Online Library Global Perspectives In Information Security Legal Social And International Issues Free Download Pdf

Information Security Applications Apr 09 2022 This book constitutes the thoroughly refereed post-proceedings of the 4th International Workshop on Information Security Applications, WISA 2003, held on Jeju Island, Korea, in August 2003. The 36 revised full papers were carefully reviewed and selected from 200 submissions. The papers are organized in topical sections on network security, mobile security; intrusion detection; Internet security; secure software, hardware, and systems; e-commerce security; digital rights management; biometrics and human interfaces; public key cryptography and key management; and applied cryptography.
Management of Information Security, Loose-Leaf Version Oct 15 2022 MANAGEMENT OF INFORMATION SECURITY, Sixth Edition prepares you to become an information security management practitioner able to secure systems and networks in a world where continuously emerging threats, ever-present attacks and the success of criminals illustrate the weaknesses in current information technologies. You'll develop both the information security skills and practical experience that organizations are looking for as they strive to ensure more secure computing environments. The text focuses on key executive and

managerial aspects of information security. It also integrates coverage of CISSP and CISM throughout to effectively prepare you for certification. Reflecting the most recent developments in the field, it includes the latest information on NIST, ISO and security governance as well as emerging concerns like Ransomware, Cloud Computing and the Internet of Things.
Long-term and Dynamical Aspects of Information Security Jan 14 2020 Contains papers which deal with computer security technology that operates in rapidly changing environments and has to adapt to their shifting conditions.
Global Perspectives on Information Security Regulations: Compliance, Controls, and Assurance Nov 11 2019 Recent decades have seen a proliferation of cybersecurity guidance in the form of government regulations and standards with which organizations must comply. As society becomes more heavily dependent on cyberspace, increasing levels of security measures will need to be established and maintained to protect the confidentiality, integrity, and availability of information. Global Perspectives on Information Security Regulations: Compliance, Controls, and Assurance summarizes current cybersecurity guidance and provides a compendium of innovative and state-of-the-art compliance and assurance practices and tools. It provides a synopsis of current cybersecurity guidance that organizations should consider so that management and their auditors can regularly evaluate their extent of compliance. Covering topics such as cybersecurity laws, deepfakes, and information protection, this premier reference source is an excellent resource for cybersecurity consultants and professionals, IT specialists, business leaders and managers, government officials, faculty and administration of both K-12 and higher education, libraries, students and educators of higher education, researchers, and academicians.
Management of Information Security Jan 18 2023 Management of Information Security, Third Edition focuses on the managerial

aspects of information security and assurance. Topics covered include access control models, information security governance, and information security program assessment and metrics. Coverage on the foundational and technical components of information security is included to reinforce key concepts. This new edition includes up-to-date information on changes in the field such as revised sections on national and international laws and international standards like the ISO 27000 series. With these updates, Management of Information Security continues to offer a unique overview of information security from a management perspective while maintaining a finger on the pulse of industry changes and academic relevance. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Network Security Jan 06 2022 Network Security is a comprehensive resource written for anyone who plans or implements network security measures, including managers and practitioners. It offers a valuable dual perspective on security: how your network looks to hackers who want to get inside, and how you need to approach it on the inside to keep them at bay. You get all the hands-on technical advice you need to succeed, but also higher-level administrative guidance for developing an effective security policy. There may be no such thing as absolute security, but, as the author clearly demonstrates, there is a huge difference between the protection offered by routine reliance on third-party products and what you can achieve by actively making informed decisions. You'll learn to do just that with this book's assessments of the risks, rewards, and trade-offs related implementing security measures. Helps you see through a hacker's eyes so you can make your network more secure. Provides technical advice that can be applied in any environment, on any platform, including help with intrusion detection systems, firewalls, encryption, anti-virus software, and digital certificates. Emphasizes a wide range of administrative considerations,

including security policies, user management, and control of services and devices. Covers techniques for enhancing the physical security of your systems and network. Explains how hackers use information-gathering to find and exploit security flaws. Examines the most effective ways to prevent hackers from gaining root access to a server. Addresses Denial of Service attacks, "malware," and spoofing. Includes appendices covering the TCP/IP protocol stack, well-known ports, and reliable sources for security warnings and updates.

The Executive MBA in Information Security Feb 24 2021 According to the Brookings Institute, an organization's information and other intangible assets account for over 80 percent of its market value. As the primary sponsors and implementers of information security programs, it is essential for those in key leadership positions to possess a solid understanding of the constantly evolving fundamental concepts of information security management. Developing this knowledge and keeping it current however, requires the time and energy that busy executives like you simply don't have. Supplying a complete overview of key concepts, The Executive MBA in Information Security provides the tools needed to ensure your organization has an effective and up-to-date information security management program in place. This one-stop resource provides a ready-to use security framework you can use to develop workable programs and includes proven tips for avoiding common pitfalls—so you can get it right the first time. Allowing for quick and easy reference, this time-saving manual provides those in key leadership positions with a lucid understanding of: The difference between information security and IT security Corporate governance and how it relates to information security Steps and processes involved in hiring the right information security staff The different functional areas related to information security Roles and responsibilities of the chief information security officer (CISO) Presenting difficult concepts in a straightforward manner,

this concise guide allows you to get up to speed, quickly and easily, on what it takes to develop a rock-solid information security management program that is as flexible as it is secure.
Information Security Management Jun 18 2020 Revised edition of: Information security for managers.
The Psychology of Information Security Aug 21 2020 The Psychology of Information Security – Resolving conflicts between security compliance and human behaviour considers information security from the seemingly opposing viewpoints of security professionals and end users to find the balance between security and productivity. It provides recommendations on aligning a security programme with wider organisational objectives, successfully managing change and improving security culture.
Information Security Nov 23 2020 For an introductory course in information security covering principles and practices. This text covers the ten domains in the Information Security Common Body of Knowledge, which are Security Management Practices, Security Architecture and Models, Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP), Law, Investigations, and Ethics, Physical Security, Operations Security, Access Control Systems and Methodology, Cryptography, Telecommunications, Network, and Internet Security.
Information Security Management Principles May 10 2022 As breaches in information security continue to make headline news, it is becoming increasingly clear that technological solutions are not the only answer. The authors outline the main management principles designed to help secure data and raise awareness of the issues involved.
Information Security Oct 03 2021
Information Security Mar 28 2021 This book constitutes the refereed proceedings of the 8th International Information Security Conference, ISC 2005, held in Singapore in September 2005. The 33 revised full papers presented together with 5 student papers were carefully reviewed and selected from 271

submissions. The papers are organized in topical sections on network security, trust and privacy, key management and protocols, public key encryption and signature, signcryption, crypto algorithm and analysis, cryptography, applications, software security, authorization, and access control.
Fundamentals of Information Systems Security Dec 17 2022 Revised and updated with the latest data in the field, Fundamentals of Information Systems Security, Third Edition provides a comprehensive overview of the essential concepts readers must know as they pursue careers in information systems security. The text opens with a discussion of the new risks, threats, and vulnerabilities associated with the transition to a digital world. Part 2 presents a high level overview of the Security+ Exam and provides students with information as they move toward this certification.
Information Security and Cryptology -- ICISC 2013 Mar 08 2022 This book constitutes the thoroughly refereed post-conference proceedings of the 16th International Conference on Information Security and Cryptology, ICISC 2013, held in Seoul, Korea in November 2013. The 31 revised full papers presented together with 2 invited talks were carefully selected from 126 submissions during two rounds of reviewing. The papers provide the latest results in research, development and applications in the field of information security and cryptology. They are organized in topical sections on secure multiparty computation, proxy re-encryption, side channel analysis and its countermeasures, cryptanalysis, embedded system security and its implementation, primitives for cryptography, digital signature, security protocol, cyber security, and public key cryptography.
Applications and Techniques in Information Security Jun 11 2022 This book constitutes the refereed proceedings of the International Conference on Applications and Techniques in Information Security, ATIS 2014, held in Melbourne, Australia, in November 2014. The 16 revised full papers and 8 short papers

presented were carefully reviewed and selected from 56 submissions. The papers are organized in topical sections on applications; curbing cyber crimes; data privacy; digital forensics; security implementations.

Cybersecurity in China May 18 2020 This book offers the first benchmarking study of China's response to the problems of security in cyber space. There are several useful descriptive books on cyber security policy in China published between 2010 and 2016. As a result, we know quite well the system for managing cyber security in China, and the history of policy responses. What we don't know so well, and where this book is useful, is how capable China has become in this domain relative to the rest of the world. This book is a health check, a report card, on China's cyber security system in the face of escalating threats from criminal gangs and hostile states. The book also offers an assessment of the effectiveness of China's efforts. It lays out the major gaps and shortcomings in China's cyber security policy. It is the first book to base itself around an assessment of China's cyber industrial complex, concluding that China does not yet have one. As Xi Jinping said in July 2016, the country's core technologies are dominated by foreigners.

Handbook of Computer Networks and Cyber Security May 30 2021 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.

Engineering Information Security Feb 07 2022 Engineering Information Security covers all aspects of information security using a systematic engineering approach and focuses on the viewpoint of how to control access to information. Includes a discussion about protecting storage of private keys, SCADA, Cloud, Sensor, and Ad Hoc networks Covers internal operations security processes of monitors, review exceptions, and plan remediation Over 15 new sections Instructor resources such as lecture slides, assignments, quizzes, and a set of questions organized as a final exam If you are an instructor and adopted this book for your course, please email ieeeproposals@wiley.com to get access to the additional instructor materials for this book.

The InfoSec Handbook Sep 14 2022 The InfoSec Handbook offers the reader an organized layout of information that is easily read and understood. Allowing beginners to enter the field and understand the key concepts and ideas, while still keeping the experienced readers updated on topics and concepts. It is intended mainly for beginners to the field of information security, written in a way that makes it easy for them to understand the detailed content of the book. The book offers a practical and simple view of the security practices while still offering somewhat

technical and detailed information relating to security. It helps the reader build a strong foundation of information, allowing them to move forward from the book with a larger knowledge base. Security is a constantly growing concern that everyone must deal with. Whether it's an average computer user or a highly skilled computer user, they are always confronted with different security risks. These risks range in danger and should always be dealt with accordingly. Unfortunately, not everyone is aware of the dangers or how to prevent them and this is where most of the issues arise in information technology (IT). When computer users do not take security into account many issues can arise from that like system compromises or loss of data and information. This is an obvious issue that is present with all computer users. This book is intended to educate the average and experienced user of what kinds of different security practices and standards exist. It will also cover how to manage security software and updates in order to be as protected as possible from all of the threats that they face. What you'll learn Essentials of information security in all forms Importance of information security in present day business Establishing an ISMS through a step by step process Best practices in implementation The various domains of information security Who this book is for Beginners to experts in information security. Table of Contents 1: Introduction to Security 2: History of Computer Security 3: Key Concepts and Principles 4: Access Controls 5: Information Systems Management 6:Application and Web Security 7: Malicious Software and Anti-Virus Software 8: Cryptography 9: Understanding Networks 10: Firewalls 11: Intrusion Detection and Prevention Systems 12: Virtual Private Networks 13: Data Backups & Cloud Computing 14: Physical Security and Biometrics 15: Social Engineering 16. Current Trends in Information Security 17. Bibliography

Global Perspectives In Information Security Oct 11 2019 Global Perspectives in Information Security, compiled by

renowned expert and professor Hossein Bidgoli, offers an expansive view of current issues in information security. Written by leading academics and practitioners from around the world, this thorough resource explores and examines a wide range of issues and perspectives in this rapidly expanding field. Perfect for students, researchers, and practitioners alike, Professor Bidgoli's book offers definitive coverage of established and cutting-edge theory and application in information security.

Cyber Security and Digital Forensics Dec 05 2021 CYBER SECURITY AND DIGITAL FORENSICS Cyber security is an incredibly important issue that is constantly changing, with new methods, processes, and technologies coming online all the time. Books like this are invaluable to professionals working in this area, to stay abreast of all of these changes. Current cyber threats are getting more complicated and advanced with the rapid evolution of adversarial techniques. Networked computing and portable electronic devices have broadened the role of digital forensics beyond traditional investigations into computer crime. The overall increase in the use of computers as a way of storing and retrieving high-security information requires appropriate security measures to protect the entire computing and communication scenario worldwide. Further, with the introduction of the internet and its underlying technology, facets of information security are becoming a primary concern to protect networks and cyber infrastructures from various threats. This groundbreaking new volume, written and edited by a wide range of professionals in this area, covers broad technical and socio-economic perspectives for the utilization of information and communication technologies and the development of practical solutions in cyber security and digital forensics. Not just for the professional working in the field, but also for the student or academic on the university level, this is a must-have for any library. Audience: Practitioners, consultants, engineers, academics, and other professionals working in the areas of cyber

analysis, cyber security, homeland security, national defense, the protection of national critical infrastructures, cyber-crime, cyber vulnerabilities, cyber-attacks related to network systems, cyber threat reduction planning, and those who provide leadership in cyber security management both in public and private sectors
Insider Threats in Cyber Security Feb 19 2023 Insider Threats in Cyber Security is a cutting edge text presenting IT and non-IT facets of insider threats together. This volume brings together a critical mass of well-established worldwide researchers, and provides a unique multidisciplinary overview. Monica van Huystee, Senior Policy Advisor at MCI, Ontario, Canada comments "The book will be a must read, so of course I'll need a copy." Insider Threats in Cyber Security covers all aspects of insider threats, from motivation to mitigation. It includes how to monitor insider threats (and what to monitor for), how to mitigate insider threats, and related topics and case studies. Insider Threats in Cyber Security is intended for a professional audience composed of the military, government policy makers and banking; financing companies focusing on the Secure Cyberspace industry. This book is also suitable for advanced-level students and researchers in computer science as a secondary text or reference book.
ISACA Certified Information Security Manager (CISM) - Practice Exams Jan 26 2021 ISACA's Certified Information Security Manager (CISM) certification indicates expertise in information security governance, program development and management, incident management and risk management. It is for those with technical expertise and experience in IS/IT security and control and wants to make the move from team player to manager. CISM can add credibility and confidence to your interactions with internal and external stakeholders, peers and regulators. ISACA's CISM brings credibility to your team and ensures alignment between the organization's information security program and its broader goals and objectives. CISM can validate your team's

commitment to compliance, security and integrity and increase customer retention.

Information Security Illuminated Aug 01 2021 A comprehensive textbook that introduces students to current information security practices and prepares them for various related certifications.

Hacking Jun 30 2021

Emerging Trends in ICT Security Mar 16 2020 Information security has become a key issue. Human resources, including all people working with information technology, play a significant role in information security issues. The key factor for human resources in relation to information security is awareness about threats, challenges, and risks lurking in the information exchange environment. Improving staff awareness of information security should be one of the significant, permanent goals in an organization's information security policies. This chapter investigates information security awareness in terms of knowledge, attitude, and behavior. Research was carried out using a survey method. To evaluate the information security awareness of staff, we developed nine components. Seven independent variables—gender, education level, IT awareness, working experience, occupation, field, and job category—were also selected for developing the conceptual model. Results showed that, among the investigated variables, gender, IT awareness, occupation field, and job category had significant correlations to information security awareness.

Information Security for Global Information Infrastructures Jul 12 2022 IFIP/SEC2000, being part of the 16th IFIP World Computer Congress (WCC2000), is being held in Beijing, China from August 21 to 25, 2000. SEC2000 is the annual conference of TCll (Information Security) of the International Federation of Information Processing. The conference focuses on the seamless integration of information security services as an integral part of the Global Information Infrastructure in the new millenniUm.

SEC2000 is sponsored by the China Computer Federation (CCF), IFIP/TCll, and Engineering Research Centre for Information Security Technology, Chinese Academy of Sciences (ERCIST, CAS). There were 180 papers submitted for inclusion, 50 papers among them have been accepted as long papers and included in this proceeding, 81 papers have been accepted as short papers and published in another proceeding. All papers presented in this conference were reviewed blindly by a minimum of two international reviewers. The authors' affiliations of the 180 submissions and the accepted 131 papers range over 26 and 25 countries or regions, respectively. We would like to appreciate all who have submitted papers to IFIP/SEC2000, and the authors of accepted papers for their on-time preparation of camera-ready fmal versions. Without their contribution there would be no conference. We wish to express our gratitude to all program committee members and other reviewers for their hard work in reviewing the papers in a short time and for contributing to the conference in different ways. We would like to thank Rein Venter for his time and expertise in compiling the fmal version of the proceedings.

Principles of Computer Security, Fourth Edition Sep 21 2020 Written by leading information security educators, this fully revised, full-color computer security textbook covers CompTIA’s fastest-growing credential, CompTIA Security+. Principles of Computer Security, Fourth Edition is a student-tested, introductory computer security textbook that provides comprehensive coverage of computer and network security fundamentals in an engaging and dynamic full-color design. In addition to teaching key computer security concepts, the textbook also fully prepares you for CompTIA Security+ exam SY0-401 with 100% coverage of all exam objectives. Each chapter begins with a list of topics to be covered and features sidebar exam and tech tips, a chapter summary, and an end-of-chapter assessment section that includes key term, multiple choice, and essay quizzes

as well as lab projects. Electronic content includes CompTIA Security+ practice exam questions and a PDF copy of the book. CompTIA Approved Quality Content (CAQC) Instructor resource materials include Online Learning Center with Instructor Manuals, PowerPoint slides featuring artwork from the book, and a test bank of questions for use as quizzes or exams Electronic content features two simulated practice exams in the Total Tester exam engine and a PDF eBook Supplemented by Principles of Computer Security Lab Manual, Fourth Edition White and Conklin are two of the most well-respected computer security educators in higher education

Psychosocial Dynamics of Cyber Security Oct 23 2020 This new volume, edited by industrial and organizational psychologists, will look at the important topic of cyber security work in the US and around the world. With contributions from experts in the fields of industrial and organizational psychology, human factors, computer science, economics, and applied anthropology, the book takes the position that employees in cyber security professions must maintain attention over long periods of time, must make decisions with imperfect information with the potential to exceed their cognitive capacity, may often need to contend with stress and fatigue, and must frequently interact with others in team settings and multiteam systems. Consequently, psychosocial dynamics become a critical driver of cyber security effectiveness. Chapters in the book reflect a multilevel perspective (individuals, teams, multiteam systems) and describe cognitive, affective and behavioral inputs, processes and outcomes that operate at each level. The book chapters also include contributions from both research scientists and cyber security policy-makers/professionals to promote a strong scientist-practitioner dynamic. The intent of the book editors is to inform both theory and practice regarding the psychosocial dynamics of cyber security work.

Algoritmes aan de macht Feb 13 2020 Stel, je staat terecht. Wie

laat je liever beslissen over je lot: een foutgevoelige want menselijke rechter of een algoritme zonder enige empathie? Stel, je koopt een zelfrijdende auto. Wil je dat die zo veel mogelijk levens redt bij een botsing, of dat hij de eigen inzittenden bevoordeelt? Stel, een nieuwe machine heeft je medische gegevens nodig om kankerpatiënten te redden. Geef je je privacy op voor het algemeen belang? Algoritmes spelen een steeds grotere rol in ons leven. Op wat voor manier precies? En is het wel verstandig om belangrijke beslissingen zo klakkeloos aan ze uit te besteden? Wiskundige Hannah Fry gidst ons langs de dilemma's van ons nieuwe, geautomatiseerde bestaan.

Implementing Information Security based on ISO 27001/ISO 27002 Dec 13 2019 Information is the currency of the information age and in many cases is the most valuable asset possessed by an organisation. Information security management is the discipline that focuses on protecting and securing these assets against the threats of natural disasters, fraud and other criminal activity, user error and system failure.Effective information security can be defined as the preservation of confidentiality, integrity and availability of information. This book describes the approach taken by many organisations to realise these objectives. It discusses how information security cannot be achieved through technological means alone, but should include factors such as the organisation s approach to risk and pragmatic day-to-day business operations.This Management Guide provides an overview of the implementation of an Information Security Management System that conforms to the requirements of ISO/IEC 27001:2005 and which uses controls derived from ISO/IEC 17799:2005. It covers the following: CertificationRiskDocumentation and Project Management issuesProcess approach and the PDCA cyclePreparation for an Audit

Advanced Methodologies and Technologies in System Security, Information Privacy, and Forensics Apr 16 2020

Cyber-attacks are rapidly becoming one of the most prevalent issues globally, and as they continue to escalate, it is imperative to explore new approaches and technologies that help ensure the security of the online community. Beyond cyber-attacks, personal information is now routinely and exclusively housed in cloud-based systems. The rising use of information technologies requires stronger information security and system procedures to reduce the risk of information breaches. Advanced Methodologies and Technologies in System Security, Information Privacy, and Forensics presents emerging research and methods on preventing information breaches and further securing system networks. While highlighting the rising concerns in information privacy and system security, this book explores the cutting-edge methods combatting digital risks and cyber threats. This book is an important resource for information technology professionals, cybercrime researchers, network analysts, government agencies, business professionals, academicians, and practitioners seeking the most up-to-date information and methodologies on cybercrime, digital terrorism, network security, and information technology ethics.

Advances in Information and Computer Security Dec 25 2020 This book constitutes the refereed proceedings of the 9th International Workshop on Security, IWSEC 2014, held in Hirosaki, Japan, in August 2014. The 13 regular papers presented together with 8 short papers in this volume were carefully reviewed and selected from 55 submissions. The focus of the workshop was on the following topics: system security, threshold cryptography, hardware security, foundation, and encryption.

Computer Network Security Sep 02 2021 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.

Network Security A Beginner's Guide 3/E Nov 04 2021 Security Smarts for the Self-Guided IT Professional Defend your network against a wide range of existing and emerging threats. Written by a Certified Information Systems Security Professional with more than 20 years of experience in the field, Network Security: A Beginner's Guide, Third Edition is fully updated to include the latest and most effective security strategies. You'll learn about the four basic types of attacks, how hackers exploit them, and how to implement information security services to protect information and systems. Perimeter, monitoring, and encryption technologies are discussed in detail. The book explains how to create and deploy an effective security policy, manage and assess risk, and perform audits. Information security best practices and standards, including ISO/IEC 27002, are covered in this practical resource. Network Security: A Beginner's Guide, Third Edition features: Lingo--Common security terms defined so that you're in the know on the job IMHO--Frank and relevant opinions based on the author's years of industry experience Budget Note--Tips for getting security technologies and processes into your organization's budget In Actual Practice--Exceptions to the rules of security explained in real-world contexts Your Plan--Customizable checklists you can use on the job now Into Action--

Tips on how, why, and when to apply new skills and techniques at work

INFORMATION SECURITY Nov 16 2022 This book offers a comprehensive introduction to the fundamental aspects of Information Security (including Web, Networked World, Systems, Applications, and Communication Channels). Security is also an essential part of e-business strategy (including protecting critical infrastructures that depend on information systems) and hence information security in the enterprise (Government, Industry, Academia, and Society) and over networks has become the primary concern. The book provides the readers with a thorough understanding of how information can be protected throughout computer networks. The concepts related to the main objectives of computer and information security systems, namely confidentiality, data integrity, authentication (entity and data origin), access control, and non-repudiation have been elucidated, providing a sound foundation in the principles of cryptography and network security. The book provides a detailed treatment of design principles of classical and modern cryptosystems through an elaborate study of cryptographic techniques, algorithms, and protocols. It covers all areas of security—using Symmetric key and Public key cryptography, hash functions, authentication techniques, biometric techniques, and stegano-graphy. Besides, techniques such as Secure Socket Layer (SSL), Firewalls, IPSec for Web security and network security are addressed as well to complete the security framework of the Internet. Finally, the author demons-trates how an online voting system can be built, showcasing information security techniques, for societal benefits. Information Security: Theory and Practice is intended as a textbook for a one-semester course in Information Security/Network Security and Crypto-graphy for B.E./B.Tech students of Computer Science and Engineering and Information Technology.

Readings & Cases in Information Security: Law & Ethics

Aug 13 2022 Readings and Cases in Information Security: Law and Ethics provides a depth of content and analytical viewpoint not found in many other books. Designed for use with any Cengage Learning security text, this resource offers readers a real-life view of information security management, including the ethical and legal issues associated with various on-the-job experiences. Included are a wide selection of foundational readings and scenarios from a variety of experts to give the reader the most realistic perspective of a career in information security. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Cyber Security and Threats Apr 28 2021 Cyber security has become a topic of concern over the past decade as private industry, public administration, commerce, and communication have gained a greater online presence. As many individual and organizational activities continue to evolve in the digital sphere, new vulnerabilities arise. Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications contains a compendium of the latest academic material on new methodologies and applications in the areas of digital security and threats. Including innovative studies on cloud security, online threat protection, and cryptography, this multi-volume book is an ideal source for IT specialists, administrators, researchers, and students interested in uncovering new ways to thwart cyber breaches and protect sensitive digital information.

Information Security of Highly Critical Wireless Networks Jul 20 2020 This SpringerBrief explores features of digital protocol wireless communications systems, and features of the emerging electrical smart grid. Both low power and high power wireless systems are described. The work also examines the cybersecurity vulnerabilities, threats and current levels of risks to critical infrastructures that rely on digital wireless technologies. Specific topics include areas of application for high criticality wireless

networks (HCWN), modeling risks and vulnerabilities, governance and management frameworks, systemic mitigation, reliable operation, assessing effectiveness and efficiency, resilience testing, and accountability of HCWN. Designed for researchers and professionals, this SpringerBrief provides essential information for avoiding malevolent uses of wireless networks. The content is also valuable for advanced-level students interested in security studies or wireless networks.