Computer Security Principles And Practice 2nd

Yeah, reviewing a book Computer Security Principles And Practice 2nd could add your near friends listings. This is just one of the solutions for you to be successful. As understood, achievement does not recommend that you have astounding points.

Comprehending as well as contract even more than extra will meet the expense of each success. next-door to, the message as well as sharpness of this Computer Security Principles And Practice 2nd can be taken as without difficulty as picked to act.

Computer Security Handbook Seymour Bosworth 2002-10-16 This is the most comprehensive book on computer security on themarket, with 23 chapters and 29 Appendices covering virtually allaspects of computer security. Chapters are contributed by recognized experts in theindustry. This title has come to be known as "Big Blue" in industrycircles and has a reputation for being the reference for computersecurity issues.
Digital Forensic Investigation of Internet of Things (IoT) Devices Reza Montasari 2020-12-09 This book provides a valuable reference for digital forensics practitioners and cyber security experts operating in various fields of law enforcement, incident response and commerce. It is also aimed at researchers seeking to obtain a more profound knowledge of Digital Forensics and Cybercrime. Furthermore, the book is an exceptional advanced text for PhD and Master degree programmes in Digital Forensics and Cyber Security. Each chapter of this book is written by an internationally-renowned expert who has extensive experience in law enforcement, industry and academia. The increasing popularity in the use of IoT devices for criminal activities means that there is a maturing discipline and industry around IoT forensics. As technology becomes cheaper and easier to deploy in an increased number of discrete, everyday objects, scope for the automated creation of personalised digital footprints becomes greater. Devices which are presently included within the Internet of Things (IoT) umbrella have a massive potential to enable and shape the way that humans interact and achieve objectives. These also forge a trail of data that can be used to triangulate and identify individuals and their actions. As such, interest and developments in autonomous vehicles, unmanned drones and ‘smart’ home appliances are creating unprecedented opportunities for the research communities to investigate the production and evaluation of evidence through the discipline of digital forensics.
Technology and Emergency Management John C. Pine 2017-08-18 The first book devoted to a critically important aspect of disaster planning, management, and mitigation Technology and Emergency Management, Second Edition describes best practices for technology use in emergency planning, response, recovery, and mitigation. It also describes the key elements that must be in place for technology to enhance the emergency management process. The tools, resources, and strategies discussed have been applied by organizations worldwide tasked with planning for and managing every variety of natural and man-made hazard and disaster. Illustrative case studies based on their experiences appear throughout the book. This new addition of the critically acclaimed guide has been fully updated and expanded to reflect significant developments occurring in the field over the past decade. It features in-depth coverage of major advances in GIS technologies, including the

development of mapping tools and high-resolution remote sensing imaging. Also covered is the increase in computer processing power and mobility and enhanced analytical capabilities for assessing the present conditions of natural systems and extrapolating from them to create accurate models of potential crisis conditions. This second edition also features a new section on cybersecurity and a new chapter on social media and disaster preparedness, response, and recovery has been added. Explores the role of technology in emergency planning, response, recovery, and mitigation efforts Explores applications of the Internet, telecommunications, and networks to emergency management, as well as geospatial technologies and their applications Reviews the elements of hazard models and the relative strengths and weaknesses of modeling programs Describes techniques for developing hazard prediction models using direct and remote sensing data Includes test questions for each chapter, and a solutions manual and PowerPoint slides are available on a companion website Technology and Emergency Management, Second Edition is a valuable working resource for practicing emergency managers and an excellent supplementary text for undergraduate and graduate students in emergency management and disaster management programs, urban and regional planning, and related fields.

Information Security Mark Stamp 2011-05-03 Now updated—your expert guide to twenty-first century information security Information security is a rapidly evolving field. As businesses and consumers become increasingly dependent on complex multinational information systems, it is more imperative than ever to protect the confidentiality and integrity of data. Featuring a wide array of new information on the most current security issues, this fully updated and revised edition of Information Security: Principles and Practice provides the skills and knowledge readers need to tackle any information security challenge. Taking a practical approach to information security by focusing on real-world examples, this book is organized around four major themes: Cryptography: classic cryptosystems, symmetric key cryptography, public key cryptography, hash functions, random numbers, information hiding, and cryptanalysis Access control: authentication and authorization, password-based security, ACLs and capabilities, multilevel security and compartments, covert channels and inference control, security models such as BLP and Biba's model, firewalls, and intrusion detection systems Protocols: simple authentication protocols, session keys, perfect forward secrecy, timestamps, SSH, SSL, IPSec, Kerberos, WEP, and GSM Software: flaws and malware, buffer overflows, viruses and worms, malware detection, software reverse engineering, digital rights management, secure software development, and operating systems security This Second Edition features new discussions of relevant security topics such as the SSH and WEP protocols, practical RSA timing attacks, botnets, and security certification. New background material has been added, including a section on the Enigma cipher and coverage of the classic "orange book" view of security. Also featured are a greatly expanded and upgraded set of homework problems and many new figures, tables, and graphs to illustrate and clarify complex topics and problems. A comprehensive solutions manual is available to assist in course development. Minimizing theory while providing clear, accessible content, Information Security remains the premier text for students and instructors in information technology, computer science, and engineering, as well as for professionals working in these fields.

Cybersecurity Henrique M. D. Santos 2022-04-28 Cybersecurity: A Practical Engineering Approach introduces the implementation of a secure cyber architecture, beginning with the identification of security risks. It then builds solutions to mitigate risks by considering the technological justification of the solutions as well as their efficiency. The process follows an engineering process model. Each module builds on a subset of the risks, discussing the knowledge necessary to approach a solution, followed by the security control architecture design and the implementation. The modular approach allows students to focus on more manageable problems, making the learning process simpler and more attractive.

XoveTIC 2019 Alberto Alvarellos González 2019-09-02 This issue of Proceedings gathers papers presented at XOVETIC2019 (A Coruña, Spain, 5-6 September 2019), a conference with the main goal of bringing together young researchers working in big data, artificial intelligence, Internet of Things, HPC(High-performance computing), cybersecurity, bioinformatics, natural language processing, 5G and others areas from the field of

ICT (Information Communications Technology), and offering a platform to present the results of their research to a national audience in Galicia and north of Portugal. This second edition aims to serve as the basis of this event, which will be consolidated over time and acquire international projection. The conference is co-funded by Xunta de Galicia and European Union. European Regional Development Fund (ERDF).

Integration of WSNs into Internet of Things Sudhir Kumar Sharma 2021-06-03 The Internet has gone from an Internet of people to an Internet of Things (IoT). This has brought forth strong levels of complexity in handling interoperability that involves the integrating of wireless sensor networks (WSNs) into IoT. This book offers insights into the evolution, usage, challenges, and proposed countermeasures associated with the integration. Focusing on the integration of WSNs into IoT and shedding further light on the subtleties of such integration, this book aims to highlight the encountered problems and provide suitable solutions. It throws light on the various types of threats that can attack both WSNs and IoT along with the recent approaches to counter them. This book is designed to be the first choice of reference at research and development centers, academic institutions, university libraries, and any institution interested in the integration of WSNs into IoT. Undergraduate and postgraduate students, Ph.D. scholars, industry technologists, young entrepreneurs, and researchers working in the field of security and privacy in IoT are the primary audience of this book.

Information Technology Control and Audit, Fourth Edition Sandra Senft 2012-07-18 The new edition of a bestseller, Information Technology Control and Audit, Fourth Edition provides a comprehensive and up-to-date overview of IT governance, controls, auditing applications, systems development, and operations. Aligned to and supporting the Control Objectives for Information and Related Technology (COBIT), it examines emerging trends and defines recent advances in technology that impact IT controls and audits—including cloud computing, web-based applications, and server virtualization. Filled with exercises, review questions, section summaries, and references for further reading, this updated and revised edition promotes the mastery of the concepts and practical implementation of controls needed to manage information technology resources effectively well into the future. Illustrating the complete IT audit process, the text: Considers the legal environment and its impact on the IT field—including IT crime issues and protection against fraud Explains how to determine risk management objectives Covers IT project management and describes the auditor’s role in the process Examines advanced topics such as virtual infrastructure security, enterprise resource planning, web application risks and controls, and cloud and mobile computing security Includes review questions, multiple-choice questions with answers, exercises, and resources for further reading in each chapter This resource-rich text includes appendices with IT audit cases, professional standards, sample audit programs, bibliography of selected publications for IT auditors, and a glossary. It also considers IT auditor career development and planning and explains how to establish a career development plan. Mapping the requirements for information systems auditor certification, this text is an ideal resource for those preparing for the Certified Information Systems Auditor (CISA) and Certified in the Governance of Enterprise IT (CGEIT) exams. Instructor's guide and PowerPoint® slides available upon qualified course adoption.

Computer Security Quiz Book S.R. Subramanya 2020-07-30 This is a quick assessment book / quiz book. It has a wide variety of over 1,700 questions, with answers on Computer Security. The questions have a wide range of difficulty levels and are designed to test a thorough understanding of the topical material. The book covers all the major topics in a typical first course in Computer Security – Cryptography, Authentication and Key Management, Software and Operating Systems Security, Malware, Attacks, Network Security, and Web Security.

Novel Algorithms and Techniques in Telecommunications and Networking Tarek Sobh 2010-01-30 Novel Algorithms and Techniques in Telecommunications and Networking includes a set of rigorously reviewed world-class manuscripts addressing and detailing state-of-the-art research projects in the areas of Industrial Electronics, Technology and Automation, Telecommunications and Networking. Novel Algorithms and Techniques in Telecommunications and Networking includes selected papers form the conference proceedings of the International Conference on Telecommunications and Networking (TeNe 08) which was part of the International Joint Conferences on Computer, Information and Systems Sciences and Engineering (CISSE 2008).

Information Security Management Principles David Alexander 2013 In today's technology-driven environment, there is an ever-increasing demand for information delivery. A compromise has to be struck between security and availability. This book is a pragmatic guide to information assurance for both business professionals and technical experts. The second edition includes the security of cloud-based resources and the contents have been revised to reflect the changes to the BCS Certification in Information Security Management Principles which the book supports.

Biometrics in a Data Driven World Sinjini Mitra 2016-12-01 Biometrics in a Data Driven World: Trends, Technologies, and Challenges aims to inform readers about the modern applications of biometrics in the context of a data-driven society, to familiarize them with the rich history of biometrics, and to provide them with a glimpse into the future of biometrics. The first section of the book discusses the fundamentals of biometrics and provides an overview of common biometric modalities, namely face, fingerprints, iris, and voice. It also discusses the history of the field, and provides an overview of emerging trends and opportunities. The second section of the book introduces readers to a wide range of biometric applications. The next part of the book is dedicated to the discussion of case studies of biometric modalities currently used on mobile applications. As smartphones and tablet computers are rapidly becoming the dominant consumer computer platforms, biometrics-based authentication is emerging as an integral part of protecting mobile devices against unauthorized access, while enabling new and highly popular applications, such as secure online payment authorization. The book concludes with a discussion of future trends and opportunities in the field of biometrics, which will pave the way for advancing research in the area of biometrics, and for the deployment of biometric technologies in real-world applications. The book is designed for individuals interested in exploring the contemporary applications of biometrics, from students to researchers and practitioners working in this field. Both undergraduate and graduate students enrolled in college-level security courses will also find this book to be an especially useful companion.

Computernetwerken James F. Kurose 2003-01-01

Database and Expert Systems Applications Gabriele Anderst-Kotsis 2019-08-19 This volume constitutes the refereed proceedings of the four workshops held at the 30th International Conference on Database and Expert Systems Applications, DEXA 2019, held in Linz, Austria, in August 2019: The 10th International Workshop on Biological Knowledge Discovery from Data, BIOKDD 2019, the 3rd International Workshop on Cyber-Security and Functional Safety in Cyber-Physical Systems, IWCFS 2019, the 1st International Workshop on Machine Learning and Knowledge Graphs, MLKgraphs2019, and the 16th International Workshop on Technologies for Information Retrieval, TIR 2019. The 26 selected papers discuss a range of topics including: knowledge discovery, biological data, cyber security, cyber-physical system, machine learning, knowledge graphs, information retriever, data base, and artificial intelligent.

Hacking Jon Mark Erickson 2004

Neural Information Processing Long Cheng 2018-12-03 The seven-volume set of LNCS 11301-11307, constitutes the proceedings of the 25th International Conference on Neural Information Processing, ICONIP 2018, held in Siem Reap, Cambodia, in December 2018. The 401 full papers presented were carefully reviewed and selected from 575 submissions. The papers address the emerging topics of theoretical research, empirical studies, and applications of neural information processing techniques across different domains. The 4th volume, LNCS 11304, is organized in topical sections on feature selection, clustering, classification, and detection.

Security Patterns in Practice Eduardo Fernandez-Buglioni 2013-06-25 Learn to combine security theory and code to produce secure systems

Security is clearly a crucial issue to consider during the design and implementation of any distributed software architecture. Security patterns are increasingly being used by developers who take security into serious consideration from the creation of their work. Written by the authority on security patterns, this unique book examines the structure and purpose of security patterns, illustrating their use with the help of detailed implementation advice, numerous code samples, and descriptions in UML. Provides an extensive, up-to-date catalog of security patterns Shares real-world case studies so you can see when and how to use security patterns in practice Details how to incorporate security from the conceptual stage Highlights tips on authentication, authorization, role-based access control, firewalls, wireless networks, middleware, VoIP, web services security, and more Author is well known and highly respected in the field of security and an expert on security patterns Security Patterns in Practice shows you how to confidently develop a secure system step by step.

Securing Social Networks in Cyberspace Al-Sakib Khan Pathan 2021-10-11 This book collates the key security and privacy concerns faced by individuals and organizations who use various social networking sites. This includes activities such as connecting with friends, colleagues, and family; sharing and posting information; managing audio, video, and photos; and all other aspects of using social media sites both professionally and personally. In the setting of the Internet of Things (IoT) that can connect millions of devices at any one time, the security of such actions is paramount. Securing Social Networks in Cyberspace discusses user privacy and trust, location privacy, protecting children, managing multimedia content, cyberbullying, and much more. Current state-of-the-art defense mechanisms that can bring long-term solutions to tackling these threats are considered in the book. This book can be used as a reference for an easy understanding of complex cybersecurity issues in social networking platforms and services. It is beneficial for academicians and graduate-level researchers. General readers may find it beneficial in protecting their social-media-related profiles.

Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2018 Aboul Ella Hassanien 2018-08-28 This book presents the proceedings of the 4th International Conference on Advanced Intelligent Systems and Informatics 2018 (AISI2018), which took place in Cairo, Egypt from September 1 to 3, 2018. This international and interdisciplinary conference, which highlighted essential research and developments in the field of informatics and intelligent systems, was organized by the Scientific Research Group in Egypt (SRGE). The book is divided into several main sections: Intelligent Systems; Robot Modeling and Control Systems; Intelligent Robotics Systems; Machine Learning Methodology and Applications; Sentiment Analysis and Arabic Text Mining; Swarm Optimizations and Applications; Deep Learning and Cloud Computing; Information Security, Hiding, and Biometric Recognition; and Data Mining, Visualization and E-learning.

Emerging Trends in ICT Security Babak Akhgar 2013-11-06 Emerging Trends in ICT Security, an edited volume, discusses the foundations and theoretical aspects of ICT security; covers trends, analytics, assessments and frameworks necessary for performance analysis and evaluation; and gives you the state-of-the-art knowledge needed for successful deployment of security solutions in many environments. Application scenarios provide you with an insider's look at security solutions deployed in real-life scenarios, including but limited to smart devices, biometrics, social media, big data security, and crowd sourcing. Provides a multidisciplinary approach to security with coverage of communication systems, information mining, policy making, and management infrastructures Discusses deployment of numerous security solutions, including, cyber defense techniques and defense against malicious code and mobile attacks Addresses application of security solutions in real-life scenarios in several environments, such as social media, big data and crowd sourcing

Principles of Computer Security, Fourth Edition Dwayne Williams 2015-12-29 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

Advanced Information Systems Engineering Workshops John Krogstie 2016-06-06 This book constitutes the thoroughly refereed proceedings of five international workshops held in Ljubljana, Slovenia, in conjunction with the 28th International Conference on Advanced Information Systems Engineering, CAiSE 2016, in June 2016. The 16 full and 9 short papers were carefully selected from 51 submissions. The associated workshops were the Third International Workshop on Advances in Services DEsign based on the Notion of CApabiliy (ASDENCA) co-arranged with the First International Workshop on Business Model Dynamics and Information Systems Engineering (BumDISE), the Fourth International Workshop on Cognitive Aspects of Information Systems Engineering (COGNISE), the First International Workshop on Energy-awareness and Big Data Management in Information Systems (EnBIS), the Second International Workshop on Enterprise Modeling (EM), and the Sixth International Workshop on Information Systems Security Engineering (WISSE).

Innovations and Advances in Computer, Information, Systems Sciences, and Engineering Khaled Elleithy 2012-08-28 Innovations and Advances in Computer, Information, Systems Sciences, and Engineering includes the proceedings of the International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE 2011). The contents of this book are a set of rigorously reviewed, world-class manuscripts addressing and detailing state-of-the-art research projects in the areas of Industrial Electronics, Technology and Automation, Telecommunications and Networking, Systems, Computing Sciences and Software Engineering, Engineering Education, Instructional Technology, Assessment, and E-learning.

Neural Information Processing Minho Lee 2013-10-29 The three volume set LNCS 8226, LNCS 8227 and LNCS 8228 constitutes the proceedings of the 20th International Conference on Neural Information Processing, ICONIP 2013, held in Daegu, Korea, in November 2013. The 180 full and 75 poster papers presented together with 4 extended abstracts were carefully reviewed and selected from numerous submissions. These papers cover all major topics of theoretical research, empirical study and applications of neural information processing research. The specific topics covered are as follows: cognitive science and artificial intelligence; learning theory, algorithms and architectures; computational neuroscience and brain imaging; vision, speech and signal processing; control, robotics and hardware technologies and novel approaches and applications.

Foundations of Computer Security David Salomon 2006-03-20 Anyone with a computer has heard of viruses, had to deal with several, and has been struggling with spam, spyware, and disk crashes. This book is intended as a starting point for those familiar with basic concepts of computers and computations and who would like to extend their knowledge into the realm of computer and network security. Its comprehensive treatment of all the major areas of computer security aims to give readers a complete foundation in the field of Computer Security. Exercises are given throughout the book and are intended to strengthening the reader’s knowledge - answers are also provided. Written in a clear, easy to understand style, aimed towards advanced undergraduates and non-experts who want to know about the security problems confronting them everyday. The technical level of the book is low and requires no mathematics, and only a basic concept of computers and computations. Foundations of Computer Security will be an invaluable tool for students and professionals alike.

Computer Security and the Internet Paul C. van Oorschot 2021-10-13 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 supplemental references provided in per-chapter endnotes 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.

Guide to Computer Network Security Joseph Migga Kizza 2020-06-03 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 diverse 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.

Emerging Trends in ICT Security Nary Subramanian 2013-11-06 Trustworthy systems are essential for critical operations—they ensure that reliability, usability, interoperability, and security are built into the systems, and that the systems deliver when they are most needed. There are environments where trustworthiness is an essential property in military, government, and civil domains. Examples include missile deployment control systems, the tax submission system of the federal government, and nuclear safety control systems. However, not many methods exist for the systematic engineering of trustworthy software systems. In this chapter we describe the application of the NFR Approach for designing a trustworthy software system. The NFR Approach, where NFR stands for “non-functional requirement,” treats trustworthiness as a goal to be achieved during the process of software development. The NFR Approach uses a structure called the Softgoal Interdependency Graph to capture the trustworthiness definition, depict architectural elements as softgoals, and rationalize the extent of trustworthiness in the design. Advantages of this approach include the ability to nurture consensus among multiple definitions of trustworthiness, capture design rationale, evaluate qualitatively the extent of trustworthiness achieved, and maintain historical records of design decisions. We apply the NFR Approach to design a trustworthy Phoenix system, which is a message-oriented middleware system used by the US Air Force.

Advanced Methodologies and Technologies in Business Operations and Management Khosrow-Pour, D.B.A., Mehdi 2018-09-14 Businesses consistently work on new projects, products, and workflows to remain competitive and successful in the modern business environment. To remain zealous, businesses must employ the most effective methods and tools in human resources, project management, and overall business plan execution as competitors work to succeed as well. Advanced Methodologies and Technologies in Business Operations and Management provides emerging research on business tools such as employee engagement, payout policies, and financial investing to promote operational success. While highlighting the challenges facing modern organizations, readers will learn how corporate social responsibility and utilizing artificial intelligence improve a company’s culture and management. This book is an ideal resource for executives and managers, researchers, accountants, and financial investors seeking current research on business operations and management.

Sustainable Intelligent Systems Amit Joshi 2021-03-06 This book discusses issues related to ICT, intelligent systems, data science, AI, machine learning, sustainable development and overall their impacts on sustainability. It provides an overview of the technologies of future. The book also discusses novel intelligent algorithms and their applications to move from a data-centric world to sustainable world. It includes research paradigms on sustainable development goals and societal impacts. The book provides an overview of cutting-edge techniques toward sustainability and ideas to help researchers who want to understand the challenges and opportunities of using smart management perspective for sustainable society. It serves as a reference to wide ranges of readers from computer science, data analysts, AI technocrats and management researchers.

Security Basics for Computer Architects Ruby B. Lee 2022-05-31 Design for security is an essential aspect of the design of future computers. However, security is not well understood by the computer architecture community. Many important security aspects have evolved over the last several decades in the cryptography, operating systems, and networking communities. This book attempts to introduce the computer architecture student, researcher, or practitioner to the basic concepts of security and threat-based design. Past work in different security communities can inform our thinking and provide a rich set of technologies for building architectural support for security into all future computers and embedded computing devices and appliances. I have tried to keep the book short, which means that many interesting topics and applications could not be included. What the book focuses on are the fundamental security concepts, across different security communities, that should be understood by any computer architect trying to design or evaluate security-aware computer architectures.

Elements of Computer Security David Salomon 2010-08-05 As our society grows ever more reliant on computers, so it also becomes more vulnerable to computer crime. Cyber attacks have been plaguing computer users since the 1980s, and computer security experts are predicting that smart telephones and other mobile devices will also become the targets of cyber security threats in the future. Developed from the author's successful Springer guide to Foundations of Computer Security, this accessible textbook/reference is fully updated and enhanced with resources for students and tutors. Topics and features: examines the physical security of computer hardware, networks, and digital data; introduces the different forms of rogue software (or malware), discusses methods for preventing and defending against malware, and describes a selection of viruses, worms and Trojans in detail; investigates the important threats to network security, and explores the subjects of authentication, spyware, and identity theft; discusses issues of privacy and trust in the online world, including children's privacy and safety; includes appendices which discuss the definition, meaning, and history of the term hacker, introduce the language of "l33t Speak", and provide a detailed virus timeline; provides numerous exercises and examples throughout the text, in addition to a Glossary of terms used in the book; supplies additional resources at the associated website, http://www.DavidSalomon.name/, including an introduction to cryptography, and answers to the exercises. Clearly and engagingly written, this concise textbook is an ideal resource for undergraduate classes on computer security. The book is mostly non-mathematical, and is suitable for anyone familiar with the basic concepts of computers and computations.

Computer Security Handbook, Set Seymour Bosworth 2012-07-18 The classic and authoritative reference in the field of computer security, now completely updated and revised With the continued presence of large-scale computers; the proliferation of desktop, laptop, and handheld computers; and the vast international networks that interconnect them, the nature and extent of threats to computer security have grown enormously. Now in its fifth edition, Computer Security Handbook continues to provide authoritative guidance to identify and to eliminate these threats where possible, as well as to lessen any losses attributable to them. With seventy-seven chapters contributed by a panel of renowned industry professionals, the new edition has increased coverage in both breadth and depth of all ten domains of the Common Body of Knowledge defined by the International Information Systems Security Certification Consortium (ISC). Of the seventy-seven chapters in the fifth edition, twenty-five chapters are completely new, including: 1. Hardware Elements of Security 2. Fundamentals of Cryptography and Steganography 3. Mathematical models of information security 4. Insider threats 5. Social engineering and low-tech attacks 6. Spam, phishing, and Trojans: attacks meant to fool 7. Biometric authentication 8. VPNs and secure remote access 9. Securing Peer2Peer, IM, SMS, and collaboration tools 10. U.S. legal and regulatory security issues, such as GLBA and SOX Whether you are in charge of many computers or just one important one, there are immediate steps you can take to safeguard your computer system and its contents. Computer Security Handbook, Fifth Edition equips you to protect the information and networks that are vital to your organization.

Biomedical Engineering Systems and Technologies Ana Fred 2013-01-03 This book constitutes the thoroughly refereed post-conference proceedings of the 4th International Joint Conference on Biomedical Engineering Systems and Technologies, BIOSTEC 2011, held in Rome, Italy, in January 2011. The 27 revised full papers presented together with one invited lecture were carefully reviewed and selected from a total of 538 submissions. The papers cover a wide range of topics and are organized in four general topical sections on biomedical electronics and devices; bioinformatics models, methods and algorithms; bio-inspired systems and signal processing; health informatics.

Guide to Vulnerability Analysis for Computer Networks and Systems Simon Parkinson 2018-09-04 This professional guide and reference examines the challenges of assessing security vulnerabilities in computing infrastructure. Various aspects of vulnerability assessment are covered in detail, including recent advancements in reducing the requirement for expert knowledge through novel applications of artificial intelligence. The work also offers a series of case studies on how to develop and perform vulnerability assessment techniques using start-of-the-art intelligent mechanisms. Topics and features: provides tutorial activities and thought-provoking questions in each chapter, together with numerous case studies; introduces the fundamentals of vulnerability assessment, and reviews the state of the art of research in this area; discusses vulnerability assessment frameworks, including frameworks for industrial control and cloud systems; examines a range of applications that make use of artificial intelligence to enhance the vulnerability assessment processes; presents visualisation techniques that can be used to assist the vulnerability assessment process. In addition to serving the needs of security practitioners and researchers, this accessible volume is also ideal for students and instructors seeking a primer on artificial intelligence for vulnerability assessment, or a supplementary text for courses on computer security, networking, and artificial intelligence.

Introduction to Machine Learning with Applications in Information Security Mark Stamp 2017-09-22 Introduction to Machine Learning with Applications in Information Security provides a class-tested introduction to a wide variety of machine learning algorithms, reinforced through realistic applications. The book is accessible and doesn’t prove theorems, or otherwise dwell on mathematical theory. The goal is to present topics at an intuitive level, with just enough detail to clarify the underlying concepts. The book covers core machine learning topics in-depth, including Hidden Markov Models, Principal Component Analysis, Support Vector Machines, and Clustering. It also includes coverage of Nearest Neighbors, Neural Networks, Boosting and AdaBoost, Random Forests, Linear Discriminant Analysis, Vector Quantization, Naive Bayes, Regression Analysis, Conditional Random Fields, and Data Analysis. Most of the examples in the book are drawn from the field of information security, with many of the machine learning applications specifically focused on malware. The applications presented are designed to demystify machine learning techniques by providing straightforward scenarios. Many of the exercises in this book require some programming, and basic computing concepts are assumed in a few of the application sections. However, anyone with a modest amount of programming experience should have no trouble with this aspect of the book. Instructor resources, including PowerPoint slides, lecture videos, and other relevant material are provided on an accompanying website: http://www.cs.sjsu.edu/~stamp/ML/. For the reader’s benefit, the figures in the book are also available in electronic form, and in color. About the Author Mark Stamp has been a Professor of Computer Science at San Jose State University since 2002. Prior to that, he worked at the National Security Agency (NSA) for seven years, and a Silicon Valley startup company for two years. He received his Ph.D. from Texas Tech University in 1992. His love affair with machine learning began in the early 1990s, when he was working at the NSA, and continues today at SJSU, where he has supervised vast numbers of master’s student projects, most of which involve a combination of information security and machine learning.

Advances in Intelligent Systems and Interactive Applications Fatos Xhafa 2017-10-30 This book presents research papers from diverse areas on novel Intelligent Systems and Interactive Systems and Applications. It gathers selected research papers presented at the 2nd International Conference on Intelligent and Interactive Systems and Applications (IISA2017), which was held on June 17–18, 2017 in Beijing, China. Interactive Intelligent Systems (IIS) are systems that interact with human beings, media or virtual agents in intelligent computing environments. The emergence of Big Data and the Internet of Things have now opened new opportunities in both academic and industrial research for the successful design and development of intelligent interactive systems. This book explores how novel interactive systems can be used to overcome various challenges and limitations previously encountered by human beings by combining machine learning algorithms and the analysis of recent trends. The book presents 125 contributions, which have been categorized into seven sections, namely: i) Autonomous Systems; ii) Pattern Recognition and Vision Systems; iii) E-Enabled Systems; iv) Mobile Computing and Intelligent Networking; v) Internet and Cloud Computing; vi) Intelligent Systems, and vii) Various Applications. It not only offers readers extensive theoretical information on Intelligent and Interactive Systems, but also introduces them to various applications in different domains.

Managing Inherent Technical Isolation Daniel Charles 2022-08-01 In the current business environment, many companies consciously or subconsciously practice a culture of inherent technical isolation (ITI). ITI exists when businesses and IT leaders in particular consistently provide preferential treatment to team members in their organizations on the basis of technical versus nontechnical competency. This book is written to not only draw attention to the ITI culture but to also promote an inclusive management practice that would eventually make the culture extinct. Essentially, the book seeks to promote a new business and technology management culture void of inherent technical isolation practices.

E-Business and Telecommunications Mohammad S. Obaidat 2020-07-13 This book contains a compilation of the revised and extended versions of the best papers presented at the 16th International Joint Conference on E-Business and Telecommunications, ICETE 2019, held in Prague, Czech Republic, in July 2019. ICETE is a joint international conference integrating four major areas of knowledge that are divided into six corresponding conferences: International Conference on Data Communication Networking, DCNET; International Conference on E-Business, ICE-B; International Conference on Optical Communication Systems, OPTICS; International Conference on Security and Cryptography, SECRYPT; International Conference on Signal Processing and Multimedia, SIGMAP; International Conference on Wireless Information Systems, WINSYS. The 11 full papers presented in the volume were carefully reviewed and selected from the 166 submissions. The papers cover the following key areas of data communication networking, e-business, security and cryptography, signal processing and multimedia applications.

Future Information Technology - II James J. (Jong Hyuk) Park 2015-01-29 The new multimedia standards (for example, MPEG-21) facilitate the seamless integration of multiple modalities into interoperable multimedia frameworks, transforming the way people work and interact with multimedia data. These key technologies and multimedia solutions interact and collaborate with each other in increasingly effective ways, contributing to the multimedia revolution and having a significant impact across a wide spectrum of consumer, business, healthcare, education, and governmental domains. This book aims to provide a complete coverage of the areas outlined and to bring together the researchers from academic and industry as well as practitioners to share ideas, challenges, and solutions relating to the multifaceted aspects of this field.