Computer Network Security Literature Review Papers

Implementing Effective IT Governance and IT Management2014 International Conference on Computer, NetworkCyber Security and the Politics of TimeProceedings of the 12th European Conference on Information Warfare and SecurityResearch Methods for Cyber SecuritySecurity, Privacy and Reliability in Computer Communications and NetworksComputer and Information Security HandbookThe Implications and Effects of Data Security Measures and Strategic Planning in a Computer Network EnvironmentCyber Security and Global Information Assurance: Threat Analysis and Response SolutionsNetworks, Security and ComplexityRecent Progress in Data Engineering and Internet TechnologyReturn on Information Security InvestmentPrinciples of Secure Network Systems DesignSecrets and LiesFuture Information TechnologyComputer and Network Security EssentialsComputer System and Network SecurityInformation Fusion for Cyber-Security AnalyticsCounter Hack ReloadedStandard Handbook for Electrical Engineers, Seventeenth EditionComputer NetworksGuide to Wireless Mesh NetworksModeling and Simulation of Computer Networks and SystemsContemporary Security StudiesComputer Network SecurityBiometrics for Network SecurityConversation and CommunityComputer and Network SecurityBlockchain Cybersecurity, Trust and PrivacySocial and Human Elements of Information Security: Emerging Trends and CountermeasuresDoes It Matter?Case Studies in Secure ComputingComputer and Information Security HandbookBluetooth Security AttacksInformation Security Management SystemsThe 2020 International Conference on Machine Learning and Big Data Analytics for IoT Security and PrivacyInformation Science AbstractsSecuring the Internet of ThingsQuality, Reliability, Security and Robustness in Heterogeneous NetworksSimulation in Computer Network Design and Modeling: Use and Analysis

Implementing Effective IT Governance and IT Management

"This book provides a valuable resource by addressing the most pressing issues facing cyber-security from both a national and global perspective"--Provided by publisher.

2014 International Conference on Computer, Network

Conversation and Community is an examination of the speech community in an Internet 'virtual community'. Based on ethnographic research on a community of users of a MUD, or 'multi-user dimension', the book describes a close-knit community united in features of their language use, shared history, and relationships to other online communities. The author invokes the notion of register, or the variety of speech adapted to the communication situation, in her discussion of how users overcome the limitations of the typed, text medium and exploit its affordances for comfortable communication. Routines, conventional vocabulary and abbreviations, syntactic and semantic phenomena, and special turn-taking and repair strategies distinguish the MUD community's register. Because the MUD is programmable, commands may be added which reflect, alter,

or reinforce the linguistic practices and culture of the community; competent speakers must also know the commands that produce the correct linguistic forms.

Cyber Security and the Politics of Time

In today's age of wireless and mobile computing, network and computer security is paramount. Case Studies in Secure Computing: Achievements and Trends gathers the latest research from researchers who share their insights and best practices through illustrative case studies. This book examines the growing security attacks and countermeasures in the stand-alone and networking worlds, along with other pertinent security issues. The many case studies capture a truly wide range of secure computing applications. Surveying the common elements in computer security attacks and defenses, the book: Describes the use of feature selection and fuzzy logic in a decision tree model for intrusion detection Introduces a set of common fuzzy-logic-based security risk estimation techniques with examples Proposes a secure authenticated multiple-key establishment protocol for wireless sensor networks Investigates various malicious activities associated with cloud computing and proposes some countermeasures Examines current and emerging security threats in long-term evolution backhaul and core networks Supplies a brief introduction to application-layer denial-of-service (DoS) attacks Illustrating the security challenges currently facing practitioners, this book presents powerful security solutions proposed by leading researchers in the field. The examination of the various case studies will help to develop the practical understanding required to stay one step ahead of the security threats on the horizon. This book will help those new to the field understand how to mitigate security threats. It will also help established practitioners fine-tune their approach to establishing robust and resilient security for next-generation computing systems.

Proceedings of the 12th European Conference on Information Warfare and Security

This new volume, Information Security Management Systems: A Novel Framework and Software as a Tool for Compliance with Information Security Standard, looks at information security management system standards, risk management associated with information security, and information security awareness within an organization. The authors aim to improve the overall ability of organizations to participate, forecast, and actively assess their information security circumstances. It is important to note that securing and keeping information from parties who do not have authorization to access such information is an extremely important issue. To address this issue, it is essential for an organization to implement an ISMS standard such as ISO 27001 to address the issue comprehensively. The authors of this new volume have constructed a novel security framework (ISF) and subsequently used this framework to develop software called Integrated Solution Modeling (ISM), a semi-automated system that will greatly help organizations comply with ISO 27001 faster and cheaper than other existing methods. In addition, ISM does not only help organizations to assess their information security compliance with ISO 27001, but it can also be used as a monitoring tool, helping organizations monitor the security statuses of their information resources as well as monitor potential threats. ISM is developed to provide solutions to solve

obstacles, difficulties, and expected challenges associated with literacy and governance of ISO 27001. It also functions to assess the RISC level of organizations towards compliance with ISO 27001. The information provide here will act as blueprints for managing information security within business organizations. It will allow users to compare and benchmark their own processes and practices against these results shown and come up with new, critical insights to aid them in information security standard (ISO 27001) adoption.

Research Methods for Cyber Security

Reid (senior product manager, Cryptometrics) introduces the technical capabilities and limitations of computer biometric systems for measuring fingerprints, eye characteristics, or other body information as a computer security measure serving a similar purpose to personal identification numbers. He describes the workings of the different types of technologies and examines some of the mathematics behind biometric systems. He also describes the conceptualization and implementation of a particular system with which he was involved. Annotation : 2004 Book News, Inc., Portland, OR (booknews.com).

Security, Privacy and Reliability in Computer Communications and Networks

Computer Networks: A Systems Approach, Fifth Edition, explores the key principles of computer networking, with examples drawn from the real world of network and protocol design. Using the Internet as the primary example, this best-selling and classic textbook explains various protocols and networking technologies. The systems-oriented approach encourages students to think about how individual network components fit into a larger, complex system of interactions. This book has a completely updated content with expanded coverage of the topics of utmost importance to networking professionals and students, including P2P, wireless, network security, and network applications such as e-mail and the Web, IP telephony and video streaming, and peer-to-peer file sharing. There is now increased focus on application layer issues where innovative and exciting research and design is currently the center of attention. Other topics include network design and architecture; the ways users can connect to a network; the concepts of switching, routing, and internetworking; end-to-end protocols; congestion control and resource allocation; and end-to-end data. Each chapter includes a problem statement, which introduces issues to be examined; shaded sidebars that elaborate on a topic or introduce a related advanced topic; What’s Next? discussions that deal with emerging issues in research, the commercial world, or society; and exercises. This book is written for graduate or upper-division undergraduate classes in computer networking. It will also be useful for industry professionals retraining for network-related assignments, as well as for network practitioners seeking to understand the workings of network protocols and the big picture of networking. Completely updated content with expanded coverage of the topics of utmost importance to networking professionals and students, including P2P, wireless, security, and applications Increased focus on application layer issues where innovative and exciting research and design is currently the center of attention Free downloadable network simulation software and lab experiments

manual available

Computer and Information Security Handbook

This book constitutes the thoroughly refereed post-conference proceedings of the 9th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, QShine 2013, which was held in National Capital Region (NCR) of India during January 2013. The 87 revised full papers were carefully selected from 169 submissions and present the recent technological developments in broadband high-speed networks, peer-to-peer networks, and wireless and mobile networks.

The Implications and Effects of Data Security Measures and Strategic Planning in a Computer Network Environment

Presents information on how to analyze risks to your networks and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to physical and network threats. Also imparts the skills and knowledge needed to identify and counter some fundamental security risks and requirements, including Internet security threats and measures (audit trails IP sniffing/spoofing etc.) and how to implement security policies and procedures. In addition, this book covers security and network design with respect to particular vulnerabilities and threats. It also covers risk assessment and mitigation and auditing and testing of security systems as well as application standards and technologies required to build secure VPNs, configure client software and server operating systems, IPsec-enabled routers, firewalls and SSL clients. This comprehensive book will provide essential knowledge and skills needed to select, design and deploy a public key infrastructure (PKI) to secure existing and future applications. * Chapters contributed by leaders in the field cover theory and practice of computer security technology, allowing the reader to develop a new level of technical expertise * Comprehensive and up-to-date coverage of security issues facilitates learning and allows the reader to remain current and fully informed from multiple viewpoints * Presents methods of analysis and problem-solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions

Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions

Securing the Internet of Things provides network and cybersecurity researchers and practitioners with both the theoretical and practical knowledge they need to know regarding security in the Internet of Things (IoT). This booming field, moving from strictly research to the marketplace, is advancing rapidly, yet security issues abound. This book explains the fundamental concepts of IoT security, describing practical solutions that account for resource limitations at IoT end-node, hybrid network architecture, communication protocols, and application characteristics. Highlighting the most important potential IoT security risks and threats, the book covers both the general theory and practical implications for people working in security in the Internet of Things. Helps researchers and practitioners understand the security architecture in IoT and the state-of-the-art in IoT security

countermeasures Explores how the threats in IoT are different from traditional ad hoc or infrastructural networks Provides a comprehensive discussion on the security challenges and solutions in RFID, WSNs, and IoT Contributed material by Dr. Imed Romdhani

Networks, Security and Complexity

Recent Progress in Data Engineering and Internet Technology

A fundamental and comprehensive framework for network security designed for military, government, industry, and academic network personnel. Scientific validation of "security on demand" through computer modeling and simulation methods. The book presents an example wherein the framework is utilized to integrate security into the operation of a network. As a result of the integration, the inherent attributes of the network may be exploited to reduce the impact of security on network performance and the security availability may be increased down to the user level. The example selected is the ATM network which is gaining widespread acceptance and use.

Return on Information Security Investment

This anniversary edition which has stood the test of time as a runaway best-seller provides a practical, straight-forward guide to achieving security throughout computer networks. No theory, no math, no fiction of what should be working but isn't, just the facts. Known as the master of cryptography, Schneier uses his extensive field experience with his own clients to dispel the myths that often mislead IT managers as they try to build secure systems. A much-touted section: Schneier's tutorial on just what cryptography (a subset of computer security) can and cannot do for them, has received far-reaching praise from both the technical and business community. Praise for Secrets and Lies "This is a business issue, not a technical one, and executives can no longer leave such decisions to techies. That's why Secrets and Lies belongs in every manager's library."-Business Week "Startlingly lively.a jewel box of little surprises you can actually use."-Fortune "Secrets is a comprehensive, well-written work on a topic few business leaders can afford to neglect."-Business 2.0 "Instead of talking algorithms to geeky programmers, [Schneier] offers a primer in practical computer security aimed at those shopping, communicating or doing business online-almost everyone, in other words."-The Economist "Schneierpeppers the book with lively anecdotes and aphorisms, making it unusually accessible."-Los Angeles Times With a new and compelling Introduction by the author, this premium edition will become a keepsake for security enthusiasts of every stripe.

Principles of Secure Network Systems Design

This book highlights several gaps that have not been addressed in existing cyber security research. It first discusses the recent attack prediction techniques that utilize one or more aspects of information to create attack prediction models. The second part is dedicated to new trends on information fusion and their applicability

to cyber security; in particular, graph data analytics for cyber security, unwanted traffic detection and control based on trust management software defined networks, security in wireless sensor networks & their applications, and emerging trends in security system design using the concept of social behavioral biometric. The book guides the design of new commercialized tools that can be introduced to improve the accuracy of existing attack prediction models. Furthermore, the book advances the use of Knowledge-based Intrusion Detection Systems (IDS) to complement existing IDS technologies. It is aimed towards cyber security researchers.

Secrets and Lies

Provides research on the social and human aspects of information security. Presents the latest trends, issues, and findings in the field.

Future Information Technology

Over the last decade, and even since the bursting of the technology bubble, pundits, consultants, and thought leaders have argued that information technology provides the edge necessary for business success. IT expert Nicholas G. Carr offers a radically different view in this eloquent and explosive book. As IT's power and presence have grown, he argues, its strategic relevance has actually decreased. IT has been transformed from a source of advantage into a commoditized "cost of doing business"--with huge implications for business management. Expanding on Carr's seminal Harvard Business Review article that generated a storm of controversy, Does IT Matter? provides a truly compelling--and unsettling--account of IT's changing business role and its leveling influence on competition. Through astute analysis of historical and contemporary examples, Carr shows that the evolution of IT closely parallels that of earlier technologies such as railroads and electric power. He goes on to lay out a new agenda for IT management, stressing cost control and risk management over innovation and investment. And he examines the broader implications for business strategy and organization as well as for the technology industry. A frame-changing statement on one of the most important business phenomena of our time, Does IT Matter? marks a crucial milepost in the debate about IT's future. An acclaimed business writer and thinker, Nicholas G. Carr is a former executive editor of the Harvard Business Review.

Computer and Network Security Essentials

The second edition of this comprehensive handbook of computer and information security provides the most complete view of computer security and privacy available. It offers in-depth coverage of security theory, technology, and practice as they relate to established technologies as well as recent advances. It explores practical solutions to many security issues. Individual chapters are authored by leading experts in the field and address the immediate and long-term challenges in the authors’ respective areas of expertise. The book is organized into 10 parts comprised of 70 contributed chapters by leading experts in the areas of networking and systems security, information management, cyber warfare and security, encryption technology, privacy, data storage, physical security, and a host of

advanced security topics. New to this edition are chapters on intrusion detection, securing the cloud, securing web apps, ethical hacking, cyber forensics, physical security, disaster recovery, cyber attack deterrence, and more. Chapters by leaders in the field on theory and practice of computer and information security technology, allowing the reader to develop a new level of technical expertise Comprehensive and up-to-date coverage of security issues allows the reader to remain current and fully informed from multiple viewpoints Presents methods of analysis and problem-solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions

Computer System and Network Security

Computer System and Network Security provides the reader with a basic understanding of the issues involved in the security of computer systems and networks. Introductory in nature, this important new book covers all aspects related to the growing field of computer security. Such complete coverage in a single text has previously been unavailable, and college professors and students, as well as professionals responsible for system security, will find this unique book a valuable source of information, either as a textbook or as a general reference. Computer System and Network Security discusses existing and potential threats to computer systems and networks and outlines the basic actions that are generally taken to protect them. The first two chapters of the text introduce the reader to the field of computer security, covering fundamental issues and objectives. The next several chapters describe security models, authentication issues, access control, intrusion detection, and damage control. Later chapters address network and database security and systems/networks connected to wide-area networks and internetworks. Other topics include firewalls, cryptography, malicious software, and security standards. The book includes case studies with information about incidents involving computer security, illustrating the problems and potential damage that can be caused when security fails. This unique reference/textbook covers all aspects of computer and network security, filling an obvious gap in the existing literature.

Information Fusion for Cyber-Security Analytics

Counter Hack Reloaded

The objective of the 2014 International Conference on Computer, Network Security and Communication Engineering (CNSCE2014) is to provide a platform for all researchers in the field of Computer, Network Security and Communication Engineering to share the most advanced knowledge from both academic and industrial world, to communicate with each other about their experience and most up-to-date research achievements, and to discuss issues and future prospects in these fields. As an international conference mixed with academia and industry, CNSCE2014 provides attendees not only the free exchange of ideas and challenges faced by these two key stakeholders and encourage future collaboration between members of these groups but also a good opportunity to make friends with scholars around the word. As the first session of the international conference on

CNSCE, it covers topics related to Computer, Network Security and Communication Engineering. CNSCE2014 has attracted many scholars, researchers and practitioners in these fields from various countries. They take this chance to get together, sharing their latest research achievements with each other. It has also achieved great success by its unique characteristics and strong academic atmosphere as well as its authority.

Standard Handbook for Electrical Engineers, Seventeenth Edition

In the era of Internet of Things (IoT), and with the explosive worldwide growth of electronic data volume and the associated needs of processing, analyzing, and storing this data, several new challenges have emerged. Particularly, there is a need for novel schemes of secure authentication, integrity protection, encryption, and non-repudiation to protect the privacy of sensitive data and to secure systems. Lightweight symmetric key cryptography and adaptive network security algorithms are in demand for mitigating these challenges. This book presents state-of-the-art research in the fields of cryptography and security in computing and communications. It covers a wide range of topics such as machine learning, intrusion detection, steganography, multi-factor authentication, and more. It is a valuable reference for researchers, engineers, practitioners, and graduate and doctoral students working in the fields of cryptography, network security, IoT, and machine learning.

Computer Networks

This book constitutes the refereed proceedings of the Third International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2005, held in St. Petersburg, Russia in September 2005. The 25 revised full papers and 12 revised short papers presented together with 5 invited papers were carefully reviewed and selected from a total of 85 submissions. The papers are organized in topical sections on mathematical models, architectures and protocols for computer network security, authentication, authorization and access control, information flow analysis, covert channels and trust management, security policy and operating system security, threat modeling, vulnerability assessment and network forensics, and intrusion detection.

Guide to Wireless Mesh Networks

Modeling and Simulation of Computer Networks and Systems

This book introduces readers to the tools needed to protect IT resources and communicate with security specialists when there is a security problem. The book covers a wide range of security topics including Cryptographic Technologies, Network Security, Security Management, Information Assurance, Security Applications, Computer Security, Hardware Security, and Biometrics and Forensics. It introduces the concepts, techniques, methods, approaches, and trends needed by security specialists to improve their security skills and capabilities. Further, it

provides a glimpse into future directions where security techniques, policies, applications, and theories are headed. The book represents a collection of carefully selected and reviewed chapters written by diverse security experts in the listed fields and edited by prominent security researchers.

Contemporary Security Studies

Computer Network Security

Biometrics for Network Security

Contemporary Security Studies is the definitive introduction to Security Studies, providing the most accessible, up-to-date guide to the subject available. Bringing together leading scholars in the field, it features an impressive breadth and depth of coverage of the different theoretical approaches to the study of security and the ever-evolving range of issues that dominate the security agenda in the 21st Century. Throughout the text, students are encouraged to question their own preconceptions and assumptions, and to use their own judgement to critically evaluate key approaches and ideas. To help them achieve this, each chapter is punctuated with helpful learning features including "key ideas", "think points" and case studies, demonstrating the real world applications and implications of the theory. In addition to covering a wide range of topical security issues--from terrorism and inter-state armed conflict to cybersecurity, health, and transnational crime--the fourth edition features a new chapter on postcolonialism and expanded coverage of critical security studies. The book is supported by an Online Resource Centre designed to help students take their learning further. For students: - Explore relevant security issues in greater depth with additional online case studies - Test your understanding of the key ideas and themes in each chapter with self-marking multiple-choice questions For registered lecturers: - Use the adaptable PowerPoint slides as the basis for lecture presentations or as hand-outs in class

Conversation and Community

This book provides the reader with the most up-to-date knowledge of blockchain in mainstream areas of security, trust, and privacy in the decentralized domain, which is timely and essential (this is due to the fact that the distributed and P2P applications is increasing day-by-day, and the attackers adopt new mechanisms to threaten the security and privacy of the users in those environments). This book also provides the technical information regarding blockchain-oriented software, applications, and tools required for the researcher and developer experts in both computing and software engineering to provide solutions and automated systems against current security, trust and privacy issues in the cyberspace. Cybersecurity, trust and privacy (CTP) are pressing needs for governments, businesses, and individuals, receiving the utmost priority for enforcement and improvement in almost any societies around the globe. Rapid advances, on the other hand, are being made in emerging blockchain technology with broadly diverse applications

that promise to better meet business and individual needs. Blockchain as a promising infrastructural technology seems to have the potential to be leveraged in different aspects of cybersecurity promoting decentralized cyberinfrastructure. Blockchain characteristics such as decentralization, verifiability and immutability may revolve current cybersecurity mechanisms for ensuring the authenticity, reliability, and integrity of data. Almost any article on the blockchain points out that the cybersecurity (and its derivatives) could be revitalized if it is supported by blockchain technology. Yet, little is known about factors related to decisions to adopt this technology, and how it can systemically be put into use to remedy current CTP's issues in the digital world. Topics of interest for this book include but not limited to: Blockchain-based authentication, authorization and accounting mechanisms Applications of blockchain technologies in digital forensic and threat hunting Blockchain-based threat intelligence and threat analytics techniques Formal specification of smart contracts Automated tools for outsmarting smart contracts Security and privacy aspects of blockchain technologies Vulnerabilities of smart contracts Blockchain for securing cyber infrastructure and internet of things networks Blockchain-based cybersecurity education systems This book provides information for security and privacy experts in all the areas of blockchain, cryptocurrency, cybersecurity, forensics, smart contracts, computer systems, computer networks, software engineering, applied artificial intelligence for computer security experts, big data analysts, and decentralized systems. Researchers, scientists and advanced level students working in computer systems, computer networks, artificial intelligence, big data will find this book useful as well.

Computer and Network Security

Blockchain Cybersecurity, Trust and Privacy

"This book reviews methodologies in computer network simulation and modeling, illustrates the benefits of simulation in computer networks design, modeling, and analysis, and identifies the main issues that face efficient and effective computer network simulation"--Provided by publisher.

Social and Human Elements of Information Security: Emerging Trends and Countermeasures

This book is a revised edition of the best selling title Implementing IT Governance (ISBN 978 90 8753 119 5).For trainers free additional material of this book is available. This can be found under the "Training Material" tab. Log in with your trainer account to access the material.In all enterprises around the world, the issues, opportunities and challenges of aligning IT more closely with the organization and effectively governing an organization s IT investments, resources, major initiatives and superior uninterrupted service is becoming a major concern of the Board and executive management. An integrated and comprehensive approach to the alignment, planning, execution and governance of IT and its resources has become critical to more effectively align, integrate, invest, measure, deploy, service and sustain the strategic and tactical direction and value proposition of IT in support of organizations.Much has been written and

documented about the individual components of IT Governance such as strategic planning, demand management, program and project management, IT service management, strategic sourcing and outsourcing, performance management, metrics, compliance and others. Much less has been written about a comprehensive and integrated approach for IT/Business Alignment, Planning, Execution and Governance. This title fills that need in the marketplace and offers readers structured and practical solutions using the best of the best practices available today. The book is divided into two parts, which cover the three critical pillars necessary to develop, execute and sustain a robust and effective IT governance environment:- Leadership, people, organization and strategy,- IT governance, its major component processes and enabling technologies.Each of the chapters also covers one or more of the following action oriented topics: - the why and what of IT: strategic planning, portfolio investment management, decision authority, etc.; - the how of IT: Program/Project Management, IT Service Management (including ITIL); Strategic Sourcing and outsourcing; performance, risk and contingency management (including COBIT, the Balanced Scorecard etc.) and leadership, team management and professional competences.

Does It Matter?

Overview and Goals Wireless communication technologies are undergoing rapid advancements. The last few years have experienced a steep growth in research in the area of wireless mesh networks (WMNs). The attractiveness of WMNs, in general, is attributed to their characteristics such as the ability to dynamically self-organize and self-con?gure, coupled with the ability to maintain mesh connectivity leading, in effect, to low set-up/installation costs, simpler maintenance tasks, and service coverage with high reliability and fault-tolerance. WMNs also support their integration with existing wireless networks such as cellular networks, WLANs, wireless-?delity (Wi-Fi), and worldwide interoperability of microwave access (WiMAX). WMNs have found u- ful applications in a broad range of domains such as broadband home networking, commercial/business networking, and community networking – particularly attr- tive in offering broadband wireless access with low initial installation and set-up costs. Even though WMNs have emerged to be attractive and they hold great promises for our future, there are several challenges that need to be addressed. Some of the wellknownchallenges areattributedtoissuesrelatingtoscalability(signi?cantdrop in throughput with the increase in the number of nodes), multicasting, offering qu- ity of service guarantees, energy ef?ciency, and security. This handbook attempts to provide a comprehensive guide on fundamental key topics coupled with new ideas and results in the areas of WMNs. The book has been prepared keeping in mind that it needs to prove itself to be a valuable resource dealing with both the important core and the specialized issues in WMNs.

Case Studies in Secure Computing

Up-to-date coverage of every facet of electric power in a single volume This fully revised, industry-standard resource offers practical details on every aspect of electric power engineering. The book contains in-depth discussions from more than 100 internationally recognized experts. Generation, transmission, distribution, operation, system protection, and switchgear are thoroughly explained. Standard

Handbook for Electrical Engineers, Seventeenth Edition, features brand-new sections on measurement and instrumentation, interconnected power grids, smart grids and microgrids, wind power, solar and photovoltaic power generation, electric machines and transformers, power system analysis, operations, stability and protection, and the electricity market. Coverage includes: •Units, symbols, constants, definitions, and conversion factors •Measurement and instrumentation •Properties of materials •Interconnected power grids •AC and DC power transmission •Power distribution •Smart grids and microgrids •Wind power generation •Solar power generation and energy storage •Substations and switch gear •Power transformers, generators, motors, and drives •Power electronics •Power system analysis, operations, stability, and protection •Electricity markets •Power quality and reliability •Lightning and overvoltage protection •Computer applications in the electric power industry •Standards in electrotechnology, telecommunications, and IT

Computer and Information Security Handbook

Future communication networks aim to build an intelligent and efficient living environment by connecting a variety of heterogeneous networks to fulfill complicated tasks. These communication networks bring significant challenges in building secure and reliable communication networks to address the numerous threat and privacy concerns. New research technologies are essential to preserve privacy, prevent attacks, and achieve the requisite reliability. Security, Privacy and Reliability in Computer Communications and Networks studies and presents recent advances reflecting the state-of-the-art research achievements in novel cryptographic algorithm design, intrusion detection, privacy preserving techniques and reliable routing protocols. Technical topics discussed in the book include: Vulnerabilities and Intrusion DetectionCryptographic Algorithms and EvaluationPrivacy Reliable Routing Protocols This book is ideal for personnel in computer communication and networking industries as well as academic staff and collegial, master, Ph.D. students in computer science, computer engineering, cyber security, information insurance and telecommunication systems.

Bluetooth Security Attacks

Setting the stage - Private efficiencies and public vulnerabilities - Is there a threat? - Literature review of conceptual framework - The vulnerability of networks and the resurrection of distance - Packets and power: the interdependency of infrastructure - Allocating scarce resources for network protection - Diversity as defense.

Information Security Management Systems

This guide empowers network and system administrators to defend their information and computing assets--whether or not they have security experience. Skoudis presents comprehensive, insider's explanations of today's most destructive hacker tools and tactics, and specific, proven countermeasures for both UNIX and Windows environments.

The 2020 International Conference on Machine Learning and

Big Data Analytics for IoT Security and Privacy

Modeling and Simulation of Computer Networks and Systems: Methodologies and Applications introduces you to a broad array of modeling and simulation issues related to computer networks and systems. It focuses on the theories, tools, applications and uses of modeling and simulation in order to effectively optimize networks. It describes methodologies for modeling and simulation of new generations of wireless and mobiles networks and cloud and grid computing systems. Drawing upon years of practical experience and using numerous examples and illustrative applications recognized experts in both academia and industry, discuss: Important and emerging topics in computer networks and systems including but not limited to; modeling, simulation, analysis and security of wireless and mobiles networks especially as they relate to next generation wireless networks Methodologies, strategies and tools, and strategies needed to build computer networks and systems modeling and simulation from the bottom up Different network performance metrics including, mobility, congestion, quality of service, security and more Modeling and Simulation of Computer Networks and Systems is a must have resource for network architects, engineers and researchers who want to gain insight into optimizing network performance through the use of modeling and simulation. Discusses important and emerging topics in computer networks and Systems including but not limited to; modeling, simulation, analysis and security of wireless and mobiles networks especially as they relate to next generation wireless networks Provides the necessary methodologies, strategies and tools needed to build computer networks and systems modeling and simulation from the bottom up Includes comprehensive review and evaluation of simulation tools and methodologies and different network performance metrics including mobility, congestion, quality of service, security and more

Information Science Abstracts

The latest inventions in internet technology influence most of business and daily activities. Internet security, internet data management, web search, data grids, cloud computing, and web-based applications play vital roles, especially in business and industry, as more transactions go online and mobile. Issues related to ubiquitous computing are becoming critical. Internet technology and data engineering should reinforce efficiency and effectiveness of business processes. These technologies should help people make better and more accurate decisions by presenting necessary information and possible consequences for the decisions. Intelligent information systems should help us better understand and manage information with ubiquitous data repository and cloud computing. This book is a compilation of some recent research findings in Internet Technology and Data Engineering. This book provides state-of-the-art accounts in computational algorithms/tools, database management and database technologies, intelligent information systems, data engineering applications, internet security, internet data management, web search, data grids, cloud computing, web-based application, and other related topics.

Securing the Internet of Things

Bluetooth technology has enjoyed tremendous success, and it's now employed in billions of devices for short-range wireless data and real-time audio or video transfer. In this book the authors provide an overview of Bluetooth security. They examine network vulnerabilities and provide a literature-review comparative analysis of recent security attacks. They analyze and explain related countermeasures, including one based on secure simple pairing, and they also propose a novel attack that works against all existing Bluetooth versions. They conclude with a discussion on future research directions. The book is appropriate for practitioners and researchers in information security, in particular those engaged in the design of networked and mobile devices.

Quality, Reliability, Security and Robustness in Heterogeneous Networks

Research Methods for Cyber Security teaches scientific methods for generating impactful knowledge, validating theories, and adding critical rigor to the cyber security field. This book shows how to develop a research plan, beginning by starting research with a question, then offers an introduction to the broad range of useful research methods for cyber security research: observational, mathematical, experimental, and applied. Each research method chapter concludes with recommended outlines and suggested templates for submission to peer reviewed venues. This book concludes with information on cross-cutting issues within cyber security research. Cyber security research contends with numerous unique issues, such as an extremely fast environment evolution, adversarial behavior, and the merging of natural and social science phenomena. Research Methods for Cyber Security addresses these concerns and much more by teaching readers not only the process of science in the context of cyber security research, but providing assistance in execution of research as well. Presents research methods from a cyber security science perspective Catalyzes the rigorous research necessary to propel the cyber security field forward Provides a guided method selection for the type of research being conducted, presented in the context of real-world usage

Simulation in Computer Network Design and Modeling: Use and Analysis

Future technology information technology stands for all of continuously evolving and converging information technologies, including digital convergence, multimedia convergence, intelligent applications, embedded systems, mobile and wireless communications, bio-inspired computing, grid and cloud computing, semantic web, user experience and HCI, security and trust computing and so on, for satisfying our ever-changing needs. In past twenty five years or so, Information Technology (IT) influenced and changed every aspect of our lives and our cultures. These proceedings foster the dissemination of state-of-the-art research in all future IT areas, including their models, services, and novel applications associated with their utilization.