Recent Ieee Paper For Bluejacking

As recognized, adventure as competently as experience not quite lesson, amusement, as well as deal can be gotten by just checking out a book **Recent Ieee Paper For Bluejacking** next it is not directly done, you could receive even more nearly this life, roughly speaking the world.

We pay for you this proper as well as simple mannerism to acquire those all. We allow Recent Ieee Paper For Bluejacking and numerous ebook collections from fictions to scientific research in any way. accompanied by them is this Recent Ieee Paper For Bluejacking that can be your partner.

eMarketing eXcellence - PR Smith 2012-10-12
'eMarketing eXcellence' offers an exciting new approach to help you build a customer-driven e-business. As the core text for the CIM's E-marketing award, the book offers a highly structured and accessible guide to a critical subject, providing a useful reference point for all students and managers involved in marketing strategy and implementation. A practical guide to creating and executing e-marketing plans, this book combines established approaches to marketing planning with the creative use of new e-models and e-tools. It is designed to support both marketers who are integrating e-marketing into their existing marketing and communications strategies and experienced e-marketers looking to optimise their e-marketing. The book shows how to: · Draw up an outline e-marketing plan · Evaluate and apply e-marketing principles & models · Integrate online and offline communications · Implement customer-driven e-marketing · Reduce costly trial and error · Measure and enhance your e-marketing · Drive your e-business forward As the core text for the CIM's new professional E-marketing Award, it provides comprehensive, critical coverage of the key areas of e-marketing planning for marketing professionals. Established marketing concepts such as customer relationship management, the marketing mix and the widely adopted SOSTAC® planning system, are re-examined in the new media context - and new approaches are defined, including business models, traffic building and web site design.

Security in Wireless Communication Networks - Yi Qian 2021-12-01
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.

Hacking Exposed Wireless - Johnny Cache 2007-04-10
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

Web and Communication Technologies and Internet-Related Social Issues - HSI 2005 - Shinji Shimojo 2005-08-25
The Internet has now become an integral part of everyday life for hundreds of millions of people around the world. The uses of the Internet have augmented commerce, communication, education, governance, entertainment, health care, etc. E-mail has become an indispensable part of life; the Web has become an indispensable source of information on just about everything; people now use governmentWebsitestoreceiveinstructionsandinformation,and?lepaperwork with the government; many major online businesses have been created, such as Amazon, eBay, Google, Travelocity, eTrade, etc. However, the uses of the Internet have also had serious negative e?ects, - cluding spam, the spreading of viruses and worms, spyware, phishing, hacking, online fraud, invasions of privacy, etc. Viruses and worms often bring down tens of millions of computers around the world; many people get duped into furni- ing their personal identi?cations, and bank and insurance account information, etc. ; hackers break into government and corporation computers to steal cri- cal data; unsubstantiated rumors about individuals or organizations spread like wild?re on the Internet, etc. Further, the uses of the Internet are creating new paradigms in areas such as copyright, governance, etc. The widespread use of peer-to-peer ?le sharing systems, started by Napster,is forcing a reassessment of the value of holding copyright on digital media. Internet postings by vocal citizens to the Web sites of the news media, governmento?ces, and elected g- ernment o?cials are impacting government policies and swaying the opinions of other citizens. The aim of the International Conference on Human.

CompTIA Security+ Study Guide - Emmett Dulaney 2017-10-05
Some copies of CompTIA Security+ Study Guide: Exam SY0-501 (9781119416876) were printed without discount exam vouchers in the front of the books. If you did not receive a discount exam voucher with your book, please visit http://media.wiley.com/product_ancillary/5X/11194168/DOWNLOAD/CompTIA_Coupon.pdf to download one. Expert preparation covering 100% of Security+ exam SY0-501 objectives CompTIA Security+ Study Guide, Seventh Edition offers invaluable preparation for Exam SY0-501. Written by an expert author team, this book covers 100% of the exam objectives with clear, concise explanation. You'll learn how to handle threats, attacks, and vulnerabilities using industry-standard tools and technologies, while understanding the role of architecture and design. From everyday tasks like identity and access management to complex topics like risk management and cryptography, this study guide helps you consolidate your knowledge base in preparation for the Security+ exam. Practical examples illustrate how these processes play out in real-world scenarios, allowing you to immediately translate essential concepts to on-

the-job application. You also gain access to the Sybex online learning environment, which features a robust toolkit for more thorough prep: flashcards, glossary of key terms, practice questions, and a pre-assessment exam equip you with everything you need to enter the exam confident in your skill set. This study guide is approved and endorsed by CompTIA, and has been fully updated to align with the latest version of the exam. Master essential security technologies, tools, and tasks Understand how Security+ concepts are applied in the real world Study on the go with electronic flashcards and more Test your knowledge along the way with hundreds of practice questions To an employer, the CompTIA Security+ certification proves that you have the knowledge base and skill set to secure applications, devices, and networks; analyze and respond to threats; participate in risk mitigation, and so much more. As data threats loom larger every day, the demand for qualified security professionals will only continue to grow. If you're ready to take the first step toward a rewarding career, CompTIA Security+ Study Guide, Seventh Edition is the ideal companion for thorough exam preparation.

Bluetooth Revealed - Brent A. Miller 2001

PLEASE PROVIDE COURSE INFORMATION PLEASE PROVIDE

IoT Security - Madhusanka Liyanage 2019-12-24

An up-to-date guide to an overview of authentication in the Internet of Things (IoT) The Internet of things (IoT) is the network of the countless physical devices that have the possibility to connect and exchange data. Among the various security requirements, authentication to the IoT is the first step to prevent the impact of attackers. IoT Security offers an important guide into the development of the many authentication mechanisms that provide IoT authentication at various levels such as user level, device level and network level. The book covers a wide range of topics including an overview of IoT and addresses in detail the security challenges at every layer by considering both the technologies and the architecture used. The authors—noted experts on the topic—provide solutions for remediation of compromised security, as well as methods for risk mitigation, and offer suggestions for prevention and improvement. In addition, IoT Security offers a variety of illustrative use cases. This important book: Offers an authoritative reference designed for use by all IoT stakeholders Includes information for securing devices at the user, device, and network levels Contains a classification of existing vulnerabilities Written by an international group of experts on the topic Provides a guide to the most current information available on IoT security Written for network operators, cloud operators, IoT device manufacturers, IoT device users, wireless users, IoT standardization organizations, and security solution developers, IoT Security is an essential guide that contains information on security features, including underlying networks, architectures, and security requirements.

Aspects of Network and Information Security - NATO Science for Peace and Security Programme 2008-06-24

Network security is concerned with creating a secure inter-connected network that is designed so that on the one hand, users cannot perform actions that they are not allowed to perform, but on the other hand, can perform the actions that they are allowed to. Network security not only involves specifying and implementing a security policy that describes access control, but also implementing an Intrusion Detection System as a tool for detecting attempted attacks or intrusions by crackers or automated attack tools and identifying security breaches such as incoming shellcode, viruses, worms, malware and trojan horses transmitted via a computer system or network. Today’s computer infrastructure is exposed to several kinds of security threats ranging from virus attacks, unauthorised data access, sniffing and password cracking. Understanding network vulnerabilities in order to protect networks from external and internal threats is vital to the world’s economy and should be given the highest priority. Computer and network security involves many important and complicated issues and this gathering of scientists will help not only in raising awareness but also in teaching participants the state-of-the-art of security techniques. Topics in network security, information security and coding are discussed in this volume.

Fundamentals of Mobile and Pervasive

Computing - Frank Adelstein 2005-01-20
The authoritative, general reference that has been sorely missing in the field of mobile computing This book teaches all the main topics via the hottest applications in a rapidlygrowing field. "Big picture" explanations of ad hoc networks and service discovery Exercises, projects, and solutions to illustrate core concepts Extensive wireless security methodologies
Proceedings of ... IEEE International Symposium on Consumer Electronics - 2004

Computational Intelligence Methods in COVID-19: Surveillance, Prevention, Prediction and Diagnosis - Khalid Raza 2020-10-16
The novel coronavirus disease 2019 (COVID-19) pandemic has posed a major threat to human life and health. This book is beneficial for interdisciplinary students, researchers, and professionals to understand COVID-19 and how computational intelligence can be used for the purpose of surveillance, control, prevention, prediction, diagnosis, and potential treatment of the disease. The book contains different aspects of COVID-19 that includes fundamental knowledge, epidemic forecast models, surveillance and tracking systems, IoT- and IoMT-based integrated systems for COVID-19, social network analysis systems for COVID-19, radiological images (CT, X-ray) based diagnosis system, and computational intelligence and in silico drug design and drug repurposing methods against COVID-19 patients. The contributing authors of this volume are experts in their fields and they are from various reputed universities and institutions across the world. This volume is a valuable and comprehensive resource for computer and data scientists, epidemiologists, radiologists, doctors, clinicians, pharmaceutical professionals, along with graduate and research students of interdisciplinary and multidisciplinary sciences.
CompTIA Network+ N10-007 Cert Guide - Anthony J. Sequeira 2018-02-12
This is the eBook version of the print title. Note that only the Amazon Kindle version or the Premium Edition eBook and Practice Test available on the Pearson IT Certification web site come with the unique access code that allows you to use the practice test software that accompanies this book. All other eBook versions do not provide access to the practice test software that accompanies the print book. Access to the companion web site is available through product registration at Pearson IT Certification; or see instructions in back pages of your eBook. Learn, prepare, and practice for CompTIA Network+ N10-007 exam success with this CompTIA approved Cert Guide from Pearson IT Certification, a leader in IT Certification learning and a CompTIA Authorized Platinum Partner. Master CompTIA Network+ N10-007 exam topics Assess your knowledge with chapter-ending quizzes Review key concepts with exam preparation tasks Practice with realistic exam questions Learn from more than 60 minutes of video mentoring CompTIA Network+ N10-007 Cert Guide is a best-of-breed exam study guide. Best-selling author and expert instructor Anthony Sequeira shares preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. The book presents you with an organized test preparation routine through the use of proven series elements and techniques. Exam topic lists make referencing easy. Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. Review questions help you assess your knowledge, and a final preparation chapter guides you through tools and resources to help you craft your final study plan. The companion website contains a host of tools to help you prepare for the exam, including: The powerful Pearson Test Prep practice test software, complete with hundreds of exam-realistic questions. The assessment engine offers you a wealth of customization options and reporting features, laying out a complete assessment of your knowledge to help you focus your study where it is needed most. More than 60 minutes of personal video mentoring 40 performance-based exercises to help you prepare for the performance-based questions on the exam The CompTIA Network+ N10-007 Hands-on Lab Simulator Lite software, complete with meaningful exercises that help you hone your

hands-on skills An interactive Exam Essentials appendix that quickly recaps all major chapter topics for easy reference A key terms glossary flash card application Memory table review exercises and answers A study planner to help you organize and optimize your study time A 10% exam discount voucher (a $27 value!) Well-regarded for its level of detail, assessment features, and challenging review questions and exercises, this CompTIA approved study guide helps you master the concepts and techniques that will enable you to succeed on the exam the first time. The CompTIA approved study guide helps you master all the topics on the Network+ exam, including: Computer networks and the OSI model Network components Ethernet IP addressing Routing traffic Wide Area Networks (WANs) Wireless Technologies Network performance Command-line utilities Network management Network policies and best practices Network security Troubleshooting Pearson Test Prep system requirements: Online: Browsers: Chrome version 40 and above; Firefox version 35 and above; Safari version 7; Internet Explorer 10, 11; Microsoft Edge; Opera. Devices: Desktop and laptop computers, tablets running on Android and iOS, smartphones with a minimum screen size of 4.7". Internet access required. Offline: Windows 10, Windows 8.1, Windows 7; Microsoft .NET Framework 4.5 Client; Pentium-class 1 GHz processor (or equivalent); 512 MB RAM; 650 MB disk space plus 50 MB for each downloaded practice exam; access to the Internet to register and download exam databases Lab Simulator Minimum System Requirements: Windows: Microsoft Windows 10, Windows 8.1, Windows 7 with SP1; Intel Pentium III or faster; 512 MB RAM (1GB recommended); 1.5 GB hard disk space; 32-bit color depth at 1024x768 resolution Mac: Apple macOS 10.13, 10.12, 10.11, 10.10; Intel Core Duo 1.83 Ghz or faster; 512 MB RAM (1 GB recommended); 1.5 GB hard disk space; 32-bit color depth at 1024x768 resolution Other applications installed during installation: Adobe AIR 3.8; Captive JRE 6

Foundations of Engineering Geology - Tony Waltham 2018-10-08

Now in full colour, the third edition of this well established book provides a readable and highly illustrated overview of the aspects of geology that are most significant to civil engineers. Sections in the book include those devoted to the main rock types, weathering, ground investigation, rock mass strength, failures of old mines, subsidence on peats and clays, sinkholes on limestone and chalk, water in landslides, slope stabilization and understanding ground conditions. The roles of both natural and man-induced processes are assessed, and this understanding is developed into an appreciation of the geological environments potentially hazardous to civil engineering and construction projects. For each style of difficult ground, available techniques of site investigation and remediation are reviewed and evaluated. Each topic is presented as a double page spread with a careful mix of text and diagrams, with tabulated reference material on parameters such as bearing strength of soils and rocks. This new edition has been comprehensively updated and covers the entire spectrum of topics of interest for both students and practitioners in the field of civil engineering.

Advances in Computer Science and Ubiquitous Computing - James J. (Jong Hyuk) Park 2016-12-01

This book presents the combined proceedings of the 8th International Conference on Computer Science and its Applications (CSA-16) and the 11st International Conference on Ubiquitous Information Technologies and Applications (CUTE 2016), both held in Bangkok, Thailand, December 19 - 21, 2016. The aim of these two meetings was to promote discussion and interaction among academics, researchers and professionals in the field of ubiquitous computing technologies. These proceedings reflect the state-of-the-art in the development of computational methods, involving theory, algorithm, numerical simulation, error and uncertainty analysis and novel application of new processing techniques in engineering, science, and other disciplines related to ubiquitous computing.

Web and Communication Technologies and Internet-related Social Issues--HSI. - 2005

Wireless Networking Technology - Stephen A. Rackley 2011-02-23

As the demand for higher bandwidth has lead to the development of increasingly complex

wireless technologies, an understanding of both wireless networking technologies and radio frequency (RF) principles is essential for implementing high performance and cost effective wireless networks. Wireless Networking Technology clearly explains the latest wireless technologies, covering all scales of wireless networking from personal (PAN) through local area (LAN) to metropolitan (MAN). Building on a comprehensive review of the underlying technologies, this practical guide contains 'how to' implementation information, including a case study that looks at the specific requirements for a voice over wireless LAN application. This invaluable resource will give engineers and managers all the necessary knowledge to design, implement and operate high performance wireless networks. · Explore in detail wireless networking technologies and understand the concepts behind RF propagation. · Gain the knowledge and skills required to install, use and troubleshoot wireless networks. · Learn how to address the problems involved in implementing a wireless network, including the impact of signal propagation on operating range, equipment inter-operability problems and many more. · Maximise the efficiency and security of your wireless network.

Energy-efficient Accelerated Curing of Concrete - Donald Wayne Pfeifer 1982-01-01

Ethical and Social Issues in the Information Age - Joseph M. Kizza 2013-03-09

An introduction to the social and policy issues which have arisen as a result of IT. Whilst it assumes a modest familiarity with computers, the book provides a guide to the issues suitable for undergraduates. In doing so, the author prompts students to consider questions such as: * How do morality and the law relate to each other? * What should be covered in a professional code of conduct for information technology professionals? * What are the ethical issues relating to copying software? * Is electronic monitoring o employees wrong? * What are the moral codes of cyberspace? Throughout, the book shows how in many ways the technological development is outpacing the ability of our legal systems, and how different paradigms applied to ethical questions often proffer conflicting conclusions. As a result, students will find this a thought-provoking and valuable survey of the new and difficult ethical questions posed by the Internet, artificial intelligence, and virtual reality.

Kali Linux Wireless Penetration Testing Cookbook - Sean-Philip Oriyano 2017-12-13

Over 60 powerful recipes to scan, exploit, and crack wireless networks for ethical purposes About This Book Expose wireless security threats through the eyes of an attacker, Recipes to help you proactively identify vulnerabilities and apply intelligent remediation, Acquire and apply key wireless pentesting skills used by industry experts Who This Book Is For If you are a security professional, administrator, and a network professional who wants to enhance their wireless penetration testing skills and knowledge then this book is for you. Some prior experience with networking security and concepts is expected. What You Will Learn Deploy and configure a wireless cyber lab that resembles an enterprise production environment Install Kali Linux 2017.3 on your laptop and configure the wireless adapter Learn the fundamentals of commonly used wireless penetration testing techniques Scan and enumerate Wireless LANs and access points Use vulnerability scanning techniques to reveal flaws and weaknesses Attack Access Points to gain access to critical networks In Detail More and more organizations are moving towards wireless networks, and Wi-Fi is a popular choice. The security of wireless networks is more important than ever before due to the widespread usage of Wi-Fi networks. This book contains recipes that will enable you to maximize the success of your wireless network testing using the advanced ethical hacking features of Kali Linux. This book will go through techniques associated with a wide range of wireless penetration tasks, including WLAN discovery scanning, WEP cracking, WPA/WPA2 cracking, attacking access point systems, operating system identification, vulnerability mapping, and validation of results. You will learn how to utilize the arsenal of tools available in Kali Linux to penetrate any wireless networking environment. You will also be shown how to identify remote services, how to assess security risks, and how various attacks are performed. By finishing the recipes, you will feel confident conducting wireless penetration tests

and will be able to protect yourself or your organization from wireless security threats. Style and approach The book will provide the foundation principles, techniques, and in-depth analysis to effectively master wireless penetration testing. It will aid you in understanding and mastering many of the most powerful and useful wireless testing techniques in the industry.

Smart Phone and Next Generation Mobile Computing - Pei Zheng 2010-07-19

This in-depth technical guide is an essential resource for anyone involved in the development of “smart mobile wireless technology, including devices, infrastructure, and applications. Written by researchers active in both academic and industry settings, it offers both a big-picture introduction to the topic and detailed insights into the technical details underlying all of the key trends. Smart Phone and Next-Generation Mobile Computing shows you how the field has evolved, its real and potential current capabilities, and the issues affecting its future direction. It lays a solid foundation for the decisions you face in your work, whether you’re a manager, engineer, designer, or entrepreneur. Covers the convergence of phone and PDA functionality on the terminal side, and the integration of different network types on the infrastructure side Compares existing and anticipated wireless technologies, focusing on 3G cellular networks and wireless LANs Evaluates terminal-side operating systems/programming environments, including Microsoft Windows Mobile, Palm OS, Symbian, J2ME, and Linux Considers the limitations of existing terminal designs and several pressing application design issues Explores challenges and possible solutions relating to the next phase of smart phone development, as it relates to services, devices, and networks Surveys a collection of promising applications, in areas ranging from gaming to law enforcement to financial processing

Software Development and Professional Practice - John Dooley 2011-10-13

Software Development and Professional Practice reveals how to design and code great software. What factors do you take into account? What makes a good design? What methods and processes are out there for designing software? Is designing small programs different than designing large ones? How can you tell a good design from a bad one? You'll learn the principles of good software design, and how to turn those principles back into great code. Software Development and Professional Practice is also about code construction—how to write great programs and make them work. What, you say? You've already written eight gazillion programs! Of course I know how to write code! Well, in this book you'll re-examine what you already do, and you'll investigate ways to improve. Using the Java language, you'll look deeply into coding standards, debugging, unit testing, modularity, and other characteristics of good programs. You'll also talk about reading code. How do you read code? What makes a program readable? Can good, readable code replace documentation? How much documentation do you really need? This book introduces you to software engineering—the application of engineering principles to the development of software. What are these engineering principles? First, all engineering efforts follow a defined process. So, you'll be spending a bit of time talking about how you run a software development project and the different phases of a project. Secondly, all engineering work has a basis in the application of science and mathematics to real-world problems. And so does software development! You'll therefore take the time to examine how to design and implement programs that solve specific problems. Finally, this book is also about human-computer interaction and user interface design issues. A poor user interface can ruin any desire to actually use a program; in this book, you'll figure out why and how to avoid those errors. Software Development and Professional Practice covers many of the topics described for the ACM Computing Curricula 2001 course C292c Software Development and Professional Practice. It is designed to be both a textbook and a manual for the working professional.

Wireless and Mobile Device Security - Jim Doherty 2021-03-31

Written by an industry expert, Wireless and Mobile Device Security explores the evolution of wired networks to wireless networking and its impact on the corporate world.

Build Your Own Security Lab - Michael Gregg

2010-08-13
If your job is to design or implement IT security solutions or if you're studying for any security certification, this is the how-to guide you've been looking for. Here's how to assess your needs, gather the tools, and create a controlled environment in which you can experiment, test, and develop the solutions that work. With liberal examples from real-world scenarios, it tells you exactly how to implement a strategy to secure your systems now and in the future. Note: CD-ROM/DVD and other supplementary materials are not included as part of eBook file.

Developing Practical Wireless Applications - Dean A. Gratton 2011-04-08
In a constant stream of new ideas, wireless technologies continue to emerge offering a range of capabilities, each affording simplicity and ease-of-use. Such diversity and choice should surely beg the question, "are manufacturers using the right technology for the right product? Developing Practical Wireless Applications will explore this question and, in doing so, will illustrate many of the wireless technologies currently available whilst drawing upon their individual strengths and weaknesses. More specifically, the book will draw your attention to the diverse collection of standardized and proprietary solutions available to manufacturers. As developers and innovators your choices are not restricted to any norm and, as such, a standardized or proprietary solution may afford you greater benefits in realising any product roadmap. Developing Practical Wireless Applications will provide you with a comprehensive understanding of how each technology works, coupled with an exploration into overlapping, complementary and competing technologies. In establishing this foundation, we will explore wireless applications in their context and address their suitability. In contrast, the book also considers the practicality of a wireless world in an attempt to better understand our audience and specific demographic groups. Coupled with a richer understanding of our consumers, along with our technology make-up we can indeed target wireless products more effectively. *Explores techniques used to attack wireless networks including WarXing, WarChalking, BlueJacking, and BlueSnarfing *Discusses applications utilizing ZigBee, NFC, RFID, Ultra-Wideband and WirelessUSB (WiMedia) *Details Bluetooth 2.x +EDR and introduces the v3.0 (BToverUWB) specification *Includes fundamental introductions to WiFi, namely 802.11i, 802.11p and 802.11n *Compares personal-area and wide-area communications including 3G, HSDPA, 4G, and WiMAX, as well as introducing Wireless Convergence

Webster's New World Hacker Dictionary - Bernadette Hlubik Schell 2006-09-05
The comprehensive hacker dictionary for security professionals, businesses, governments, legal professionals, and others dealing with cyberspace Hackers. Crackers. Phreakers. Black hats. White hats. Cybercrime. Logfiles. Anonymous Digital Cash. ARP Redirect. Cyberspace has a language all its own. Understanding it is vital if you're concerned about Internet security, national security, or even personal security. As recent events have proven, you don't have to own a computer to be the victim of cybercrime—crackers have accessed information in the records of large, respected organizations, institutions, and even the military. This is your guide to understanding hacker terminology. It's up to date and comprehensive, with: Clear, concise, and accurate definitions of more than 875 hacker terms Entries spanning key information-technology security concepts, organizations, case studies, laws, theories, and tools Entries covering general terms, legal terms, legal cases, and people Suggested further reading for definitions This unique book provides a chronology of hacker-related developments beginning with the advent of the computer and continuing through current events in what is identified as today's Fear of a Cyber-Apocalypse Era. An appendix entitled "How Do Hackers Break into Computers?" details some of the ways crackers access and steal information. Knowledge is power. With this dictionary, you're better equipped to be a white hat and guard against cybercrime.

Future Data and Security Engineering. Big Data, Security and Privacy, Smart City and Industry 4.0 Applications - Tran Khanh Dang 2021-11-13
This book constitutes the proceedings of the 8th International Conference on Future Data and Security Engineering, FDSE 2021, held in Ho

Chi Minh City, Vietnam, in November 2021.* The 28 full papers and 8 short were carefully reviewed and selected from 168 submissions. The selected papers are organized into the following topical headings: big data analytics and distributed systems; security and privacy engineering; industry 4.0 and smart city: data analytics and security; blockchain and access control; data analytics and healthcare systems; and short papers: security and data engineering. * The conference was held virtually due to the COVID-19 pandemic.

2016 3rd International Conference on Electronic Design (ICED) - IEEE Staff 2016-08-11

This conference will focus on future technologies, which cover Internet of Thing (IoT), Information and Communication Technology (ICT), green technology communication technology, electronic design, nanotechnology, biomedical e health technology, multimedia technology, mobile and wireless communication technologies, wireless sensor networks, system on chip (SOC) technology and embedded computing technology

Guide to Bluetooth Security - Karen Scarfone 2009-05-01

This document provides info. to organizations on the security capabilities of Bluetooth and provide recommendations to organizations employing Bluetooth technologies on securing them effectively. It discusses Bluetooth technologies and security capabilities in technical detail. This document assumes that the readers have at least some operating system, wireless networking, and security knowledge. Because of the constantly changing nature of the wireless security industry and the threats and vulnerabilities to the technologies, readers are strongly encouraged to take advantage of other resources (including those listed in this document) for more current and detailed information. Illustrations.

Guide to Network Security - Michael E. Whitman 2012-09-20

GUIDE TO NETWORK SECURITY is a wide-ranging new text that provides a detailed review of the network security field, including essential terminology, the history of the discipline, and practical techniques to manage implementation of network security solutions. It begins with an overview of information, network, and web security, emphasizing the role of data communications and encryption. The authors then explore network perimeter defense technologies and methods, including access controls, firewalls, VPNs, and intrusion detection systems, as well as applied cryptography in public key infrastructure, wireless security, and web commerce. The final section covers additional topics relevant for information security practitioners, such as assessing network security, professional careers in the field, and contingency planning. Perfect for both aspiring and active IT professionals, GUIDE TO NETWORK SECURITY is an ideal resource for students who want to help organizations protect critical information assets and secure their systems and networks, both by recognizing current threats and vulnerabilities, and by designing and developing the secure systems of the future. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

When Gadgets Betray Us - Robert Vamosi 2011-03-29

Technology is evolving faster than we are. As our mobile phones, mp3 players, cars, and digital cameras become more and more complex, we understand less and less about how they actually work and what personal details these gadgets might reveal about us. Robert Vamosi, an award-winning journalist and analyst who has been covering digital security issues for more than a decade, shows us the dark side of all that digital capability and convenience. Hotel-room TV remotes can be used to steal our account information and spy on what we've been watching, toll-booth transponders receive unencrypted EZ Pass or FasTrak info that can be stolen and cloned, and our cars monitor and store data about our driving habits that can be used in court against us. When Gadgets Betray Us gives us a glimpse into the secret lives of our gadgets and helps us to better understand -- and manage -- these very real risks.

Guidelines on Firewalls and Firewall Policy - Karen Scarfone 2010-03

This updated report provides an overview of firewall technology, and helps organizations plan for and implement effective firewalls. It explains

the technical features of firewalls, the types of firewalls that are available for implementation by organizations, and their security capabilities. Organizations are advised on the placement of firewalls within the network architecture, and on the selection, implementation, testing, and management of firewalls. Other issues covered in detail are the development of firewall policies, and recommendations on the types of network traffic that should be prohibited. The appendices contain helpful supporting material, including a glossary and lists of acronyms and abreviations; and listings of in-print and online resources. Illus.

A Dictionary of Information Security Terms, Abbreviations and Acronyms - 2007-03

This Dictionary is an invaluable resource for people grappling with security terminology for the first time. Rather than a dry technical dictionary, the book is written in an accessible style that enables managers and novices to quickly grasp the meaning of information security terms. Example definitions: 'Bluesnarfing an attack on a Bluetooth enabled device that allows download of all contact details along with other information without leaving any trace of the attack.' 'Digital certificate (sometimes called a Server ID) is an encrypted file that attests to the authenticity of the owner of a public key, used in public key encryption; the certificate is created by a trusted third party known as a certificate authority (CA). The digital certificate is proven to be authentic because it decrypts correctly using the public key of the CA.' 'Pharming Criminal activity resulting in users being redirected from entered, correct website address t

Certified Ethical Hacker (CEH) Foundation Guide - Sagar Ajay Rahalkar 2016-11-29

Prepare for the CEH training course and exam by gaining a solid foundation of knowledge of key fundamentals such as operating systems, databases, networking, programming, cloud, and virtualization. Based on this foundation, the book moves ahead with simple concepts from the hacking world. The Certified Ethical Hacker (CEH) Foundation Guide also takes you through various career paths available upon completion of the CEH course and also prepares you to face job interviews when applying as an ethical hacker. The book explains the concepts with the help of practical real-world scenarios and examples. You'll also work with hands-on exercises at the end of each chapter to get a feel of the subject. Thus this book would be a valuable resource to any individual planning to prepare for the CEH certification course. What You Will Learn Gain the basics of hacking (apps, wireless devices, and mobile platforms) Discover useful aspects of databases and operating systems from a hacking perspective Develop sharper programming and networking skills for the exam Explore the penetration testing life cycle Bypass security appliances like IDS, IPS, and honeypots Grasp the key concepts of cryptography Discover the career paths available after certification Revise key interview questions for a certified ethical hacker Who This Book Is For Beginners in the field of ethical hacking and information security, particularly those who are interested in the CEH course and certification.

Wireless Networks For Dummies - Barry D. Lewis 2004-10-27

You’ve probably heard the expression, “It’s timeto cut the cord.” Well, it may be time to “cut thecables” at your office and free yourself from your desk andcomputer. Wireless networks are the waves of thefuture—literally. Wireless Networks For Dummies guidesyou from design through implementation to ongoing protection ofyour system and your information so you can: Remain connected to the office in airports and hotels Access the Internet and other network resources in thelunchroom, conference room, or anywhere there’s an accesspoint Use your PDA or laptop to query your database from thewarehouse or the boardroom Check e-mail wirelessly when you’re on the road Get rid of the cable clutter in your office Wireless Networks For Dummies was coauthored by Barry D.Lewis, CISSP, and Peter T. Davis, who also coauthored ComputerSecurity For Dummies. Barry Lewis is president of aninformation security consulting firm and an internationally knownleader of security seminars. Peter Davis is founder of a firmspecializing in the security, audit, and control of information.Together, they cut through the cables, clutter, and confusion andhelp you: Get off to a quick start and get mobile with IrDA (InfraredData Association) and Bluetooth Perform a site survey and select the

right standard, mode,access point, channel and antenna Check online to verify degree of interoperability of devicesfrom various vendors Install clients and set up roaming Combat security threats such as war driving, jamming,hijacking, and man-in-the-middle attacks Implement security and controls such as MAC (Media AccessControl) and protocol filtering, WEP (Wireless Equivalent Privacy),WPA, (Wi-Fi Protected Access), EAP (Extensible AuthenticationProtocol), and VPN (Virtual Private Network) Set up multiple access points to form a larger wirelessnetwork Complete with suggestions of places to get connected, Web siteswhere you can get more information, tools you can use to monitorand improve security, and more, Wireless Networks ForDummies helps you pull the plug and go wireless!

The Official CompTIA Security+ Self-Paced Study Guide (Exam SY0-601) - CompTIA 2020-11-12

CompTIA Security+ Study Guide (Exam SY0-601)

Hack the Stack - Michael Gregg 2006-11-06

This book looks at network security in a new and refreshing way. It guides readers step-by-step through the "stack" -- the seven layers of a network. Each chapter focuses on one layer of the stack along with the attacks, vulnerabilities, and exploits that can be found at that layer. The book even includes a chapter on the mythical eighth layer: The people layer. This book is designed to offer readers a deeper understanding of many common vulnerabilities and the ways in which attacker’s exploit, manipulate, misuse, and abuse protocols and applications. The authors guide the readers through this process by using tools such as Ethereal (sniffer) and Snort (IDS). The sniffer is used to help readers understand how the protocols should work and what the various attacks are doing to break them. IDS is used to demonstrate the format of specific signatures and provide the reader with the skills needed to recognize and detect attacks when they occur. What makes this book unique is that it presents the material in a layer by layer approach which offers the readers a way to learn about exploits in a manner similar to which they most likely originally learned networking. This methodology makes this book a useful tool to not only security professionals but also for networking professionals, application programmers, and others. All of the primary protocols such as IP, ICMP, TCP are discussed but each from a security perspective. The authors convey the mindset of the attacker by examining how seemingly small flaws are often the catalyst of potential threats. The book considers the general kinds of things that may be monitored that would have alerted users of an attack. * Remember being a child and wanting to take something apart, like a phone, to see how it worked? This book is for you then as it details how specific hacker tools and techniques accomplish the things they do. * This book will not only give you knowledge of security tools but will provide you the ability to design more robust security solutions * Anyone can tell you what a tool does but this book shows you how the tool works

IEEE Membership Directory - Institute of Electrical and Electronics Engineers 2001

Wireless Network Security - Wolfgang Osterhage 2018-05-03

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.

Bluetooth Security Attacks - Keijo Haataja 2013-10-28

Bluetooth technology has enjoyed tremendous success, and it's now employed in billions of devices for short-range wireless data and real-time audio or video transfer. In this book the

authors provide an overview of Bluetooth security. They examine network vulnerabilities and provide a literature-review comparative analysis of recent security attacks. They analyze and explain related countermeasures, including one based on secure simple pairing, and they also propose a novel attack that works against all existing Bluetooth versions. They conclude with a discussion on future research directions. The book is appropriate for practitioners and researchers in information security, in particular those engaged in the design of networked and mobile devices.

CompTIA Security+ Guide to Network Security Fundamentals - Mark Ciampa 2017-10-20

Comprehensive, practical, and completely up to date, best-selling COMPTIA SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS, 6e, provides a thorough introduction to network and computer security that prepares you for professional certification and career success. Mapped to the new CompTIA Security+ SY0-501 Certification Exam, the text provides comprehensive coverage of all domain objectives. The sixth edition also includes expansive coverage of embedded device security, attacks and defenses, and the latest developments and trends in information security, including new software tools to assess security. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.