Information Systems Security Godbole Wiley India

INFORMATION SYSTEMS SECURITY: SECURITY MANAGEMENT, METRICS, FRAMEWORKS AND BEST PRACTICES (With CD)Mergers, Acquisitions, and Corporate RestructuringsComputational Intelligence and Information TechnologySecurity in Computing and CommunicationsFundamentals of Cyber SecurityPediatric UrologyInformation SecurityApplied CryptographyDried Blood SpotsThe Cyber Risk HandbookAnti-Hacker Tool Kit, Fourth EditionAdvances in Network Security and ApplicationsGuide to Computer Forensics and InvestigationsCyber Security Policy GuidebookMaking Healthcare GreenNetwork Security BibleComputer SecurityHarnessing Green ITWeb TechNetwork Security For DummiesPediatric Robotic and Reconstructive UrologyIntroduction to Computer Networks and CybersecurityCybersecurity ??? Attack and Defense StrategiesCryptography & Network Security (Sie) 2EAdvanced Materials for Agriculture, Food, and Environmental SafetySoftware-Enabled ControlData Mining in Drug DiscoveryCyber ForensicsMaking Healthcare GreenThe Postcolonial Studies DictionaryCybersecurity For DummiesDatabase SystemsComputer Forensics and Cyber CrimeCryptography and Network Security (SIE)Sense and Avoid in UASPrinciples of Information SecuritySoftware Quality AssuranceCybersecurity for BeginnersCybersecurityCloud Security

INFORMATION SYSTEMS SECURITY: SECURITY MANAGEMENT, METRICS, FRAMEWORKS AND BEST PRACTICES (With CD)

This book constitutes the proceedings of the 4th International Conference on Network Security and Applications held in Chennai, India, in July 2011. The 63 revised full papers presented were carefully reviewed and selected from numerous submissions. The papers address all technical and practical aspects of security and its applications for wired and wireless networks and are organized in topical sections on network security and applications, ad hoc, sensor and ubiquitous computing, as well as peer-to-peer networks and trust management.

Mergers, Acquisitions, and Corporate Restructurings

This book offers examples of how data science, big data, analytics, and cloud technology can be used in healthcare to significantly improve a hospital’s IT Energy Efficiency along with information on the best ways to improve energy efficiency for healthcare in a cost effective manner. The book builds on the work done in other sectors (mainly data centers) in effectively measuring and improving IT energy efficiency and includes case studies illustrating power and cooling requirements within Green Healthcare. Making Healthcare Green will appeal to professionals and researchers working in the areas of analytics and energy efficiency within the healthcare fields.

Computational Intelligence and Information Technology

A completely up-to-date resource on computer security Assuming no previous experience in the field of computer security, this must-have book walks you through the many essential aspects of this vast topic, from the newest advances in software and technology to the most recent information on Web applications security. This new edition includes sections on Windows NT, CORBA, and Java and discusses cross-site scripting and JavaScript hacking as well as SQL injection. Serving as a helpful introduction, this self-study guide is a wonderful starting point for examining the variety of competing security systems and what makes them different from one another. Unravels the complex topic of computer security and breaks it down in such a way as to serve as an ideal introduction for beginners in the field of computer security Examines the foundations of computer security and its basic principles Addresses username and password, password protection, single sign-on, and more Discusses operating system integrity, hardware security features, and memory Covers Unix security, Windows security, database security, network security, web security, and software security Packed with in-depth coverage, this resource spares no details when it comes to the critical topic of computer security.

Security in Computing and Communications

Discusses open systems, object orientation, software agents, domain-specific languages, component architectures, as well as the dramatic IT-enabled improvements in memory, communication, and processing resources that are now available for sophisticated control algorithms to exploit. Useful for practitioners and researchers in the fields of real-time systems, aerospace engineering, embedded systems, and artificial intelligence.

Fundamentals of Cyber Security

Your expert guide to information security As businesses and consumers become more dependent on complexmultinational information systems, the need to understand anddevise sound information security systems has never been greater.This title takes a practical approach to information security byfocusing on real-world examples. While not sidestepping the theory,the emphasis is on developing the skills and knowledge thatsecurity and information technology students and professionals needto face their challenges. The book is organized around four majorthemes: * Cryptography: classic cryptosystems, symmetric key cryptography,public key cryptography, hash functions, random numbers,information hiding, and cryptanalysis * Access control: authentication and authorization, password-basedsecurity, ACLs and capabilities, multilevel and multilateralsecurity, covert channels and inference control, BLP and Biba'smodels, firewalls, and intrusion detection systems * Protocols: simple authentication protocols, session keys, perfectforward secrecy, timestamps, SSL, IPSec, Kerberos, and GSM * Software: flaws and malware, buffer overflows, viruses and worms,software reverse engineering, digital rights management, securesoftware development, and operating systems security Additional features include numerous figures and tables toillustrate and clarify complex topics, as well as problems-rangingfrom basic to challenging-to help readers apply their newlydeveloped skills. A solutions manual and a set of classroom-testedPowerPoint(r) slides will assist instructors in their coursedevelopment. Students and professors in information technology,computer science, and engineering, and professionals working in thefield will find this reference most useful to solve theirinformation security issues. An Instructor's Manual presenting detailed solutions to all theproblems in the book is available from the Wiley editorialdepartment. An Instructor Support FTP site is also available.

Pediatric Urology

The book focuses on the role of advanced materials in the food, water and environmental applications. The monitoring of harmful organisms and toxicants in water, food and beverages is mainly discussed in the respective chapters. The senior contributors write on the following topics: Layered double hydroxides and environment Corrosion resistance of aluminium alloys of silanes New generation material for the removal of arsenic from water Prediction and optimization of heavy clay products quality Enhancement of physical and mechanical properties of fiber Environment friendly acrylates latices Nanoparticles for trace analysis of toxins Recent development on gold nanomaterial as catalyst Nanosized metal oxide based adsorbents for heavy metal removal Phytosynthesized transition metal nanoparticles- novel functional agents for textiles Kinetics and equilibrium modeling Magnetic nanoparticles for heavy metal removal Potential applications of nanoparticles as antipathogens Gas barrier properties of biopolymer based nanocomposites: Application in food packing Application of zero-valent iron nanoparticles for environmental clean up Environmental application of novel TiO2 nanoparticles

Information Security

“Ultimately, this is a remarkable book, a practicaltestimonial, and a comprehensive bibliography rolled into one. Itis a single, bright sword cut across the various murky green ITtopics. And if my mistakes and lessons learned through the green ITjourney are any indication, this book will be used every day byfolks interested in greening IT.” — Simon Y. Liu, Ph.D. & Ed.D.,Editor-in-Chief, IT Professional Magazine, IEEEComputer Society, Director, U.S. National AgriculturalLibrary This book presents a holistic perspective on Green IT bydiscussing its various facets and showing how to strategicallyembrace it Harnessing Green IT: Principles andPractices examines various ways of making computing andinformation systems greener – environmentally sustainable -,as well as several means of using Information Technology (IT) as atool and an enabler to improve the environmental sustainability.The book focuses on both greening of IT and greening by IT –complimentary approaches to attaining environmental sustainability. In a single volume, it comprehensively covers severalkey aspects of

Green IT - green technologies, design, standards,maturity models, strategies and adoption -, and presents a clearapproach to greening IT encompassing green use, green disposal,green design, and green manufacturing. It also illustrates how tostrategically apply green IT in practice in several areas. Key Features: Presents a comprehensive coverage of key topics of importanceand practical relevance - green technologies, design,standards, maturity models, strategies and adoption Highlights several useful approaches to embracing green IT inseveral areas Features chapters written by accomplished experts from industryand academia who have first-hand knowledge and expertise inspecific areas of green IT Presents a set of review and discussion questions for eachchapter that will help the readers to examine and explore the greenIT domain further Includes a companion website providing resources forfurther information and presentation slides This book will be an invaluable resource for IT Professionals,academics, students, researchers, project leaders/managers, ITbusiness executives, CIOs, CTOs and anyone interested in Green ITand harnessing it to enhance our environment.

Applied Cryptography

This book offers examples of how data science, big data, analytics, and cloud technology can be used in healthcare to significantly improve a hospital’s IT Energy Efficiency along with information on the best ways to improve energy efficiency for healthcare in a cost effective manner. The book builds on the work done in other sectors (mainly data centers) in effectively measuring and improving IT energy efficiency and includes case studies illustrating power and cooling requirements within Green Healthcare. Making Healthcare Green will appeal to professionals and researchers working in the areas of analytics and energy efficiency within the healthcare fields.

Dried Blood Spots

Pediatric Urology: Surgical Complications and Management, 2nd edition focuses 100% on the most common problems that can occur during pediatric urologic surgery, and how best to resolve them, ensuring the best possible outcome for the patient. As well as being thoroughly revised with the latest in management guidelines, brand new to this edition are a host of clinical case studies highlighting real-life problems during urologic surgery and the tips and tricks used by the surgeon to resolve issues faced. These will be invaluable for urology trainees learning their trade as well as for those preparing for Board or other specialty exams. Chapters will include problem solving sections as well as key take-home points. In addition, high-quality teaching videos showing urologic surgery in action will be included via the companion website - again proving an invaluable tool for all those seeking to improve their surgical skills. Edited by an experienced and international trio of urologists, they will recruit the world’s leading experts, resulting in a uniform, high-quality and evidence-based approach to the topic. Pediatric Urology: Surgical Complications and Management, 2nd edition is essential reading for all urologists, especially those specialising in pediatric urology and urologic surgery, as well as general surgeons.

The Cyber Risk Handbook

The essential M&A primer, updated with the latest research and statistics Mergers, Acquisitions, and Corporate Restructurings provides a comprehensive look at the field's growth and development, and places M&As in realistic context amidst changing trends, legislation, and global perspectives. All-inclusive coverage merges expert discussion with extensive graphs, research, and case studies to show how M&As can be used successfully, how each form works, and how they are governed by the laws of major countries. Strategies and motives are carefully analyzed alongside legalities each step of the way, and specific techniques are dissected to provide deep insight into real-world operations. This new seventh edition has been revised to improve clarity and approachability, and features the latest research and data to provide the most accurate assessment of the current M&A landscape. Ancillary materials include PowerPoint slides, a sample syllabus, and a test bank to facilitate training and streamline comprehension. As the global economy slows, merger and acquisition activity is expected to increase. This book provides an M&A primer for business executives and financial managers seeking a deeper understanding of how corporate restructuring can work for their companies. Understand the many forms of M&As, and the laws that govern them Learn the offensive and defensive techniques used during hostile acquisitions Delve into the strategies and motives that inspire M&As Access the latest data, research, and case studies on private equity, ethics, corporate governance, and more From large megadeals to various forms of downsizing, a full range of restructuring practices are currently being used to revitalize and supercharge companies around the world. Mergers, Acquisitions, and Corporate Restructurings is an essential resource for executives needing to quickly get up to date to plan their own company's next moves.

Anti-Hacker Tool Kit, Fourth Edition

An informative and comprehensive book on the applications andtechniques of dried blood spot sampling Dried blood spot (DBS) sampling involves the collection of asmall volume of blood, via a simple prick or other means, from astudy subject onto a cellulose or polymer paper card, which isfollowed by drying and transfer to the laboratory for analysis. Formany years, this method of blood sample collection has beenextensively utilized in some important areas of human healthcare(for example, newborn screening for inherited metabolic disordersand HIV-related epidemiological studies). Because of its advantagesover conventional blood, plasma, or serum sample collection, DBSsampling has been valued by the pharmaceutical industry in drugresearch and development. Dried Blood Spots: Applications and Techniques featurescontributions from an international team of leading scientists inthe field. Their contributions present a unique resource on thehistory, principles, procedures, methodologies, applications, andemerging technologies related to DBS. Presented in three parts, the book thoroughly examines: Applications of DBS sampling and associated procedures andmethodologies in various human healthcare studies Applications and perspectives of DBS sampling in drug researchand development, and therapeutic drug monitoring New technologies and emerging applications related to DBSsampling and analysis Dried Blood Spots: Applications and Techniques is avaluable working guide for researchers, professionals, and studentsin healthcare, medical science, diagnostics, clinical chemistry,and pharmaceuticals, etc.

Advances in Network Security and Applications

There is increasing interest in the potential of UAV (Unmanned Aerial Vehicle) and MAV (Micro Air Vehicle) technology and their wide ranging applications including defence missions, reconnaissance and surveillance, border patrol, disaster zone assessment and atmospheric research. High investment levels from the military sector globally is driving research and development and increasing the viability of autonomous platforms as replacements for the remotely piloted vehicles more commonly in use. UAV/UAS pose a number of new challenges, with the autonomy and in particular collision avoidance, detect and avoid, or sense and avoid, as the most challenging one, involving both regulatory and technical issues. Sense and Avoid in UAS: Research and Applications covers the problem of detect, sense and avoid in UAS (Unmanned Aircraft Systems) in depth and combines the theoretical and application results by leading academics and researchers from industry and academia. Key features: Presents a holistic view of the sense and avoid problem in the wider application of autonomous systems Includes information on human factors, regulatory issues and navigation, control, aerodynamics and physics aspects of the sense and avoid problem in UAS Provides professional, scientific and reliable content that is easy to understand, and Includes contributions from leading engineers and researchers in the field Sense and Avoid in UAS: Research and Applications is an invaluable source of original and specialised information. It acts as a reference manual for practising engineers and advanced theoretical researchers and also forms a useful resource for younger engineers and postgraduate students. With its credible sources and thorough review process, Sense and Avoid in UAS: Research and Applications provides a reliable source of information in an area that is fast expanding but scarcely covered.

Guide to Computer Forensics and Investigations

"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.

Cyber Security Policy Guidebook

Robotic urological surgery is one of the most significant urological developments in recent years. It allows for greater precision than laparoscopic methods while retaining quicker recovery time and reduced morbidity over classical open surgical techniques. For children, where the room for error is already reduced because of smaller anatomy, it takes on even more importance for urologists. As a result, robotic surgery is rightly considered one of the most exciting contemporary developments in pediatric urology. Pediatric Robotic and Reconstructive Urology: A Comprehensive Guide provides specialist and trainees with an innovative text and video guide to this dynamic area, in order to aid mastery of robotic approaches and improve the care of pediatric patients. Full-color throughout and including over 130 color images, this comprehensive guide covers key areas including: Training, instrumentation and physiology of robotic urologic surgery Surgical planning and techniques involved Adult reconstructive principles applicable to pediatrics Management of complications, outcomes and future perspectives for pediatric urologic surgery Also included are 30 high-quality surgical videos illustrating robotic surgery in action, accessed via a companion website, thus providing the perfect visual tool for the user. With chapters authored by the leading names in the field, and expertly edited by Mohan Gundeti, this ground-breaking book is essential reading for all pediatric urologists, pediatric surgeons and general urologists, whether experienced or in training. Of related interest Smith's Textbook of Endourology, 3E Smith, ISBN 9781444335545 Pediatric Urology: Surgical Complications and Management Wilcox, ISBN 9781405162685

Making Healthcare Green

This book provides an easy insight into the essentials of cybersecurity, even if you have a non-technical background. You may be a business person keen to understand this important subject area or an information security specialist looking to update your knowledge. 'The world has changed more in the past 10 years than in any 10 year period in human history Technology is no longer a peripheral servant, it shapes our daily lives. Companies that can use technology wisely and well are booming, companies that make bad or no technology choices collapse and disappear. The cloud, smart devices and the ability to connect almost any object to the internet are an essential landscape to use but are also fraught with new risks and dangers of a magnitude never seen before.' ALSO featuring an alphabetical section at the back of the book to help you translate many of the main cybersecurity technical terms into plain, non-technical English. This is the second edition of this book with updates and additional content.

Network Security Bible

Actionable guidance and expert perspective for real-world cybersecurity The Cyber Risk Handbook is the practitioner's guide to implementing, measuring and improving the counter-cyber capabilities of the modern enterprise. The first resource of its kind, this book provides authoritative guidance for real-world situations, and cross-functional solutions for enterprise-wide improvement. Beginning with an overview of counter-cyber evolution, the discussion quickly turns practical with design and implementation guidance for the range of capabilities expected of a robust cyber risk management system that is integrated with the enterprise risk management (ERM) system. Expert contributors from around the globe weigh in on specialized topics with tools and techniques to help any type or size of organization create a robust system tailored to its needs. Chapter summaries of required capabilities are aggregated to provide a new cyber risk maturity model used to benchmark capabilities and to road-map gap-improvement. Cyber risk is a fast-growing enterprise risk, not just an IT risk. Yet seldom is guidance provided as to what this means. This book is the first to tackle in detail those enterprise-wide capabilities expected by Board, CEO and Internal Audit, of the diverse executive management functions that need to team up with the Information Security function in order to provide integrated solutions. Learn how cyber risk management can be integrated to better protect your enterprise Design and benchmark new and improved practical counter-cyber capabilities Examine planning and implementation approaches, models, methods, and more Adopt a new cyber risk maturity model tailored to your enterprise needs The need to manage cyber risk across the enterprise—inclusive of the IT operations—is a growing concern as massive data breaches make the news on an alarmingly frequent basis. With a cyber risk management system now a business-necessary requirement, practitioners need to assess the effectiveness of their current system, and measure its gap-improvement over time in response to a dynamic and fast-moving threat landscape. The Cyber Risk Handbook brings the world's best thinking to bear on aligning that system to the enterprise and vice-a-versa. Every functional head of any organization must have a copy at-hand to understand their role in achieving that alignment.

Computer Security

A must-have, hands-on guide for working in the cybersecurityprofession Cybersecurity involves preventative methods to protectinformation from attacks. It requires a thorough understanding ofpotential threats, such as viruses and other malicious code, aswell as system vulnerability and security architecture. Thisessential book addresses cybersecurity strategies that includeidentity management, risk management, and incident management, andalso serves as a detailed guide for anyone looking to enter thesecurity profession. Doubling as the text for a cybersecuritycourse, it is also a useful reference for cybersecurity testing, ITtest/development, and system/network administration. Covers everything from basic network administration securityskills through advanced command line scripting, tool customization,and log analysis skills Dives deeper into such intense topics as wireshark/tcpdumpfiltering, Google hacks, Windows/Linux scripting, Metasploitcommand line, and tool customizations Delves into network administration for Windows, Linux, andVMware Examines penetration testing, cyber investigations, firewallconfiguration, and security tool customization Shares techniques for cybersecurity testing, planning, andreporting Cybersecurity: Managing Systems, Conducting Testing, andInvestigating Intrusions is a comprehensive and authoritativelook at the critical topic of cybersecurity from start tofinish.

Harnessing Green IT

CNN is reporting that a vicious new virus is wreaking havoc on theworld’s computer networks. Somebody’s hacked one ofyour favorite Web sites and stolen thousands of credit cardnumbers. The FBI just released a new report on computer crimethat’s got you shaking in your boots. The experts will tellyou that keeping your network safe from the cyber-wolves howlingafter your assets is complicated, expensive, and best left to them.But the truth is, anybody with a working knowledge of networks andcomputers can do just about everything necessary to defend theirnetwork against most security threats. Network Security For Dummies arms you with quick, easy,low-cost solutions to all your network security concerns. Whetheryour network consists of one computer with a high-speed Internetconnection or hundreds of workstations distributed across dozens oflocations, you’ll find what you need to confidently: Identify your network’s security weaknesses Install an intrusion detection system Use simple, economical techniques to secure your data Defend against viruses Keep hackers at bay Plug security holes in individual applications Build a secure network from scratch Leading national expert Chey Cobb fills you in on the basics ofdata security, and he explains more complex options you can use tokeep your network safe as your grow your business. Among otherthings, you’ll explore: Developing risk assessments and security plans Choosing controls without breaking the bank Anti-virus software, firewalls, intrusion detection systems andaccess controls Addressing Unix, Windows and Mac security issues Patching holes in email, databases, Windows Media Player,NetMeeting, AOL Instant Messenger, and other individualapplications Securing a wireless network E-Commerce security Incident response and disaster recovery Whether you run a storefront tax preparing business oryou’re the network administrator at a multinationalaccounting giant, your computer assets are your business. LetNetwork Security For Dummies provide you with provenstrategies and techniques for keeping your precious assetssafe.

Web Tech

This revised third edition presents the subject with the help of learning objectives (LO) guided by Bloom's Taxonomy and supports outcome-based learning. It discusses concepts from elementary to advanced levels with focus on mathematical preliminaries. Numerous solved examples, algorithms, illustrations & usage of fictitious characters make the text interesting and simple to read. Salient Features: Dedicated section on Elementary Mathematics Pseudo codes used to illustrate implementation of algorithm Includes new topics on Shannon's theory and Perfect Secrecy, Unicity Distance and Redundancy of Language Interesting elements introduced through QR codes - Solutions to select chapter-end problems (End of every chapter) - 19 Proofs of theorems (Appendix Q) - Secured Electronic Transaction (Appendix R) Enhanced Pedagogical Features: - Solved Examples: 260 - Exercises: 400 - Review Questions: 200 - Illustration: 400

Network Security For Dummies

Software Quality Assurance (SQA) as a professional domain is becoming increasingly important. This book provides practical insight into the topic of Software Quality Assurance. It covers discussion on the importance of software quality assurance in the business of Information Technology, covers key practices like Reviews, Verification & Validation. It also discusses people issues and other barriers in successful implementatin of Quality Management Systems in organization. This work presents methodologies, concepts as well as practical scenarios while deploying Quality Assurance practices and integrates the underlying principle into a complete reference book on this topic. -- Publisher description.

Pediatric Robotic and Reconstructive Urology

Introduction to Computer Networks and Cybersecurity

Enhance your organization's secure posture by improving your attack and defense strategies Key Features Gain a clear understanding of the attack methods, and patterns to recognize abnormal behavior within your organization with Blue Team tactics. Learn to unique techniques to gather exploitation intelligence, identify risk and demonstrate impact with Red Team and Blue Team strategies. A practical guide that will give you hands-on experience to mitigate risks and prevent attackers from infiltrating your system. Book Description The book will start talking about the security posture before moving to Red Team tactics, where you will learn the basic syntax for the Windows and Linux tools that are commonly used to perform the necessary operations. You will also gain hands-on experience of using new Red Team techniques with powerful tools such as python and PowerShell, which will enable you to discover vulnerabilities in your system and how to exploit them. Moving on, you will learn how a system is usually compromised by adversaries, and how they hack user's identity, and the various tools used by the Red Team to find vulnerabilities in a system. In the next section, you will learn about the defense strategies followed by the Blue Team to enhance the overall security of a system. You will also learn about an in-depth strategy to ensure that there are security controls in each network layer, and how you can carry out the recovery process of a compromised system. Finally, you will learn how to create a vulnerability management strategy and the different techniques for manual log analysis. By the end of this book, you will be well-versed with Red Team and Blue Team techniques and will have learned the techniques used nowadays to attack and defend systems. What you will learn Learn the importance of having a solid foundation for your security posture Understand the attack strategy using cyber security kill chain Learn how to enhance your defense strategy by improving your security policies, hardening your network, implementing active sensors, and leveraging threat intelligence Learn how to perform an incident investigation Get an in-depth understanding of the recovery process Understand continuous security monitoring and how to implement a vulnerability management strategy Learn how to perform log analysis to identify suspicious activities Who this book is for This book aims at IT professional who want to venture the IT security domain. IT pentester, Security consultants, and ethical hackers will also find this course useful. Prior knowledge of penetration testing would be beneficial.

Cybersecurity ??? Attack and Defense Strategies

A must for working network and security professionals as well as anyone in IS seeking to build competence in the increasingly important field of security Written by three high-profile experts, including Eric Cole, an ex-CIA security guru who appears regularly on CNN and elsewhere in the media, and Ronald Krutz, a security pioneer who cowrote The CISSP Prep Guide and other security bestsellers Covers everything from basic security principles and practices to the latest security threats and responses, including proven methods for diagnosing network vulnerabilities and insider secrets for boosting security effectiveness

Cryptography & Network Security (Sie) 2E

Cyber Forensics is a textbook designed for the undergraduate engineering students of computer science and information technology programs for the related course. The book will be equally useful as a primer for students from diverse backgrounds to help understanding how cyber media is misusedfor committing crime and the associated forensic principles and tools to unravel it. It will also be useful for cyber forensic professionals, cybercrime investigators, and computer professionals for implementing security measures to protect their digital assets.Beginning with a chapter on computer networks and security, the book moves onto discussing cybercrime, its classification, and its contemporary and future trends in the subsequent chapters. The core discussion of forensic principles, processes, and cases are discussed at length in the succeedingchapters before ending with dedicated chapters on cyber laws both in the Indian and International context along with interesting case-studies.

Advanced Materials for Agriculture, Food, and Environmental Safety

Protect your business and family against cyber attacks Cybersecurity is the protection against the unauthorized or criminal use of electronic data and the practice of ensuring the integrity, confidentiality, and availability of information. Being "cyber-secure" means that a person or organization has both protected itself against attacks by cyber criminals and other online scoundrels, and ensured that it has the ability to recover if it is attacked. If keeping your business or your family safe from cybersecurity threats is on your to-do list, Cybersecurity For Dummies will introduce you to the basics of becoming cyber-secure! You’ll learn what threats exist, and how to identify, protect against, detect, and respond to these threats, as well as how to recover if you have been breached! The who and why of cybersecurity threats Basic cybersecurity concepts What to do to be cyber-secure Cybersecurity careers What to think about to stay cybersecure in the future Now is the time to identify vulnerabilities that may make you a victim of cyber-crime — and to defend yourself before it is too late.

Software-Enabled Control

Description-The book has been written in such a way that the concepts are explained in detail, givingadequate emphasis on examples. To make clarity on the topic, diagrams are given extensively throughout the text. Various questions are included that vary widely in type and difficulty to understand the text. This text is user-focused and has been highly updated including topics, pictures and examples. The book features the most current research findings in all aspects of information Security. From successfully implementing technology change to understanding the human factors in IT utilization, these volumes address many of the core concepts and organizational applications, implications of information technology in organizations.Key FeaturesA* Comprehensive coverage of various aspects of cyber security concepts.A* Simple language, crystal clear approach, straight forward comprehensible presentation. A* Adopting user-friendly classroom lecture style. A* The concepts are duly supported by several examples. A* Previous years question papers are also included. A* The important set of questions comprising of more than 90 questions with short answers are also included. Table of Contents:Chapter-1 : Introduction to Information SystemsChapter-2 : Information SecurityChapter-3 : Application SecurityChapter-4 : Security ThreatsChapter-5 : Development of secure Information SystemChapter-6 : Security Issues In HardwareChapter-7 : Security PoliciesChapter-8 : Information Security Standards

Data Mining in Drug Discovery

This book constitutes the proceedings of the First International Conference on Computational Intelligence and Information Technology, CIIT 2011, held in Pune, India, in November 2011. The 58 revised full papers, 67 revised short papers, and 32 poster papers presented were carefully reviewed and selected from 483 initial submissions. The papers are contributed by innovative academics and industrial experts in the field of computer science, information technology, computational engineering, mobile communication and security and offer a stage to a common forum, where a constructive dialog on theoretical concepts, practical ideas and results of the state of the art can be developed.

Cyber Forensics

If a network is not secure, how valuable is it? Introduction to Computer Networks and Cybersecurity takes an integrated approach to networking and cybersecurity, highlighting the interconnections so that you quickly understand the complex design issues in modern networks. This full-color book uses a wealth of examples and illustrations to effective

Making Healthcare Green

The fourth edition of Principles of Information Security explores the field of information security and assurance with updated content including new innovations in technology and methodologies. Students will revel in the comprehensive coverage that includes a historical overview of information security, discussions on risk management and security technology, current certification information, and more. The text builds on internationally-recognized standards and bodies of knowledge to provide the knowledge and skills students need for their future roles as business decision-makers. Information security in the modern organization is a management issue which technology alone cannot answer; it is a problem that has important economic consequences for which management will be held accountable. Students can feel confident that they are using a standards-based, content-driven resource to prepare for their work in the field. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

The Postcolonial Studies Dictionary

Written for drug developers rather than computer scientists, this monograph adopts a systematic approach to mining scientific data sources, covering all key steps in rational drug discovery, from compound screening to lead compound selection and personalized medicine. Clearly divided into four sections, the first part discusses the different data sources available, both commercial and non-commercial, while the next section looks at the role and value of data mining in drug discovery. The third part compares the most common applications and strategies for polypharmacology, where data mining can substantially enhance the research effort. The final section of the book is devoted to systems biology approaches for compound testing. Throughout the book, industrial and academic drug discovery strategies are addressed, with contributors coming from both areas, enabling an informed decision on when and which data mining tools to use for one's own drug discovery project.

Cybersecurity For Dummies

Database Systems

Defend against today's most devious attacks Fully revised to include cutting-edge new tools for your security arsenal, Anti-Hacker Tool Kit, Fourth Edition reveals how to protect your network from a wide range of nefarious exploits. You'll get detailed explanations of each tool’s function along with best practices for configuration and implementation illustrated by code samples and up-to-date, real-world case studies. This new edition includes references to short videos that demonstrate several of the tools in action. Organized by category, this practical guide makes it easy to quickly find the solution you need to safeguard your system from the latest, most devastating hacks. Demonstrates how to configure and use these and other essential tools: Virtual machines and emulators: Oracle VirtualBox, VMware Player, VirtualPC, Parallels, and open-source options Vulnerability scanners: OpenVAS, Metasploit File system monitors: AIDE, Samhain, Tripwire Windows auditing tools: Nbtstat, Cain, MBSA, PsTools Command-line networking tools: Netcat, Cryptcat, Ncat, Socat Port forwarders and redirectors: SSH, Datapipe, FPipe, WinRelay Port scanners: Nmap, THC-Amap Network sniffers and injectors: WinDump, Wireshark, ettercap, hping, kismet, aircrack, snort Network defenses: firewalls, packet filters, and intrusion detection systems War dialers: ToneLoc, THC-Scan, WarVOX Web application hacking utilities: Nikto, HTTP utilities, ZAP, Sqlmap Password cracking and brute-force tools: John the Ripper, L0phtCrack, HashCat, pwdump, THC-Hydra Forensic utilities: dd, Sleuth Kit, Autopsy, Security Onion Privacy tools: Ghostery, Tor, GnuPG, Truecrypt, Pidgin-OTR

Computer Forensics and Cyber Crime

This new Dictionary features a thoughtfully collated collection of over 150 jargon-free definitions of key terms and concepts in postcolonial theory. Features a brief introduction to postcolonial theory and a list of suggested further reading that includes the texts in which many of these terms originated Each entry includes the origins of the term, where traceable; a detailed explanation of its perceived meaning; and examples of the term’s use in literary-cultural texts Incorporates terms and concepts from multiple disciplines, including anthropology, literary studies, science, economics, globalization studies, politics, and philosophy Provides an ideal companion text to the forthcoming Postcolonial Studies: An Anthology, which is also edited by Pramod K. Nayar, a highly-respected authority in the field

Cryptography and Network Security (SIE)

This book constitutes the refereed proceedings of the International Symposium on Security in Computing and Communications, SSCC 2014, held in Delhi, India, in September 2013. The 36 revised full papers presented together with 12 work-in-progress papers were carefully reviewed and selected from 132 submissions. The papers are organized in topical sections on security and privacy in networked systems; authentication and access control systems; encryption and cryptography; system and network security; work-in-progress.

Sense and Avoid in UAS

Database Systems: A Pragmatic Approach is a classroom textbook for use by students who are learning about relational databases, and the professors who teach them. It discusses the database as an essential component of a software system, as well as a valuable, mission critical corporate resource. The book is based on lecture notes that have been tested and proven over several years, with outstanding results. It also exemplifies mastery of the technique of combining and balancing theory with practice, to give students their best chance at success. Upholding his aim for brevity, comprehensive coverage, and relevance, author Elvis C. Foster's practical and methodical discussion style gets straight to the salient issues, and avoids unnecessary fluff as well as an overkill of theoretical calculations. The book discusses concepts, principles, design, implementation, and management issues of databases. Each chapter is organized systematically into brief, reader-friendly sections, with itemization of the important points to be remembered. It adopts a methodical and pragmatic approach to solving database systems problems. Diagrams and illustrations also sum up the salient points to enhance learning. Additionally, the book includes a number of Foster's original methodologies that add clarity and creativity to the database modeling and design experience while making a novel contribution to the discipline. Everything combines to make Database Systems: A Pragmatic Approach an excellent textbook for students, and an excellent resource on theory for the practitioner.

Principles of Information Security

The leading introduction to computer crime and forensicsis now fully updated to reflect today's newest attacks, laws, and investigatory best practices. Packed with new case studies, examples, and statistics, Computer Forensics and Cyber Crime, Third Edition adds up-to-the-minute coverage of smartphones, cloud computing, GPS, Mac OS X, Linux, Stuxnet, cyberbullying, cyberterrorism, search and seizure, online gambling, and much more. Covers all forms of modern and traditional computer crime, defines all relevant terms, and explains all technical and legal concepts in plain English, so students can succeed even if they have no technical, legal, or investigatory background.

Software Quality Assurance

Market_Desc: · Undergraduate and graduate level students of different universities and examination syllabus for international certifications in security domain· Teachers of security topics Special Features: · Written by an experienced industry professional working in the domain, a professional with extensive experience in teaching at various levels (student seminars, industry workshops) as well as research.· A comprehensive treatment and truly a treatise on the subject of Information Security· Coverage of SOX and SAS 70 aspects for Asset Management in the context of information systems security.· Covers SOX and SAS 70 aspects for Asset Management in the context of Information Systems Security. · Detailed explaination of topics Privacy and Biometric Controls .· IT Risk Analysis covered.· Review questions and reference material pointers after each chapter.· Ample figures to illustrate key points - over 250 figures!· All this is in a single book that should prove as a valuable reference on the topic to students and professionals. Useful for candidates appearing for the CISA certification exam. Maps well with the CBOK for CSTE and CSQA Certifications. About The Book: Information and communication systems can be exposed to intrusion and risks, within the overall architecture and design of these systems. These areas of risks can span the entire gamut of information systems including databases, networks, applications, internet-based communication, web services, mobile technologies and people issues associated with all of them. It is vital for businesses to be fully aware of security risks associated with their systems as well as the regulatory body pressures; and develop and implement an effective strategy to handle those risks.This book covers all of the aforementioned issues in depth. It covers all significant aspects of security, as it deals with ICT, and provides practicing ICT security professionals explanations to various aspects of information systems, their corresponding security risks and how to embark on strategic approaches to reduce and, preferably, eliminate those risks. Written by an experienced industry professional working in the domain, with extensive experience in teaching at various levels as well as research, this book is truly a treatise on the subject of Information Security.Covers SOX and SAS 70 aspects for Asset Management in the context of Information Systems Security. IT Risk Analysis covered.Detailed explanation of topics Privacy and Biometric Controls .Review questions and reference material pointers after each chapter.

Cybersecurity for Beginners

Learners will master the skills necessary to launch and complete a successful computer investigation with the updated fourth edition of this popular book, GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS. This resource guides readers through conducting a high-tech investigation, from acquiring digital evidence to reporting its findings. Updated coverage includes new software and technologies as well as up-to-date reference sections. Learn how to set up a forensics lab, how to acquire the proper and necessary tools, and how to conduct the investigation and subsequent digital analysis. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Cybersecurity

From the world's most renowned security technologist, Bruce Schneier, this 20th Anniversary Edition is the most definitive reference on cryptography ever published and is the seminal work on cryptography. Cryptographic techniques have applications far beyond the obvious uses of encoding and decoding information. For developers who need to know about capabilities, such as digital signatures, that depend on cryptographic techniques, there's no better overview than Applied Cryptography, the definitive book on the subject. Bruce Schneier covers general classes of cryptographic protocols and then specific techniques, detailing the inner workings of real-world cryptographic algorithms including the Data Encryption Standard and RSA public-key cryptosystems. The book includes source-code listings and extensive advice on the practical aspects of cryptography implementation, such as the importance of generating truly random numbers and of keeping keys secure. ". . .the best introduction to cryptography I've ever seen. . . .The book the National Security Agency wanted never to be published. . . ." -Wired Magazine ". . .monumental . . . fascinating . . . comprehensive . . . the definitive work on cryptography for computer programmers . . ." -Dr. Dobb's Journal ". . .easily ranks as one of the most authoritative in its field." -PC Magazine The book details how programmers and electronic communications professionals can use cryptography-the technique of enciphering and deciphering messages-to maintain the privacy of computer data. It describes dozens of cryptography algorithms, gives practical advice on how to implement them into cryptographic software, and shows how they can be used to solve security problems. The book shows programmers who design computer applications, networks, and storage systems how they can build security into their software and systems. With a new Introduction by the author, this premium edition will be a keepsake for all those committed to computer and cyber security.

Cloud Security

Well-known security experts decipher the most challenging aspect of cloud computing-security Cloud computing allows for both large and small organizations to have the opportunity to use Internet-based services so that they can reduce start-up costs, lower capital expenditures, use services on a pay-as-you-use basis, access applications only as needed, and quickly reduce or increase capacities. However, these benefits are accompanied by a myriad of security issues, and this valuable book tackles the most common security challenges that cloud computing faces. The authors offer you years of unparalleled expertise and knowledge as they discuss the extremely challenging topics of data ownership, privacy protections, data mobility, quality of service and service levels, bandwidth costs, data protection, and support. As the most current and complete guide to helping you find your way through a maze of security minefields, this book is mandatory reading if you are involved in any aspect of cloud computing. Coverage Includes: Cloud Computing Fundamentals Cloud Computing Architecture Cloud Computing Software Security Fundamentals Cloud Computing Risks Issues Cloud Computing Security Challenges Cloud Computing Security Architecture Cloud Computing Life Cycle Issues Useful Next Steps and Approaches

ROMANCE ACTION & ADVENTURE MYSTERY & THRILLER BIOGRAPHIES & HISTORY CHILDREN’S YOUNG ADULT FANTASY HISTORICAL FICTION HORROR LITERARY FICTION NON-FICTION SCIENCE FICTION