Usrp2 Documentation

CMOS Cellular Receiver Front-EndsSecurity and Privacy in Smart GridsSoftware Defined RadioImplementing Software Defined RadioPlatform Interference in Wireless SystemsSeven Deadliest Unified Communications AttacksIntroduction to Communication SystemsMobile Multimedia CommunicationsThe Mac Hacker's HandbookSeven Deadliest Wireless Technologies AttacksSoftware Defined RadioSoftware Defined Radio Using MATLAB & Simulink and the RTL-SDRWho Knew Patients Could Be This FunnyMicro Power SourcesFile Structures : An Object-Oriented Approach with C++, 3/eDigital Communication Systems Using MATLAB and SimulinkCognitive Radio Mobile Ad Hoc NetworksSelected Areas in Cryptography -- SAC 2013Modern Communications Jamming Principles and TechniquesObservation of the Earth and its EnvironmentHacking Exposed WirelessThe GENI BookSoftware Defined Radio2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge DiscoveryCognitive Radio-Oriented Wireless NetworksSeven Deadliest Social Network AttacksiOS Hacker's HandbookTask Scheduling for Parallel SystemsWhite Space CommunicationSeven Deadliest Microsoft AttacksGetting Started with OpenBTSThe Sparse Fourier TransformWireless Sensor NetworksSeven Deadliest Network AttacksInternet of Things (IoT)Cognitive Radio Oriented Wireless NetworksDigital CommunicationsSecurity of Ad-hoc and Sensor NetworksReal-Time SystemsKali Linux Wireless Penetration Testing: Beginner's Guide

CMOS Cellular Receiver Front-Ends

This book constitutes the thoroughly refereed conference proceedings of the 12th International Conference on Cognitive Radio Oriented Wireless Networks, CROWNCOM 2017, held in Lisbon, Portugal, in September 2017. The 28 revised full papers presented were carefully reviewed and selected from numerous submissions and cover the evolution of cognitive radio technology pertaining to 5G networks. The papers are clustered to topics on spectrum management; network management; trials, test beds, and tools; PHY and sensing; spectrum management.

Security and Privacy in Smart Grids

This book, edited by four of the leaders of the National Science Foundation’s Global Environment and Network Innovations (GENI) project, gives the reader a tour of the history, architecture, future, and applications of GENI. Built over the past decade by hundreds of leading computer scientists and engineers, GENI is a nationwide network used daily by thousands of computer scientists to explore the next Cloud and Internet and the applications and services they enable, which will transform our communities and our lives. Since by design it runs on existing computing and networking equipment and over the standard commodity Internet, it is poised for explosive growth and transformational impact over the next five years.

Over 70 of the builders of GENI have contributed to present its development, architecture, and implementation, both as a standalone US project and as a federated peer with similar projects worldwide, forming the core of a worldwide network. Applications and services enabled by GENI, from smarter cities to intensive collaboration to immersive education, are discussed. The book also explores the concepts and technologies that transform the Internet from a shared transport network to a collection of “slices” -- private, on-the-fly application-specific nationwide networks with guarantees of privacy and responsiveness. The reader will learn the motivation for building GENI and the experience of its precursor infrastructures, the architecture and implementation of the GENI infrastructure, its deployment across the United States and worldwide, the new network applications and services enabled by and running on the GENI infrastructure, and its international collaborations and extensions. This book is useful for academics in the networking and distributed systems areas, Chief Information Officers in the academic, private, and government sectors, and network and information architects.

Software Defined Radio

Seven Deadliest Network Attacks identifies seven classes of network attacks and discusses how the attack works, including tools to accomplish the attack, the risks of the attack, and how to defend against the attack. This book pinpoints the most dangerous hacks and exploits specific to networks, laying out the anatomy of these attacks including how to make your system more secure. You will discover the best ways to defend against these vicious hacks with step-by-step instruction and learn techniques to make your computer and network impenetrable. The book consists of seven chapters that deal with the following attacks: denial of service; war dialing; penetration testing; protocol tunneling; spanning tree attacks; man-in-the-middle; and password replay. These attacks are not mutually exclusive and were chosen because they help illustrate different aspects of network security. The principles on which they rely are unlikely to vanish any time soon, and they allow for the possibility of gaining something of interest to the attacker, from money to high-value data. This book is intended to provide practical, usable information. However, the world of network security is evolving very rapidly, and the attack that works today may (hopefully) not work tomorrow. It is more important, then, to understand the principles on which the attacks and exploits are based in order to properly plan either a network attack or a network defense. Seven Deadliest Network Attacks will appeal to information security professionals of all levels, network admins, and recreational hackers. Knowledge is power, find out about the most dominant attacks currently waging war on computers and networks globally Discover the best ways to defend against these vicious attacks; step-by-step instruction shows you how Institute countermeasures, don’t be caught defenseless again, and learn techniques to make your computer and network impenetrable

Implementing Software Defined Radio

An accessible undergraduate textbook introducing key fundamental principles behind modern communication systems, supported by exercises, software problems and lab exercises.

Platform Interference in Wireless Systems

Seven Deadliest Microsoft Attacks explores some of the deadliest attacks made against Microsoft software and networks and how these attacks can impact the confidentiality, integrity, and availability of the most closely guarded company secrets. If you need to keep up with the latest hacks, attacks, and exploits effecting Microsoft products, this book is for you. It pinpoints the most dangerous hacks and exploits specific to Microsoft applications, laying out the anatomy of these attacks including how to make your system more secure. You will discover the best ways to defend against these vicious hacks with step-by-step instruction and learn techniques to make your computer and network impenetrable. The book consists of seven chapters that cover the seven deadliest attacks against Microsoft software and networks: attacks against Windows passwords; escalation attacks; stored procedure attacks; mail service attacks; client-side ActiveX and macro attacks; Web service attacks; and multi-tier attacks. Each chapter provides an overview of a single Microsoft software product, how it is used, and some of the core functionality behind the software. Furthermore, each chapter explores the anatomy of attacks against the software, the dangers of an attack, and possible defenses to help prevent the attacks described in the scenarios. This book will be a valuable resource for those responsible for oversight of network security for either small or large organizations. It will also benefit those interested in learning the details behind attacks against Microsoft infrastructure, products, and services; and how to defend against them. Network administrators and integrators will find value in learning how attacks can be executed, and transfer knowledge gained from this book into improving existing deployment and integration practices. Windows Operating System-Password Attacks Active Directory-Escalation of Privilege SQL Server-Stored Procedure Attacks Exchange Server-Mail Service Attacks Office-Macros and ActiveX Internet Information Serives(IIS)-Web Serive Attacks SharePoint-Multi-tier Attacks

Seven Deadliest Unified Communications Attacks

As more and more vulnerabilities are found in the Mac OS X (Leopard) operating system, security researchers are realizing the importance of developing proof-of-concept exploits for those vulnerabilities. This unique tome is the first book to uncover the flaws in the Mac OS X operating system—and how to deal with them. Written by two white hat hackers, this book is aimed at making vital information known so that you can find ways to secure your Mac OS X systems, and examines the sorts of attacks that are prevented by Leopard’s security defenses, what attacks aren’t, and how to best handle those weaknesses.

Introduction to Communication Systems

Seven Deadliest Unified Communications Attacks provides a comprehensive coverage of the seven most dangerous hacks and exploits specific to Unified Communications (UC) and lays out the anatomy of these attacks including how to make your system more secure. You will discover the best ways to defend against these vicious hacks with step-by-step instruction and learn techniques to make your computer and network impenetrable. The book describes the intersection of the various communication technologies that make up UC, including Voice over IP (VoIP), instant message (IM), and other collaboration technologies. There are seven chapters that focus on the following: attacks against the UC ecosystem and UC endpoints; eavesdropping and modification attacks; control channel attacks; attacks on Session Initiation Protocol (SIP) trunks and public switched telephone network (PSTN) interconnection; attacks on identity; and attacks against distributed systems. Each chapter begins with an introduction to the threat along with some examples of the problem. This is followed by discussions of the anatomy, dangers, and future outlook of the threat as well as specific strategies on how to defend systems against the threat. The discussions of each threat are also organized around the themes of confidentiality, integrity, and availability. This book will be of interest to information security professionals of all levels as well as recreational hackers. Knowledge is power, find out about the most dominant attacks currently waging war on computers and networks globally Discover the best ways to defend against these vicious attacks; step-by-step instruction shows you how Institute countermeasures, don’t be caught defenseless again, and learn techniques to make your computer and network impenetrable

Mobile Multimedia Communications

The following listing represents a survey and a short description of 'Earth Observing Mis sions' in alphabetical order. The listing in Part A considers completed-, operational-as well as planned missions on an international scale (Earth observations from space know no na tional boundaries). A look into past activities is important for reasons of heritage, context and of perspective. The document is intended for all who want to keep track of missions and sensors in the fast -growing field of Earth observations. There cannot be any claim to com pleteness, although a considerable effort was made to collect and integrate all known mis sions and sensors into this book. Earth observation by remote sensing changes our view and perception of the world. We be gin to realize the global character of remote sensing, its multidimensional and complemen tary nature, its vast potential to many disciplines, its importance to mankind as a whole. Re mote sensing permits for the first time in history a total system view of the Earth. The view from space toward Earth has brought about sweeping revisions in the Earth sciences, in par ticular in such fields as meteorology, oceanology, hydrology, geology, geography, forestry, agriculture, geodynamics, solar-terrestrial interactions, and many others.

The Mac Hacker's Handbook

The availability of the RTL-SDR device for less than $20 brings software defined radio (SDR) to the home and work desktops of EE students, professional engineers and the maker community. The RTL-SDR can be used to acquire and sample RF (radio frequency) signals transmitted in the frequency range 25MHz to 1.75GHz, and the MATLAB and Simulink environment can be used to develop receivers using first principles DSP (digital signal processing) algorithms. Signals that the RTL-SDR hardware can receive include: FM radio, UHF band signals, ISM signals, GSM, 3G and LTE mobile radio, GPS and satellite signals, and any that the reader can (legally) transmit of course! In this book we introduce readers to SDR methods by viewing and analysing downconverted RF signals in the time and frequency domains, and then provide extensive DSP enabled SDR design exercises which the reader can learn from. The hands-on SDR design examples begin with simple AM and FM receivers, and move on to the more challenging aspects of PHY layer DSP, where receive filter chains, real-time channelisers, and advanced concepts such as carrier synchronisers, digital PLL designs and QPSK timing and phase synchronisers are implemented. In the book we will also show how the RTL-SDR can be used with SDR transmitters to develop complete communication systems, capable of transmitting payloads such as simple text strings, images and audio across the lab desktop.

Seven Deadliest Wireless Technologies Attacks

The Fourier transform is one of the most fundamental tools for computing the frequency representation of signals. It plays a central role in signal processing, communications, audio and video compression, medical imaging, genomics, astronomy, as well as many other areas. Because of its widespread use, fast algorithms for computing the Fourier transform can benefit a large number of applications. The fastest algorithm for computing the Fourier transform is the Fast Fourier Transform (FFT), which runs in near-linear time making it an indispensable tool for many applications. However, today, the runtime of the FFT algorithm is no longer fast enough especially for big data problems where each dataset can be few terabytes. Hence, faster algorithms that run in sublinear time, i.e., do not even sample all the data points, have become necessary. This book addresses the above problem by developing the Sparse Fourier Transform algorithms and building practical systems that use these algorithms to solve key problems in six different applications: wireless networks; mobile systems; computer graphics; medical imaging; biochemistry; and digital circuits. This is a revised version of the thesis that won the 2016 ACM Doctoral Dissertation Award.

Software Defined Radio

Software Defined Radio makes wireless communications easier, more efficient, and more reliable. This book bridges the gap

between academic research and practical implementation. When beginning a project, practicing engineers, technical managers, and graduate students can save countless hours by considering the concepts presented in these pages. The author covers the myriad options and trade-offs available when selecting an appropriate hardware architecture. As demonstrated here, the choice between hardware- and software-centric architecture can mean the difference between meeting an aggressive schedule and bogging down in endless design iterations. Because of the author's experience overseeing dozens of failed and successful developments, he is able to present many real-life examples. Some of the key concepts covered are: Choosing the right architecture for the market – laboratory, military, or commercial, Hardware platforms – FPGAs, GPPs, specialized and hybrid devices, Standardization efforts to ensure interoperability and portabilitym State-of-the-art components for radio frequency, mixed-signal, and baseband processing. The text requires only minimal knowledge of wireless communications; whenever possible, qualitative arguments are used instead of equations. An appendix provides a quick overview of wireless communications and introduces most of the concepts the readers will need to take advantage of the material. An essential introduction to SDR, this book is sure to be an invaluable addition to any technical bookshelf.

Software Defined Radio Using MATLAB & Simulink and the RTL-SDR

The papers included in this issue of ECS Transactions were originally presented in the symposium ¿Micro Power Sources¿, held during the PRiME 2008 joint international meeting of The Electrochemical Society and The Electrochemical Society of Japan, with the technical cosponsorship of the Japan Society of Applied Physics, the Korean Electrochemical Society, the Electrochemistry Division of the Royal Australian Chemical Institute, and the Chinese Society of Electrochemistry. This meeting was held in Honolulu, Hawaii, from October 12 to 17, 2008.

Who Knew Patients Could Be This Funny

Micro Power Sources

Software defined radio (SDR) is a hot topic in the telecommunications field, with regard to wireless technology. It is one of the most important topics of research in the area of mobile and personal communications. SDR is viewed as the enabler of global roaming and a platform for the introduction of new technologies and services into existing live networks. It therefore gives networks a greater flexibility into mobile communications. It bridges the inter-disciplinary gap in the field as SDR covers two areas of development, namely software development and digital signal processing and the internet. It extends well beyond the simple re-configuration of air interface parameters to cover the whole system from the network to service

creation and application development. Reconfigurability entails the pervasive use of software reconfiguration, empowering upgrades or patching of any element of the network and of the services and applications running on it. It cuts across the types of bearer radio systems (Paging to cellular, wireless local area network to microwave, terrestrial to satellite, personal communications to broadcasting) enable the integration of many of today's disparate systems in the same hardware platform. Also it cuts across generation (second to third to fourth). This volume complements the already published volumes 1 and 2 of the Wiley Series in Software Radio. The book discusses the requirements for reconfigurability and then introduces network architectures and functions for reconfigurable terminals. Finally it deals with reconfiguration in the network. The book also provides a comprehensive view on reconfigurability in three very active research projects as CAST, MOBIVAS and TRUST/SCOUT. Key features include: Presents new research in wireless communications Summarises the results of an extensive research program on software defined radios in Europe Provides a comprehensive view on reconfigurability in three very active research projects as CAST (Configurable radio with Advanced Sodftware Technology), MOBIVAS (Downloadable MOBIle Value Added Services through Software Radio and Switching Integrated Platforms), TRUST (Transparently Re-configurable Ubiquitous Terminal) and SCOUT (Smart User-Centric Communciation Environment).

File Structures : An Object-Oriented Approach with C++, 3/e

Digital Communication using MATLAB and Simulink is intended for a broad audience. For the student taking a traditional course, the text provides simulations of the MATLAB and Simulink systems, and the opportunity to go beyond the lecture or laboratory and develop investigations and projects. For the professional, the text facilitates an expansive review of and experience with the tenets of digital communication systems.

Digital Communication Systems Using MATLAB and Simulink

Software defined radio (SDR) is one of the most important topics of research, and indeed development, in the area of mobile and personal communications. SDR is viewed as an enabler of global roaming and as a unique platform for the rapid introduction of new services into existing live networks. It therefore promises mobile communication networks a major increase in flexibility and capability. SDR brings together two key technologies of the last decade - digital radio and downloadable software. It encompasses not only reconfiguration of the air interface parameters of handset and basestation products but also the whole mobile network, to facilitate the dynamic introduction of new functionality and mass-customised applications to the user's terminal, post-purchase. This edited book, contributed by internationally respected researchers and industry practitioners, describes the current technological status of radio frequency design, data conversion, reconfigurable signal processing hardware, and software issues at all levels of the protocol stack and network. The book provides a holistic treatment of SDR addressing the full breadth of relevant technologies - radio frequency design,

signal processing and software - at all levels. As such it provides a solid grounding for a new generation of wireless engineers for whom radio design in future will assume dynamic flexibility as a given. In particular it explores * The unique demands of SDR upon the RF subsystem and their implications for front end design methodologies * The recent concepts of the 'digital front end' and 'parametrization' * The role and key influence of data conversion technologies and devices within software radio, essential to robust product design * The evolution of signal processing technologies, describing new architectural approaches * Requirements and options for software download * Advances in 'soft' protocols and 'on-the-fly' software reconfiguration * Management of terminal reconfiguration and its network implications * The concepts of the waveform description language The book also includes coverage of * Potential breakthrough technologies, such as superconducting RSFQ technology and the possible future role of MEMS in RF circuitry * Competing approaches, eg all-software radios implemented on commodity computing vs advanced processing architectures that dynamically optimise their configuration to match the algorithm requirements at a point in time The book opens with an introductory chapter by Stephen Blust, Chair of the ITU-R WP8F Committee and Chair of the SDR Forum presenting a framework for SDR, in terms of definitions, evolutionary perspectives, introductory timescales and regulation. Suitable for today's engineers, technical staff and researchers within the wireless industry, the book will also appeal to marketing and commercial managers who need to understand the basics and potential of the technology for future product development. Its balance of industrial and academic contributors also makes it suitable as a text for graduate and post-graduate courses aiming to prepare the next generation of wireless engineers.

Cognitive Radio Mobile Ad Hoc Networks

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

Selected Areas in Cryptography -- SAC 2013

Discover all the security risks and exploits that can threateniOS-based mobile devices iOS is Apple's mobile operating system for the iPhone and iPad.With the introduction of iOS5, many security issues have come tolight. This book explains and discusses them all. The award-winningauthor team, experts in Mac and iOS security, examines thevulnerabilities and the internals of iOS to show how attacks can bemitigated. The book explains how the operating system works, itsoverall security architecture, and the security risks associatedwith it, as well as exploits, rootkits, and other payloadsdeveloped for it. Covers iOS security architecture, vulnerability hunting,exploit writing, and how iOS jailbreaks work Explores iOS enterprise and encryption, code signing and memoryprotection, sandboxing, iPhone fuzzing, exploitation, ROP payloads,and baseband attacks Also examines kernel debugging and exploitation Companion website includes source code and tools to facilitateyour efforts iOS Hacker's Handbook arms you with the tools needed toidentify, understand, and foil iOS attacks.

Modern Communications Jamming Principles and Techniques

Seven Deadliest Social Network Attacks describes the seven deadliest social networking attacks and how to defend against them. This book pinpoints the most dangerous hacks and exploits specific to social networks like Facebook, Twitter, and MySpace, and provides a comprehensive view into how such attacks have impacted the livelihood and lives of adults and children. It lays out the anatomy of these attacks, including how to make your system more secure. You will discover the best ways to defend against these vicious hacks with step-by-step instruction and learn techniques to make your computer and network impenetrable. The book is separated into seven chapters, with each focusing on a specific type of attack that has been furthered with social networking tools and devices. These are: social networking infrastructure attacks; malware attacks; phishing attacks; Evil Twin Attacks; identity theft; cyberbullying; and physical threat. Each chapter takes readers through a detailed overview of a particular attack to demonstrate how it was used, what was accomplished as a result, and the ensuing consequences. In addition to analyzing the anatomy of the attacks, the book offers insights into how to develop mitigation strategies, including forecasts of where these types of attacks are heading. This book can serve as a reference guide to anyone who is or will be involved in oversight roles within the information security field. It will also benefit those involved or interested in providing defense mechanisms surrounding social media as well as information security professionals at all levels, those in the teaching profession, and recreational hackers. Knowledge is power, find out about the most dominant attacks currently waging war on computers and networks globally Discover the best ways to defend against these vicious attacks; step-by-step instruction shows you how Institute countermeasures, don’t be caught defenseless again, and learn techniques to make your computer and network impenetrable

Observation of the Earth and its Environment

Funny Things Patients Say This handy size journal has given you plenty of room to write down all the funny, amusing or moving quotes and sayings that you will love to record and remember your patients by. This beautifully made and bound notebook has a unique and amusing design with a blank page in-between to stop any ink bleed or impression damage. This also gives you extra room for your own comments, thoughts and memories. Product Description: 6"x.9" 112 pages Uniquely designed cover High quality, white paper Matte cover Check out our other great notebooks and journals, by clicking on the "Author Name" link just below the title of this journal. Other Ideas On Who Would Love This Notebook Best Friends Gift Anniversary Gift Wedding Gift Graduation Gift End of School Year Gift Ideal for Nurse Week Gift Thank You Nurse Gift Nurse Appreciation Gift Scroll up and Look Inside and then Click BUY NOW to get this great Notebook TODAY

Hacking Exposed Wireless

The GENI Book

This monograph presents a collection of major developments leading toward the implementation of white space technology - an emerging wireless standard for using wireless spectrum in locations where it is unused by licensed users. Some of the key research areas in the field are covered. These include emerging standards, technical insights from early pilots and simulations, software defined radio platforms, geo-location spectrum databases and current white space spectrum usage in India and South Africa.

Software Defined Radio

Deploy your own private mobile network with OpenBTS, the open source software project that converts between the GSM and UMTS wireless radio interface and open IP protocols. With this hands-on, step-by-step guide, you'll learn how to use OpenBTS to construct simple, flexible, and inexpensive mobile networks with software. OpenBTS can distribute any internet connection as a mobile network across a large geographic region, and provide connectivity to remote devices in the Internet of Things. Ideal for telecom and software engineers new to this technology, this book helps you build a basic OpenBTS network with voice and SMS services and data capabilities. From there, you can create your own niche product or experimental feature. Select hardware, and set up a base operating system for your project Configure, troubleshoot, and use performance-tuning techniques Expand to a true multinode mobile network complete with Mobility and Handover Add general packet radio service (GPRS) data connectivity, ideal for IoT devices Build applications on top of the OpenBTS NodeManager control and event APIs

2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery

Cognitive Radio-Oriented Wireless Networks

Seven Deadliest Social Network Attacks

"Ad hoc and sensor networks present unique challenges in the area of security given their lack of a secure infrastructure, dynamic topology and severe resource restraints. The research presented in the six articles comprising this volume cover a variety of topics including trust establishment in Mobile Ad-Hoc Networks (MANETs), security of vehicular ad-hoc networks, secure aggregation in sensor networks, detecting misbehaviors in ad-hoc networks, secure group communication, and distributed signature protocols for ad-hoc networks. Ad-hoc and sensor networks will become increasingly more important, especially in the areas of military defense and disaster recovery, said Dr. Ning, co-editor. Security is a big concern in these networks, so researchers are working on developing security systems that provide multiple lines of defense, including detection of physical attacks and compromised nodes. Examples of ad-hoc and sensor networks that are currently being developed are vehicular networks that allow the transmission of traffic information, networks that allow tanks and fighter jets to communicate directly on the battlefield and sensor networks that use multiple sensor nodes to monitor an environment."

iOS Hacker's Handbook

This book constitutes the refereed proceedings of the 14th International Conference on Cognitive Radio-Oriented Wireless Networks, CROWNCOM 2019, held in Poznan, Poland, in June 2019. The 30 revised full papers were selected from 48 submissions and present a large scope of research topic also covering IoT in 5G and how cognitive mechanisms shall help leveraging access for numerous devices; mmWave and how specific propagation and operation in these bands bring new sharing mechanisms ; how resource allocation amongst bands (including offload mechanisms) shall be solved. The key focus will be on how rich data analysis can improve the delivery of above defined services.

Task Scheduling for Parallel Systems

CMOS Cellular Receiver Front-Ends: from Specification to Realization deals with the design of the receive path of a highly-

integrated CMOS cellular transceiver for the GSM-1800 cellular system. The complete design trajectory is covered, starting from the documents describing the standard down to the systematic development of CMOS receiver ICs that comply to the standard. The design of CMOS receivers is tackled at all abstraction levels: from architecture level, via circuit level, down to the device level, and the other way around. The theoretical core of the book discusses the fundamental and more advanced aspects of RF CMOS design. It focuses specifically on all aspects of the design of high-performance CMOS low-noise amplifiers.

White Space Communication

Cognitive radios (CR) technology is capable of sensing its surrounding environment and adapting its internal states by making corresponding changes in certain operating parameters. CR is envisaged to solve the problems of the limited available spectrum and the inefficiency in the spectrum usage. CR has been considered in mobile ad hoc networks (MANETs), which enable wireless devices to dynamically establish networks without necessarily using a fixed infrastructure. The changing spectrum environment and the importance of protecting the transmission of the licensed users of the spectrum mainly differentiate classical MANETs from CR-MANETs. The cognitive capability and re-configurability of CR-MANETs have opened up several areas of research which have been explored extensively and continue to attract research and development. The book will describe CR-MANETs concepts, intrinsic properties and research challenges of CR-MANETs. Distributed spectrum management functionalities, such as spectrum sensing and sharing, will be presented. The design, optimization and performance evaluation of security issues and upper layers in CR-MANETs, such as transport and application layers, will be investigated.

Seven Deadliest Microsoft Attacks

The Software Communications Architecture (SCA) establishes an implementation-independent framework for the development of Joint Tactical Radio System software configurable radios. It specifies the Operating Environment, services and interfaces that applications use. Software Defined Radio: The Software Communications Architecture focuses on the issues and benefits associated with developing a radio system in compliance with the SCA specification. This book provides a comprehensive, practical introduction to building a SCA-compliant system taking the reader through the historical and conceptual background to help filling in the gaps between the intent of the SCA specification and the practice. Key features: Presents a practical approach to the Software Communications Architecture Provides an example-oriented understanding of the usage of the SCA and thus allows the reader to extend the concepts and practice to more complicated multi-processor distributed environments. Covers the Operating Environment: a Core framework, CORBA middleware, POSIX operating systems and Domain profiles. Features an accompanying website with appendices, and links to further information on the

SCA. This invaluable reference will provide applications programmers, designers, professional researchers, wireless manufacturers and operators with an indispensable guide to the Software Communications Architecture. Advanced undergraduate and postgraduate students on mobile and wireless communications courses will also find this to be an excellent guide to the topic.

Getting Started with OpenBTS

The clear, easy-to-understand introduction to digital communications Completely updated coverage of today's most critical technologies Step-by-step implementation coverage Trellis-coded modulation, fading channels, Reed-Solomon codes, encryption, and more Exclusive coverage of maximizing performance with advanced "turbo codes" "This is a remarkably comprehensive treatment of the field, covering in considerable detail modulation, coding (both source and channel), encryption, multiple access and spread spectrum. It can serve both as an excellent introduction for the graduate student with some background in probability theory or as a valuable reference for the practicing ommunication system engineer. For both communities, the treatment is clear and well presented." - Andrew Viterbi, The Viterbi Group Master every key digital communications technology, concept, and technique. Digital Communications, Second Edition is a thoroughly revised and updated edition of the field's classic, best-selling introduction. With remarkable clarity, Dr. Bernard Sklar introduces every digital communication technology at the heart of today's wireless and Internet revolutions, providing a unified structure and context for understanding them -- all without sacrificing mathematical precision. Sklar begins by introducing the fundamentals of signals, spectra, formatting, and baseband transmission. Next, he presents practical coverage of virtually every contemporary modulation, coding, and signal processing technique, with numeric examples and step-by-step implementation guidance. Coverage includes: Signals and processing steps: from information source through transmitter, channel, receiver, and information sink Key tradeoffs: signal-to-noise ratios, probability of error, and bandwidth expenditure Trellis-coded modulation and Reed-Solomon codes: what's behind the math Synchronization and spread spectrum solutions Fading channels: causes, effects, and techniques for withstanding fading The first complete how-to guide to turbo codes: squeezing maximum performance out of digital connections Implementing encryption with PGP, the de facto industry standard Whether you're building wireless systems, xDSL, fiber or coax-based services, satellite networks, or Internet infrastructure, Sklar presents the theory and the practical implementation details you need. With nearly 500 illustrations and 300 problems and exercises, there's never been a faster way to master advanced digital communications. CD-ROM INCLUDED The CD-ROM contains a complete educational version of Elanix' SystemView DSP design software, as well as detailed notes for getting started, a comprehensive DSP tutorial, and over 50 additional communications exercises.

The Sparse Fourier Transform

Presenting the work of prominent researchers working on smart grids and related fields around the world, Security and Privacy in Smart Grids identifies state-of-the-art approaches and novel technologies for smart grid communication and security. It investigates the fundamental aspects and applications of smart grid security and privacy and reports on the latest advances in the range of related areas—making it an ideal reference for students, researchers, and engineers in these fields. The book explains grid security development and deployment and introduces novel approaches for securing today's smart grids. Supplying an overview of recommendations for a technical smart grid infrastructure, the book describes how to minimize power consumption and utility expenditure in data centers. It also: Details the challenges of cybersecurity for smart grid communication infrastructures Covers the regulations and standards relevant to smart grid security Explains how to conduct vulnerability assessments for substation automation systems Considers smart grid automation, SCADA system security, and smart grid security in the last mile The book's chapters work together to provide you with a framework for implementing effective security through this growing system. Numerous figures, illustrations, graphs, and charts are included to aid in comprehension. With coverage that includes direct attacks, smart meters, and attacks via networks, this versatile reference presents actionable suggestions you can put to use immediately to prevent such attacks.

Wireless Sensor Networks

If you are a security professional, pentester, or anyone interested in getting to grips with wireless penetration testing, this is the book for you. Some familiarity with Kali Linux and wireless concepts is beneficial.

Seven Deadliest Network Attacks

This edition features a wealth of new material on urban warfare, including a computer simulation of EW architecture alternatives for land-based forces based on urban constraints. It also includes an expanded section on time-hopped spread spectrum communications, more details on modern communication system technologies such as CDMA and OFDM, and an in-depth discussion on sources of urban noise. This practical resource is focused on showing the reader how to design and build jammers specifically targeted at spread spectrum, anti-jam communications. Moreover, it gives assistance in evaluating the expected performance of jamming systems against modern communications systems, and discover the best waveform to use to counter communication systems designed to be effective in jamming environments. While mathematical derivations in general are avoided, the book presents error rate performance equations for most modern digital anti-jam communication systems

Internet of Things (IoT)

Seven Deadliest Wireless Technologies Attacks provides a comprehensive view of the seven different attacks against popular wireless protocols and systems. This book pinpoints the most dangerous hacks and exploits specific to wireless technologies, laying out the anatomy of these attacks, including how to make your system more secure. You will discover the best ways to defend against these vicious hacks with step-by-step instruction and learn techniques to make your computer and network impenetrable. Each chapter includes an example real attack scenario, an analysis of the attack, and methods for mitigating the attack. Common themes will emerge throughout the book, but each wireless technology has its own unique quirks that make it useful to attackers in different ways, making understanding all of them important to overall security as rarely is just one wireless technology in use at a home or office. The book contains seven chapters that cover the following: infrastructure attacks, client attacks, Bluetooth attacks, RFID attacks; and attacks on analog wireless devices, cell phones, PDAs, and other hybrid devices. A chapter deals with the problem of bad encryption. It demonstrates how something that was supposed to protect communications can end up providing less security than advertised. This book is intended for information security professionals of all levels, as well as wireless device developers and recreational hackers. Attacks detailed in this book include: 802.11 Wireless—Infrastructure Attacks 802.11 Wireless—Client Attacks Bluetooth Attacks RFID Attacks Analog Wireless Device Attacks Bad Encryption Attacks on Cell Phones, PDAs and Other Hybrid Devices

Cognitive Radio Oriented Wireless Networks

This book constitutes the thoroughly refereed post-conference proceedings of the 7th International ICST Conference on Mobile Multimedia Communications (MOBIMEDIA 2011) held in Cagliari, Italy, in September 2011 The 26 revised full papers presented were carefully selected from numerous submissions and focus topics such as quality of experience, dynamic spectrum access wireless networks in the TV white spaces, media streaming, mobile visual search, image processing and transmission, and mobile applications.

Digital Communications

Intra-system EMC problems are becoming increasingly common in mobile devices, ranging from notebook PCs to cell phones, with RF/wireless capbilities. These issues range from minor annoyances to serious glitches which impede the functioning of the device. This book gives a thourough review of electromagnetic theory (including Maxwell's equations), discusses possible sources and causes of intra-system interference, shows to use models and analysis to discover potential sources of intra-system EMC in a design, how to use appropriate tests and measurements to detect intra-system EMC problems, and finally extensively discusses measures to mitigate or totally eliminate intra-system EMC problems. With more and more mobile devices incorporating wirless capability (often with multiple wireless systems, such as Bluetooth and WiFi),

this book should be part of the reference shelf of every RF/wireless engineer and mobile device designer. *Addresses a growing problem in RF/wireless devices----interference created inside the devices, which impair their operation *Covers devices, ranging from laptop PCs to mobile phones to Bluetooth headsets *Explains the sources of such intra-system interference, how to detect and measure such interference, design techniques for mitigating the interference, and proven techniques for eliminating the interference

Security of Ad-hoc and Sensor Networks

A new model for task scheduling that dramatically improves the efficiency of parallel systems Task scheduling for parallel systems can become a quagmire of heuristics, models, and methods that have been developed over the past decades. The author of this innovative text cuts through the confusion and complexity by presenting a consistent and comprehensive theoretical framework along with realistic parallel system models. These new models, based on an investigation of the concepts and principles underlying task scheduling, take into account heterogeneity, contention for communication resources, and the involvement of the processor in communications. For readers who may be new to task scheduling, the first chapters are essential. They serve as an excellent introduction to programming parallel systems, and they place task scheduling within the context of the program parallelization process. The author then reviews the basics of graph theory, discussing the major graph models used to represent parallel programs. Next, the author introduces his task scheduling framework. He carefully explains the theoretical background of this framework and provides several examples to enable readers to fully understand how it greatly simplifies and, at the same time, enhances the ability to schedule. The second half of the text examines both basic and advanced scheduling techniques, offering readers a thorough understanding of the principles underlying scheduling algorithms. The final two chapters address communication contention in scheduling and processor involvement in communications. Each chapter features exercises that help readers put their new skills into practice. An extensive bibliography leads to additional information for further research. Finally, the use of figures and examples helps readers better visualize and understand complex concepts and processes. Researchers and students in distributed and parallel computer systems will find that this text dramatically improves their ability to schedule tasks accurately and efficiently.

Real-Time Systems

This book constitutes the proceedings of the 20th International Conference on Selected Areas in Cryptography, SAC 2013, held in Burnaby, Canada, in August 2013. The 26 papers presented in this volume were carefully reviewed and selected from 98 submissions. They are organized in topical sections named: lattices; discrete logarithms; stream ciphers and authenticated encryption; post-quantum (hash-based and system solving); white box crypto; block ciphers; elliptic curves,

pairings and RSA; hash functions and MACs; and side-channel attacks. The book also contains 3 full-length invited talks.

Kali Linux Wireless Penetration Testing: Beginner's Guide

This books objective is to explore the concepts and applications related to Internet of Things with the vision to identify and address existing challenges. Additionally, the book provides future research directions in this domain, and explores the different applications of IoT and its associated technologies. Studies investigate applications for crowd sensing and sourcing, as well as smart applications to healthcare solutions, agriculture and intelligent disaster management. This book will appeal to students, practitioners, industry professionals and researchers working in the field of IoT and its integration with other technologies to develop comprehensive solutions to real-life problems

ROMANCE ACTION & ADVENTURE MYSTERY & THRILLER BIOGRAPHIES & HISTORY CHILDREN'S YOUNG ADULT FANTASY HISTORICAL FICTION HORROR LITERARY FICTION NON-FICTION SCIENCE FICTION