Wi Foo The Secrets Of Wireless Hacking

The first comprehensive guide to discovering and preventingattacks on the Android OS As the Android operating system continues to increase its shareof the smartphone market, smartphone hacking remains a growingthreat. Written by experts who rank among the world's foremostAndroid security researchers, this book presents vulnerabilitydiscovery, analysis, and exploitation tools for the good guys.Following a detailed explanation of how the Android OS works andits overall security architecture, the authors examine howvulnerabilities can be discovered and exploits developed forvarious system components, preparing you to defend againstthem. If you are a mobile device administrator, security researcher,Android app developer, or consultant responsible for evaluatingAndroid security, you will find this guide is essential to yourtoolbox. A crack team of leading Android security researchers explainAndroid security risks, security design and architecture, rooting,fuzz testing, and vulnerability analysis Covers Android application building blocks and security as wellas debugging and auditing Android apps Prepares mobile device administrators, security researchers,Android app developers, and security consultants to defend Androidsystems against attack Android Hacker's Handbook is the first comprehensiveresource for IT professionals charged with smartphonesecurity.

The mobile information society has revolutionised the way we work, communicate and socialise. Mobile phones, wireless free communication and associated technologies such as WANs, LANs, and PANs, cellular networks, SMS, 3G, Bluetooth, Blackberry and WiFi are seen as the driving force of the advanced society. The roots of today's explosion in wireless technology can be traced back to the deregulation of AT&T in the US and the Post Office and British Telecom in the UK, as well as Nokia's groundbreaking approach to the design and marketing of the mobile phone. Providing a succinct introduction to the field of mobile and wireless communications, this book: Begins with the basics of radio technology and offers an overview of key scientific terms and concepts for the student reader Addresses the social and economic implications of mobile and wireless technologies, such as the effects of the deregulation of telephone systems Uses a range of case studies and examples of mobile and wireless communication, legislation and practices from the UK, US, Canada, mainland Europe, the Far East and Australia Contains illustrations and tables to help explain technical concepts and show the growth and change in mobile technologies Features a glossary of technical terms, annotated further reading at the end of each chapter and web links for further study and research Mobile and Wireless Communications is a key resource for students on a range of social scientific courses, including media and communications, sociology, public policy, and management studies, as well as a useful introduction to the field for researchers and general readers.

The explosive demand for mobile communications is driving the development of wireless technology at an unprecedented pace. Unfortunately, this exceptional growth is also giving rise to a myriad of security issues at all levels-from subscriber to network operator to service provider. Providing technicians and designers with a critical and comprehens

This book describes new approaches to wireless security enabled by the recent development of new core technologies for Wi-Fi/802.11. It shows how the new approaches work and how they should be applied for maximum effect. For system administrators, product designers, or advanced home users.

Android Hacker's Handbook

Understand and Implement Effective PCI Data Security Standard Compliance

Essentials of Short-Range Wireless

Industrial Communication Systems

Strategies, Tactics, Logic and Framework

Computerworld

Controller-Based Wireless LAN Fundamentals An end-to-end reference guide to design, deploy, manage, and secure 802.11 wireless networks As wired networks are increasingly replaced with 802.11n wireless connections, enterprise users are shifting to centralized, next-generation architectures built around Wireless LAN Controllers (WLC). These networks will increasingly run business-critical voice, data, and video applications that once required wired Ethernet. In Controller-Based Wireless LAN Fundamentals, three senior Cisco wireless experts bring together all the practical and conceptual knowledge professionals need to confidently design, configure, deploy, manage, and troubleshoot 802.11n networks with Cisco Unified Wireless Network (CUWN) technologies. The authors first introduce the core principles, components, and advantages of next-generation wireless networks built with Cisco offerings. Drawing on their pioneering experience, the authors present tips, insights, and best practices for network design and implementation as well as detailed configuration examples. Next, they illuminate key technologies ranging from WLCs to Lightweight Access Point Protocol (LWAPP) and Control and Provisioning of Wireless Access Points (CAPWAP), Fixed Mobile Convergence to WiFi Voice. They also show how to take advantage of the CUWN's end-to-end security, automatic configuration, self-healing, and integrated management capabilities. This book serves as a practical, hands-on reference for all network administrators, designers, and engineers through the entire project lifecycle, and an authoritative learning tool for new wireless certification programs. This is the only book that Fully covers the principles and components of next-generation wireless networks built with Cisco WLCs and Cisco 802.11n AP Brings together real-world tips, insights, and best practices for designing and implementing next-generation wireless networks Presents start-to-finish configuration examples for common deployment scenarios Reflects the extensive first-hand experience of Cisco experts Gain an operational and design-level understanding of WLAN Controller (WLC) architectures, related technologies, and the problems they solve Understand 802.11n, MIMO, and protocols developed to support WLC architecture Use Cisco technologies to enhance wireless network reliability, resilience, and scalability while reducing operating expenses Safeguard your assets using Cisco Unified Wireless Network's advanced security features Design wireless networks capable of serving as an enterprise's primary or only access network and supporting advanced mobility services Utilize Cisco Wireless Control System (WCS) to plan, deploy, monitor, troubleshoot, and report on wireless networks throughout their lifecycles Configure Cisco wireless LANs for multicasting Quickly troubleshoot problems with Cisco controller-based wireless LANs This book is part of the Cisco Press® Fundamentals Series. Books in this series introduce networking professionals to new networking technologies, covering network topologies, sample deployment concepts, protocols, and management techniques. Category: Wireless Covers: Cisco Controller-Based Wireless LANs

Hands-On Ethical Hacking and Network Defense, Second Edition provides an in-depth understanding of how to effectively protect computer networks. This book describes the tools and penetration testing methodologies used by ethical hackers and provides a thorough discussion of what and who an ethical hacker is and how important they are in protecting corporate and government data from cyber attacks. Readers are provided with updated computer security resources that describe new vulnerabilities and innovative methods to protect networks. Also included is a thorough update of federal and state computer crime laws, as well as changes in penalties for illegal computer hacking. With cyber-terrorism and corporate espionage threatening the fiber of our world, the need for trained network security professionals continues to grow. Hands-On Ethical Hacking and Network Defense, Second Edition provides a structured knowledge base to prepare readers to be security professionals who understand how to protect a network by using the skills and tools of an ethical hacker. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

The potential of embedded systems ranges from the simplicity of sharing digital media to the coordination of a variety of complex joint actions carried out between collections of networked devices. The book explores the emerging use of embedded systems and wireless technologies from theoretical and practical applications and their applications in agriculture, environment, public health, domotics, and public transportation, among others.

Communications represent a strategic sector for privacy protection and for personal, company, national and international security. The interception, damage or lost of information during communication can generate material and non material economic damages from both a personal and collective point of view. The purpose of this book is to give the reader information relating to all aspects of communications security, beginning at the base ideas and building to reach the most advanced and updated concepts. The book will be of interest to integrated system designers, telecommunication designers, system engineers, system analysts, security managers, technicians, intelligence personnel, security personnel, police, army, private investigators, scientists, graduate and postgraduate students and anyone that needs to communicate in a secure way.

Cisco Security Secrets & Solutions

Wi-Foo

Trust and Privacy in Digital Business

Web Technology

Cyber Warfare and Cyber Terrorism

Industrial Network Security

PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance, Second Edition, discusses not only how to apply PCI in a practical and cost-effective way but more importantly why. The book explains what the Payment Card Industry Data Security Standard (PCI DSS) is and why it is here to stay; how it applies to information technology (IT) and information security professionals and their organization; how to deal with PCI assessors; and how to plan and manage PCI DSS project. It also describes the technologies referenced by PCI DSS and how PCI DSS relates to laws, frameworks, and regulations. This book is for IT managers and company managers who need to understand how PCI DSS applies to their organizations. It is for the small- and medium-size businesses that do not have an IT department to delegate to. It is for large organizations whose PCI DSS project scope is immense. It is also for all organizations that need to grasp the concepts of PCI DSS and how to implement an effective security framework that is also compliant. Completely updated to follow the PCI DSS standard 1.2.1 Packed with help to develop and implement an effective security strategy to keep infrastructure compliant and secure Both authors have broad information security backgrounds, including extensive PCI DSS experience

The definitive guide to penetrating and defending wireless networks. Straight from the field, this is the definitive guide to hacking wireless networks. Authored by world-renowned wireless security auditors, this hands-on, practical guide covers everything you need to attack -- or protect -- any wireless network. The authors introduce the 'battlefield, ' exposing today's 'wide open' 802.11 wireless networks and their attackers. One step at a time, you'll master the attacker's entire arsenal of hardware and software tools: crucial knowledge for crackers and auditors alike. Next, you'll learn systematic countermeasures for building hardened wireless 'citadels''including cryptography-based techniques, authentication, wireless VPNs, intrusion detection, and more. Coverage includes: Step-by-step walkthroughs and explanations of typical attacks Building wireless hacking/auditing toolkit: detailed recommendations, ranging from discovery tools to chipsets and antennas Wardriving: network mapping and site surveying Potential weaknesses in current and emerging standards, including 802.11i, PPTP, and IPSec Implementing strong, multilayered defenses Wireless IDS: why attackers aren't as untraceable as they think Wireless hacking and the law: what's legal, what isn't If you're a hacker or security auditor, this book will get you in. If you're a netadmin, sysadmin, consultant, or home user, it will keep everyone else out.

Secure Your Wireless Networks the Hacking Exposed Way Defend against the latest pervasive and devastating wireless attacks using the tactical security information contained in this comprehensive volume. Hacking Exposed Wireless reveals how hackers zero in on susceptible networks and peripherals, gain access, and execute debilitating attacks. Find out how to plug security holes in Wi-Fi/802.11 and Bluetooth systems and devices. You'll also learn how to launch wireless exploits from Metasploit, employ bulletproof authentication and encryption, and sidestep insecure wireless hotspots. The book includes vital details on new, previously unpublished attacks alongside real-world countermeasures. Understand the concepts behind RF electronics, Wi-Fi/802.11, and Bluetooth Find out how hackers use NetStumbler, WiSPY, Kismet, KisMAC, and AiroPeek to target vulnerable wireless networks Defend against WEP key brute-force, aircrack, and traffic injection hacks Crack WEP at new speeds using Field Programmable Gate Arrays or your spare PS3 CPU cycles Prevent rogue AP and certificate authentication attacks Perform packet injection from Linux Launch DoS attacks using device driver-independent tools Exploit wireless device drivers using the Metasploit 3.0 Framework Identify and avoid malicious hotspots Deploy WPA/802.11i authentication and encryption using PEAP, FreeRADIUS, and WPA pre-shared keys

Provides information on how hackers target exposed computer networks and gain access and ways to stop these intrusions, covering such topics as routers, firewalls, and VPN vulnerabilities.

Hands-On Ethical Hacking and Network Defense

Cyberwar Stories from the Digital Front

First International Conference, ICeND 2011, Dar-es-Salaam, Tanzania, August 3-5, 2011, Proceedings

Advanced Defenses Against Hardcore Hacks

Wireless and Mobile Network Security

Second International Conference, e-Forensics 2009, Adelaide, Australia, January 19-21, 2009, Revised Selected Papers

This volume is number 67 in the series Advances in Computers that began back in 1960. This is the longest continuously published series of books that chronicles the evolution of the computer industry. Each year three volumes are produced presenting approximately 20 chapters that describe the latest technology in the use of computers today. Volume 67, subtitled "Web technology," presents 6 chapters that show the impact that the World Wide Web is having on our society today. The general theme running throughout the volume is the ubiquity of web services. Topics such as wireless access and its problems and reliability of web communications are emphasized. Key features: In-depth surveys and tutorials on software development approaches Well-known authors and researchers in the field Extensive bibliographies with most chapters All chapters focus on Internet and web technology issues Discussion of wireless communication and forensic issues, currently important research areas In-depth surveys and tutorials on software development approaches Well-known authors and researchers in the field Extensive bibliographies with most chapters All chapters focus on Internet and web technology issues Discussion of wireless communication and forensic issues, currently important research areas

"This book reviews problems, issues, and presentations of the newest research in the field of cyberwarfare and cyberterrorism. While enormous efficiencies have been gained as a result of computers and telecommunications technologies, use of these systems and networks translates into a major concentration of information resources, createing a vulnerability to a host of attacks and exploitations"--Provided by publisher.

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.

Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems describes an approach to ensure the security of industrial networks by taking into account the unique network, protocol, and application characteristics of an industrial control system, along with various compliance controls. It offers guidance on deployment and configuration, and it explains why, where, and how security controls should be implemented. Divided into 11 chapters, the book explains the basics of Ethernet and Transmission Control Protocol/Internet Protocol (TCP/IP) networking communications and the SCADA and field bus protocols. It also discusses industrial networks as they relate to "critical infrastructure and cyber security, potential risks and consequences of a cyber attack against an industrial control system, compliance controls in relation to network security practices, industrial network protocols, such as Modbus and DNP3, assessment of vulnerabilities and risk, how to secure enclaves, regulatory compliance standards applicable to industrial network security, and common pitfalls and mistakes, like complacency and deployment errors. This book is a valuable resource for plant operators and information security analysts, as well as compliance officers who want to pass an audit with minimal penalties and/or fines. Covers implementation guidelines for security measures of critical infrastructure Applies the security measures for system-specific compliance Discusses common pitfalls and mistakes and how to avoid them

Security Monitoring for Internal Intrusions

Encyclopedia of Mobile Computing and Commerce

Extrusion Detection

Third International Conference, TrustBus 2006, Krakow, Poland, September 4-8, 2006, Proceedings

Embedded Systems and Wireless Technology

Extreme Exploits

IT Convergence and Services is proceedings of the 3rd FTRA International Conference on Information Technology Convergence and Services (ITCS-11) and the FTRA International Conference on Intelligent Robotics, Automations, telecommunication facilities, and applications (IRoA-11). The topics of ITCS and IRoA cover the current hot topics satisfying the world-wide ever-changing needs. The ITCS-11 will be the most comprehensive conference focused on the various aspects of advances in information technology convergence, applications, and services. The ITCS-11 will provide an opportunity for academic and industry professionals to discuss the latest issues and progress in the area of ITCS. In addition, the conference will publish high quality papers which are closely related to the various theories, modeling, and practical applications in ITCS. The main scope of ITCS-11 is as follows. Computational Science and Applications Electrical and Electronics Engineering and Technology Manufacturing Technology and Services Management Information Systems and Services Electronic Commerce, Business and Management Vehicular Systems and Communications Bio-inspired Computing and Applications IT Medical Engineering Modeling and Services for Intelligent Building, Town, and City The IRoA is a major forum for scientists, engineers, and practitioners throughout the world to present the latest research, results, ideas, developments and applications in all areas of intelligent robotics and automations. The main scope of IRoA-11 is as follows. Intelligent Robotics & Perception systems Automations & Control Telecommunication Facilities Artificial Intelligence The IRoA is a major forum for scientists, engineers, and practitioners throughout the world to present the latest research, results, ideas, developments and applications in all areas of intelligent robotics and automations. The main scope of IRoA-11 is as follows. Intelligent Robotics & Perception systems Automations & Control Telecommunication Facilities Artificial Intelligence

The credit card industry established the PCI Data Security Standards to provide a minimum standard for how vendors should protect data to ensure it is not stolen by fraudsters. PCI Compliance, 3e, provides the information readers need to understand the current PCI Data Security standards, which have recently been updated to version 2.0, and how to effectively implement security within your company to be compliant with the credit card industry guidelines and protect sensitive and personally identifiable information. Security breaches continue to occur on a regular basis, affecting millions of customers and costing companies millions of dollars in fines and reparations. That doesn't include the effects such security breaches have on the reputation of the companies that suffer attacks. PCI Compliance, 3e, helps readers avoid costly breaches and inefficient compliance initiatives to keep their infrastructure secure. Provides a clear explanation of PCI Provides practical case studies, fraud studies, and analysis of PCI The first book to address version 2.0 updates to the PCI DSS, security strategy to keep your infrastructure PCI compliant

In the wake of the growing use of wireless communications, new types of security risks have evolved. Wireless Security covers the major topic of wireless communications with relevance both to organizations and private users. The technological background of these applications and protocols is laid out and presented in detail. Special emphasis is placed on the IEEE 802.11x-Standards that have been introduced for WLAN technology. Other technologies covered besides WLAN include: mobile phones, bluetooth and infrared. In each chapter a major part is devoted to security risks and provisions including encryption and authentication philosophies. Elaborate checklists have been provided to help IT administrators and security officers to achieve the maximum possible security in their installations, when using wireless technology. The book offers all necessary background information to this complex technological subject. It is at the same time a guideline and a working tool to implement a security strategy in organizations, assists in documenting the actual security status of existing installations, helps to avoid pitfalls, when operating in a wireless environment, and in configuring the necessary components.

Provides research on security issues in various wireless communications, recent advances in wireless security, the wireless security model, and future directions in wireless security.

What Developers and IT Professionals Should Know

Real 802.11 Security

Theories and Applications

Assessing Information Security

Privacy

Handbook of Communications Security

For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network.

The Second International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia (e-Forensics 2009) took place in Adelaide, South Australia during January 19-21, 2009, at the Australian National Wine Centre, University of Adelaide. In addition to the peer-reviewed academic papers presented in this volume, the c- ference featured a significant number of plenary contributions from recognized - tional and international leaders in digital forensic investigation. Keynote speaker Andy Jones, head of security research at British Telecom, outlined the emerging challenges of investigation as new devices enter the market. These - clude the impact of solid-state memory, ultra-portable devices, and distributed storage - also known as cloud computing. The plenary session on Digital Forensics Practice included Troy O'Malley, Que- sland Police Service, who outlined the paperless case file system now in use in Que- sland, noting that efficiency and efficacy gains in using the system have now meant that police can arrive at a suspect's home before the suspect! Joseph Razik, represe- ing Patrick Perrot of the Institut de Recherche Criminelle de la Gendarmerie Nati- ale, France, summarized research activities in speech, image, video and multimedia at the IRCGN. The plenary session on The Interaction Between Technology and Law brought a legal perspective to the technological challenges of digital forensic investigation.

For engineers, product designers, and technical marketers who need to design a cost-effective, easy-to-use, short-range wireless product that works, this practical guide is a must-have. It explains and compares the major wireless standards - Bluetooth, Wi-Fi, 802.11abgn, ZigBee, and 802.15.4 - enabling you to choose the best standard for your product. Packed with practical insights based on the author's 10 years of design experience, and highlighting pitfalls and trade-offs in performance and cost, this book will ensure you get the most out of your chosen standard by teaching you how to tailor it for your specific implementation. With information on intellectual property rights and licensing, production test, and regulatory approvals, as well as analysis of the market for wireless products, this resource truly provides everything you need to design and implement a successful short-range wireless product.

This book constitutes the refereed proceedings of the Third International Conference on Trust and Privacy in Digital Business, TrustBus 2006, held in conjunction with DEXA 2006. The book presents 24 carefully reviewed, revised full papers, organized in topical sections on privacy and identity management, security and risk management, security requirements and development, privacy enhancing technologies and privacy management, access control models, trust and reputation, security protocols and more.

Advances in Computers

PCI Compliance

Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems

Wireless Network Security

Wireless Security

Handbook of Research on Wireless Security

Wireless communications have become indispensable part of our lives. The book deals with the security of such wireless communication. The technological background of these applications have been presented in detail. Special emphasis has been laid on the IEEE 802.11x-standards that have been developed for this technology. A major part of the book is devoted to security risks, encryption and authentication. Checklists have been provided to help IT administrators and security officers to achieve the maximum possible security in their installations, when using wireless technology. This is the second edition of the book. The updates include the latest the IEEE 802.11-standard, an updated chapter on PDA, the increased relevance of smart phones and tablets, widespread use of WLAN with increased security risks.

Wireless Network Security Theories and Applications discusses the relevant security technologies, vulnerabilities, and potential threats, and introduces the corresponding security standards and protocols, as well as provides solutions to security concerns. Authors of each chapter in this book, mostly top researchers in relevant research fields in the U.S. and China, presented their research findings and results about the security of the following types of wireless networks: Wireless Cellular Networks, Wireless Local Area Networks (WLANs), Wireless Metropolitan Area Networks (WMANs), Bluetooth Networks and Communications, Vehicular Ad Hoc Networks (VANETs), Wireless Sensor Networks (WSNs), Wireless Mesh Networks (WMNs), and Radio Frequency Identification (RFID). The audience of this book may include professors, researchers, graduate students, and professionals in the areas of Wireless Networks, Network Security and Information Security, Information Privacy and Assurance, as well as Digital Forensics. Lei Chen is an Assistant Professor at Sam Houston State University, USA; Jiahuang Ji is an Associate Professor at Sam Houston State University, USA; Zihong Zhang is a Sr. software engineer at Jacobs Technology, USA under NASA contract.

This book constitutes the proceedings of the First International Conferences on e-Technologies and Networks for Development, ICeND 2011, held in Dar-es-Salaam, Tanzania, in August 2011. The 29 revised full papers presented were carefully reviewed and selected from 90 initial submissions. The papers address new advances in the internet technologies, networking, e-learning, software applications, Computer Systems, and digital information and data communications technologies - as well technical as practical aspects.

The "Encyclopedia of Mobile Computing and Commerce" presents current trends in mobile computing and their commercial applications. Hundreds of internationally renowned scholars and practitioners have written comprehensive articles exploring such topics as location and context awareness, mobile networks, mobile services, the socio impact of mobile technology, and mobile software engineering.

Software Development

Encyclopedia of Internet Technologies and Applications

Forensics in Telecommunications, Information and Multimedia

ITCS & IRoA 2011

Theory and Practical Applications

The Industrial Electronics Handbook, Second Edition, Industrial Communications Systems combines traditional and newer, more specialized knowledge that helps industrial electronics engineers develop practical solutions for the design and implementation of high-power applications. Embracing the broad technological scope of the field, this collection explores fundamental areas, including analog and digital circuits, electronics, electromagnetic machines, signal processing, and industrial control and communications systems. It also facilitates the use of intelligent systems—such as neural networks, fuzzy systems, and evolutionary methods—in terms of a hierarchical structure that makes factory control and supervision more efficient by addressing the needs of all production components. Enhancing its value, this fully updated collection presents research and global trends as published in the IEEE Transactions on Industrial Electronics Journal, one of the largest and most respected publications in the field. Modern communication systems in factories use many different—and increasingly sophisticated—systems to send and receive information. Industrial Communication Systems spans the full gamut of concepts that engineers require to maintain a well-designed, reliable communications system that can ensure successful operation of any production process. Delving into the subject, this volume covers: Technical principles Application-specific areas Technologies Internet programming Outlook, including trends and expected challenges Other volumes in the set: Fundamentals of Industrial Electronics Power Electronics and Motor Drives Control and Mechatronics Intelligent Systems

Provides the most thorough examination of Internet technologies and applications for researchers in a variety of related fields. For the average Internet consumer, as well as for experts in the field of networking and Internet technologies.

The author describes real-life cases of computer crimes and investigations.

Essentials of Short-Range WirelessCambridge University Press

IT Convergence and Services

Wi-Fi Protected Access and 802.11i

Hacking Exposed Wireless

Second Edition

e-Technologies and Networks for Development

Hacking Exposed Cisco Networks

Provides information on how to prevent, detect, and mitigate a security attack that comes from within a company.

Here is the first book to focus solely on Cisco network hacking, security auditing, and defense issues. Using the proven Hacking Exposed methodology, this book shows you how to locate and patch system vulnerabilities by looking at your Cisco network through the eyes of a hacker. The book covers device-specific and network-centered attacks and defenses and offers real-world case studies.

The Wireless Security Handbook provides a well-rounded overview of wireless network security. It examines wireless from multiple perspectives, including those of an auditor, security architect, and hacker. This wide scope benefits anyone who has to administer, secure, hack, or conduct business on a wireless network. This text tackles wirele

From a leader in the field, the first book on how to build privacy safeguards into web sites and applications, a topic of growing importance.

Cryptography and Network Security

Wireless Security Handbook

Security of Mobile Communications

EBOOK: Mobile and Wireless Communications: An Introduction

An end-to-end reference guide to design, deploy, manage, and secure 802.11 wireless networks

High-tech Crimes Revealed

This book has been written keeping in mind syllabi of all Indian universities and optimized the contents of the book accordingly. These students are the book's primary audience. Cryptographic concepts are explained using diagrams to illustrate component relationships and data flows. At every step aim is to examine the relationship between the security measures and the vulnerabilities they address. This will guide readers in safely applying cryptographic techniques. This book is also intended for people who know very little about cryptography but need to make technical decisions about cryptographic security. many people face this situation when they need to transmit business data safely over the Internet. This often includes people responsible for the data, like business analysts and managers. as well as those who must install and maintain the protections, like information systems administrators and managers. This book requires no prior knowledge of cryptography or related mathematics. Descriptions of low-level crypto mechanisms focus on presenting the concepts instead of the details. This book is intended as a reference book for professional cryptographers, presenting the techniques and algorithms of greatest interest of the current practitioner, along with the supporting motivation and background material. It also provides a comprehensive source from which to learn cryptography, serving both students and instructors. In addition, the rigorous treatment, breadth, and extensive bibliographic material should make it an important reference for research professionals. While composing this book my intention was not to introduce a collection of new techniques and protocols, but rather to selectively present techniques from those currently available in the public domain.

A comprehensive handbook for computer security professionals explains how to identify and assess network vulnerabilities and furnishes a broad spectrum of advanced methodologies, solutions, and security tools to defend one's system against sophisticated hackers and provide a secure network infrastructure. Original. (Advanced)

This book deals with the philosophy, strategy and tactics of soliciting, managing and conducting information security audits of all flavours. It will give readers the founding principles around information security assessments and why they are important, whilst providing a fluid framework for developing an astute 'information security mind' capable of rapid adaptation to evolving technologies, markets, regulations, and laws.

Controller-Based Wireless LAN Fundamentals

Murder is Final