International Journal Of Security And Networks

Adopting the Tune of Phrase: An Mental Symphony within **International Journal Of Security And Networks**

In some sort of used by monitors and the ceaseless chatter of immediate interaction, the melodic splendor and mental symphony created by the written word often disappear in to the back ground, eclipsed by the relentless sound and disturbances that permeate our lives. However, located within the pages of **International Journal Of Security And Networks** a wonderful literary prize overflowing with organic thoughts, lies an immersive symphony waiting to be embraced. Constructed by a wonderful musician of language, this fascinating masterpiece conducts visitors on an emotional journey, well unraveling the concealed melodies and profound affect resonating within each carefully crafted phrase. Within the depths with this moving examination, we shall explore the book is central harmonies, analyze their enthralling publishing fashion, and surrender ourselves to the profound resonance that echoes in the depths of readers souls.

Online Social Networks Security Brij B. Gupta 2021-02-26 In recent years, virtual meeting technology has become a part of the everyday lives of more and more people, often with the help of global online social networks (OSNs). These help users to build both social and professional links on a worldwide scale. The sharing of information and opinions are important features of OSNs. Users can describe recent activities and interests, share photos, videos, applications, and much more. The use of OSNs has increased at a rapid rate. Google+, Facebook, Twitter, LinkedIn, Sina Weibo, VKontakte, and Mixi are all OSNs that have become the preferred way of communication for a vast number of daily active users. Users spend substantial amounts of time updating their information, communicating with other users, and browsing one another’s accounts. OSNs obliterate geographical distance and can breach economic barrier. This popularity has made OSNs a fascinating test bed for cyberattacks comprising Cross-Site Scripting, SQL injection, DDoS, phishing, spamming, fake profile, spammer, etc. OSNs security: Principles, Algorithm, Applications, and Perspectives describe various attacks, classifying them, explaining their consequences, and offering. It also highlights some key contributions related to the current defensive approaches. Moreover, it shows how machine-learning and deep-learning methods can mitigate attacks on OSNs. Different technological solutions that have been proposed are also discussed. The topics, methodologies, and outcomes included in this book will help readers learn the importance of incentives in any technical solution to handle attacks against OSNs. The best practices and guidelines will show how to implement various attack-mitigation methodologies.

Quality, Reliability, Security and Robustness in Heterogeneous Networks Xi Zhang 2012-04-23 This book constitutes the thoroughly refereed post-conference proceedings of the 7th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, QShine 2010. The 37 revised full papers presented along with 7 papers from the allocated Dedicated Short Range Communications Workshop, DSRC 2010, were carefully selected from numerous submissions. Conference papers are organized into 9 technical sessions, covering the topics of cognitive radio networks, security, resource allocation, wireless protocols and algorithms, advanced networking systems, sensor networks, scheduling and optimization, routing

protocols, multimedia and stream processing. Workshop papers are organized into two sessions: DSRC networks and DSRC security.

Handbook Of Security And Networks Xiao Yang 2011-04-14 This valuable handbook is a comprehensive compilation of state-of-art advances on security in computer networks. More than 40 internationally recognized authorities in the field of security and networks contribute articles in their areas of expertise. These international researchers and practitioners are from highly-respected universities, renowned research institutions and IT companies from all over the world. Each self-contained chapter covers one essential research topic on security in computer networks. Through the efforts of all the authors, all chapters are written in a uniformed style; each containing a comprehensive overview, the latest pioneering work and future research direction of a research topic.

Embedded and Multimedia Computing Technology and Service James J. (Jong Hyuk) Park 2012-08-31 The 7th International Conference on Embedded and Multimedia Computing (EMC-12), will be held in Gwangju, Korea on September 6 - 8, 2012. EMC-12 will be the most comprehensive conference focused on the various aspects of advances in Embedded and Multimedia (EM) Computing. EMC-12 will provide an opportunity for academic and industry professionals to discuss the latest issues and progress in the area of EM. In addition, the conference will publish high quality papers which are closely related to the various theories and practical applications in EM. Furthermore, we expect that the conference and its publications will be a trigger for further related research and technology improvements in this important subject. The EMC-12 is the next event, in a series of highly successful International Conference on Embedded and Multimedia Computing, previously held as EMC 2011 (China, Aug. 2011), EMC 2010 (Philippines, Aug. 2010), EM-Com 2009 (Korea, Dec. 2009), UMC-08 (Australia, Oct. 2008), ESO-08(China, Dec. 2008), UMS-08 (Korea, April, 2008), UMS-07(Singapore, Jan. 2007), ESO-07(Taiwan, Dec. 2007), ESO-06(Korea, Aug. 2006).

Security of Self-Organizing Networks Al-Sakib Khan Pathan 2016-04-19 Reflecting recent advancements, Security of Self-Organizing Networks: MANET, WSN, WMN, VANET explores wireless network security from all angles. It begins with a review of fundamental security topics and often-used terms to set the foundation for the following chapters. Examining critical security issues in a range of wireless networks, the book proposes specific solutions to security threats. Ideal for those with a basic understanding of network security, the text provides a clear examination of the key aspects of security in self-organizing networks and other networks that use wireless technology for communications. The book is organized into four sections for ease of reference: General Topics—Security of Wireless and Self-Organizing Networks Mobile Ad-Hoc Network and Vehicular Ad-Hoc Network Security Wireless Sensor Network Security Wireless Mesh Network Security Highlighting potential threats to network security, most chapters are written in a tutorial manner. However, some of the chapters include mathematical equations and detailed analysis for advanced readers. Guiding you through the latest trends, issues, and advances in network security, the text includes questions and sample answers in each chapter to reinforce understanding.

Security and Privacy Issues in Internet of Medical Things Rajkumar Buyya 2023-02-24 Security and Privacy Issues in Internet of Medical Things addresses the security challenges faced by healthcare providers and patients. As IoMT devices are vulnerable to cyberattacks, and a security breach through IoMT devices may act as a pathway for hackers to enter hospital networks, the book covers a very timely topic. The incorporation of blockchain in the healthcare environment has given birth to the Internet of Medical Things (IoMT), which consists of a collection of healthcare systems that espouse groundbreaking technologies. Systems consist of inter-linked sensors, wearable technology devices and clinical frameworks that perform explicit, secure machine-to-machine and cloud platform communications. The significance of IoMT in the field of healthcare is undoubtedly a win-win

situation for patients through technology enhancements and a collection of analytics that helps in better diagnosis and treatment. Due to higher accuracy levels, IoMT devices are more reliable in reporting and data tracking and help avoid human errors and incorrect reporting. Provides methods for constructing novel IoMT architectures and middleware services for healthcare applications to protect and secure patient data and privacy Presents readers with information security and privacy models for IoMT, including Artificial Intelligence and Deep Learning, Data Storage security, Cloud, Fog and Edge computing security, and Wireless sensor device security Provides readers with case studies for real-world applications of IoMT security, including risk assessment for IoMT, Ethical issues in IoMT, Security assessment frameworks, and Threat-based security analysis for IoMT *Security and Organization Within IoT and Smart Cities* Kayhan Zrar Ghafoor 2021 This book aims to provide the latest research developments and results in the domain of AI techniques for smart cyber ecosystems. It presents a holistic insight into AI-enabled theoretic approaches and methodology in IoT networking, security analytics using AI tools and network automation, which ultimately enable intelligent cyber space. This book will be a valuable resource for students, researchers, engineers and policy makers working in various areas related to cybersecurity and privacy for Smart Cities. This book includes chapters titled "An Overview of the Artificial Intelligence Evolution and Its Fundamental Concepts, and Their Relationship with IoT Security", "Smart City: Evolution and Fundamental Concepts", "Advances in AI-Based Security for Internet of Things in Wireless Virtualization Environment", "A Conceptual Model for Optimal Resource Sharing of Networked Microgrids Focusing Uncertainty: Paving Path to Eco-friendly Smart Cities", "A Novel Framework for a Cyber Secure Smart City", "Contemplating Security Challenges and Threats for Smart Cities", "Self-Monitoring Obfuscated IoT Network", "Introduction to Side Channel Attacks and Investigation of Power Analysis and Fault Injection Attack Techniques", "Collaborative Digital Forensic Investigations Model for Law Enforcement: Oman as a Case Study", "Understanding Security Requirements and Challenges in the Industrial Internet of Things: A Review", "5G Security and the Internet of Things", "The Problem of Deepfake Videos and How to Counteract Them in Smart Cities", "The Rise of Ransomware Aided by Vulnerable IoT Devices", "Security Issues in Self-Driving Cars within Smart Cities", and "Trust-Aware Crowd Associated Network-Based Approach for Optimal Waste Management in Smart Cities". This book provides state-of-the-art research results and discusses current issues, challenges, solutions and recent trends related to security and organization within IoT and Smart Cities. We expect this book to be of significant importance not only to researchers and practitioners in academia, government agencies and industries, but also for policy makers and system managers. We anticipate this book to be a valuable resource for all those working in this new and exciting area, and a "must have" for all university libraries.

Security and Privacy Management, Techniques, and Protocols Maleh, Yassine 2018-04-06 The security of information and communication technology is a high priority for any organization. By examining the current problems and challenges this domain is facing, more efficient strategies can be established to safeguard personal information against invasive pressures. Security and Privacy Management, Techniques, and Protocols is a critical scholarly resource that examines emerging protocols and methods for effective management of information security at organizations. Featuring coverage on a broad range of topics such as cryptography, secure routing protocols, and wireless security, this book is geared towards academicians, engineers, IT specialists, researchers, and students seeking current research on security and privacy management.

Cyber-Assurance for the Internet of Things Tyson T. Brooks 2017-01-04 Presents an Cyber-Assurance approach to the Internet of Things (IoT) This book discusses the cyber-assurance needs of the IoT environment, highlighting key information assurance (IA) IoT issues and identifying the

associated security implications. Through contributions from cyber-assurance, IA, information security and IoT industry practitioners and experts, the text covers fundamental and advanced concepts necessary to grasp current IA issues, challenges, and solutions for the IoT. The future trends in IoT infrastructures, architectures and applications are also examined. Other topics discussed include the IA protection of IoT systems and information being stored, processed or transmitted from unauthorized access or modification of machine-2-machine (M2M) devices, radio-frequency identification (RFID) networks, wireless sensor networks, smart grids, and supervisory control and data acquisition (SCADA) systems. The book also discusses IA measures necessary to detect, protect, and defend IoT information and networks/systems to ensure their availability, integrity, authentication, confidentially, and non-repudiation. Discusses current research and emerging trends in IA theory, applications, architecture and information security in the IoT based on theoretical aspects and studies of practical applications Aids readers in understanding how to design and build cyber-assurance into the IoT Exposes engineers and designers to new strategies and emerging standards, and promotes active development of cyber-assurance Covers challenging issues as well as potential solutions, encouraging discussion and debate amongst those in the field Cyber-Assurance for the Internet of Things is written for researchers and professionals working in the field of wireless technologies, information security architecture, and security system design. This book will also serve as a reference for professors and students involved in IA and IoT networking. Tyson T. Brooks is an Adjunct Professor in the School of Information Studies at Syracuse University; he also works with the Center for Information and Systems Assurance and Trust (CISAT) at Syracuse University, and is an information security technologist and science-practitioner. Dr. Brooks is the founder/Editor-in-Chief of the International Journal of Internet of Things and Cyber-Assurance, an associate editor for the Journal of Enterprise Architecture, the International Journal of Cloud Computing and Services Science, and the International Journal of Information and Network Security.

Privacy Solutions and Security Frameworks in Information Protection Nemati, Hamid 2012-09-30 While information technology continues to play a vital role in every aspect of our lives, there is a greater need for the security and protection of this information. Ensuring the trustworthiness and integrity is important in order for data to be used appropriately. Privacy Solutions and Security Frameworks in Information Protection explores the areas of concern in guaranteeing the security and privacy of data and related technologies. This reference source includes a range of topics in information security and privacy provided for a diverse readership ranging from academic and professional researchers to industry practitioners.

Cybersecurity and Privacy in Cyber Physical Systems Yassine Maleh 2019 Cybersecurity and Privacy in Cyber-Physical Systems collects and reports on recent high-quality research that addresses different problems related to cybersecurity and privacy in cyber-physical systems (CPSs). It Presents high-quality contributions addressing related theoretical and practical aspects Improves the reader's awareness of cybersecurity and privacy in CPSs Analyzes and presents the state of the art of CPSs, cybersecurity, and related technologies and methodologies Highlights and discusses recent developments and emerging trends in cybersecurity and privacy in CPSs Proposes new models, practical solutions, and technological advances related to cybersecurity and privacy in CPSs Discusses new cybersecurity and privacy models, prototypes, and protocols for CPSs This comprehensive book promotes high-quality research by bringing together researchers and experts in CPS security and privacy from around the world to share their knowledge of the different aspects of CPS security. Cybersecurity and Privacy in Cyber-Physical Systems is ideally suited for policymakers, industrial engineers, researchers, academics, and professionals seeking a thorough understanding of the principles of cybersecurity and privacy in CPSs. They will learn about promising solutions to these research problems and identify unresolved and challenging

problems for their own research. Readers will also have an overview of CPS cybersecurity and privacy design. P> Discusses new cybersecurity and privacy models, prototypes, and protocols for CPSs This comprehensive book promotes high-quality research by bringing together researchers and experts in CPS security and privacy from around the world to share their knowledge of the different aspects of CPS security. Cybersecurity and Privacy in Cyber-Physical Systems is ideally suited for policymakers, industrial engineers, researchers, academics, and professionals seeking a thorough understanding of the principles of cybersecurity and privacy in CPSs. They will learn about promising solutions to these research problems and identify unresolved and challenging problems for their own research. Readers will also have an overview of CPS cybersecurity and privacy design.

Security and Trust in Online Social Networks Barbara Carminati 2013-12-01 The enormous success and diffusion that online social networks (OSNs) are encountering nowadays is vastly apparent. Users' social interactions now occur using online social media as communication channels; personal information and activities are easily exchanged both for recreational and business purposes in order to obtain social or economic advantages. In this scenario, OSNs are considered critical applications with respect to the security of users and their resources, for their characteristics alone: the large amount of personal information they manage, big economic upturn connected to their commercial use, strict interconnection among users and resources characterizing them, as well as user attitude to easily share private data and activities with strangers. In this book, we discuss three main research topics connected to security in online social networks: (i) trust management, because trust can be intended as a measure of the perception of security (in terms of risks/benefits) that users in an OSN have with respect to other (unknown/little-known) parties; (ii) controlled information sharing, because in OSNs, where personal information is not only connected to user profiles, but spans across users' social activities and interactions, users must be provided with the possibility to directly control information flows; and (iii) identity management, because OSNs are subjected more and more to malicious attacks that, with respect to traditional ones, have the advantage of being more effective by leveraging the social network as a new medium for reaching victims. For each of these research topics, in this book we provide both theoretical concepts as well as an overview of the main solutions that commercial/non-commercial actors have proposed over the years. We also discuss some of the most promising research directions in these fields.

Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security Gupta, Brij 2016-05-16 Internet usage has become a facet of everyday life, especially as more technological advances have made it easier to connect to the web from virtually anywhere in the developed world. However, with this increased usage comes heightened threats to security within digital environments. The Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security identifies emergent research and techniques being utilized in the field of cryptology and cyber threat prevention. Featuring theoretical perspectives, best practices, and future research directions, this handbook of research is a vital resource for professionals, researchers, faculty members, scientists, graduate students, scholars, and software developers interested in threat identification and prevention.

Handbook of Computer Networks and Cyber Security Brij B. Gupta 2019-12-31 This handbook introduces the basic principles and fundamentals of cyber security towards establishing an understanding of how to protect computers from hackers and adversaries. The highly informative subject matter of this handbook, includes various concepts, models, and terminologies along with examples and illustrations to demonstrate substantial technical details of the field. It motivates the readers to exercise better protection and defense mechanisms to deal with attackers and mitigate the situation. This handbook also outlines some of the exciting areas of future research where the existing approaches can be implemented. Exponential increase in the use of computers as a means of storing and

retrieving security-intensive information, requires placement of adequate security measures to safeguard the entire computing and communication scenario. With the advent of Internet and its underlying technologies, information security aspects are becoming a prime concern towards protecting the networks and the cyber ecosystem from variety of threats, which is illustrated in this handbook. This handbook primarily targets professionals in security, privacy and trust to use and improve the reliability of businesses in a distributed manner, as well as computer scientists and software developers, who are seeking to carry out research and develop software in information and cyber security. Researchers and advanced-level students in computer science will also benefit from this reference.

Security in Wireless Ad Hoc and Sensor Networks Erdal Cayirci 2008-12-30 This book provides an in-depth guide to security in wireless ad hoc and sensor networks Security in Wireless Ad Hoc and Sensor Networks introduces the reader to the fundamentals and key issues related to wireless ad hoc networking, with an emphasis on security. It discusses the security attacks and counter measures in wireless ad hoc, sensor and mesh networks, and briefly presents the standards on related topics. The authors offer a clear exposition of various challenges and solutions in this field including bootstrapping, key distribution and exchange, authentication issues, privacy, anonymity and tamper resilience. Key Features: Introduces the fundamentals and key issues of the new technologies followed by comprehensive presentation on security attacks and counter measures Covers Denial of Service (DoS) attacks, hardware aspects of secure wireless ad hoc and sensor networks and secure routing Contains information on cryptographic primitives and electronic warfare Includes problems at the end of each chapter to enhance learning. This book is well suited for graduate students in computer, electrical and communications engineering and computer science departments, researchers in academia and industry, as well as C4I engineers and officers in the military. Wireless network designers for internet service providers and mobile communications operators will also find this book very useful.

Handbook of Research on Network Forensics and Analysis Techniques Shrivastava, Gulshan 2018-04-06 With the rapid advancement in technology, myriad new threats have emerged in online environments. The broad spectrum of these digital risks requires new and innovative methods for protection against cybercrimes. The Handbook of Research on Network Forensics and Analysis Techniques is a current research publication that examines the advancements and growth of forensic research from a relatively obscure tradecraft to an important part of many investigations. Featuring coverage on a broad range of topics including cryptocurrency, hand-based biometrics, and cyberterrorism, this publication is geared toward professionals, computer forensics practitioners, engineers, researchers, and academics seeking relevant research on the development of forensic tools.

IoT Souvik Pal 2020-06-03 IOT: Security and Privacy Paradigm covers the evolution of security and privacy issues in the Internet of Things (IoT). It focuses on bringing all security and privacy related technologies into one source, so that students, researchers, and practitioners can refer to this book for easy understanding of IoT security and privacy issues. This edited book uses Security Engineering and Privacy-by-Design principles to design a secure IoT ecosystem and to implement cyber-security solutions. This book takes the readers on a journey that begins with understanding the security issues in IoT-enabled technologies and how it can be applied in various aspects. It walks readers through engaging with security challenges and builds a safe infrastructure for IoT devices. The book helps readers gain an understand of security architecture through IoT and describes the state of the art of IoT countermeasures. It also differentiates security threats in IoT-enabled infrastructure from traditional ad hoc or infrastructural networks, and provides a comprehensive discussion on the security challenges and solutions in RFID, WSNs, in IoT. This book aims to provide the concepts of related technologies and novel findings of the researchers

through its chapter organization. The primary audience includes specialists, researchers, graduate students, designers, experts and engineers who are focused on research and security related issues. Souvik Pal, PhD, has worked as Assistant Professor in Nalanda Institute of Technology, Bhubaneswar, and JIS College of Engineering, Kolkata (NAAC "A" Accredited College). He is the organizing Chair and Plenary Speaker of RICE Conference in Vietnam; and organizing co-convener of ICICIT, Tunisia. He has served in many conferences as chair, keynote speaker, and he also chaired international conference sessions and presented session talks internationally. His research area includes Cloud Computing, Big Data, Wireless Sensor Network (WSN), Internet of Things, and Data Analytics. Vicente García-Díaz, PhD, is an Associate Professor in the Department of Computer Science at the University of Oviedo (Languages and Computer Systems area). He is also the editor of several special issues in prestigious journals such as Scientific Programming and International Journal of Interactive Multimedia and Artificial Intelligence. His research interests include eLearning, machine learning and the use of domain specific languages in different areas. Dac-Nhuong Le, PhD, is Deputy-Head of Faculty of Information Technology, and Vice-Director of Information Technology Apply and Foreign Language Training Center, Haiphong University, Vietnam. His area of research includes: evaluation computing and approximate algorithms, network communication, security and vulnerability, network performance analysis and simulation, cloud computing, IoT and image processing in biomedical. Presently, he is serving on the editorial board of several international journals and has authored nine computer science books published by Springer, Wiley, CRC Press, Lambert Publication, and Scholar Press.

Security Solutions and Applied Cryptography in Smart Grid Communications Ferrag, Mohamed Amine 2016-11-29 Electrical energy usage is increasing every year due to population growth and new forms of consumption. As such, it is increasingly imperative to research methods of energy control and safe use. Security Solutions and Applied Cryptography in Smart Grid Communications is a pivotal reference source for the latest research on the development of smart grid technology and best practices of utilization. Featuring extensive coverage across a range of relevant perspectives and topics, such as threat detection, authentication, and intrusion detection, this book is ideally designed for academicians, researchers, engineers and students seeking current research on ways in which to implement smart grid platforms all over the globe.

Security and Resilience in Intelligent Data-Centric Systems and Communication Networks Massimo Ficco 2017-09-29 Security and Resilience in Intelligent Data-Centric Systems and Communication Networks presents current, state-of-the-art work on novel research in theoretical and practical resilience and security aspects of intelligent data-centric critical systems and networks. The book analyzes concepts and technologies that are successfully used in the implementation of intelligent data-centric critical systems and communication networks, also touching on future developments. In addition, readers will find in-demand information for domain experts and developers who want to understand and realize the aspects (opportunities and challenges) of using emerging technologies for designing and developing more secure and resilient intelligent data-centric critical systems and communication networks. Topics covered include airports, seaports, rail transport systems, plants for the provision of water and energy, and business transactional systems. The book is well suited for researchers and PhD interested in the use of security and resilient computing technologies. Includes tools and techniques to prevent and avoid both accidental and malicious behaviors Explains the state-of-the-art technological solutions for main issues hindering the development of monitoring and reaction solutions Describes new methods and technologies, advanced prototypes, systems, tools and techniques of future direction

Next Generation Wireless Network Security and Privacy Lakhtaria, Kamaljit I. 2015-10-13 As information resources migrate to the Cloud and to local and global networks, protecting sensitive

data becomes ever more important. In the modern, globally-interconnected world, security and privacy are ubiquitous concerns. Next Generation Wireless Network Security and Privacy addresses real-world problems affecting the security of information communications in modern networks. With a focus on recent developments and solutions, as well as common weaknesses and threats, this book benefits academicians, advanced-level students, researchers, computer scientists, and software development specialists. This cutting-edge reference work features chapters on topics including UMTS security, procedural and architectural solutions, common security issues, and modern cryptographic algorithms, among others.

Security and Privacy in Smart Grids Yang Xiao 2013-07-22 Presenting the work of prominent researchers working on smart grids and related fields around the world, Security and Privacy in Smart Grids identifies state-of-the-art approaches and novel technologies for smart grid communication and security. It investigates the fundamental aspects and applications of smart grid security and privacy and reports on the latest advances in the range of related areas—making it an ideal reference for students, researchers, and engineers in these fields. The book explains grid security development and deployment and introduces novel approaches for securing today's smart grids. Supplying an overview of recommendations for a technical smart grid infrastructure, the book describes how to minimize power consumption and utility expenditure in data centers. It also: Details the challenges of cybersecurity for smart grid communication infrastructures Covers the regulations and standards relevant to smart grid security Explains how to conduct vulnerability assessments for substation automation systems Considers smart grid automation, SCADA system security, and smart grid security in the last mile The book's chapters work together to provide you with a framework for implementing effective security through this growing system. Numerous figures, illustrations, graphs, and charts are included to aid in comprehension. With coverage that includes direct attacks, smart meters, and attacks via networks, this versatile reference presents actionable suggestions you can put to use immediately to prevent such attacks.

Special Issue on the Third IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS-07) George O. M. Yee 2008

Security and Privacy in Smart Sensor Networks Maleh, Yassine 2018-05-09 Security and privacy protection within computer networks can be a challenge. By examining the current problems and challenges this domain is facing, more efficient strategies can be established to safeguard personal information against invasive pressures. Security and Privacy in Smart Sensor Networks is a critical scholarly resource that examines recent developments and emerging trends in smart sensor security and privacy by providing new models, practical solutions, and technological advances related to security. Featuring coverage on a broad range of topics such as cloud security, encryption, and intrusion detection systems, this book is geared towards academicians, engineers, IT specialists, researchers, and students seeking current research on authentication and intrusion detection.

Wireless Networks and Security Shafiullah Khan 2013-01-26 "Wireless Networks and Security" provides a broad coverage of wireless security issues including cryptographic coprocessors, encryption, authentication, key management, attacks and countermeasures, secure routing, secure medium access control, intrusion detection, epidemics, security performance analysis, security issues in applications. The contributions identify various vulnerabilities in the physical layer, MAC layer, network layer, transport layer, and application layer, and focus on ways of strengthening security mechanisms and services throughout the layers. This carefully edited monograph is targeting for researchers, post-graduate students in universities, academics, and industry practitioners or professionals.

An Interdisciplinary Approach to Modern Network Security Sabyasachi Pramanik 2022-05-02 An Interdisciplinary Approach to Modern Network Security presents the latest methodologies and trends in detecting and preventing network

threats. Investigating the potential of current and emerging security technologies, this publication is an all-inclusive reference source for academicians, researchers, students, professionals, practitioners, network analysts and technology specialists interested in the simulation and application of computer network protection. It presents theoretical frameworks and the latest research findings in network security technologies, while analyzing malicious threats which can compromise network integrity. It discusses the security and optimization of computer networks for use in a variety of disciplines and fields. Touching on such matters as mobile and VPN security, IP spoofing and intrusion detection, this edited collection emboldens the efforts of researchers, academics and network administrators working in both the public and private sectors. This edited compilation includes chapters covering topics such as attacks and countermeasures, mobile wireless networking, intrusion detection systems, next-generation firewalls, web security and much more.
Information and communication systems are an essential component of our society, forcing us to become dependent on these infrastructures. At the same time, these systems are undergoing a convergence and interconnection process that has its benefits, but also raises specific threats to user interests. Citizens and organizations must feel safe when using cyberspace facilities in order to benefit from its advantages. This book is interdisciplinary in the sense that it covers a wide range of topics like network security threats, attacks, tools and procedures to mitigate the effects of malware and common network attacks, network security architecture and deep learning methods of intrusion detection.
Security Solutions for Hyperconnectivity and the Internet of Things Dawson, Maurice 2016-08-30 The Internet of Things describes a world in which smart technologies enable objects with a network to communicate with each other and interface with humans effortlessly. This connected world of convenience and technology does not come without its drawbacks, as interconnectivity implies hackability. Security Solutions for Hyperconnectivity and the Internet of Things offers insights from cutting-edge research about the strategies and techniques that can be implemented to protect against cyber-attacks. Calling for revolutionary protection strategies to reassess security, this book is an essential resource for programmers, engineers, business professionals, researchers, and advanced students in relevant fields.
Managing Security Services in Heterogenous Networks R. Thandeeswaran 2020-12-31 A heterogeneous network is a network which connects computers and other devices with different operating systems, protocols, or access technologies. By definition, managing heterogenous networks is more difficult that homogenous networks. Confidentiality, integrity, availability (CIA) remain the foundation of security. This book sheds light upon security threats, defenses, and remediation on various networking and data processing domains, including wired networks, wireless networks, mobile ad-hoc networks, wireless sensor networks, and social networks through the prisms of confidentiality, integrity, availability, authentication, and access control. The book is broken into different chapters that explore central subjects and themes in the development of the heterogenous networks we see today. The chapters look at: Access control methods in cloud-enabled Internet of Things Secure routing algorithms for mobile ad-hoc networks Building security trust in mobile ad-hoc networks using soft computing methods The use and development of Blockchain technology, with a particular focus on the nonce-free hash generation in Blockchain Password authentication and keystroke biometrics Health care data analytics over Big Data Bluetooth: and its open issues for managing security services in heterogenous networks Managing Security Services in Heterogenous Networks will be a valuable resource for a whole host of undergraduate and postgraduate students studying related topics, as well as career professionals who have to effectively manage heterogenous networks in the workplace.
Security and Privacy in Smart Sensor Networks Yassine Maleh 2018-02-19 "This book explores current research on how to implement smart

sensor networks, covering a range of perspectives and relevant topics, such as threat and attacks detection, lightweight crypto and security solutions, authentication and intrusion detection"-- *Security of Networks and Services in an All-Connected World* Daphne Tuncer 2017-06-29 This book is open access under a CC BY 4.0 license. This book constitutes the refereed proceedings of the 11th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2017, held in Zurich, Switzerland, in July 2017. The 8 full papers presented together with 11 short papers were carefully reviewed and selected from 24 submissions. The papers are organized in the following topical sections: security management; management of cloud environments and services, evaluation and experimental study of rich network services; security, intrusion detection, and configuration; autonomic and self-management solutions; and methods for the protection of infrastructure.

Blockchain Technology Sonali Vyas 2022-04-13 This book is for anyone who wants to gain an understanding of Blockchain technology and its potential. The book is research-oriented and covers different verticals of Blockchain technology. It discusses the characteristics and features of Blockchain, includes techniques, challenges, and future trends, along with case studies for deeper understanding. Blockchain Technology: Exploring Opportunities, Challenges, and Applications covers the core concepts related to Blockchain technology starting from scratch. The algorithms, concepts, and application areas are discussed according to current market trends and industry needs. It presents different application areas of industry and academia and discusses the characteristics and features of this technology. It also explores the challenges and future trends and provides an understanding of new opportunities. This book is for anyone at the beginner to intermediate level that wants to learn about the core concepts related to Blockchain technology.

Deep Learning Strategies for Security Enhancement in Wireless Sensor Networks Sagayam, K. Martin 2020-06-12 Wireless sensor networks have gained significant attention industrially and academically due to their wide range of uses in various fields. Because of their vast amount of applications, wireless sensor networks are vulnerable to a variety of security attacks. The protection of wireless sensor networks remains a challenge due to their resource-constrained nature, which is why researchers have begun applying several branches of artificial intelligence to advance the security of these networks. Research is needed on the development of security practices in wireless sensor networks by using smart technologies. Deep Learning Strategies for Security Enhancement in Wireless Sensor Networks provides emerging research exploring the theoretical and practical advancements of security protocols in wireless sensor networks using artificial intelligence-based techniques. Featuring coverage on a broad range of topics such as clustering protocols, intrusion detection, and energy harvesting, this book is ideally designed for researchers, developers, IT professionals, educators, policymakers, practitioners, scientists, theorists, engineers, academicians, and students seeking current research on integrating intelligent techniques into sensor networks for more reliable security practices.

Networks and Network Analysis for Defence and Security Anthony J. Masys 2014-02-10 Networks and Network Analysis for Defence and Security discusses relevant theoretical frameworks and applications of network analysis in support of the defence and security domains. This book details real world applications of network analysis to support defence and security. Shocks to regional, national and global systems stemming from natural hazards, acts of armed violence, terrorism and serious and organized crime have significant defence and security implications. Today, nations face an uncertain and complex security landscape in which threats impact/target the physical, social, economic and cyber domains. Threats to national security, such as that against critical infrastructures not only stem from man-made acts but also from natural hazards. Katrina (2005), Fukushima (2011) and Hurricane Sandy (2012) are examples highlighting the vulnerability of critical infrastructures to

natural hazards and the crippling effect they have on the social and economic well-being of a community and a nation. With this dynamic and complex threat landscape, network analysis has emerged as a key enabler in supporting defence and security. With the advent of 'big data' and increasing processing power, network analysis can reveal insights with regards to structural and dynamic properties thereby facilitating greater understanding of complex networks, their entities, interdependencies, vulnerabilities to produce insights for creative solutions. This book will be well positioned to inform defence, security and intelligence professionals and researchers with regards to leading methodologies and approaches.

Security in IoT Social Networks Fadi Al-Turjman 2020-11-03 Security in IoT Social Networks takes a deep dive into security threats and risks, focusing on real-world social and financial effects. Mining and analyzing enormously vast networks is a vital part of exploiting Big Data. This book provides insight into the technological aspects of modeling, searching, and mining for corresponding research issues, as well as designing and analyzing models for resolving such challenges. The book will help start-ups grow, providing research directions concerning security mechanisms and protocols for social information networks. The book covers structural analysis of large social information networks, elucidating models and algorithms and their fundamental properties. Moreover, this book includes smart solutions based on artificial intelligence, machine learning, and deep learning for enhancing the performance of social information network security protocols and models. This book is a detailed reference for academicians, professionals, and young researchers. The wide range of topics provides extensive information and data for future research challenges in present-day social information networks. Provides several characteristics of social, network, and physical security associated with social information networks Presents the security mechanisms and events related to social information networks Covers emerging topics, such as network information structures like on-line social networks, heterogeneous and homogeneous information networks, and modern information networks Includes smart solutions based on artificial intelligence, machine learning, and deep learning for enhancing the performance of social information network security protocols and models

Security Issues for Wireless Sensor Networks Parag Verma 2022-04-19 Wireless sensor networks (WSNs) have attracted high interest over the last few decades in the wireless and mobile computing research community. Applications of WSNs are numerous and growing, including indoor deployment scenarios in the home and office to outdoor deployment in an adversary's territory in a tactical background. However, due to their distributed nature and deployment in remote areas, these networks are vulnerable to numerous security threats that can adversely affect their performance. This problem is more critical if the network is deployed for some mission-critical applications, such as in a tactical battlefield. Random failure of nodes is also very likely in real-life deployment scenarios. Due to resource constraints in the sensor nodes, a traditional security mechanism with high overhead of computation and communication is not feasible in WSNs. Design and implementation of secure WSNs is, therefore, a particularly challenging task. This book covers a comprehensive discussion on state-of-the-art security technologies for WSNs. It identifies various possible attacks at different layers of the communication protocol stack in a typical WSN and presents their possible countermeasures. A brief discussion on the future direction of research in WSN security is also included.

Advances in Malware and Data-Driven Network Security Gupta, Brij B. 2021-11-12 Every day approximately three-hundred thousand to four-hundred thousand new malware are registered, many of them being adware and variants of previously known malware. Anti-virus companies and researchers cannot deal with such a deluge of malware – to analyze and build patches. The only way to scale the efforts is to build algorithms to enable machines to analyze malware and classify and cluster them to such a level of granularity that it will enable humans (or

machines) to gain critical insights about them and build solutions that are specific enough to detect and thwart existing malware and generic-enough to thwart future variants. Advances in Malware and Data-Driven Network Security comprehensively covers data-driven malware security with an emphasis on using statistical, machine learning, and AI as well as the current trends in ML/statistical approaches to detecting, clustering, and classification of cyber-threats. Providing information on advances in malware and data-driven network security as well as future research directions, it is ideal for graduate students, academicians, faculty members, scientists, software developers, security analysts, computer engineers, programmers, IT specialists, and researchers who are seeking to learn and carry out research in the area of malware and data-driven network security.

Security and Privacy Issues in IoT Devices and Sensor Networks Sudhir Kumar Sharma 2020-10-15 Security and Privacy Issues in IoT Devices and Sensor Networks investigates security breach issues in IoT and sensor networks, exploring various solutions. The book follows a two-fold approach, first focusing on the fundamentals and theory surrounding sensor networks and IoT security. It then explores practical solutions that can be implemented to develop security for these elements, providing case studies to enhance understanding. Machine learning techniques are covered, as well as other security paradigms, such as cloud security and cryptocurrency technologies. The book highlights how these techniques can be applied to identify attacks and vulnerabilities, preserve privacy, and enhance data security. This in-depth reference is ideal for industry professionals dealing with WSN and IoT systems who want to enhance the security of these systems. Additionally, researchers, material developers and technology specialists dealing with the multifarious aspects of data privacy and security enhancement will benefit from the book's comprehensive information. Provides insights into the latest research trends and theory in the field of sensor networks and IoT security Presents machine learning-based solutions for data security enhancement Discusses the challenges to implement various security techniques Informs on how analytics can be used in security and privacy

Computer Network Security Joseph Migga Kizza 2005-04-07 A comprehensive survey of computer network security concepts, methods, and practices. This authoritative volume provides an optimal description of the principles and applications of computer network security in particular, and cyberspace security in general. The book is thematically divided into three segments: Part I describes the operation and security conditions surrounding computer networks; Part II builds from there and exposes readers to the prevailing security situation based on a constant security threat; and Part III - the core - presents readers with most of the best practices and solutions currently in use. It is intended as both a teaching tool and reference. This broad-ranging text/reference comprehensively surveys computer network security concepts, methods, and practices and covers network security tools, policies, and administrative goals in an integrated manner. It is an essential security resource for undergraduate or graduate study, practitioners in networks, and professionals who develop and maintain secure computer network systems.

Security in Sensor Networks Yang Xiao 2016-04-19 Sensor networks differ from traditional networks in many aspects including their limited energy, memory space, and computational capability. These differentiators create unique security vulnerabilities. Security in Sensor Networks covers all aspects of the subject, serving as an invaluable reference for researchers, educators, and practition

Handbook of Research on Intrusion Detection Systems Gupta, Brij B. 2020-02-07 Businesses in today’s world are adopting technology-enabled operating models that aim to improve growth, revenue, and identify emerging markets. However, most of these businesses are not suited to defend themselves from the cyber risks that come with these data-driven practices. To further prevent these threats, they need to have a complete understanding of modern network security solutions and the ability to manage,

address, and respond to security breaches. The Handbook of Research on Intrusion Detection Systems provides emerging research exploring the theoretical and practical aspects of prominent and effective techniques used to detect and contain breaches within the fields of data science and cybersecurity. Featuring coverage on a broad range of topics such as botnet detection, cryptography, and access control models, this book is ideally designed for security analysts, scientists, researchers, programmers, developers, IT professionals, scholars, students, administrators, and faculty members seeking research on current advancements in network security technology.

Network Security Technologies: Design and Applications Amine, Abdelmalek 2013-11-30 Recent advances in technologies have created a need for solving security problems in a systematic way. With this in mind, network security technologies have been produced in order to ensure the security of software and communication functionalities at basic, enhanced, and architectural levels. Network Security Technologies: Design and Applications presents theoretical frameworks and the latest research findings in network security technologies while analyzing malicious threats which can compromise network integrity. This book is an essential tool for researchers and professionals interested in improving their understanding of the strategic role of trust at different levels of information and knowledge society.