

Usrp 2 User Guide

Annotation Standards play a key role in the success of the communications industry, as enablers of global systems interoperability IEEE CSCN aims for closing the gap between researchers, scientists and standards experts from academia, industry and different standardization bodies It will serve as a platform for presenting and discussing standards related topics in the areas of communications, networking and related disciplines, facilitating standards development as well as cooperation among the key players.

The first comprehensive guide to discovering and preventing attacks on the Android OS As the Android operating system continues to increase its share of the smartphone market, smartphone hacking remains a growing threat. Written by experts who rank among the world's foremost Android security researchers, this book presents vulnerability discovery, analysis, and exploitation tools for the good guys. Following a detailed explanation of how the Android OS works and its overall security architecture, the authors examine how vulnerabilities can be discovered and exploits developed for various system components, preparing you to defend against them. If you are a mobile device administrator, security researcher, Android app developer, or consultant responsible for evaluating Android security, you will find this guide is essential to your toolbox. A crack team of leading Android security researchers explain Android security risks, security design and architecture, rooting, fuzz testing, and vulnerability analysis Covers Android application building blocks and security as well as debugging and auditing Android apps Prepares mobile device administrators, security researchers, Android app developers, and security consultants to defend Android systems against attack Android Hacker's Handbook is the first comprehensive resource for IT professionals charged with smartphone security.

In many penetration tests, there is a lot of useful information to be gathered from the radios used by organizations. These radios can include two-way radios used by guards, wireless headsets, cordless phones and wireless cameras. Wireless Reconnaissance in Penetration Testing describes the many ways that a penetration tester can gather and apply the information available from radio traffic. Stopping attacks means thinking like an attacker, and understanding all the ways that attackers gather information, or in industry terms profile, specific targets. With information from what equipment to use and how to find frequency information, to tips for reducing radio information leakage, to actual case studies describing how this information can be used to attack computer systems, this book is the go-to resource for penetration testing and radio profiling. Author Matthew Neely is a respected and well-known expert and speaker on radio reconnaissance and penetration testing Includes real-world case studies of actual penetration tests using radio profiling Covers data leakage, frequency, attacks, and information gathering

This book constitutes the proceedings of the International Conference on Internet of Things, ICIOT 2019, held as part of SCF 2019, in San Diego, CA, USA, in June 2019. The 8 full and 3 short papers presented in this volume were carefully reviewed and selected from 16 submissions. With the rapid advancements of mobile Internet, cloud computing and big data, device-centric traditional Internet of Things (IoT) is now moving into a new era which is termed as Internet of Things Services (IOTS). In this era, sensors and other types of sensing devices, wired and wireless networks, platforms and tools, data processing/visualization/analysis and integration engines, and other components of traditional IoT are interconnected through innovative services to realize the value of connected things, people, and virtual Internet spaces.

This IBM® Redbooks® publication is intended to make System Programmers, Operators, and Availability Managers aware of the enhancements to recent releases of IBM z/OS® and its major subsystems in the area of planned outage avoidance. It is a follow-on to, rather than a replacement for, z/OS Planned Outage Avoidance Checklist, SG24-7328. Its primary objective is to bring together in one place information that is already available, but widely dispersed. It also presents a different perspective on planned outage avoidance. Most businesses care about application availability rather than the availability of a specific system. Also, a planned outage is not necessarily a bad thing, if it does not affect application availability. In fact, running for too long without an IPL or subsystem restart might have a negative impact on application availability because it impacts your ability to apply preventive service. Therefore, this book places more focus on decoupling the ability to make changes and updates to your system from IPLing or restarting your systems.

The Handbook of Smart Antennas for RFID Systems is a single comprehensive reference on the smart antenna technologies applied to RFID. This book will provide a timely reference book for researchers and students in the areas of both smart antennas and RFID technologies. It is the first book to combine two of the most important wireless technologies together in one book. The handbook will feature chapters by leading experts in both academia and industry offering an in-depth description of terminologies and concepts related to smart antennas in various RFID systems applications. Some topics are: adaptive beamforming for RFID smart antennas, multiuser interference suppression in RFID tag reading, phased array antennas for RFID applications, smart antennas in wireless systems and market analysis and case studies of RFID smart antennas. This handbook will cover the latest achievements in the designs and applications for smart antennas for RFID as well as the basic concepts, terms, protocols, systems architectures and case studies in smart antennas for RFID readers and tags.

"This unique resource provides you with a practical approach to quickly learning the software-defined radio concepts you need to know for your work in the field. By prototyping and evaluating actual digital communication systems capable of performing "over-the-air" wireless data transmission and reception, this volume helps you attain a first-hand understanding of critical design trade-offs and issues. Moreover you gain a sense of the actual "real-world" operational behavior of these systems. With the purchase of the book, you gain access to several ready-made Simulink experiments at the publisher's website. This collection of laboratory experiments, along with several examples, enables you to successfully implement the designs discussed the book in a short period of time. These files can be executed using MATLAB version R2011b or later. "

With the intriguing development of technologies in several industries, along with the advent of ubiquitous computational resources, there are now ample opportunities to develop innovative computational technologies in order to solve a wide range of issues concerning uncertainty, imprecision, and vagueness in various real-life problems. The challenge of blending modern computational techniques with traditional computing methods has inspired researchers and academics alike to focus on developing innovative computational techniques. In the near future, computational techniques may provide vital solutions by effectively using evolving technologies such as computer vision, natural language processing, deep learning, machine learning, scientific computing, and computational vision. A vast number of intelligent computational algorithms are emerging, along with increasing computational power, which has significantly expanded the potential for developing intelligent applications. These proceedings of the International Conference on Inventive Computation Technologies [ICICT 2019] cover innovative computing applications in the areas of data mining, big data processing, information management, and security.

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 portability 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.

The book covers the most recent developments in machine learning, signal analysis, and their applications. It covers the topics of machine intelligence such as: deep learning, soft computing approaches, support vector machines (SVMs), least square SVMs (LSSVMs) and their variants; and covers the topics of signal analysis such as: biomedical signals including electroencephalogram (EEG), magnetoencephalography (MEG), electrocardiogram (ECG) and electromyogram (EMG) as well as other signals such as speech signals, communication signals, vibration signals, image, and video. Further, it analyzes normal and abnormal categories of real-world signals, for example normal and epileptic EEG signals using numerous classification techniques. The book is envisioned for researchers and graduate students in Computer Science and Engineering, Electrical Engineering, Applied Mathematics, and Biomedical Signal Processing.

This is the first book on digital fingerprinting that comprehensively covers the major areas of study in a range of information security areas including authentication schemes, intrusion detection, forensic analysis and more. Available techniques for assurance are limited and authentication schemes are potentially vulnerable to the theft of digital tokens or secrets. Intrusion detection can be thwarted by spoofing or impersonating devices, and forensic analysis is incapable of demonstrably tying a particular device to specific digital evidence. This book presents an innovative and effective approach that addresses these concerns. This book introduces the origins and scientific underpinnings of digital fingerprinting. It also proposes a unified framework for digital fingerprinting, evaluates methodologies and includes examples and case studies. The last chapter of this book covers the future directions of digital fingerprinting. This book is designed for practitioners and researchers working in the security field and military. Advanced-level students focused on computer science and engineering will find this book beneficial as secondary textbook or reference.

This book collects articles presented at the 13th International Conference on Information Technology- New Generations, April, 2016, in Las Vegas, NV USA. It includes over 100 chapters on critical areas of IT including Web Technology, Communications, Security, and Data Mining.

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.

This book constitutes the refereed proceedings of the Cryptographers' Track at the RSA Conference 2009, CT-RSA 2009, held in San Francisco, CA, USA in April 2009. The 31 revised full papers presented were carefully reviewed and selected from 93 submissions. The papers are organized in topical sections on identity-based encryption, protocol analysis, two-party protocols, more than signatures, collisions for hash functions, cryptanalysis, alternative encryption, privacy and anonymity, efficiency improvements, multi-party protocols, security of encryption schemes as well as countermeasures and faults.

An author subject index to selected general interest periodicals of reference value in libraries.

Based on the popular Artech House classic, Digital Communication Systems Engineering with Software-Defined Radio, this book provides a practical approach to quickly learning the software-defined radio (SDR) concepts needed for work in the field. This up-to-date volume guides readers on how to quickly prototype wireless designs using SDR for real-world testing and experimentation. This book explores advanced wireless communication techniques such as OFDM, LTE, WLA, and hardware targeting. Readers will gain an understanding of the core concepts behind wireless hardware, such as the radio frequency front-end, analog-to-digital and digital-to-analog converters, as well as various processing technologies. Moreover, this volume includes chapters on timing estimation, matched filtering, frame synchronization message decoding, and source coding. The orthogonal frequency division multiplexing is explained and details about HDL code generation and deployment are provided. The book concludes with coverage of the WLAN toolbox with OFDM beacon reception and the LTE toolbox with downlink reception. Multiple case studies are provided throughout the book. Both MATLAB and Simulink source code are included to assist readers with their projects in the field.

White Space Communication Advances, Developments and Engineering Challenges Springer

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 This book constitutes revised and selected papers from the 6th International Symposium on Security and Privacy in Social Networks and Big Data, SocialSec 2020, held in Tianjin, China, in September 2020. The 38 full papers presented in this volume were carefully reviewed and selected from a total of 111 submissions. The papers are organized according to the topical sections on big data security; social networks; privacy-preserving and security.

Take a practitioner's approach in analyzing the Internet of Things (IoT) devices and the security issues facing an IoT architecture. You'll review the architecture's central components, from hardware communication interfaces, such as UART and SPI, to radio protocols, such as BLE or ZigBee. You'll also learn to assess a device physically by opening it, looking at the PCB, and identifying the chipsets and interfaces. You'll then use that information to gain entry to the device or to perform other actions, such as dumping encryption keys and firmware. As the IoT rises to one of the most popular tech trends, manufacturers need to take necessary steps to secure devices and protect them from attackers. The IoT Hacker's Handbook breaks down the Internet of Things, exploits it, and reveals how these devices can be built securely. What You'll Learn Perform a threat model of a real-world IoT device and locate all possible attacker entry points Use reverse engineering of firmware binaries to identify security issues Analyze, assess, and identify security issues in exploited ARM and MIPS based binaries Sniff, capture, and exploit radio communication protocols, such as Bluetooth Low Energy (BLE), and ZigBee Who This Book is For Those interested in learning about IoT security, such as pentesters working in different domains, embedded device developers, or IT people wanting to move to an Internet of Things security role.

Modern cars are more computerized than ever. Infotainment and navigation systems, Wi-Fi, automatic software updates, and other innovations aim to make driving more convenient. But vehicle technologies haven't kept pace with today's more hostile security environment, leaving millions vulnerable to attack. The Car Hacker's Handbook will give you a deeper understanding of the computer systems and embedded software in modern vehicles. It begins by examining vulnerabilities and providing detailed explanations of communications over the CAN bus and between devices and systems. Then, once you have an understanding of a vehicle's communication network, you'll learn how to intercept data and perform specific hacks to track vehicles, unlock doors, glitch engines, flood communication, and more. With a focus on low-cost, open source hacking tools such as Metasploit, Wireshark, Kayak, can-utils, and ChipWhisperer, The Car Hacker's Handbook will show you how to: –Build an accurate threat model for your vehicle –Reverse engineer the CAN bus to fake engine signals –Exploit vulnerabilities in diagnostic and data-logging systems –Hack the ECU and other firmware and embedded systems –Feed exploits through infotainment and vehicle-to-vehicle communication systems –Override factory settings with performance-tuning techniques –Build physical and virtual test benches to try out exploits safely If you're curious about automotive security and have the urge to hack a two-ton computer, make The Car Hacker's Handbook your first stop.

This book contains a selection of articles from The 2015 World Conference on Information Systems and Technologies (WorldCIST'15), held between the 1st and 3rd of April in Funchal, Madeira, Portugal, a global forum for researchers and practitioners to present and discuss recent results and innovations, current trends, professional experiences and challenges of modern Information Systems and Technologies research, technological development and applications. The main topics covered are: Information and Knowledge Management; Organizational Models and Information Systems; Intelligent and Decision Support Systems; Big Data Analytics and Applications; Software Systems, Architectures, Applications and Tools; Multimedia Systems and Applications; Computer Networks, Mobility and Pervasive Systems; Human-Computer Interaction; Health Informatics; Information Technologies in Education; Information Technologies in Radio communications.

This book presents the latest innovative research findings, methods, and development techniques related to intelligent social networks and collaborative systems, intelligent networking systems, mobile collaborative systems, and secure intelligent cloud systems. Offering both theoretical and practical perspectives, it also reveals synergies among various paradigms in the multi-disciplinary field of intelligent collaborative systems. With the rapid development of the Internet, we are experiencing a shift from the traditional sharing of information and applications as the main purpose of the Web to an emergent paradigm that places people at the very centre of networks, making full use of their connections, relations, and collaboration. Social networks also play a major role in the dynamics and structure of intelligent Web-based networking and collaborative systems. Virtual campuses, communities and organizations strongly leverage intelligent networking and collaborative systems through a wide variety of formal and informal electronic relations, such as business-to-business, peer-to-peer, and many types of online collaborative learning interactions, including the emerging e-learning systems. This has resulted in entangled systems that need to be managed efficiently and autonomously. In addition, while the latest powerful technologies based on grid and wireless infrastructures as well as cloud computing are currently greatly enhancing collaborative and networking applications, they are also facing new challenges. The principal purpose of the research and development community is to stimulate research that will lead to the creation of responsive environments for networking and, in the long term, the development of adaptive, secure, mobile, and intuitive intelligent systems for collaborative work and learning.

This book discusses the security issues in a wide range of wireless devices and systems, such as RFID, Bluetooth, ZigBee, GSM, LTE, and GPS. It collects the findings of recent research by the UnicornTeam at 360 Technology, and reviews the state-of-the-art literature on wireless security. The book also offers detailed case studies and theoretical treatments – specifically it lists numerous laboratory procedures, results, plots, commands and screenshots from real-world experiments. It is a valuable reference guide for practitioners and researchers who want to learn more about the advanced research findings and use the off-the-shelf tools to explore the wireless world.

A technical manual describing the history, construction, calibration of the NanoVNA. Explains model differences, application and use of the device. 52 illustrations (photos and screenshots), 20 in color.

This book gathers selected research papers presented at the International Conference on Communication and Intelligent Systems (ICCIS 2019), organised by Swami Keshvanand Institute of

Technology, Management & Gramothan (SKIT), Jaipur, India and Rajasthan Technical University, Kota, India on 9–10 November 2019. This book presents a collection of state-of-the-art research work involving cutting-edge technologies for communication and intelligent systems. Over the past few years, advances in artificial intelligence and machine learning have sparked new research efforts around the globe, which explore novel ways of developing intelligent systems and smart communication technologies. The book presents single- and multi-disciplinary research on these themes in order to make the latest results available in a single, readily accessible source.

A comprehensive guide to the RTL2832U RTL-SDR software defined radio by the authors of the RTL-SDR Blog. The RTL-SDR is a super cheap software defined radio based on DVB-T TV dongles that can be found for under \$20. This book is about tips and tutorials that show you how to get the most out of your RTL-SDR dongle. Most projects described in this book are also compatible with other wideband SDRs such as the HackRF, Airspy and SDRPlay RSP. What's in the book? Learn how to set up your RTL-SDR with various free software defined radio programs such as SDR#, HSDR, SDR-Radio and more. Learn all the little tricks and oddities that the dongle has. A whole chapter dedicated to improving the RTL-SDR's performance. Dozens of tutorials for fun RTL-SDR based projects such as ADS-B aircraft radar, AIS boat radar, ACARS decoding, receiving NOAA and Meteor-M2 weather satellite images, listening to and following trunked radios, decoding digital voice P25/DMR signals, decoding weather balloon telemetry, receiving DAB radio, analysing GSM and listening to TETRA signals, decoding pagers, receiving various HF signals such as ham radio modes, weatherfax and DRM radio, decoding digital D-STAR voice, an introduction to GNU Radio, decoding RDS, decoding APRS, measuring filters and SWR with low cost equipment, receiving Inmarsat, Outernet and Iridium L-Band satellite data, and many many more projects! Guide to antennas, cables and adapters. Third Edition Released 20 December 2016.

Each release of data facility storage management subsystem (DFSMS) builds upon the previous version to provide enhanced storage management, data access, device support, program management, and distributed data access for the z/OS® platform in a system-managed storage environment. This IBM® Redbooks® publication provides a summary of the functions and enhancements in z/OS V1R11 DFSMS. It provides you with the information that you need to understand and evaluate the content of this DFSMS release, along with practical implementation hints and tips. Also included are enhancements that were made available through an enabling PTF that has been integrated into z/OS DFSMS V1R11. This book was written for storage professionals and system programmers who have experience with the components of DFSMS. It provides sufficient information so that you can start prioritizing the implementation of new functions and evaluating their applicability in your DFSMS environment.

The definitive guide to hacking the world of the Internet of Things (IoT) -- Internet connected devices such as medical devices, home assistants, smart home appliances and more. Drawing from the real-life exploits of five highly regarded IoT security researchers, Practical IoT Hacking teaches you how to test IoT systems, devices, and protocols to mitigate risk. The book begins by walking you through common threats and a threat modeling framework. You'll develop a security testing methodology, discover the art of passive reconnaissance, and assess security on all layers of an IoT system. Next, you'll perform VLAN hopping, crack MQTT authentication, abuse UPnP, develop an mDNS poisoner, and craft WS-Discovery attacks. You'll tackle both hardware hacking and radio hacking, with in-depth coverage of attacks against embedded IoT devices and RFID systems. You'll also learn how to:

- Write a DICOM service scanner as an NSE module
- Hack a microcontroller through the UART and SWD interfaces
- Reverse engineer firmware and analyze mobile companion apps
- Develop an NFC fuzzer using Proxmark3
- Hack a smart home by jamming wireless alarms, playing back IP camera feeds, and controlling a smart treadmill

The tools and devices you'll use are affordable and readily available, so you can easily practice what you learn. Whether you're a security researcher, IT team member, or hacking hobbyist, you'll find Practical IoT Hacking indispensable in your efforts to hack all the things

REQUIREMENTS: Basic knowledge of Linux command line, TCP/IP, and programming

As the material anchors of globalization, North America's global port cities channel flows of commodities, capital, and tourists. This book explores how economic globalization processes have shaped these cities' political institutions, social structures, and urban identities since the mid-1970s. Although the impacts of financialization on global cities have been widely discussed, it is curious that how the global integration of commodity chains actually happens spatially — creating a quantitatively new, global organization of production, distribution, and consumption processes — remains understudied. The book uses New York City, Los Angeles, Vancouver, and Montreal as case studies of how once-redundant spaces have been reorganized, and crucially, reinterpreted, so as to accommodate new flows of goods and people — and how, in these processes, social, environmental, and security costs of global production networks have been shifted to the public.

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

This book, written by experts from universities and major industrial research laboratories, is devoted to the very hot topic of cognitive radio and networking for cooperative coexistence of heterogeneous wireless networks. Selected highly relevant advanced research is presented on spectrum sensing and progress toward the realization of accurate radio environment mapping, biomimetic learning for self-organizing networks, security threats (with a special focus on primary user emulation attack), and cognition as a tool for green next-generation networks. The research activities covered include work undertaken within the framework of the European COST Action IC0902, which is geared towards the definition of a European platform for cognitive radio and networks. Communications engineers, R&D engineers, researchers, and students will all benefit from this complete reference on recent advances in wireless communications and the design and implementation of cognitive radio systems and networks.

[Copyright: dc1f7e9e2d4b88d5f4294bcd0b02fed2](https://doi.org/10.1002/9781119988888.ch02)