. With its practical, conversational writing style and step-by-step examples, this text is a must-have resource for those entering the world of information systems security. New to the Second Edition: - New material on cloud computing, risk analysis, IP mobility, OMNIBus, and Agile Software Development. - Includes the most recent updates in Information Systems Security laws, certificates, standards, amendments, and the proposed Federal Information Security Amendments Act of 2013 and HITECH Act. - Provides new cases and examples pulled from real-world scenarios. - Updated data, tables, and sidebars provide the most current information in the field.

Contemporary Security Management, Fourth Edition, identifies and condenses into clear language the principal functions and responsibilities for security professionals in supervisory and managerial positions. Managers will learn to understand the mission of the corporate security department and how the mission intersects with the missions of other departments. The book assists managers with the critical interactions they will have with decision makers at all levels of an organization, keeping them aware of the many corporate rules, business laws, and protocols of the industry in which the corporation operates. Coverage includes the latest trends in ethics, interviewing, liability, and security-related standards. The book provides concise information on understanding budgeting, acquisition of capital equipment, employee performance rating, delegated authority, project management, counseling, and hiring. Productivity, protection of corporate assets, and monitoring of contract services and guard force operations are also detailed, as well as how to build quality relationships with leaders of external organizations, such as police, fire and emergency response agencies, and the Department of Homeland Security. Focuses on the evolving characteristics of major security threats confronting any organization Assists aspirants for senior security positions in matching their personal expertise and interests with particular areas of security management Includes updated information on the latest trends in ethics, interviewing, liability, and security-related standards

Updated and revised, The Essentials of Computer Organization and Architecture, Third Edition is a comprehensive resource that addresses all of the necessary organization and architecture topics, yet is appropriate for the one-term course.

Readers discover a wealth of focused overview information security with a thorough treatment of how to most effectively administer it with MANAGEMENT OF INFORMATION SECURITY, 5E. Information throughout helps readers become information security management practitioners able to secure systems and networks in a world where continuously emerging threats, ever-present attacks, and the success of criminals illustrate the weaknesses in current information technologies.

Current and future professional managers complete this book with the exceptional blend of skills and experiences to develop and manage the more secure computing environments that today's organizations need. This edition offers a tightened focus on key executive and managerial aspects of information security while still emphasizing the important foundational material to reinforce key concepts. Updated content reflects the most recent developments in the field, including NIST, ISO, and security governance. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

The Essentials of Computer Organization and Architecture

Global Logistics and Supply Chain Management

Information Security

The Hardware/Software Interface

Occupational Outlook Handbook

Computer Security - ESORICS 94

Rely on this practical, end-to-end guide on cyber safety and online security written expressly for a non-technical audience. You will have just what you need to protect yourself—step by step, without judgment, and with as little jargon as possible. Just how secure is your computer right now? You probably don't really know. Computers and the Internet have revolutionized the modern world, but if you're like most people, you have no clue how these things work and don't know the real threats. Protecting your computer defending a medieval castle. While moats, walls, drawbridges, and castle guards can be effective, you'd go broke trying to build something dragon-proof. This book is not about protecting yourself from a targeted attack by the NSA: it's about armoring yourself against common hackers and mass surveillance. There are dozens of no-brainer things we all should be doing to protect our computers and safeguard our data—just like wearing a seat belt, installing smoke alarms, and putting on sunscreen. Author Carey Parker structured this book to give you maximum benefit with minimum effort. If you just want to know what to do, every chapter has a complete checklist with step-by-step instructions and pictures. The book contains more than 150 tips to make you and your family safer. It includes: Added steps for Windows 10 (Spring 2018) and Mac OS X High Sierra Expanded coverage on mobile device safety Expanded coverage on safety for kids online More than 150 tips with complete step-by-step instructions and pictures What Solve your password problems once and for all Browse the web safely and with confidence Block online tracking and dangerous ads Choose the right antivirus software for you Send files and messages securely Set up secure home networking Conduct secure shopping and banking online Lock down social media accounts Create automated backups of all your devices Manage your home computers Use your smartphone and tablet safely Safeguard your kids online And more! Who This Book Is For Those who use compu

and mobile devices, but don't really know (or frankly care) how they work. This book is for people who just want to know what they need to do to protect themselves—step by step, without judgment, and with as little jargon as possible.

Hacker Techniques, Tools, and Incident Handling, Third Edition begins with an examination of the landscape, key terms, and concepts that a security professional needs to know about hackers and computer criminals who break into networks, steal information, and corrupt data. It goes on to review the technical overview of hacking: how attacks target networks and the methodology they follow. The final section studies those methods that are most effective when dealing with hacking attacks, especially in an age of

reliance on the Web. Written by subject matter experts, with numerous real-world examples, Hacker Techniques, Tools, and Incident Handling, Third Edition provides readers with a clear, comprehensive introduction to the many threats on our Internet environment and security and what can be done to combat them.

This timely textbook presents a comprehensive guide to the core topics in cybersecurity, covering issues of security that extend beyond traditional computer networks to the ubiquitous mobile communications and online social networks that have become part of our daily lives. In the context of our growing dependence on an ever-changing digital ecosystem, this book stresses the importance of security awareness, whether in our homes, our businesses, or our public spaces. This fully updated new edition features new material on the security issues raised by blockchain technology, and its use in logistics, digital ledgers, payments systems, and digital contracts. Topics and features: Explores the full range of security risks and vulnerabilities in all connected digital systems Inspires debate over future developments and improvements necessary to enhance the security of personal, public, and private enterprise systems Raises thought-provoking questions regarding legislative, legal, social, technical, and ethical challenges, such as the

tension between privacy and security Describes the fundamentals of traditional computer network security, and common threats to security Reviews the current landscape of tools, algorithms, and professional best practices in use to maintain security of digital systems Discusses the security issues introduced by the latest generation of network technologies, including mobile systems, cloud computing, and blockchain Presents exercises of varying levels of difficulty at the end of each chapter, and concludes with a selection of practical projects Offers supplementary material for students and instructors at an associated website, including slides, additional projects, and syllabus suggestions This important textbook/reference is an invaluable resource for students of computer science, engineering, and information management, as well as for practitioners working in data- and information-intensive industries.

This set of books represents a detailed compendium of authoritative, research-based entries that define the contemporary state of knowledge on technology.-Provided by publisher.

Management of Information Security

Computer Security Handbook

Safe Computing in the Information Age

Guide to Computer Forensics and Investigations

Applied Corporate Finance, 4th Edition

Principles and Practices

If you thought hacking was just about mischief-makers hunched over computers in the basement, think again. As seasoned author Wallace Wang explains, hacking can also mean questioning the status quo, looking for your own truths and never accepting at face value anything authorities say or do. The completely revised fourth edition of this offbeat, non-technical book examines what hackers do, how they do it, and how you can protect yourself. Written in the same informative, hugely successful, Steal This Computer Book 4.0 will expand your mind and raise your eyebrows. New chapters discuss the hacker mentality, social engineering and lock picking, exploiting P2P file-sharing networks, and how people manipulate search engines and pop-up ads to obtain and use personal information. Wang also takes issue with the media for "hacking" the news and presenting the public with self-serving stories of questionable accuracy. Inside, you'll discover--How to programs and rootkits work and how to defend against them--How hackers steal software and defeat copy-protection mechanisms--How to tell if your machine is being attacked and what you can do to protect it--Where the hackers are, how they probe a target and sneak into a computer, and what they do once they get inside--How corporations use hacker techniques to infect your computer and invade your privacy--How you can lock down your computer to protect your data

book's CD If you've ever logged onto a website, conducted an online transaction, sent or received email, used a networked computer or even watched the evening news, you may have already been tricked, tracked, hacked, and manipulated. As the saying goes, just because you're paranoid doesn't mean they aren't after you. And, as Wallace Wang reveals, they probably are. The companion CD contains hundreds of megabytes of 100% FREE hacking and security related programs, like Trojan horse detectors, and much, much more. CD compatible with Windows, Mac, and Linux.

Fully updated computer security essentials--mapped to the CompTIA Security+ SY0-601 exam Save 10% on any CompTIA exam voucher! Coupon code inside. Learn IT security fundamentals while getting complete coverage of the objectives for the latest release of CompTIA Security+ certification exam SY0-601. This thoroughly revised, full-color textbook covers how to secure hardware, systems, and software. It addresses new threats and cloud environments, and provides additional

Written by a team of highly respected security educators, Principles of Computer Security: CompTIA Security+TM and Beyond, Sixth Edition (Exam SY0-601) will help you become a CompTIA-certified computer security expert while also preparing you for a successful career. Find out how to: Ensure operational, organizational, and physical security Use cryptography and public key infrastructures (PKIs) Secure remote access, wireless networks, and virtual private networks (VPNs) Secure network devices, operating systems, and applications Prevent network attacks, such as denial of service, spoofing, hijacking, and password guessing Combat viruses, worms, Trojan horses, and rootkits Manage e-mail, instant messaging, and web security Explore secure software development requirements Implement disaster recovery and business continuity measures Handle computer forensics and incident response Understand legal, ethical, and privacy issues Online content feat

customized quizzes by chapter or exam objective Each chapter includes: Learning objectives Real-world examples Try This! and Cross Check exercises Tech Tips, Notes, and Warnings Exam Tips End-of-chapter quizzes and lab projects

The Model Rules of Professional Conduct provides an up-to-date resource for information on legal ethics. Federal, state and local courts in all jurisdictions look to the Rules for guidance in solving lawyer malpractice cases, disciplinary actions, disqualification issues, sanctions questions and much more. In this volume, black-letter Rules of Professional Conduct are followed by numbered Comments that explain each Rule's purpose and provide suggestions for its practical application.

Given situations, review those instances where discretionary action is possible, and define the nature of the relationship between you and your clients, colleagues and the courts.

Specifically oriented to the needs of information systems students, PRINCIPLES OF INFORMATION SECURITY, 5e delivers the latest technology and developments from the field. Taking a managerial approach, this bestseller teaches all the aspects of information security--not just the technical control perspective. It provides a broad review of the entire field of information security, background on many related elements, and enough detail to facilitate understanding of the topic. It covers

and an overview of how to manage an information security program. Current and relevant, the fifth edition includes the latest practices, fresh examples, updated material on technical security controls, emerging legislative issues, new coverage of digital forensics, and hands-on application of ethical issues in IS security. It is the ultimate resource for future business decision-makers. Important Notice: Media content referenced within the product description or the product text may

Corporate Computer Security

Third European Symposium on Research in Computer Security, Brighton, United Kingdom, November 7 - 9, 1994. Proceedings

Corporate Computer and Network Security

Private Security and the Investigative Process, Third Edition

A Guide for Book Publishing and Corporate Communications

Principles of Information Security

This volume constitutes the proceedings of the Third European Symposium on Research in Computer Security, held in Brighton, UK in November 1994. The 26 papers presented in the book in revised versions were carefully selected from a total of 79 submissions; they cover many current aspects of computer security research and advanced applications. The papers are grouped in sections on high security assurance software, key management, authentication, digital payment, distributed systems, access control, databases, and measures.

Praise for the first and second editions: "The Copyeditor's Handbook brims with valuable information, good advice, and helpful suggestions for novice copyeditors and experienced practitioners. It is comforting to know that current and future copyeditors will be able to turn to this handbook. I'm placing this work, which fills a huge gap in the literature, right beside my dictionary, and will highly recommend it to all my colleagues and students."—Alice Levine, Lecturer, The Denver Publishing Institute, and freelance editor "A definite 'must have' for the beginning to intermediate editor or author, and even the experienced editor. An indispensable reference tool."—Kim Hawley, President, The Chicago Book Clinic "This is the book that every teacher of editing has been waiting for: thorough, clear, authoritative, up-to-date, and sane."—Beth Luey, Director, Scholarly Publishing Program, Arizona State University "This book warms the cockles of the copyediting heart. It is thorough, useful, helpful, and smart. And it fills a huge vacuum."—Constance Hale, author of *Sin and Syntax and Wired Style* "An excellent resource. The Copyeditor's Handbook should sit on every business editor's shelf, next to the in-house style guide."—Erika Henik, Research Publications Manager, Banc of America Securities LLC "The first three chapters alone are worth the cover price. It's a book that acknowledges an assortment of vexing copyediting questions and offers multiple answers to most of them."—Gary Hernandez, Technical Communication "An excellent textbook to teach the essentials of copyediting. An excellent reference work for workplace writing."—Mark Armstrong, Business Communication Quarterly "Straightforward, sound advice for beginning or intermediate copyeditors working with pencil or

online."—Frisquilla S. Taylor, The Editorial Eye "Lays out the copyeditor's obligations with humor, style, and perspective."—Walter Paggi, Science Editor

This book provides a concise yet comprehensive overview of computer and Internet security, suitable for a one-term introductory course for junior/senior undergrad or first-year graduate students. It is also suitable for self-study by anyone seeking a solid footing in security – including software developers and computing professionals, technical managers and government staff. An overriding focus is on brevity, without sacrificing breadth of core topics or technical detail within them. The aim is to enable a broad understanding in roughly 350 pages. Further prioritization is supported by designating as optional selected content within this. Fundamental academic concepts are reinforced by specifics and examples, and related to applied problems and real-world incidents. The first chapter provides a gentle overview and 20 design principles for security. The ten chapters that follow provide a framework for understanding computer and Internet security. They regularly refer back to the principles, with supporting examples. These principles are the conceptual counterparts of security-related error patterns that have been recurring in software and system designs for over 50 years. The book is "elementary" in that it assumes no background in security, but unlike "soft" high-level texts it does not avoid low-level details, instead it selectively dives into fine points for exemplary topics to concretely illustrate concepts and principles. The book is rigorous in the sense of being technically sound, but avoids both mathematical proofs and lengthy source-code examples that typically make books inaccessible to general audiences. Knowledge of elementary operating system and networking concepts is helpful, but review sections summarize the essential background. For graduate students, inline exercises and

updates and this chapter end provide a bridge to further topics and a springboard to the research literature for those in industry and government. pointers are provided to helpful surveys and relevant standards, e.g., documents from the Internet Engineering Task Force (IETF), and the U.S. National Institute of Standards and Technology.

Discover the latest trends, developments and technology in information security today with Whitman/Mattord's market-leading PRINCIPLES OF INFORMATION SECURITY, 7th Edition. Designed specifically to meet the needs of those studying information systems, this edition's balanced focus addresses all aspects of information security, rather than simply offering a technical control perspective. This overview explores important trends and examines what is needed to manage an effective information security program. A new module details incident response and detection strategies. In addition, current, relevant updates highlight the latest practices in security operations as well as legislative issues, information management toolsets and digital forensics. Coverage of the most recent policies and guidelines that correspond to federal and international standards further prepare you for success both in information systems and as a business decision-maker. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Firewalls Don't Stop Dragons

Network Security Essentials: Applications and Standards (For VTU)

A Comprehensive Guide to Securing Your Information in a Moving World

Fundamentals of Information Systems Security

Steal This Computer Book 4.0

Security in Computing

Using MIS is the book that teaches students how people use information systems to solve business problems. Building on students' experience and knowledge base from personal MIS to workgroup MIS to enterprise MIS, this text stresses the important role of Information Systems in satisfying business objectives. Realistic examples, mini-cases, case applications, and thought-provoking review material with projects promote active learning. This text is beneficial to the business professional interested in a basic understanding of management information systems today.

Global Logistics and Supply Chain Management is a comprehensive, fully up-to-date introduction to the subject. Addressing both practical and strategic perspectives, this revised and updated fourth edition offers readers a balanced and integrated presentation of Logistics and Supply Chain Management (LSCM) concepts, practices, technologies, and applications. Contributions from experts in specific areas of LSCM provide readers with real-world insights on supply chain relationships, transport security, inventory management, supply chain designs, the challenges inherent to globalization and international trade, and more. The text examines how information, materials, products, and services flow across the public and private sectors and around the world. Detailed case studies highlight LSCM practices and strategies in a wide range of contexts, from humanitarian aid and pharmaceutical supply chains to semi-automated distribution centers and port and air cargo logistics. Examples of LSCM in global corporations such as Dell Computer and Jaguar Land Rover highlight the role of new and emerging technologies. This edition features new and expanded discussion of contemporary topics including sustainability, supply chain vulnerability, and reverse logistics, and places greater emphasis on operations management.

For introductory courses in IT Security. A strong business focus through a solid technical presentation of security tools. Corporate Computer Security provides a strong business focus along with a solid technical understanding of security tools. This text gives students the IT security skills they need for the workplace. This edition is more business focused and contains additional hands-on projects, coverage of wireless and data security, and case studies. This program will provide a better teaching and learning experience-for you and your students. Here's how: Encourage Student's to Apply Concepts: Each chapter now contains new hands-on projects that use contemporary software. Business Environment Focus: This edition includes more of a focus on the business applications of the concepts. Emphasis has been placed on securing corporate information systems, rather than just hosts in general. Keep Your Course Current and Relevant: New examples, exercises, and research findings appear throughout the text.

Written by leading information security educators, this fully revised, full-color computer security textbook covers CompTIA's fastest-growing credential, CompTIA Security+. Principles of Computer Security, Fourth Edition is a student-tested, introductory computer security textbook that provides comprehensive coverage of computer and network security fundamentals in an engaging and dynamic full-color design. In addition to teaching key computer security concepts, the textbook also fully prepares you for CompTIA Security+ exam SY0-401 with 100% coverage of all exam objectives. Each chapter begins with a list of topics to be covered and features sidebar exam and tech tips, a chapter summary, and an end-of-chapter assessment section that includes key term, multiple choice, and essay quizzes as well as lab projects. Electronic content includes CompTIA Security+ practice exam questions and a PDF copy of the book. Key features: CompTIA Approved Quality Content (CAQC) Electronic content features two simulated practice exams in the Total Tester exam engine and a PDF eBook Supplemented by Principles of Computer Security Lab Manual, Fourth Edition, available separately White and Conklin are two of the most well-respected computer security educators in higher education Instructor resource materials for adopting instructors include: Instructor Manual, PowerPoint slides featuring artwork from the book, and a test bank of questions for use as quizzes or exams Answers to the end of chapter sections are not included in the book and are

only available to adopting instructors Learn how to: Ensure operational, organizational, and physical security Use cryptography and public key infrastructures (PKIs) Secure remote access, wireless networks, and virtual private networks (VPNs) Authenticate users and lock down mobile devices Harden network devices, operating systems, and applications Prevent network attacks, such as denial of service, spoofing, hijacking, and password guessing Combat viruses, worms, Trojan horses, and rootkits Manage e-mail, instant messaging, and web security Explore secure software development requirements Implement disaster recovery and business continuity measures Handle computer forensics and incident response Understand legal, ethical, and privacy issues

Making Passwords Secure

The Copyeditor's Handbook

Art and Science

Computer Organization and Design

Fixing the Weakest Link in Cybersecurity

Detailing best practices and trade secrets for private sector security investigations, Private Security and the Investigative Process, Third Edition provides complete coverage of the investigative process. Fully updated, this edition covers emerging technology, revised legal and practical considerations for conducting interviews, and new information on case evaluation. Written by a recognized expert in security, criminal justice, ethics, and the law—with over three decades of experience—the updated edition of this popular text covers concepts and techniques that can be applied to a variety of investigations including fraud, insurance, private, and criminal. It details the collection and preservation of evidence, the handling of witnesses, surveillance techniques, background investigations, and report writing. This new edition includes: More than 80 new or updated forms, checklists, charts, and illustrations

Updated proprietary information from Pinkerton, Wackenhut, and other leading security companies Increased emphasis on software and technological support products A closer examination of periodical literature and government publications Authoritative, yet accessible, this book is an important reference for private investigators and security professionals. Complete with numerous forms, checklists, and web exercises, it provides the tools and understanding required to conduct investigations that are professional, ethical, and effective.

Law of the Internet, Fourth Edition is a quickly update up-to-date legal resource covering electronic commerce and online contracts, privacy and network security, intellectual property and online content management, secure electronic transactions, cryptography, and digital signatures, protecting intellectual property online - patents, trademarks, and copyright Electronic commerce and contracting Online financial services and electronic payments Antitrust issues, including pricing, bundling and tying Internet network security Taxation of electronic commerce Defamation and the Internet Obscene and indecent materials on the Internet Regulation of Internet access and interoperability The authors George B. Delta and Jeffrey H. Matsura – two Internet legal experts who advise America's top high-tech companies – demonstrate exactly how courts, legislators and treaties expand traditional law into the new context of the Internet and its commercial applications, with all the citations you'll need. The Law of the Internet also brings you up to date on all of the recent legal, commercial, and technical issues surrounding the Internet and provides you with the knowledge to thrive in the digital marketplace. Special features of this two-volume resource include timesaving checklists and references to online resources.

Information Security: Principles and Practices, Second Edition Everything You Need to Know About Modern Computer Security, in One Book Clearly explains all facets of information security in all 10 domains of the latest Information Security Common Body of Knowledge (ISC)² CBKl. Thoroughly updated for today's challenges, technologies, procedures, and best practices. The perfect resource for anyone pursuing an IT security career. Fully updated for the newest technologies and best practices, Information Security: Principles and Practices, Second Edition thoroughly covers all 10 domains of today's Information Security Common Body of Knowledge. Two highly experienced security practitioners have brought together all the foundational knowledge you need to succeed in today's IT and business environments. They offer easy-to-understand, practical coverage of topics ranging from security management and physical security to cryptography and application development security. This edition fully addresses new trends that are transforming security, from cloud services to mobile applications, "Bring Your Own Device" (BYOD) strategies to today's increasingly rigorous compliance requirements. Throughout, you'll find updated case studies, review questions, and exercises all designed to reveal today's real-world IT security challenges and help you overcome them. Learn how to -- Recognize the evolving role of IT security -- Identify the best new opportunities in the field -- Discover today's core information security principles of success -- Understand certification programs and the CBK -- Master today's best practices for governance and risk management -- Architect and design systems to maximize security -- Plan for business continuity -- Understand the legal, investigatory, and ethical requirements associated with IT security -- Improve physical and operational security -- Implement effective access control systems -- Effectively utilize cryptography -- Improve network and Internet security -- Define more effective security policies and standards -- Preview the future of information security

Computer Security: Principles and Practice, 2e, is ideal for courses in Computer/Network Security. In recent years, the need for education in computer security and related topics has grown dramatically – and is essential for anyone studying Computer Science or Computer Engineering. This is the only text available to provide integrated, comprehensive, up-to-date coverage of the broad range of topics in this subject. In addition to an extensive pedagogical program, the book provides unparalleled support for both research and modeling projects, giving students a broader perspective. The Text and Academic Authors Association named Computer Security: Principles and Practice, 1e, the winner of the Textbook Excellence Award for the best Computer Science textbook of 2008.

Corporate Finance

What They Won't Tell You About the Internet

Tools and Jewels from Malware to Bitcoin

Mobile Device Security

Encyclopedia of Information Science and Technology

Hacker Techniques, Tools, and Incident Handling

As each generation of portable electronic devices and storage media becomes smaller, higher in capacity, and easier to transport, it's becoming increasingly difficult to protect the data on these devices while still enabling their productive use in the workplace. Explaining how mobile devices can create backdoor security threats, Mobile Device Security: A Comprehensive Guide to Securing Your Information in a Moving World specifies immediate actions you can take to defend against these threats. It begins by introducing and defining the concepts essential to understanding the security threats to contemporary mobile devices, and then takes readers through all the policy, process, and technology decisions that must be made to create an effective security strategy. Highlighting the risks inherent when mobilizing data, the text supplies a proven methodology for identifying, analyzing, and evaluating these risks. It examines the various methods used to store and transport mobile data and illustrates how the security of that data changes as it moves from place to place. Addressing the technical, operational, and compliance issues relevant to a comprehensive mobile security policy, the text:Provides methods for modeling the interaction between mobile data and mobile devices--detailing the advantages and disadvantages of eachExplains how to use encryption and access controls to protect your data Describes how to layer different technologies to create a resilient mobile data protection programProvides examples of effective mobile security policies and discusses the implications of different policy approachesHighlights the essential elements of a mobile security business case and provides examples of the information such proposals should containReviews the most common mobile device controls and discusses the options for implementing them in your mobile environmentSecuring your mobile data requires the proper balance between security, user acceptance, technology capabilities, and resource commitment. Supplying real-life examples and authoritative guidance, this

concise resource walks through the security program and provides the understanding needed to develop a customized approach to securing your information.

Passwords are not the problem. The management of passwords is the real security nightmare. User authentication is the most ignored risk to enterprise cybersecurity. When end users are allowed to generate, know, remember, type and manage their own passwords, IT has inadvertently surrendered the job title Network Security Manager to employees - the weakest link in the cybersecurity chain. Dovell Bonnett reveals the

truth about the elephant in the room that no one wants to mention: Expensive backend security is worthless when the virtual front door has a lousy lock! Dovell proves that making passwords secure is not only possible, passwords can actually become an effective, cost efficient and user friendly feature of robust cybersecurity. After examining how encryption keys are secured, this book introduces a new strategy called Password Authentication Infrastructure (PAI) that rivals digital certificates. Passwords are not going away. What needs to be fixed is how passwords are managed.

Aswath Damodaran, distinguished author, Professor of Finance, and David Margolis, Teaching Fellow at the NYU Stern School of Business, have delivered the newest edition of Applied Corporate Finance. This readable text provides the practical advice students and practitioners need rather than a sole concentration on debate theory, assumptions, or models. Like no other text of its kind, Applied Corporate Finance, 4th Edition applies corporate finance to real companies. It now contains six real-world core companies to study and follow. Business decisions are classified for students into three groups: investment, financing, and dividend decisions.

The Comprehensive Guide to Computer Security, Extensively Revised with Newer Technologies, Methods, Ideas, and Examples In this updated guide, University of California at Davis Computer Security Laboratory co-director Matt Bishop offers clear, rigorous, and thorough coverage of modern computer security. Reflecting dramatic growth in the quantity, complexity, and consequences of security incidents, Computer Security, Second Edition, links core principles with technologies, methodologies, and ideas that have emerged since the first edition's publication. Writing for advanced undergraduates, graduate students, and IT professionals, Bishop covers foundational issues, policies, cryptography, systems design, assurance, and much more. He thoroughly addresses malware, vulnerability analysis, auditing, intrusion detection, and best-practice responses to attacks. In addition to new examples throughout, Bishop presents entirely new chapters on availability policy models and attack analysis. Understand computer security goals, problems, and challenges, and the deep links between theory and practice Learn how computer scientists seek to prove whether systems are secure Define security policies for confidentiality, integrity, availability, and more Analyze policies to reflect core questions of trust, and use them to constrain operations and change Implement cryptography as one component of a wider computer and network security strategy Use system-oriented techniques to establish effective security mechanisms, defining who can act and what they can do Set appropriate security goals for a system or product, and ascertain how well it meets them Recognize program flaws and malicious logic, and detect attackers seeking to exploit them This is both a comprehensive text, explaining the most fundamental and pervasive aspects of the field, and a detailed reference. It will help you align security concepts with realistic policies, successfully implement your policies, and thoughtfully manage the trade-offs that inevitably arise. Register your book for convenient access to downloads, updates, and/or corrections as they become available. See inside book for details.

Principles of Computer Security, Fourth Edition

Model Rules of Professional Conduct

Computer Security Fundamentals

Pearson New International Edition

Law of the Internet, 4th Edition

Computer Security

Updated with the latest advances from the field, GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS, Fifth Edition combines all-encompassing topic coverage and authoritative information from seasoned experts to deliver the most comprehensive forensics resource available. This proven author team's wide ranging areas of expertise mirror the breadth of coverage provided in the book, which focuses on techniques and practices for gathering and analyzing evidence used to solve crimes involving computers. Providing clear instruction on the tools and techniques of the trade, it introduces readers to every step of the computer forensics investigation-from lab set-up to testifying in court. It also details step-by-step guidance on how to use current forensics software. Appropriate for learners new to the field, it is also an excellent refresher and technology update for professionals in law enforcement, investigations, or computer security. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Computers at Risk presents a comprehensive agenda for developing nationwide policies and practices for computer security. Specific recommendations are provided for industry and for government agencies engaged in computer security activities. The volume also outlines problems and opportunities in computer security research, recommends ways to improve the research infrastructure, and suggests topics for investigators. The book explores the diversity of the field, the need to engineer countermeasures based on speculation of what experts think computer attackers may do next, why the technology community has failed to respond to the need for enhanced security systems, how innovators could be encouraged to bring more options to the marketplace, and balancing the importance of security against the right of privacy.

Corporate Computer SecurityPrentice Hall

One-volume coverage of all the core concepts, terminology, issues, and practical skills modern computer security professionals need to know * *The most up-to-date computer security concepts text on the market. *Strong coverage and comprehensive analysis of key attacks, including denial of service, malware, and viruses. *Covers oft-neglected subject areas such as cyberterrorism, computer fraud, and industrial espionage. *Contains end-of-chapter exercises, projects, review questions, and plenty of realworld tips. Computer Security Fundamentals, Second Edition is designed to be the ideal one volume gateway into the entire field of computer security. It brings together thoroughly updated coverage of all basic concepts, terminology, and issues, along with the practical skills essential to security. Drawing on his extensive experience as both an IT professional and instructor, Chuck Easttom thoroughly covers core topics such as vulnerability assessment, virus attacks, buffer overflow, hacking, spyware, network defense, firewalls, VPNs, Intrusion Detection Systems, and passwords. Unlike many other authors, however, he also fully addresses more specialized issues, including cyber terrorism, industrial espionage and encryption - including public/private key systems, digital signatures, and certificates. This edition has been extensively updated to address the latest issues and technologies, including cyberbullying/cyberstalking, session hijacking, steganography, and more. Its examples have been updated to reflect the current state-of-the-art in both attacks and defense. End-of-chapter exercises, projects, and review questions guide readers in applying the knowledge they've gained, and Easttom offers many tips that readers would otherwise have to discover through hard experience.

Using MIS

A Step-by-Step Guide to Computer Security for Non-Techies

Computers at Risk

For introductory courses in IT Security. A strong business focus through a solid technical presentation of security tools. Boyle/Panko provides a strong business focus along with a solid technical understanding of security tools. This text gives students the IT security skills they need for the workplace. This edition is more business focused and contains additional hands-on projects, coverage of wireless and data security, and case studies.