Information Security Theory And Practices Smart Cards Le And Ubiquitous Computing Systems First Ifip Tc6 Wg 88 Wg 112 International Computer Science Security And Cryptology

This volume constitutes the refereed proceedings of the 5th IFIP WG 11.2 International Workshop on Information Security Theory and Practices: Security and Privacy of Mobile Devices in Wireless Communication, WISTP 2011, held in Heraklion, Crete, Greece, in June 2011. The 19 revised full papers and 8 short papers presented together with a keynote speech were carefully reviewed and selected from 80 submissions. They are organized in topical sections on mobile authentication and access control, lightweight authentication, algorithms, hardware implementation, security and cryptography, security attacks and measures, security attacks, security and trust, and mobile application security and privacy.

High-level overview of the information security field. Covers key concepts like confidentiality, integrity, and availability, then dives into practical applications of these ideas in the areas of operational, physical, network, application, and operating system security. In this high-level survey of the information security field, best-selling author Jason Andress covers the basics of a wide variety of topics, from authentication and authorization to maintaining confidentiality and performing penetration testing. Using real-world security breaches as examples, Foundations of Information Security explores common applications of these concepts, such as operations security, network design, hardening and patching operating systems, securing mobile devices, as well as tools for assessing the security of hosts and applications. You'll also learn the basics of topics like: • Multifactor authentication and how biometrics and hardware tokens can be used to harden the authentication process • The principles behind modern cryptography, including symmetric and asymmetric algorithms, hashes, and certificates • The laws and regulations that protect systems and data • Anti-malware tools, firewalls, and intrusion detection systems • Vulnerabilities such as buffer overflows and race conditions A valuable resource for beginning security professionals, network systems administrators, or anyone new to the field, Foundations of Information Security is a great place to start your journey into the dynamic and rewarding field of information security.

Information Systems (IS) are a nearly omnipresent aspect of the modern world, playing crucial roles in the fields of science and engineering, business and law, art and culture, politics and government, and many others. As such, identity theft and unauthorized access to these systems are serious concerns. Theory and Practice of Cryptography Solutions for Secure Information Systems explores current trends in IS security technologies, techniques, and concerns, primarily through the use of cryptographic tools to safeguard valuable information resources. This reference book serves the needs of professionals, academics, and students requiring dedicated information systems free from outside interference, as well as developers of secure IS applications. This book is part of the Advances in Information Security, Privacy, and Ethics series collection.

Managing Information Security offers focused coverage of how to protect mission critical systems, and how to deploy security management systems, IT security, ID management, intrusion detection and prevention systems, computer forensics, network forensics, firewalls, penetration testing, vulnerability assessment, and more. It offers in-depth coverage of the current technology and practice as it relates to information security management solutions. 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. Chapters contributed by leaders in the field covering foundational and practical aspects of information security management, allowing the reader to develop a new level of technical expertise found nowhere else Comprehensive coverage by leading experts allows the reader to put current technologies to work Presents methods of analysis and problem solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions

Introductory textbook in the important area of network security for undergraduate and graduate students Comprehensively covers fundamental concepts with newer topics such as electronic cash, bit-coin, P2P, SHA-3, E-voting, and Zigbee security Fully updated to reflect new developments in network security Introduces a chapter on Cloud security, a very popular and essential topic Uses everyday examples that most computer users experience to illustrate important principles and mechanisms Features a companion website with Powerpoint slides for lectures and solution manuals to selected exercise problems, available at http://www.cs.uml.edu/~wang/NetSec

This volume constitutes the refereed proceedings of the First IFIP TC6 / WG 8.8 / WG 11.2 International Workshop on Information Security Theory and Practices: Smart Cards, Mobile and Ubiquitous Computing Systems, WISTP 2007, held in Heraklion, Crete, Greece in May 2007. The 20 revised full papers are organized in topical sections on mobility, hardware and cryptography, privacy, cryptography schemes, smart cards, and small devices.

This volume constitutes the refereed proceedings of the 6th IFIP WG 11.2 International Workshop on Information Security Theory and Practice: Security, Privacy and Trust in Computing Systems and Ambient Intelligent Ecosystems, WISTP 2012, held in Egham, UK, in June 2012. The 9 revised full papers and 8 short papers presented together with three keynote speeches were carefully reviewed and selected from numerous submissions. They are organized in topical sections on protocols, privacy, policy and access control, multi-party computation, cryptography, and mobile security.

Organizations, worldwide, have adopted practical and applied approaches for mitigating risks and managing information security program. Considering complexities of a large-scale, distributed IT environments, security should be proactively planned for and prepared ahead, rather than as used as reactions to changes in the landscape. Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions presents high-quality research papers and practice articles on management and governance issues in the field of information security. The main focus of the book is to provide an organization with insights into practical and applied solutions, frameworks, technologies and practices on technological and organizational factors. The book aims to be a collection of knowledge for professionals, scholars, researchers and academicians working in this field that is fast evolving and growing as an area of information assurance.

This text introduces a complete and concise view of network security. It provides in-depth theoretical coverage of recent advancements and practical solutions to network security threats, including the most recent topics on wireless network security.

This volume constitutes the refereed proceedings of the 4th IFIP WG 11.2 International Workshop on Information Security Theory and Practices: Security and Privacy of Pervasive Systems and Smart Devices, WISTP 2010, held in Passau, Germany, in April 2010. The 20 revised full papers and 10 short papers were carefully reviewed and selected from 69 submissions. They are organized in topical sections on embedded security, protocols, highly constrained embedded systems, security, smart card security, algorithms, hardware implementations, embedded systems and anonymity/database security.

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.

The Growing Imperative Need for Effective Information Security Governance With monotonous regularity, headlines announce ever more spectacular failures of information security and mounting losses. The succession of corporate debacles and dramatic control failures in recent years underscores the necessity for information security to be tightly integrated into the fabric of every organization. The protection of an organization's most valuable asset information can no longer be relegated to low-level technical personnel, but must be considered an essential element of corporate governance that is critical to organizational success and survival. Written by an industry expert, Information Security Governance is the first book-length treatment of this important topic, providing readers with a step-by-step approach to developing and managing an effective information security program. Beginning with a general overview of governance, the book covers: The business case for information security Defining roles and responsibilities Developing strategic metrics Determining information security outcomes Setting security governance objectives Establishing risk management objectives Developing a cost-effective security strategy A sample strategy development The steps for implementing an effective strategy Developing meaningful security program development metrics Designing relevant information security management metrics Defining incident management and response metrics Complemented with action plans and sample policies that demonstrate to readers how to put these ideas into practice, Information Security Governance is indispensable reading for any professional who is involved in information security and assurance.

This new textbook provides students with a comprehensive and accessible introduction to the subject of security studies, with a strong emphasis on the use of case studies. In addition to presenting the major theoretical perspectives, the book examines a range of important and controversial topics in modern debates, covering both traditional military and non-military security issues, such as proliferation, humanitarian intervention, food security and environmental security. Unlike most standard textbooks, the volume also offers a wide range of case studies – including chapters on the USA, China, the Middle East, Russia, Africa, the Arctic, the Middle East, Europe and Latin America – providing detailed analyses of important global security issues. The 34 chapters contain pedagogical features such as textboxes, summary points and recommended further reading and are divided into five thematic sections: Conceptual and Theoretical Military Security Non-Military Security Institutions and Security Case Studies This textbook will be essential reading for all students of security studies and highly recommended for students of critical security studies, human security, peace and conflict studies, foreign policy and International Relations in general.

As retail businesses migrate to the digital realm, internal information theft incidents continue to threaten on-line and off-line retail operations. The evolving propagation of internal information theft has surpassed the traditional techniques of crime prevention practices. Many business organizations search for internal information theft prevention guides that fit into their retail business operation, only to be inundated with generic and theoretical models. This book examines applicable methods for retail businesses to effectively prevent internal information theft. Information Theft Prevention offers readers a comprehensive understanding of the current status of the retail sector information theft prevention models in relation to the internationally recognized benchmark of information security. It presents simple and effective management processes for ensuring better information system security, fostering a proactive approach to internal information theft prevention. Furthermore, it builds on well-defined retail business cases to identify applicable solutions for businesses today. Integrating the retail business operations and information system security practices, the book identifies ways to coordinate efforts across a business in order to achieve the best results. IT security managers and professionals, financial frauds consultants, cyber security professionals and crime prevention professionals will find this book a valuable resource for identifying and creating tools to prevent internal information theft.

This completely revised and expanded second edition of SSL and TLS: Theory and Practice provides an overview and a comprehensive discussion of the Secure Sockets Layer (SSL), Transport Layer Security (TLS), and Datagram TLS (DTLS) protocols that are omnipresent in today's e-commerce and e-business applications and respective security solutions. It provides complete details on the theory and practice of the protocols, offering readers a solid understanding of their design principles and modes of operation. Updates to this edition include coverage of the recent attacks against the protocols, newly specified extensions and firewall traversal, as well as recent developments related to public key certificates and respective infrastructures. This book targets software developers, security professionals, consultants, protocol designers, and chief security officers who will gain insight and perspective on the many details of the SSL, TLS, and DTLS protocols, such as cipher suites, certificate management, and alert messages. The book also comprehensively discusses the advantages and disadvantages of the protocols compared to other Internet security protocols and provides the details necessary to correctly implement the protocols while saving time on the security practitioner's side.

To deal with security issues effectively, knowledge of theories alone is not sufficient. Practical experience is essential. Helpful for beginners and industry practitioners, this book develops a concrete outlook, providing readers with basic concepts and an awareness of industry standards and best practices. Chapters address cryptography and network security, system-level security, and applications for network security. The book also examines application level attacks, practical software security, and securing application-specific networks. Ganguly Debashis speaks about Network and Application Security

Over the last decade, differential privacy (DP) has emerged as the de facto standard privacy notion for research in privacy-preserving data analysis and publishing. The DP notion offers strong privacy guarantee and has been applied to many data analysis tasks. This Synthesis Lecture is the first of two volumes on differential privacy. This lecture differs from the existing books and surveys on differential privacy in that we take an approach balancing theory and practice. We focus on empirical accuracy performances of algorithms rather than asymptotic accuracy guarantees. At the same time, we try to explain why these algorithms have those empirical accuracy performances. We also take a balanced approach regarding the semantic meanings of differential privacy, explaining both its strong guarantees and its limitations. We start

by inspecting the definition and basic properties of DP, and the main primitives for achieving DP. Then, we give a detailed discussion on the the semantic privacy guarantee provided by DP and the caveats when applying DP. Next, we review the state of the art mechanisms for publishing histograms for low-dimensional datasets, mechanisms for conducting machine learning tasks such as classification, regression, and clustering, and mechanisms for publishing information to answer marginal queries for high-dimensional datasets. Finally, we explain the sparse vector technique, including the many errors that have been made in the literature using it. The planned Volume 2 will cover usage of DP in other settings, including high-dimensional datasets, graph datasets, local setting, location privacy, and so on. We will also discuss various relaxations of DP.

This volume constitutes the refereed proceedings of the 10th IFIP WG 11.2 International Conference on Information Security Theory and Practices, WISTP 2016, held in Heraklion, Crete, Greece, in September 2016. The 13 revised full papers and 5 short papers presented together in this book were carefully reviewed and selected from 29 submissions. WISTP 2016 sought original submissions from academia and industry presenting novel research on all theoretical and practical aspects of security and privacy, as well as experimental studies of fielded systems, the application of security technology, the implementation of systems, and lessons learned. The papers are organized in topical sections on authentication and key management; secure hardware systems; attacks to software and network systems; and access control and data protection.

This volume constitutes the refereed proceedings of the 7th IFIP WG 11.2 International Workshop on Information Security Theory and Practices: Security and Privacy of Mobile Devices in Wireless Communication, WISTP 2013, held in Heraklion, Crete, Greece, in May 2013. The 9 revised full papers presented together with two keynote speeches were carefully reviewed and selected from 19 submissions. The scope of the workshop spans the theoretical aspects of cryptography and cryptanalysis, mobile security, smart cards and embedded devices.

This volume constitutes the refereed proceedings of the Second IFIP WG 11.2 International Workshop on Information Security Theory and Practices: Smart Devices, Convergence and Next Generation Networks, WISTP 2008, held in Seville, Spain, in May 2008. The 10 revised full papers presented were carefully reviewed and selected from numerous submissions for inclusion in the book; they examine the rapid development of information technologies and the transition to next generation networks. The papers focus on the security of these complex and resource-constrained systems and are organized in topical sections on smart devices, network security, convergence, and cryptography.

In today?s globalized world, businesses and governments rely heavily on technology for storing and protecting essential information and data. Despite the benefits that computing systems offer, there remains an assortment of issues and challenges in maintaining the integrity and confidentiality of these databases. As professionals become more dependent cyberspace, there is a need for research on modern strategies and concepts for improving the security and safety of these technologies. Modern Theories and Practices for Cyber Ethics and Security Compliance is a collection of innovative research on the concepts, models, issues, challenges, innovations, and mitigation strategies needed to improve cyber protection. While highlighting topics including database governance, cryptography, and intrusion detection, this book provides guidelines for the protection, safety, and security of business data and national infrastructure from cyber-attacks. It is ideally designed for security analysts, law enforcement, researchers, legal practitioners, policymakers, business professionals, governments, strategists, educators, and students seeking current research on combative solutions for cyber threats and attacks.

Information security cannot be effectively managed unless secure methods and standards are integrated into all phases of the information security life cycle. And, although the international community has been aggressively engaged in developing security standards for network and information security worldwide, there are few textbooks available that

This volume in the Advances in Management Information Systems series covers the managerial landscape of information security.

This volume constitutes the refereed proceedings of the 12th IFIP WG 11.2 International Conference on Information Security Theory and Practices, WISTP 2018, held in Brussels, Belgium, in December 2018. The 13 revised full papers and 2 short papers presented were carefully reviewed and selected from 45 submissions. The papers are organized in the following topical sections: real world; cryptography; artificial learning; cybersecurity; and Internet of things.

ROADMAP TO INFORMATION SECURITY: FOR IT AND INFOSEC MANAGERS provides a solid overview of information security and its relationship to the information needs of an organization. Content is tailored to the unique needs of information systems professionals who find themselves brought in to the intricacies of information security responsibilities. The book is written for a wide variety of audiences looking to step up to emerging security challenges, ranging from students to experienced professionals. This book is designed to guide the information technology manager in dealing with the challenges associated with the security aspects of their role, providing concise guidance on assessing and improving an organization's security. The content helps IT managers to handle an assignment to an information security role in ways that conform to expectations and requirements, while supporting the goals of the manager in building and maintaining a solid information security program. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Annotation This volume constitutes the refereed proceedings of the 4th IFIP WG 11.2 International Workshop on Information Security Theory and Practices: Security and Privacy of Pervasive Systems and Smart Devices, WISTP 2010, held in Passau, Germany, in April 2010. The 20 revised full papers and 10 short papers were carefully reviewed and selected from 69 submissions. They are organized in topical sections on embedded security, protocols, highly constrained embedded systems, security, smart card security, algorithms, hardware implementations, embedded systems and anonymity/database security.

This volume constitutes the refereed proceedings of the 13th IFIP WG 11.2 International Conference on Information Security Theory and Practices, WISTP 2019, held in Paris, France, in December 2019. The 12 full papers and 2 short papers presented were carefully reviewed and selected from 42 submissions. The papers are organized in the following topical sections: authentication; cryptography; threats; cybersecurity; and Internet of Things.

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

Information Security and Optimization maintains a practical perspective while offering theoretical explanations. The book explores concepts that are essential for academics as well as organizations. It discusses aspects of techniques and tools—definitions, usage, and analysis—that are invaluable for scholars ranging from those just beginning in the field to established experts. What are the policy standards? What are vulnerabilities and how can one patch them? How can data be transmitted securely? How can data in the cloud or cryptocurrency in the

blockchain be secured? How can algorithms be optimized? These are some of the possible queries that are answered here effectively using examples from real life and case studies. Features: A wide range of case studies and examples derived from real-life scenarios that map theoretical explanations with real incidents. Descriptions of security tools related to digital forensics with their unique features, and the working steps for acquiring hands-on experience. Novel contributions in designing organization security policies and lightweight cryptography. Presentation of real-world use of blockchain technology and biometrics in cryptocurrency and personalized authentication systems. Discussion and analysis of security in the cloud that is important because of extensive use of cloud services to meet organizational and research demands such as data storage and computing requirements. Information Security and Optimization is equally helpful for undergraduate and postgraduate students as well as for researchers working in the domain. It can be recommended as a reference or textbook for courses related to cybersecurity.

This volume constitutes the refereed proceedings of the 8th IFIP WG 11.2 International Workshop on Information Security Theory and Practices, WISTP 2014, held in Heraklion, Crete, Greece, in June/July 2014. The 8 revised full papers and 6 short papers presented together with 2 keynote talks were carefully reviewed and selected from 33 submissions. The papers have been organized in topical sections on cryptography and cryptanalysis, smart cards and embedded devices, and privacy.

Information Security Theory and Practice9th IFIP WG 11.2 International Conference, WISTP 2015, Heraklion, Crete, Greece, August 24-25, 2015. ProceedingsSpringer

Presents theories and models associated with information privacy and safeguard practices to help anchor and guide the development of technologies, standards, and best practices. Provides recent, comprehensive coverage of all issues related to information security and ethics, as well as the opportunities, future challenges, and emerging trends related to this subject.

Your expert guide to information security As businesses and consumers become more dependent on complexmultinational information systems, the need to understand anddevise sound information security systems has never been greater.This title takes a practical approach to information security byfocusing on real-world examples. While not sidestepping the theory,the emphasis is on developing the skills and knowledge thatsecurity and information technology students and professionals needto face their challenges. The book is organized around four majorthemes: * Cryptography: classic cryptosystems, symmetric key cryptography,public key cryptography, hash functions, random numbers,information hiding, and cryptanalysis * Access control: authentication and authorization, password-basedsecurity, ACLs and capabilities, multilevel and multilateralsecurity, covert channels and inference control, BLP and Biba'smodels, firewalls, and intrusion detection systems * Protocols: simple authentication protocols, session keys, perfectforward secrecy, timestamps, SSL, IPSec, Kerberos, and GSM * Software: flaws and malware, buffer overflows, viruses and worms,software reverse engineering, digital rights management, securesoftware development, and operating systems security Additional features include numerous figures and tables toillustrate and clarify complex topics, as well as problems-rangingfrom basic to challenging-to help readers apply their newlydeveloped skills. A solutions manual and a set of classroom-testedPowerPoint(r) slides will assist instructors in their coursedevelopment. Students and professors in information technology,computer science, and engineering, and professionals working in thefield will find this reference most useful to solve theirinformation security issues. An Instructor's Manual presenting detailed solutions to all theproblems in the book is available from the Wiley editorialdepartment. An Instructor Support FTP site is also available.

Most introductory texts provide a technology-based survey of methods and techniques that leaves the reader without a clear understanding of the interrelationships between methods and techniques. By providing a strategy-based introduction, the reader is given a clear understanding of how to provide overlapping defenses for critical information. This understanding provides a basis for engineering and risk-management decisions in the defense of information. Information security is a rapidly growing field, with a projected need for thousands of professionals within the next decade in the government sector alone. It is also a field that has changed in the last decade from a largely theory-based discipline to an experience-based discipline. This shift in the field has left several of the classic texts with a strongly dated feel. Provides a broad introduction to the methods and techniques in the field of information security Offers a strategy-based view of these tools and techniques, facilitating selection of overlapping methods for in-depth defense of information Provides very current view of the emerging standards of practice in information security

This volume constitutes the refereed proceedings of the Third IFIP WG 11.2 International Workshop on Information Security Theory and Practice: Smart Devices, Pervasive Systems, and Ubiquitous Networks, WISTP 2009 held in Brussels, Belgium in September 2009. The 12 revised full papers presented were carefully reviewed and selected from 27 submissions for inclusion in the book; they are organized in topical sections on mobility, attacks and secure implementations, performance and security, and cryptography.

This volume constitutes the refereed proceedings of the 9th IFIP WG 11.2 International Conference(formerly Workshop) on Information Security Theory and Practices, WISTP 2015, held in Heraklion, Crete, Greece, in August 2015. The 14 revised full papers and 4 short papers presented together were carefully reviewed and selected from 52 submissions. WISTP 2015 sought original submissions from academia and industry presenting novel research on all theoretical and practical aspects of security and privacy, as well as experimental studies of elded systems, the application of security technology, the implementation of systems, and lessons learned. We encouraged submissions from other communities such as law, business, and policy that present these communities' perspectives on technological issues.

This volume constitutes the refereed proceedings of the 11th IFIP WG 11.2 International Conference on Information Security Theory and Practices, WISTP 2017, held in Heraklion, Crete, Greece, in September 2017. The 8 revised full papers and 4 short papers presented were carefully reviewed and selected from 35 submissions. The papers are organized in the following topical sections: security in emerging systems; security of data; trusted execution; defenses and evaluation; and protocols and algorithms.

As part of the Syngress Basics series, The Basics of Information Security provides you with fundamental knowledge of information security in both theoretical and practical aspects. Author Jason Andress gives you the basic knowledge needed to understand the key concepts of confidentiality, integrity, and availability, and then dives into practical applications of these ideas in the areas of operational, physical, network, application, and operating system security. The Basics of Information Security gives you clear-non-technical explanations of how infosec works and how to apply these principles whether you're in the IT field or want to understand how it affects your career and business. The new Second Edition has been updated for the latest trends and threats, including new material on many infosec subjects. Learn about information security without wading through a huge textbook Covers both theoretical and practical aspects of information security Provides a broad view of the information security field in a concise manner All-new Second Edition updated for the latest information security trends and threats, including material on incident response, social engineering, security awareness, risk management, and legal/regulatory issues

Security Science integrates the multi-disciplined practice areas of security into a single structured body of knowledge, where each chapter takes an evidence-based approach to one of the core knowledge categories. The authors give practitioners and students the underlying scientific perspective based on robust underlying theories, principles, models or frameworks. Demonstrating the relationships and underlying concepts, they present an approach to each core security function within the context of both organizational security and homeland security. The book is unique in its application of the scientific method to the increasingly challenging tasks of preventing crime and foiling terrorist attacks. Incorporating the latest security theories and principles, it considers security from both a national and corporate perspective, applied at a strategic and tactical level. It provides a rational basis for complex decisions and begins the process of defining the emerging discipline of security science. A fresh and provocative approach to the key facets of security Presentation of theories and models for a reasoned approach to decision making Strategic and tactical support for corporate leaders handling security challenges Methodologies for protecting national assets in government and private sectors Exploration of security's emerging body of knowledge across domains

This book provides readers insights into cyber maneuvering or adaptive and intelligent cyber defense. It describes the required models and security supporting functions that enable the analysis of potential threats, detection of attacks, and implementation of countermeasures while expending attacker resources and preserving user experience. This book not only presents significant education-oriented content, but uses advanced content to reveal a blueprint for helping network security professionals design and implement a secure Software-Defined Infrastructure (SDI) for cloud networking environments. These solutions are a less intrusive alternative to security countermeasures taken at the host level and offer centralized control of the distributed network. The concepts, techniques, and strategies discussed in this book are ideal for students, educators, and security practitioners looking for a clear and concise text to avant-garde cyber security installations or simply to use as a reference. Hand-on labs and lecture slides are located at http://virtualnetworksecurity.thothlab.com/. Features Discusses virtual network security concepts Considers proactive security using moving target defense Reviews attack representation models based on attack graphs and attack trees Examines service function chaining in virtual networks with security considerations Recognizes machine learning and AI in network security

Copyright: 6c41a925634e034b96fa64c488006683