Gsm Pstn Wireless Home Security Alarm Manual

Finally--a single volume guide to really effective security for both voice and data wireless networks! More and more data and voice communications are going via wireless at some point between the sender and intended recipient. As a result, truly "bulletproof" wireless security is now more than a desirable feature--instead, it's a necessity to protect essential personal and business data from hackers and eavesdroppers. In this handy reference, Praphul Chandra gives you the conceptual and practical tools every RF, wireless, and network engineer needs for high-security wireless applications. Inside this book you'll find coverage of these essential topics: + Cryptographic protocols used in wireless networks. + Key-based protocols, including key exchange and authentication techniques + Various types of wireless network attacks, including reflection, session hijacks, and Fluhrer-Mantin-Shamir (FMS) attacks. + Encryption/decryption standards and methods. + Multi-layered security architectures. + Secure sockets layer (SSL) and transport layer security (TLS) protocols. + Cellular telephone network architectures and their vulnerabilities. + Modulation techniques, such as direct-sequence spread spectrum (DSSS) and orthogonal frequency division multiplexing (OFDM) And you'll also find coverage on such cutting-edge topics as security techniques for ad hoc networks and protecting Bluetooth networks. If you're serious about wireless security, then this title belongs on your reference bookshelf!

CSIE 2011 is an international scientific Congress for distinguished scholars engaged in scientific, engineering and technological research, dedicated to build a platform for exploring and discussing the future of Computer Science and Information Engineering with existing and

potential application scenarios. The congress has been held twice, in Los Angeles, USA for the first and in Changchun, China for the second time, each of which attracted a large number of researchers from all over the world. The congress turns out to develop a spirit of cooperation that leads to new friendship for addressing a wide variety of ongoing problems in this vibrant area of technology and fostering more collaboration over the world. The congress, CSIE 2011, received 2483 full paper and abstract submissions from 27 countries and regions over the world. Through a rigorous peer review process, all submissions were refereed based on their quality of content, level of innovation, significance, originality and legibility. 688 papers have been accepted for the international congress proceedings ultimately.

Exploit and defend against the latest wireless network attacks Learn to exploit weaknesses in wireless network environments using the innovative techniques in this thoroughly updated guide. Inside, you'll find concise technical overviews, the latest attack methods, and ready-to-deploy countermeasures. Find out how to leverage wireless eavesdropping, break encryption systems, deliver remote exploits, and manipulate 802.11 clients, and learn how attackers impersonate cellular networks. Hacking Exposed Wireless, Third Edition features expert coverage of ever-expanding threats that affect leading-edge technologies, including Bluetooth Low Energy, Software Defined Radio (SDR), ZigBee, and Z-Wave. Assemble a wireless attack toolkit and master the hacker's weapons Effectively scan and enumerate WiFi networks and client devices Leverage advanced wireless attack tools, including Wifite, Scapy, Pyrit, Metasploit, KillerBee, and the Aircrack-ng suite Develop and launch client-side attacks using Ettercap and the WiFi Pineapple Hack cellular networks with Airprobe, Kraken, Pytacle, and YateBTS Exploit holes in WPA and WPA2 personal and enterprise security schemes Leverage

rogue hotspots to deliver remote access software through fraudulent software updates Eavesdrop on Bluetooth Classic and Bluetooth Low Energy traffic Capture and evaluate proprietary wireless technology with Software Defined Radio tools Explore vulnerabilities in ZigBee and Z-Wave-connected smart homes and offices Attack remote wireless networks using compromised Windows systems and built-in tools

This invaluable reference book focuses on the air interface of mobile networks at different layers according to the OSI Reference Model. It provides an overview of several wireless communication systems as well as mobile satellite systems, followed by detailed analysis of radio resource management issues.

This book summarizes various approaches for the automatic detection of health threats to older patients at home living alone. The text begins by briefly describing those who would most benefit from healthcare supervision. The book then summarizes possible scenarios for monitoring an older patient at home, deriving the common functional requirements for monitoring technology. Next, the work identifies the state of the art of technological monitoring approaches that are practically applicable to geriatric patients. A survey is presented on a range of such interdisciplinary fields as smart homes, telemonitoring, ambient intelligence, ambient assisted living, gerontechnology, and aging-in-place technology. The book discusses relevant experimental studies, highlighting the application of sensor fusion, signal processing and machine learning techniques. Finally, the text discusses future challenges, offering a number of suggestions for further research directions.

In multimedia and communication environments all documents must be protected against attacks. The movie Forrest Gump showed how multimedia documents can be manipulated.

The required security can be achieved by a number of different security measures. This book provides an overview of the current research in Multimedia and Communication Security. A broad variety of subjects are addressed including: network security; attacks; cryptographic techniques; healthcare and telemedicine; security infrastructures; payment systems; access control; models and policies; auditing and firewalls. This volume contains the selected proceedings of the joint conference on Communications and Multimedia Security; organized by the International Federation for Information processing and supported by the Austrian Computer Society, Gesellschaft fuer Informatik e.V. and TeleTrust Deutschland e.V. The conference took place in Essen, Germany, in September 1996

Vast, complex technologies, countless relevant topics, seemingly limitless documentation of standards and recommendations... In a field as dynamic as wireless technology, how is one to keep up when the very task of deciding which publications to read and which resources belong on your shelf can be daunting? Wireless Technology: Protocols, Standards, and Techniques has sorted it out for you. From basic principles to the state of the art, it furnishes clear, concise descriptions of second and third generation wireless technologies. The bestselling author of the Foundations of Mobile Radio Engineering has gathered together the most up-to-date networking standards, techniques, and protocols and incorporated clear, concise treatments of the necessary background material to form the most current and complete wireless reference available. However bumpy the road may seem, the migration to a wireless world is inevitable. Whether you are a communications engineer, network analyst or designer, electrical engineer, or computer engineer, keeping up in this rapidly evolving field is imperative. This book will help you stay at the forefront of your field and contribute to making the wireless world a reality.

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.

Charged with ensuring the confidentiality, integrity, availability, and delivery of all forms of an entity's information, Information Assurance (IA) professionals require a fundamental understanding of a wide range of specializations, including digital forensics, fraud examination, systems engineering, security risk management, privacy, and compliance. Establishing this understanding and keeping it up to date requires a resource with coverage as diverse as the field it covers. Filling this need, the Encyclopedia of Information Assurance presents an up-to-date collection of peer-reviewed articles and references written by authorities in their fields. From risk management and privacy to auditing and compliance, the encyclopedia’s four volumes provide comprehensive coverage of the key topics related to information assurance.

This complete IA resource: Supplies the understanding needed to help prevent the misuse of sensitive information Explains how to maintain the integrity of critical systems Details effective tools, techniques, and methods for protecting personal and corporate data against the latest threats Provides valuable examples, case studies, and discussions on how to address common and emerging IA challenges Placing the wisdom of leading researchers and practitioners at your fingertips, this authoritative reference provides the knowledge and insight needed to avoid common pitfalls and stay one step ahead of evolving threats. Also Available Online This Taylor & Francis encyclopedia is also available through online subscription, offering a variety of extra benefits for researchers, students, and librarians, including: ? Citation tracking and alerts ? Active reference linking ? Saved searches and marked lists ? HTML and PDF format options Contact Taylor and Francis for more information or to inquire about subscription options and print/online combination packages. US: (Tel) 1.888.318.2367; (E-mail) e-reference@taylorandfrancis.com International: (Tel) +44 (0) 20 7017 6062; (E-mail) online.sales@tandf.co.uk

Now updated—your expert guide to twenty-first century information security Information security is a rapidly evolving field. As businesses and consumers become increasingly dependent on complex multinational information systems, it is more imperative than ever to protect the confidentiality and integrity of data. Featuring a wide array of new information on the most current security issues, this fully updated and revised edition of

Information Security: Principles and Practice provides the skills and knowledge readers need to tackle any information security challenge. Taking a practical approach to information security by focusing on real-world examples, this book is organized around four major themes: Cryptography: classic cryptosystems, symmetric key cryptography, public key cryptography, hash functions, random numbers, information hiding, and cryptanalysis Access control: authentication and authorization, password-based security, ACLs and capabilities, multilevel security and compartments, covert channels and inference control, security models such as BLP and Biba's model, firewalls, and intrusion detection systems Protocols: simple authentication protocols, session keys, perfect forward secrecy, timestamps, SSH, SSL, IPSec, Kerberos, WEP, and GSM Software: flaws and malware, buffer overflows, viruses and worms, malware detection, software reverse engineering, digital rights management, secure software development, and operating systems security This Second Edition features new discussions of relevant security topics such as the SSH and WEP protocols, practical RSA timing attacks, botnets, and security certification. New background material has been added, including a section on the Enigma cipher and coverage of the classic "orange book" view of security. Also featured are a greatly expanded and upgraded set of homework problems and many new figures, tables, and graphs to illustrate and clarify complex topics and problems. A comprehensive solutions manual is available to assist in course development. Minimizing theory while providing clear, accessible content, Information

Security remains the premier text for students and instructors in information technology, computer science, and engineering, as well as for professionals working in these fields.

Created through a student-tested, faculty-approved review process with input from more than 250 students and faculty, GOVT is an engaging and accessible solution to accommodate the diverse learning styles of today's learners at a value-based price. Focusing on the current and historical conflicts and controversies that define America as a nation, GOVT is a streamlined and extremely current text for the American Government course. Its motivating debate theme and appealing modern format speak directly to today's student. A full suite of learning tools--correlated to the text chapter-by-chapter--are available through CourseMate and include an eBook, Chapter In Review cards, videos, simulations, podcasts, and quizzes that allow students to learn and study wherever they are and whenever they have time.

This book describes the technologies involved in all aspects of a large networking system and how the various devices can interact and communicate with each other. Using a bottom up approach the authors demonstrate how it is feasible, for instance, for a cellular device user to communicate, via the all-purpose TCP/IP protocols, with a wireless notebook computer user, traversing all the way through a base station in a cellular wireless network (e.g., GSM, CDMA), a public switched network (PSTN), the Internet, an intranet, a local area network (LAN), and a wireless LAN access point. The information bits, in travelling through this long path, are processed by numerous

disparate communication technologies. The authors also describe the technologies involved in infrastructure less wireless networks.

This comprehensive book gives you a hands-on understanding of the techniques and architectures being used to provide voice and data services over wireless networks. It serves as a unified "how it works" guide to wireless Internet telecommunications, systematically addressing each of the technological components and how they fit together. You get a clear picture of protocols like RTP for multimedia transport and SIP for session control signaling, and see what's being done to tackle tough challenges in QoS control, mobility management, and security in the wireless environment. The book discusses at length the cutting-edge IP Multimedia Sub-System (IMS) of UMTS to illustrate how each of these crucial components can be successfully implemented in a real-world wireless IP system.

Intruder Alarms provides a definitive and fully up-to-date guide to the specification, systems design, integration, installation and maintenance of intruder alarm systems. It has been written to be the essential handbook for installation engineers and security professionals working in this rapidly expanding and developing area. The third edition includes new material on systems integration, digital systems, wireless and remote signalling technologies, and electrical safety. The revision has brought coverage fully in line with the new European standards (EN50131 / BS EN 50131-1), with their implications summarised in a new appendix. The coverage has also been carefully

matched to the requirements of the new Knowledge of Security and Emergency Alarm Systems from City & Guilds (1852). * An hugely popular practical guide for installation engineers and security professionals now in its third edition * Essential reading for managers responsible for the commissioning and maintenance of security alarm systems * Third edition is fully matched to the new European standards (EN50131 / BS EN 50131-1) * Coverage meets City & Guilds specifications for the new 1852 Security Alarm course

Receive comprehensive instruction on the fundamentals of wireless security from three leading international voices in the field Security in Wireless Communication Networks delivers a thorough grounding in wireless communication security. The distinguished authors pay particular attention to wireless specific issues, like authentication protocols for various wireless communication networks, encryption algorithms and integrity schemes on radio channels, lessons learned from designing secure wireless systems and standardization for security in wireless systems. The book addresses how engineers, administrators, and others involved in the design and maintenance of wireless networks can achieve security while retaining the broadcast nature of the system, with all of its inherent harshness and interference. Readers will learn: A comprehensive introduction to the background of wireless communication network security, including a broad overview of wireless communication networks, security services, the mathematics crucial to the subject, and cryptographic techniques An

exploration of wireless local area network security, including Bluetooth security, Wi-Fi security, and body area network security An examination of wide area wireless network security, including treatments of 2G, 3G, and 4G Discussions of future development in wireless security, including 5G, and vehicular ad-hoc network security Perfect for undergraduate and graduate students in programs related to wireless communication, Security in Wireless Communication Networks will also earn a place in the libraries of professors, researchers, scientists, engineers, industry managers, consultants, and members of government security agencies who seek to improve their understanding of wireless security protocols and practices.

Section A: Basic Of E-Commerce And Its Application 1. Introduction To E-Commerce 2. Business Models Of E-Commerce 3. B2B E-Commerce And Edi 4. Business Applications Of E-Commerce Section B: Technologies For E-Commerce 5. E-Commerce Technology 6. Electronic Payment Systems 7. Security Issues In E-Commerce 8. Role Of Social Media In E-Commerce Industry Section C: M-Commerce And Its Implementation 9. Mobile Commerce And Wap 10. Mobile Commerce Risk, Security And Payments Methods 11. Mobile Money-Infrastructure And Fraud Prevention For M-Payment Section D: Legal Issues 12. Legal And Ethical Issues 13. Cyber Laws 14. Webhosting Section E: Online Marketing And Website Designing 16. Search Engine Optimization (Seo) 17. Tools For Website Design Section F: Security Issues In E-Commerce 18. Few Security Guidelines For Developing E-Commerce

Applications 19. E-Commerce Testing Process Section G: Current Trends In E-Commerce 20. Current Trends In Electronic World

With the rapid evolution of multimedia communications, engineers and other professionals are generally forced to hoard a plethora of different texts and journals to maintain a solid grasp on essential ideas and techniques in the field. Wireless Multimedia Communications provides researchers and students with a primary reference to help readers take maximum advantage of current systems and uncover opportunities to propose new and novel protocols, applications, and services. Extract the Essentials of System Design, Analysis, Implementation A complete technical reference, the text condenses the essential topics of core wireless multimedia communication technologies, convergence, QoS, and security that apply to everything from networking to communications systems, signal processing, and security. From extensive existing literature, the authors distill the central tenets and primary methods of analysis, design, and implementation, to reflect the latest technologies and architectural concepts. The book addresses emerging challenges to inform the system standardization process and help engineers combat the high error rates and stringent delay constraints that remain a significant challenge to various applications and services. Keep Pace with Detailed Techniques to Optimize Technology The authors identify causes of information loss in point-to-point signal transmission through wireless channels, and then they discuss techniques to minimize that loss. They use examples

that illustrate the differences in implementing various systems, ranging from cellular voice telephony to wireless Internet access. Each chapter has been carefully organized with the latest information to serve dual purposes as an easy-to-reference guide for professionals and as a principal text for senior-level university students.

This book will cover network management security issues and currently available security mechanisms by discussing how network architectures have evolved into the contemporary NGNs which support converged services (voice, video, TV, interactive information exchange, and classic data communications). It will also analyze existing security standards and their applicability to securing network management. This book will review 21st century security concepts of authentication, authorization, confidentiality, integrity, nonrepudiation, vulnerabilities, threats, risks, and effective approaches to encryption and associated credentials management/control. The book will highlight deficiencies in existing protocols used for management and the transport of management information.

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.

This book covers many aspects of security for mobility including current developments, underlying technologies, network security, mobile code issues, application security and the future.

Designed as a textbook for the undergraduate students of electronics and communication engineering, electronics and electrical engineering, computer science and engineering, and information technology, this compact and well organized text presents many recent topics in the fastest growing field of communication. Beginning with an introduction to modern wireless communication systems, this text covers the basic concepts of cellular and capacity improvement in cellular systems, propagation mechanisms in wireless communication, fading channels, diversity techniques and wireless standards such as GSM, GPRS and UMTS. It concludes with a description on wireless LAN concepts and Bluetooth technology. This book also presents various important topics such as CDMA, MIMO, OFDM, smart antennas and MC-CDMA techniques that have emerged recently. KEY FEATURES : Provides worked out practical problems in cellular capacity improvement and wireless propagation Emphasizes the purpose of diversity and implementation issues. Analyzes thoroughly the diversity combining techniques with probability density functions. Gives step-by-step

treatment on the evolution of wireless communi-cations till 4G. Explains PAPR reduction in MC-CDMA. Besides undergraduate students, this book will also be useful to the postgraduate students for the courses in wireless communication/mobile communication, researchers and practicing engineers in the field of wireless communication.

Introduces aspects on security threats and their countermeasures in both fixed and wireless networks, advising on how countermeasures can provide secure communication infrastructures. Enables the reader to understand the risks of inappropriate network security, what mechanisms and protocols can be deployed to counter these risks, and how these mechanisms and protocols work.

This book, suitable for IS/IT courses and self study, presents a comprehensive coverage of the technical as well as business/management aspects of mobile computing and wireless communications. Instead of one narrow topic, this classroom tested book covers the major building blocks (mobile applications, mobile computing platforms, wireless networks, architectures, security, and management) of mobile computing and wireless communications. Numerous real-life case studies and examples highlight the key points. The book starts with a discussion of m-business and m-government initiatives and examines mobile computing applications such as mobile messaging, m-commerce, M-CRM, M-portals, M-SCM, mobile agents, and sensor applications. The role of wireless Internet and Mobile IP is explained and the mobile

computing platforms are analyzed with a discussion of wireless middleware, wireless gateways, mobile application servers, WAP, i-mode, J2ME, BREW, Mobile Internet Toolkit, and Mobile Web Services. The wireless networks are discussed at length with a review of wireless communication principles, wireless LANs with emphasis on 802.11 LANs, Bluetooth, wireless sensor networks, UWB (Ultra Wideband), cellular networks ranging from 1G to 5G, wireless local loops, FSO (Free Space Optics), satellites communications, and deep space networks. The book concludes with a review of the architectural, security, and management/support issues and their role in building, deploying and managing wireless systems in modern settings.

Recent Advances in Computer Science and Information EngineeringVolume 2Springer Science & Business Media

The Handbook of Information Security is a definitive 3-volume handbook that offers coverage of both established and cutting-edge theories and developments on information and computer security. The text contains 180 articles from over 200 leading experts, providing the benchmark resource for information security, network security, information privacy, and information warfare.

"Real-time Systems' Quality of Service" examines the attainability of efficiency, economy, and ease of use, which make up the quality of service of technologically advanced products. "Real-time Systems' Quality of Service" reviews the state of the art in quality of service evaluation for real-time systems. It gives a classification of the

relevant parameters for quality of service evaluation and also determines the critical points in the design and development process of real-time systems – where performance criteria should be applied or checked. Then, software development and certification standards are assessed, and finally the authors elaborate on how the suggested criteria should be applied to the design, development, and certification process of real-time systems. "Real-time Systems' Quality of Service" will guide researchers and postgraduates in embedded and real-time systems through the process of introducing quality of service parameters into real-time systems.

Addressing the growing need to integrate effective security features into wireless communication systems, this book offers an overview of wireless security, as well the technical 'know-how' practitioners need to understand and work with the security concepts and techniques used for 2nd, 3rd, and 4th generation mobile networks.

A relative newcomer to the field of wireless communications, ad hoc networking is growing quickly, both in its importance and its applications. With rapid advances in hardware, software, and protocols, ad hoc networks are now coming of age, and the time has come to bring together into one reference their principles, technologies, and techniques. The Handbook of Ad Hoc Wireless Networks does exactly that. Experts from around the world have joined forces to create the definitive reference for the field. From the basic concepts, techniques, systems, and protocols of wireless communication to the particulars of ad hoc network routing methods, power,

connections, traffic management, and security, this handbook covers virtually every aspect of ad hoc wireless networking. It includes a section that explores several routing methods and protocols directly related to implementing ad hoc networks in a variety of applications. The benefits of ad hoc wireless networks are many, but several challenges remain. Organized for easy reference, The Handbook of Ad Hoc Wireless Networks is your opportunity to gain quick familiarity with the state of the art, have at your disposal the only complete reference on the subject available, and prepare to meet the technological and implementation challenges you'll encounter in practice.

This book describes the current and most probable future wireless security solutions. The focus is on the technical discussion of existing systems and new trends like Internet of Things (IoT). It also discusses existing and potential security threats, presents methods for protecting systems, operators and end-users, describes security systems attack types and the new dangers in the ever-evolving Internet. The book functions as a practical guide describing the evolvement of the wireless environment, and how to ensure the fluent continuum of the new functionalities, whilst minimizing the potential risks in network security.

"This book combines research from esteemed experts on security issues in various wireless communications, recent advances in wireless security, the wireless security model, and future directions in wireless security. As an innovative reference source forstudents, educators, faculty members, researchers, engineers in the field of wireless

security, it will make an invaluable addition to any library collection"--Provided by publisher.

Wireless communication is one of the fastest growing fields in the engineering world today. Rapid growth in the domain of wireless communication systems, services and application has drastically changed the way we live, work and communicate. Wireless communication offers a broad and dynamic technological field, which has stimulated incredible excitements and technological advancements over last few decades. The expectations from wireless communication technology are increasing every day. This is placing enormous challenges to wireless system designers. Moreover, this has created an ever increasing demand for conceptually strong and well versed communication engineers who understand the wireless technology and its future possibilities. In recent years, significant progress in wireless communication system design has taken place, which will continue in future. Especially for last two decades, the research contributions in wireless communication system design have resulted in several new concepts and inventions at remarkable speed. A text book is indeed required to offer familiarity with such developments and underlying concepts, to be taught in the classroom to future engineers. This is one of the motivations for writing this book. Practically no book can be up to date in this field, due to the fast ongoing research and developments. The new developments are announced almost every day. Teaching directly from the research papers in the classroom cannot build the necessary foundation. Therefore need for a

textbook is unavoidable, which is integral to learning, and is an essential source to build the concept. The prime goal of this book is to cooperate in the learning process. This book is based on current research as well as classical text books in the field, and aims to provide in depth understanding on fundamental concepts, which form the basis of wireless communication and build the platform, on which current developments can be understood and future contributions can be made. This book is written in self-explanatory manner to facilitate critical thinking and to support self study. Special emphasis has been given in this book to systematically organize and present the wide domain of wireless communication technology. Extra care has been taken to present the contents and the concepts in user friendly way to enable an easy understanding. Therefore the language of this book is made to make one feel, listening to a classroom lecture. This makes learning straight forward. Sometimes, the explanation could seem to be oversimplified, this is in order to support wide spectrum of readers as well as to clarify the hazy picture. A book of this kind, which addresses a fast developing technology, the frequent use of acronyms and abbreviations is almost inevitable. A care has been taken to spell the acronyms and abbreviations as frequently as practically suitable in the text. Besides, a list of acronyms and abbreviations has also been provided.

This book provides an overview of the current state of the art in wireless networks around the globe, focusing on utilizing the latest artificial intelligence and soft computing

techniques to provide design frameworks for wireless networks. These techniques play a vital role in developing a more robust algorithm suitable for the dynamic and heterogeneous environment, making the network self-managed, self-operational, and self-configurational, and efficiently reducing uncertainties and imprecise information. This book provides a thorough examination and analysis of cutting-edge research and security solutions in wireless and mobile networks. It begins with coverage of the basic security concepts and fundamentals which underpin and provide the knowledge necessary for understanding and evaluating security issues, challenges, and solutions. This material will be of invaluable use to all those working in the network security field, and especially to the many people entering the field. The next area of focus is on the security issues and available solutions associated with off-the-shelf wireless and mobile technologies such as Bluetooth, WiFi, WiMax, 2G, and 3G. There is coverage of the security techniques used to protect applications downloaded by mobile terminals through mobile cellular networks, and finally the book addresses security issues and solutions in emerging wireless and mobile technologies such as ad hoc and sensor networks, cellular 4G and IMS networks.

"This book examines the current scope of theoretical and practical applications on the security of mobile and wireless communications, covering fundamental concepts of current issues, challenges, and solutions in wireless and mobile networks"--Provided by publisher.

2009 CHOICE AWARD OUTSTANDING ACADEMIC TITLE Information and communications security is a hot topic in private industry as well as in government agencies. This book provides a complete conceptual treatment of securing information and transporting it over a secure network in a manner that does not require a strong mathematical background. It stresses why information security is important, what is being done about it, how it applies to networks, and an overview of its key issues. It is written for anyone who needs to understand these important topics at a conceptual rather than a technical level.