Wi Foo The Secrets Of Wireless Hacking

RAY WALSH

PCI Compliance Addison-Wesley Professional
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.
Encyclopedia of Internet Technologies and Applications Springer Science & Business Media
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.

Wi-Foo Cambridge University Press
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.
EBOOK: Mobile and Wireless Communications: An Introduction CRC Press
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.
PCI Compliance IGI Global
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.
Industrial Communication Systems Pearson Education
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.
Hacking Exposed Cisco Networks Elsevier
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.
Essentials of Short-Range Wireless Addison-Wesley Professional
Provides information on how to prevent, detect, and mitigate a security attack that comes from within a company.
Murder is Final Lulu.com
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.
Extrusion Detection Springer Science & Business Media
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.
Wireless Network Security Essentials of Short-Range Wireless
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.
Wireless and Mobile Network Security Elsevier
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
Computerworld McGraw Hill Professional
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)
Industrial Network Security Elsevier
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.
Family Secrets IGI Global
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
e-Technologies and Networks for Development John Wiley & Sons
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.
Wireless Network Security Springer
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
Wireless Security CRC Press
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

Embedded Systems and Wireless Technology WIT Press
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
Dr. Dobb's Journal Springer Science & Business Media
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.