Mechanics Of User Identification And Authentication Fundamentals Of Identity Management Hardcover 2007 Author Dobromir Todorov

Recognizing the artifice ways to acquire this book **Mechanics Of User Identification And Authentication Fundamentals Of Identity Management Hardcover 2007 Author Dobromir Todorov** is additionally useful. You have remained in right site to start getting this info. acquire the Mechanics Of User Identification And Authentication Fundamentals Of Identity Management Hardcover 2007 Author Dobromir Todorov belong to that we have enough money here and check out the link.

You could purchase guide Mechanics Of User Identification And Authentication Fundamentals Of Identity Management Hardcover 2007 Author Dobromir Todorov or get it as soon as feasible. You could quickly download this Mechanics Of User Identification And Authentication Fundamentals Of Identity Management Hardcover 2007 Author Dobromir Todorov after getting deal. So, bearing in mind you require the books swiftly, you can straight get it. Its correspondingly very simple and therefore fats, isnt it? You have to favor to in this aerate

Oracle Identity Management - Marlin B. Pohlman 2008-04-09
In today’s competitive marketplace with its focus on profit, maintaining integrity can often be a challenge. Further complicating this challenge is the fact that those assigned to the task of assuring accountability within an organization often have little, if any, visibility into the inner workings of that organization. Oracle Identity Management: Governance, Risk, and Compliance Architecture is the definitive guide for corporate stewards who are struggling with the challenge of meeting regulatory compliance pressures while embarking on the path of process and system remediation. The text is written by Marlin Pohlman, a director with Oracle who is recognized as one of the primary educators worldwide on identity management, regulatory compliance, and corporate governance. In the book’s first chapters, Dr. Pohlman examines multinational regulations and delves into the nature of governance, risk, and compliance. He also cites common standards, illustrating a number of well-known compliance frameworks. He then focuses on specific software components that will enable secure business operations. To complete the picture, he discusses elements of the Oracle architecture, which permit reporting essential to the regulatory compliance process, and the vaulting solutions and data hubs, which collect, enforce, and store policy information. Examining case studies from the five most regulated business verticals, financial services, retail, pharma-life sciences, higher education, and the US public sector, this work teaches corporation stewards how to: Attain and maintain high levels of integrity Eliminate redundancy and excessive expense in identity management Map solutions directly to region and legislation Hold providers accountable for contracted services Identity management is the first line of defense in the corporate internal ecosystem. Reconcilingtheory and practicality, this volume makes sure that defense is workable, responsive, and effective.
Human Bond Communication - Sudhir Dixit 2017-03-27
This book approaches the topic area of the Internet of Things (IoT) from the perspective of the five types of human communication. Through this perspective on the human communication types, the book aims to specifically address how IoT technologies can support humans and their endeavors. The book explores the fields of sensors, wireless, physiology, biology, wearables, and the Internet. This book is organized with five sections, each covering a central theme; Section 1: The basics of human bond communication Section 2: Relevance IoT, BAN and PAN Section 3: Applications of HBC Section 4: Security, Privacy and Regulatory Challenges Section 5: The Big Picture (Where do we go from here?)
Zero Trust Networks - Evan Gilman 2017-06-19
The perimeter defenses guarding your network perhaps are not as secure as you think. Hosts behind the firewall have no defenses of their own, so when a host in the "trusted" zone is breached, access to your data center is not far behind. That’s an all-too-familiar scenario today. With this practical book, you’ll learn the principles behind zero trust architecture, along with details necessary to implement it. The Zero Trust Model treats all hosts as if they’re internet-facing, and considers the entire network to be compromised and hostile. By taking this approach, you’ll focus on building strong authentication, authorization, and encryption throughout, while providing compartmentalized access and better operational agility. Understand how perimeter-based defenses have evolved to become the broken model we use today Explore two case studies of zero trust in production networks on the client side (Google) and on the server side (PagerDuty) Get example configuration for open source tools that you can use to build a zero trust network Learn how to migrate from a perimeter-based network to a zero trust network in production
Digital Privacy - Alessandro Acquisti 2007-12-22
While traveling the data highway through the global village, most people, if they think about it at all, consider privacy a non-forfeitable right. They expect to have control over the ways in which their personal information is obtained, distributed, shared, and used by any other entity. According to recent surveys, privacy, and anonymity are the fundamental issues of concern for most Internet users, ranked higher than ease-of-use, spam, cost, and security. Digital Privacy: Theory, Techniques, and Practices covers state-of-the-art technologies, best practices, and research results, as well as legal, regulatory, and ethical issues. Editors Alessandro Acquisti, Stefanos Gritzalis, Costas Lambrinoudakis, and Sabrina De Capitani di Vimercati, established researchers whose work enjoys worldwide recognition, draw on contributions from experts in academia, industry, and government to delineate theoretical, technical, and practical aspects of digital privacy. They provide an up-to-date, integrated approach to privacy issues that spells out what digital privacy is and covers the threats, rights, and provisions of the legal framework in terms of technical counter measures for the protection of an individual’s privacy. The work includes coverage of protocols, mechanisms, applications, architectures, systems, and experimental studies. Even though the utilization of personal information can improve customer services, increase revenues, and lower business costs, it can be easily misused and lead to violations of privacy. Important legal, regulatory, and ethical issues have emerged, prompting the need for an urgent and consistent response by electronic societies. Currently there is no book available that combines such a wide range of privacy topics with such a stellar cast of contributors. Filling that void, Digital Privacy: Theory, Techniques, and Practices gives you the foundation for building effective and legal privacy protocols into your business processes.
Information Security The Complete Reference, Second Edition - Mark Rhodes-Ousley 2013-04-03
Develop and implement an effective end-to-end security program Today’s complex world of mobile platforms, cloud computing, and ubiquitous data access puts new security demands on every IT professional. Information Security: The Complete Reference, Second Edition (previously titled Network Security: The Complete Reference) is the only comprehensive book that offers vendor-neutral details on all aspects of information protection, with an eye toward the evolving threat landscape. Thoroughly revised and expanded to cover all aspects of modern information security—from concepts to details—this edition provides a one-stop reference equally applicable to the beginner and the seasoned professional. Find out how to build a holistic security program based on proven methodology, risk analysis, compliance, and business needs. You’ll learn how to successfully protect data, networks, computers, and applications. In-depth chapters cover data protection, encryption, information rights management, network security,

intrusion detection and prevention, Unix and Windows security, virtual and cloud security, secure application development, disaster recovery, forensics, and real-world attacks and countermeasures. Included is an extensive security glossary, as well as standards-based references. This is a great resource for professionals and students alike. Understand security concepts and building blocks Identify vulnerabilities and mitigate risk Optimize authentication and authorization Use IRM and encryption to protect unstructured data Defend storage devices, databases, and software Protect network routers, switches, and firewalls Secure VPN, wireless, VoIP, and PBX infrastructure Design intrusion detection and prevention systems Develop secure Windows, Java, and mobile applications Perform incident response and forensic analysis

Current Trends in Web Engineering - Irene Garrigós 2018-02-21

This book constitutes the refereed thoroughly refereed post-workshop proceedings of the 17th International Conference on Web Engineering, ICWE 2017, held in Rome, Italy, in June 2017. The 24 revised full papers were selected from 34 submissions. The workshops complement the main conference, and explore new trends on core topics of Web engineering. The workshop committee accepted five workshops of which the following four contributed papers to this volume: - 2nd International Workshop on Liquid Multi-Device Software and 1st International Workshop on Engineering the Web of Things - International Workshop on The Practice Of The Open Web (practi-O-web 2017) - 3rd International Workshop on Natural Language Processing for Informal Text (NLPIT 2017) - 3rd International Workshop on Mining the Social Web (SoWeMine 2017).

Software Deployment, Updating, and Patching - Bill Stackpole 2007-12-17

The deployment of software patches can be just as challenging as building entirely new workstations. Training and support issues can haunt even the most successful software launch for months. Preparing for the rigors of software deployment includes not just implementing change, but training employees, predicting and mitigating pitfalls, and managin

Computer Fundamentals - Anita Goel 2010-09

Computer Fundamentals is specifically designed to be used at the beginner level. It covers all the basic hardware and software concepts in computers and its peripherals in a very lucid manner.

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.

Integrating a Usable Security Protocol into User Authentication Services Design Process - Christina Braz 2018-11-08

There is an intrinsic conflict between creating secure systems and usable systems. But usability and security can be made synergistic by providing requirements and design tools with specific usable security principles earlier in the requirements and design phase. In certain situations, it is possible to increase usability and security by revisiting design decisions made in the past; in others, to align security and usability by changing the regulatory environment in which the computers operate. This book addresses creation of a usable security protocol for user authentication as a natural outcome of the requirements and design phase of the authentication method development life cycle.

New Knowledge in Information Systems and Technologies - Álvaro Rocha 2019-03-29

This book includes a selection of articles from The 2019 World Conference on Information Systems and Technologies (WorldCIST'19), held from April 16 to 19, at La Toja, Spain. WorldCIST is a global forum for researchers and practitioners to present and discuss recent results and innovations, current trends, professional experiences and challenges in modern information systems and technologies research, together with their technological development and applications. The book covers a number of topics, including A) Information and Knowledge Management; B) Organizational Models and Information Systems; C) Software and Systems Modeling; D) Software Systems, Architectures, Applications and Tools; E) Multimedia Systems and Applications; F) Computer Networks, Mobility and Pervasive Systems; G) Intelligent and Decision Support Systems; H) Big Data Analytics and Applications; I) Human–Computer Interaction; J) Ethics, Computers & Security; K) Health Informatics; L) Information Technologies in Education; M) Information Technologies in Radiocommunications; and N) Technologies for Biomedical Applications.

Fundamentals of Communications and Networking - Michael G. Solomon 2021-01-15

Today's networks are required to support an increasing array of real-time communication methods. Video chat and live resources put demands on networks that were previously unimagined. Written to be accessible to all, Fundamentals of Communications and Networking, Third Edition helps readers better understand today's networks and the way they support the evolving requirements of different types of organizations. While displaying technical depth, this new edition presents an evolutionary perspective of data networking from the early years to the local area networking boom, to advanced IP data networks that support multimedia and real-time applications. The Third Edition is loaded with real-world examples, network designs, and network scenarios that provide the reader with a wealth of data networking information and practical implementation tips. Key Features of the third Edition: - Introduces network basics by describing how networks work - Discusses how networks support the increasing demands of advanced communications - Illustrates how to map the right technology to an organization's needs and business goals - Outlines how businesses use networks to solve business problems, both technically and operationally.

Building an Effective Information Security Policy Architecture - Sandy Bacik 2008-05-20

Information security teams are charged with developing and maintaining a set of documents that will protect the assets of an enterprise from constant threats and risks. In order for these safeguards and controls to be effective, they must suit the particular business needs of the enterprise. A guide for security professionals, Building an Effective Information Security Policy Architecture explains how to review, develop, and implement a security architecture for any size enterprise, whether it is a global company or a SMB. Through the use of questionnaires and interviews, the book demonstrates how to evaluate an organization's culture and its ability to meet various security standards and requirements. Because the effectiveness of a policy is dependent on cooperation and compliance, the author also provides tips on how to communicate the policy and gain support for it. Suitable for any level of technical aptitude, this book serves a guide for evaluating the business needs and risks of an enterprise and incorporating this information into an effective security policy architecture.

Microsoft Windows Security Fundamentals - Jan De Clercq 2011-04-08

This is the first of two books serving as an expanded and up-dated version of Windows Server 2003 Security Infrastructures for Windows 2003 Server R2 and SP1 & SP2. The authors choose to encompass this material within two books in order to illustrate the intricacies of the different paths used to secure MS Windows server networks. Since its release in 2003 the Microsoft Exchange server has had two important updates, SP1 and SP2. SP1, allows users to increase their security, reliability and simplify the administration of the program. Within SP1, Microsoft has implemented R2 which improves identity and access management across security-related boundaries. R2 also improves branch office server management and increases the efficiency of storage setup and management. The second update, SP2 minimizes spam,

pop-ups and unwanted downloads. These two updated have added an enormous amount of programming security to the server software. * Covers all SP1 and SP2 updates * Details strategies for patch management * Provides key techniques to maintain security application upgrades and updates

Mechanics of User Identification and Authentication - Dobromir Todorov 2007-06-18

User identification and authentication are essential parts of information security. Users must authenticate as they access their computer systems at work or at home every day. Yet do users understand how and why they are actually being authenticated, the security level of the authentication mechanism that they are using, and the potential impacts o

Digital Rights Management - Grace Agnew 2008-09-30

This book provides an overview of digital rights management (DRM), including: an overview of terminology and issues facing libraries, plus an overview of the technology including standards and off-the-shelf products. It discusses the role and implications of DRM for existing library services, such as integrated library management systems, electronic reserves, commercial database licenses, digital asset management systems and digital library repositories. It also discusses the impact that DRM 'trusted system' technologies, already in use in complementary areas, such as course management systems and web-based digital media distribution, may have on libraries. It also discusses strategies for implementing DRM in libraries and archives for safeguarding intellectual property in the web environment. A practical guide that places DRM within the context of the services and practices of the library and offers guidance on getting started An understandable overview of the technologies and standards involved in digital rights management An overview of the DRM landscape beyond libraries, with an emphasis on how this landscape impacts libraries and shapes DRM generally. In particular, the e-learning and digital media distribution arenas are embracing DRM, with significant potential impact

Biometric User Authentication for IT Security - Claus Vielhauer 2005-09-06

Biometric user authentication techniques evoke an enormous interest by science, industry and society. Scientists and developers constantly pursue technology for automated determination or confirmation of the identity of subjects based on measurements of physiological or behavioral traits of humans. Biometric User Authentication for IT Security: From Fundamentals to Handwriting conveys general principals of passive (physiological traits such as fingerprint, iris, face) and active (learned and trained behavior such as voice, handwriting and gait) biometric recognition techniques to the reader. Unlike other publications in this area that concentrate on passive schemes, this professional book reflects a more comprehensive analysis of one particular active biometric technique: handwriting. Aspects that are thoroughly discussed include sensor characteristic dependency, attack scenarios, and the generation of cryptographic keys from handwriting.

Mechanics of User Identification and Authentication - Dobromir Todorov 2007-06-18

User identification and authentication are essential parts of information security. Users must authenticate as they access their computer systems at work or at home every day. Yet do users understand how and why they are actually being authenticated, the security level of the authentication mechanism that they are using, and the potential impacts of selecting one authentication mechanism or another? Introducing key concepts, Mechanics of User Identification and Authentication: Fundamentals of Identity Management outlines the process of controlled access to resources through authentication, authorization, and accounting in an in-depth, yet accessible manner. It examines today's security landscape and the specific threats to user authentication. The book then outlines the process of controlled access to resources and discusses the types of user credentials that can be presented as proof of identity prior to accessing a computer system. It also contains an overview on cryptography that includes the essential approaches and terms required for understanding how user authentication works. This book provides specific information on the user authentication process for both UNIX and Windows. Addressing more advanced applications and services, the author presents common security models such as GSSAPI and discusses authentication architecture. Each method is illustrated with a specific authentication scenario.

Digital Identity Management in Formal Education - Alan Moran 2021-09-21

Digital Identity Management in Formal Education offers a broad analysis of the online self considered from educational policy, technological, legal and social perspectives. This book introduces the reader to the notion that digital identity is a multifaceted topic which requires a broad and systematic approach that is rooted in risk-based policy. It provides educational technologists, leaders and decision-makers with an accessible, jargon-free guide to their responsibilities towards students and instructors in today's digitally networked schools and universities. Real-life examples illustrate how digital identities impact management and delivery, privacy and transactions, governance and accountability, and other interconnected choices in the use of technology-enabled services in formal learning.

Advances in Digital Forensics VI - Kam-Pui Chow 2010-11-26

Advances in Digital Forensics VI describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: Themes and Issues, Forensic Techniques, Internet Crime Investigations, Live Forensics, Advanced Forensic Techniques, and Forensic Tools. This book is the sixth volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of twenty-one edited papers from the Sixth Annual IFIP WG 11.9 International Conference on Digital Forensics, held at the University of Hong Kong, Hong Kong, China, in January 2010.

Integrated Information and Computing Systems for Natural, Spatial, and Social Sciences - Rückemann, Claus-Peter 2012-10-31

The 21st century has seen a number of advancements in technology, including the use of high performance computing. Computing resources are being used by the science and economy fields for data processing, simulation, and modeling. These innovations aid in the support of production, logistics, and mobility processes. Integrated Information and Computing Systems for Natural, Spatial, and Social Sciences covers a carefully selected spectrum of the most up to date issues, revealing the benefits, dynamism, potential, and challenges of information and computing system application scenarios and components from a wide spectrum of prominent disciplines. This comprehensive collection offers important guidance on the development stage of the universal solution to information and computing systems for researchers as well as industry decision makers and developers.

Encyclopedia of Cryptography and Security - Henk C.A. van Tilborg 2014-07-08

Expanded into two volumes, the Second Edition of Springer's Encyclopedia of Cryptography and Security brings the latest and most comprehensive coverage of the topic: Definitive information on cryptography and information security from highly regarded researchers Effective tool for professionals in many fields and researchers of all levels Extensive resource with more than 700 contributions in Second Edition 5643 references, more than twice the number of references that appear in the First Edition With over 300 new entries, appearing in an A-Z format, the Encyclopedia of Cryptography and Security provides easy, intuitive access to information on all aspects of cryptography and security. As a critical enhancement to the First Edition's base of 464 entries, the information in the Encyclopedia is relevant for researchers and professionals alike. Topics for this comprehensive reference were elected, written, and peer-reviewed by a pool of distinguished researchers in the field. The Second Edition's editorial board now includes 34 scholars, which was expanded from 18 members in the First Edition. Representing the work of researchers from over 30 countries, the Encyclopedia is broad in scope, covering everything from authentication and identification to quantum cryptography and web security. The text's practical style is instructional, yet fosters investigation. Each area presents concepts, designs, and specific implementations. The highly-structured essays in this work include synonyms, a definition and discussion of the topic, bibliographies, and links to related literature. Extensive cross-references to other entries within the Encyclopedia support efficient, user-friendly searches for immediate access to relevant information. Key concepts presented in the Encyclopedia of Cryptography and Security include: Authentication and identification; Block ciphers and stream ciphers; Computational issues; Copy protection; Cryptanalysis and security; Cryptographic protocols; Electronic payment and digital certificates; Elliptic curve cryptography; Factorization algorithms and primality tests; Hash functions and MACs; Historical systems; Identity-based cryptography; Implementation aspects for smart cards and standards; Key management; Multiparty computations like voting schemes; Public key cryptography; Quantum cryptography; Secret sharing schemes; Sequences;

Web Security. Topics covered: Data Structures, Cryptography and Information Theory; Data Encryption; Coding and Information Theory; Appl.Mathematics/Computational Methods of Engineering; Applications of Mathematics; Complexity. This authoritative reference will be published in two formats: print and online. The online edition features hyperlinks to cross-references, in addition to significant research.

Fundamentals of Computer Security - Josef Pieprzyk 2013-03-09

This reference work looks at modern concepts of computer security. It introduces the basic mathematical background necessary to follow computer security concepts before moving on to modern developments in cryptography. The concepts are presented clearly and illustrated by numerous examples. Subjects covered include: private-key and public-key encryption, hashing, digital signatures, authentication, secret sharing, group-oriented cryptography, and many others. The section on intrusion detection and access control provide examples of security systems implemented as a part of operating system. Database and network security is also discussed. The final chapters introduce modern e- business systems based on digital cash.

Future-Proof Software-Systems - Frank J. Furrer 2019-09-25

This book focuses on software architecture and the value of architecture in the development of long-lived, mission-critical, trustworthy software-systems. The author introduces and demonstrates the powerful strategy of “Managed Evolution,” along with the engineering best practice known as “Principle-based Architecting.” The book examines in detail architecture principles for e.g., Business Value, Changeability, Resilience, and Dependability. The author argues that the software development community has a strong responsibility to produce and operate useful, dependable, and trustworthy software. Software should at the same time provide business value and guarantee many quality-of-service properties, including security, safety, performance, and integrity. As Dr. Furrer states, “Producing dependable software is a balancing act between investing in the implementation of business functionality and investing in the quality-of-service properties of the software-systems.” The book presents extensive coverage of such concepts as: Principle-Based Architecting Managed Evolution Strategy The Future Principles for Business Value Legacy Software Modernization/Migration Architecture Principles for Changeability Architecture Principles for Resilience Architecture Principles for Dependability The text is supplemented with numerous figures, tables, examples and illustrative quotations. Future-Proof Software-Systems provides a set of good engineering practices, devised for integration into most software development processes dedicated to the creation of software-systems that incorporate Managed Evolution.

How to Achieve 27001 Certification - Sigurjon Thor Arnason 2007-11-28

The security criteria of the International Standards Organization (ISO) provides an excellent foundation for identifying and addressing business risks through a disciplined security management process. Using security standards ISO 17799 and ISO 27001 as a basis, How to Achieve 27001 Certification: An Example of Applied Compliance Management helps an organization align its security and organizational goals so it can generate effective security, compliance, and management programs. The authors offer insight from their own experiences, providing questions and answers to determine an organization's information security strengths and weaknesses with respect to the standard. They also present step-by-step information to help an organization plan an implementation, as well as prepare for certification and audit. Security is no longer a luxury for an organization, it is a legislative mandate. A formal methodology that helps an organization define and execute an ISMS is essential in order to perform and prove due diligence in upholding stakeholder interests and legislative compliance. Providing a good starting point for novices, as well as finely tuned nuances for seasoned security professionals, this book is an invaluable resource for anyone involved with meeting an organization's security, certification, and compliance needs.

Information Technology Control and Audit - Sandra Senft 2008-11-18

The headline-grabbing financial scandals of recent years have led to a great urgency regarding organizational governance and security. Information technology is the engine that runs modern organizations, and as such, it must be well-managed and controlled. Organizations and individuals are dependent on network environment technologies, increasing t

Business Resumption Planning - Leo A. Wrobel 2008-11-18

Offering hundreds of tips, templates, checklists, and pointers to information in the public domain, Business Resumption Planning, Second Edition assists you in creating a rock solid recovery plan for any size organization. It provides the information you need in order to coordinate first responders to meet any disaster scenario head on, whet

CISO Soft Skills - Ron Collette 2008-11-21

As organizations struggle to implement effective security measures, all too often they focus solely on the tangible elements, such as developing security policies or risk management implementations. While these items are very important, they are only half of the equation necessary to ensure security success. CISO Soft Skills: Securing Organizations Impaired by Employee Politics, Apathy, and Intolerant Perspectives presents tools that empower security practitioners to identify the intangible negative influencers of security that plague most organizations, and provides techniques to identify, minimize, and overcome these pitfalls. The book begins by explaining how using the wrong criteria to measure security can result in a claim of adequate security when objective assessment demonstrates this not to be the case. The authors instead recommend that organizations measure the success of their efforts using a practical approach that illustrates both the tangible and intangible requirements needed by a healthy security effort. The middle section discusses the root causes that negatively influence both a CISO and an organization’s ability to truly secure itself. These root causes include: Employee apathy Employee myopia or tunnel vision Employee primacy, often exhibited as office politics The infancy of the information security discipline These chapters explain what a CISO can do about these security constraints, providing numerous practical and actionable exercises, tools, and techniques to identify, limit, and compensate for the influence of security constraints in any type of organization. The final chapters discuss some proactive techniques that CISOs can utilize to effectively secure challenging work environments. Reflecting the experience and solutions of those that are in the trenches of modern organizations, this volume provides practical ideas that can make a difference in the daily lives of security practitioners.

Information Technology Control and Audit, Third Edition - Sandra Senft 2010-12-12

The headline-grabbing financial scandals of recent years have led to a great urgency regarding organizational governance and security. Information technology is the engine that runs modern organizations, and as such, it must be well-managed and controlled. Organizations and individuals are dependent on network environment technologies, increasing the importance of security and privacy. The field has answered this sense of urgency with advances that have improved the ability to both control the technology and audit the information that is the lifeblood of modern business. Reflects the Latest Technological Advances Updated and revised, this third edition of Information Technology Control and Audit continues to present a comprehensive overview for IT professionals and auditors. Aligned to the CobiT control objectives, it provides a fundamental understanding of IT governance, controls, auditing applications, systems development, and operations. Demonstrating why controls and audits are critical, and defining advances in technology designed to support them, this volume meets the increasing need for audit and control professionals to understand information technology and the controls required to manage this key resource. A Powerful Primer for the CISA and CGEIT Exams Supporting and analyzing the CobiT model, this text prepares IT professionals for the CISA and CGEIT exams. With summary sections, exercises, review questions, and references for further readings, it promotes the mastery of the concepts and practical implementation of controls needed to effectively manage information technology resources. New in the Third Edition: Reorganized and expanded to align to the CobiT objectives Supports study for both the CISA and CGEIT exams Includes chapters on IT financial and sourcing management Adds a section on Delivery and Support control objectives Includes additional content on audit and control of outsourcing, change management, risk management, and compliance

12 More Essential Skills for Software Architects - Dave Hendricksen 2015

This indispensable new handbook focuses on 12 specific skills every software architect needs to succeed: skills involved in becoming a superior technologist and an outstanding technical champion in your organization. Focuses on three sets of skills that will have the greatest impact on your ability to succeed and ascend: Product Development Skills: Partnership, Discovery, Modeling, Leverage, and Estimating Oversight Skills: Platform/Project Oversight, Capital Planning, and Risk Management Visionary Skills: Road Mapping, Researching, Trend Awareness, and Branding Unlike most software architecture guides, Hendricken's books place real-world practice in the context of the development organization and the

business, and help you blend the optimal mix of both hard and soft skills. Both valuable initial instruction and a lasting reference, this guide will can help you earn and succeed in your next software architecture role -- in any organization, at any level.

Computational Intelligence and Efficiency in Engineering Systems - Grzegorz Borowik 2015-03-10

This carefully edited and reviewed volume addresses the increasingly popular demand for seeking more clarity in the data that we are immersed in. It offers excellent examples of the intelligent ubiquitous computation, as well as recent advances in systems engineering and informatics. The content represents state-of-the-art foundations for researchers in the domain of modern computation, computer science, system engineering and networking, with many examples that are set in industrial application context. The book includes the carefully selected best contributions to APCASE 2014, the 2nd Asia-Pacific Conference on Computer Aided System Engineering, held February 10-12, 2014 in South Kuta, Bali, Indonesia. The book consists of four main parts that cover data-oriented engineering science research in a wide range of applications: computational models and knowledge discovery; communications networks and cloud computing; computer-based systems; and data-oriented and software-intensive systems.

Cyber Forensics - Albert Marcella, Jr. 2007-12-19

Designed as an introduction and overview to the field, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition integrates theory and practice to present the policies, procedures, methodologies, and legal ramifications and implications of a cyber forensic investigation. The authors guide you step-by-step through the basics of investigation and introduce the tools and procedures required to legally seize and forensically evaluate a suspect machine. Updating and expanding information on concealment techniques, new technologies, hardware, software, and relevant new legislation, this second edition delineates the scope and goals of cyber forensics to reveal and track legal and illegal activity. Beginning with an introduction and definition of cyber forensics, chapters explain the rules of evidence and chain of custody in maintaining legally valid electronic evidence. They describe how to begin an investigation and employ investigative methodology, as well as establish standard operating procedures for the field and cyber forensic laboratory. The authors provide an in depth examination of the manipulation of technology to conceal illegal activities and the use of cyber forensics to uncover them. They discuss topics and issues such as conducting a cyber forensic investigation within both the local and federal legal framework, and evaluating the current data security and integrity exposure of multifunctional devices. Cyber Forensics includes details and tips on taking control of a suspect computer or PDA and its "operating" environment, mitigating potential exposures and risks to chain of custody, and establishing and following a flowchart for the seizure of electronic evidence. An extensive list of appendices include websites, organizations, pertinent legislation, further readings, best practice recommendations, more information on hardware and software, and a recap of the federal rules of civil procedure.

Information Assurance Architecture - Keith D. Willett 2008-06-24

Now that information has become the lifeblood of your organization, you must be especially vigilant about assuring it. The hacker, spy, or cyber-thief of today can breach any barrier if it remains unchanged long enough or has even the tiniest leak. In Information Assurance Architecture, Keith D. Willett draws on his over 25 years of technical, security, and business experience to provide a framework for organizations to align information assurance with the enterprise and their overall mission. The Tools to Protect Your Secrets from Exposure This work provides the security industry with the know-how to create a formal information assurance architecture that complements an enterprise architecture, systems engineering, and the enterprise life cycle management (ELCM). Information Assurance Architecture consists of a framework, a process, and many supporting tools, templates and methodologies. The framework provides a reference model for the consideration of security in many contexts and from various perspectives; the process provides direction on how to apply that framework. Mr. Willett teaches readers how to identify and use the right tools for the right job. Furthermore, he demonstrates a disciplined approach in thinking about, planning, implementing and managing security, emphasizing that solid solutions can be made impenetrable when they are seamlessly integrated with the whole of an enterprise. Understand the Enterprise Context This book covers many information assurance subjects, including disaster recovery and firewalls. The objective is to present security services and security mechanisms in the context of information assurance architecture, and in an enterprise context of managing business risk. Anyone who utilizes the concepts taught in these pages will find them to be a valuable weapon in the arsenal of information protection.

How to Complete a Risk Assessment in 5 Days or Less - Thomas R. Peltier 2008-11-18

Successful security professionals have had to modify the process of responding to new threats in the high-profile, ultra-connected business environment. But just because a threat exists does not mean that your organization is at risk. This is what risk assessment is all about. How to Complete a Risk Assessment in 5 Days or Less demonstrates how to identify threats your company faces and then determine if those threats pose a real risk to the organization. To help you determine the best way to mitigate risk levels in any given situation, How to Complete a Risk Assessment in 5 Days or Less includes more than 350 pages of user-friendly checklists, forms, questionnaires, and sample assessments. Presents Case Studies and Examples of all Risk Management Components Based on the seminars of information security expert Tom Peltier, this volume provides the processes that you can easily employ in your organization to assess risk. Answers such FAQs as: Why should a risk analysis be conducted? Who should review the results? How is the success measured? Always conscious of the bottom line, Peltier discusses the cost-benefit of risk mitigation and looks at specific ways to manage costs. He supports his conclusions with numerous case studies and diagrams that show you how to apply risk management skills in your organization—and it’s not limited to information security risk assessment. You can apply these techniques to any area of your business. This step-by-step guide to conducting risk assessments gives you the knowledgebase and the skill set you need to achieve a speedy and highly-effective risk analysis assessment in a matter of days.

Business Resumption Planning, Second Edition - Leo A. Wrobel 2008-11-18

Offering hundreds of tips, templates, checklists, and pointers to information in the public domain, Business Resumption Planning, Second Edition assists you in creating a rock solid recovery plan for any size organization. It provides the information you need in order to coordinate first responders to meet any disaster scenario head on, whether involving computers, telecommunications, or infrastructure in a timely and effective manner. What’s New in the Second Edition: · The latest techniques for conducting an efficient Business Impact Analysis and an accurate Failure Mode Effects Analysis (FMEA) · Advice on how to successfully recover from Ground Zero events, such as those involving Oklahoma City, the World Trade Center (WTC), and Hurricane Katrina · Tips for recovery teams and first responders, including how to maintain “4Ci” (Command, Control, Communications, Computers and intelligence) during a disaster · An examination of legal ramifications resulting from a failure to plan—including new liability issues that directly affect you · An explanation of how the recently enacted Sarbanes-Oxley Act of 2002 impacts your planning effort · Plans and templates that assess vulnerability in WANs, Open Networks, physical facilities, environmentals, and enhanced services The book contains actual case studies and examples illustrating the vulnerabilities of today’s mission critical systems. It details the proactive steps you should take now to first assess your exposure, then eliminate it. The book also includes a CD-ROM that contains worksheets, checklists, audit forms, work breakdown structures, and reports.

Enterprise Architecture A to Z - Daniel Minoli 2008-06-19

Driven by the need and desire to reduce costs, organizations are faced with a set of decisions that require analytical scrutiny. Enterprise Architecture A to Z: Frameworks, Business Process Modeling, SOA, and Infrastructure Technology examines cost-saving trends in architecture planning, administration, and management. To establish a framework for discussion, this book begins by evaluating the role of Enterprise Architecture Planning and Service-Oriented Architecture (SOA) modeling. It provides an extensive review of the most widely deployed architecture framework models. In particular, the book discusses The Open Group Architecture Framework (TOGAF) and the Zachman Architectural Framework (ZAF) in detail, as well as formal architecture standards and all four layers of these models: the business architecture, the information architecture, the solution architecture, and the technology architecture. The first part of the text focuses on the upper layers of the architecture framework, while the second part focuses on the technology architecture. In this second section, the author presents an assessment of storage technologies and networking and addresses regulatory and security issues. Additional coverage includes high-speed communication mechanisms such as Ethernet, WAN and Internet communication technologies, broadband communications, and chargeback models. Daniel Minoli has written a number of columns and books on the

high-tech industry and has many years of technical hands-on and managerial experience at top financial companies and telecom/networking providers. He brings a wealth of knowledge and practical experience to these pages. By reviewing the strategies in this book, CIOs, CTOs, and senior managers are empowered by a set of progressive approaches to designing state-of-the-art IT data centers.

ICCSM2013-Proceedings of the International Conference on Cloud Security Management - Barbara Endicott-Popovsky 2013-01-09

Security Technology, Disaster Recovery and Business Continuity - Wai-chi Fang 2010-11-25

Welcome to the proceedings of the 2010 International Conferences on Security Te- nology (SecTech 2010), and Disaster Recovery and Business Continuity (DRBC 2010) – two of the partnering events of the Second International Mega-Conference on Future Generation Information Technology (FGIT 2010). SecTech and DRBC bring together researchers from academia and industry as well as practitioners to share ideas, problems and solutions relating to the multifaceted aspects of security and disaster recovery methodologies, including their links to c- putational sciences, mathematics and information technology. In total, 1,630 papers were submitted to FGIT 2010 from 30 countries, which - cludes 250 papers submitted to SecTech/DRBC 2010. The submitted papers went through a rigorous reviewing process: 395 of the 1,630 papers were accepted for FGIT 2010, while 57 papers were accepted for SecTech/DRBC 2010. Of the 250 papers 10 were selected for the special FGIT 2010 volume published by Springer in the LNCS series. 34 papers are published in this volume, and 13 papers were wi- drawn due to technical reasons. We would like to acknowledge the great effort of the SecTech/DRBC 2010 Int- national Advisory Boards and members of the International Program Committees, as well as all the organizations and individuals who supported the idea of publishing this volume of proceedings, including SERSC and Springer. Also, the success of these two conferences would not have been possible without the huge support from our sponsors and the work of the Chairs and Organizing Committee.

Web Application Security, A Beginner's Guide - Bryan Sullivan 2011-12-06

Security Smarts for the Self-Guided IT Professional “Get to know the hackers—or plan on getting hacked. Sullivan and Liu have created a savvy, essentials-based approach to web app security packed with immediately applicable tools for any information security practitioner sharpening his or her tools or just starting out.” —Ryan McGeehan, Security Manager, Facebook, Inc. Secure web applications from today's most devious hackers. Web Application Security: A Beginner's Guide helps you stock your security toolkit, prevent common hacks, and defend quickly against malicious attacks. This practical resource includes chapters on authentication, authorization, and session management, along with browser, database, and file security--all supported by true stories from industry. You'll also get best practices for vulnerability detection and secure development, as well as a chapter that covers essential security fundamentals. This book's templates, checklists, and examples are designed to help you get started right away. Web Application Security: A Beginner's Guide features: Lingo--Common security terms defined so that you're in the know on the job IMHO--Frank and relevant opinions based on the authors' years of industry experience Budget Note--Tips for getting security technologies and processes into your organization's budget In Actual Practice--Exceptions to the rules of security explained in real-world contexts Your Plan--Customizable checklists you can use on the job now Into Action--Tips on how, why, and when to apply new skills and techniques at work

Fundamentals of Information Systems Security - David Kim 2013-07-11

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