Gnu Radio Usrp Tutorial Wordpress

The Mac Hacker's Handbook
Mobile Phone Security and Forensics
NanoVNA Users Manual
RTP
Getting Started with OpenBTS
Fundamentals of Digital Communication Systems
Field Expedient SDR: Basic Digital Communications (black and White Version)
The LabVIEW Style Book
Multirate Signal Processing For Communication Systems
Security and Privacy for Implantable Medical Devices
Practical recipes on implementing information gathering, network security, intrusion detection, and post-exploitation
Have Fun while Voiding your Warranty
Basic Electronics and Linear Circuits
Communication System Design Using DSP Algorithms
Signaling System No. 7 (SS7/C7)
Afternoons with Mr. Hogan
Galactic Radio Astronomy
Data-Driven Modeling of Cyber-Physical Systems using Side-Channel Analysis
Practical Hardware Pentesting
Inside Radio: An Attack and Defense Guide
IoT Penetration Testing Cookbook
Circuits, Programs & Applications Featuring the 8052-BASIC Microcontroller
Chronyk
Linux Security Secrets and Solutions
Man-made radio noise
Housing, Land, and Property Rights in Post-Conflict United Nations and Other Peace Operations
Indoor Geolocation Science and Technology
Really Cheap Software Defined Radio
A Guide to the NanoVNA
Hardware Hacking
A Comparative Survey and Proposal for Reform
The Lean Startup
Genetic Algorithms in Java Basics
Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition
Wireless Communications from the Ground Up
Moffett Field, California
The Kraken Wakes
A guide to attacking embedded systems and protecting them against the most common hardware attacks
Hacking Exposed Linux

LOGAN RICH

The Mac Hacker's Handbook Elsevier
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
Mobile Phone Security and Forensics Stylus Publishing, LLC
This Book Provides The Communications Engineer Involved In The Physical Layer Of Communications Systems, The Signal Processing Techniques And Design Tools Needed To Develop Efficient Algorithms For The Design Of Various Systems. These Systems Include Satellite Modems, Cable Modems, Wire-Line Modems, Cell-Phones, Various Radios, Multi-Channel Receivers, Audio Encoders, Surveillance Receivers, Laboratory Instruments, And Various Sonar And Radar Systems. The Emphasis Woven Through The Book Material Is That Of Intuitive Understanding Obtained By The Liberal Use Of Figures And Examples. The Book Contains Examples Of All These Types Of Systems. The Book Also Will Contain Matlab Script Files That Implement The Examples As Well As Design Tools For Filters Similar To The Examples.
NanoVNA Users Manual lakeview research llc
A complete, practical guide to the world's most popular signaling system, including SIGTRAN, GSM-MAP, and Intelligent Networks. Provides in-depth coverage of the SS7 protocols, including implementation details Covers SS7 over IP (SIGTRAN) using real-world examples Covers SS7/C7 from both a North American and European perspective, providing a broad international understanding of the technology and associated standards Explains mobile wireless concepts and signaling, including mobile application part (MAP) Provides a thorough explanation of the Intelligent Network (IN) and associated protocols (INAP/AIN) Signaling System No. 7 (SS7) is a signaling network and protocol that is used globally to bring telecommunications networks, both fixed-line and cellular, to life. SS7 has numerous applications and is at the very heart of telecommunications. Setting up phone calls, providing cellular roaming and messaging, and supplying converged voice and data services

are only a few of the ways that SS7 is used in the communications network. SS7 also provides the point of interconnection between converging voice and data networks. This transition, which affects everyone who works with the data network, has bolstered the need for practical and applied information on SS7. In short, anyone who is interested in telecommunications should have a solid understanding of SS7. Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services will help you understand SS7 from several perspectives. It examines the framework and architecture of SS7, as well as how it is used to provide today's telecommunications services. It also examines each level of the SS7 protocol-all the way down to the bit level of messages. In addition, the SIGTRAN standards are discussed in detail, showing the migration from SS7 to IP and explaining how SS7 information is transported over IP.

RTP Modern Library

This new edition provides both theoretical and practical background of security and forensics for mobile phones. The author discusses confidentiality, integrity, and availability threats in mobile telephones to provide background for the rest of the book. Security and secrets of mobile phones are discussed including software and hardware interception, fraud and other malicious techniques used “against” users. The purpose of this book is to raise user awareness in regards to security and privacy threats present in the use of mobile phones while readers will also learn where forensics data reside in the mobile phone and the network and how to conduct a relevant analysis. The information on denial of service attacks has been thoroughly updated for the new edition. Also, a major addition to this edition is a section discussing software defined radio and open source tools for mobile phones.

Getting Started with OpenBTS McGraw Hill Professional

Precise and accurate localization is one of the fundamental scientific and engineering technologies needed for the applications enabling the emergence of the Smart World and the Internet of Things (IoT). Popularity of localization technology began when the GPS became open for commercial applications in early 1990s. Since most commercial localization applications are for indoors and GPS does not work indoors, the discovery of opportunistic indoor geolocation technologies began in mid-1990s. Because of the complexity and diversity of the science and technology involved in indoor Geolocation, this area has emerged as its own discipline over the past two decades. At the time of this writing, received signal strength (RSS) based Wi-Fi localization is dominating the commercial market complementing cell tower localization and GPS technologies using the time of arrival (TOA) technology. Wi-Fi localization technology takes advantage of the random deployment of Wi-Fi devices worldwide to support indoor and urban area localization for hundreds of thousands of applications on smart devices. Public safety and military applications demand more precise localization for first responders and military applications deploy

specialized infrastructure for more precise indoor geolocation. To enhance the performance both industries are examining hybrid localization techniques. Hybrid algorithms use a variety of sensors to measure the speed and direction of movement and integrate them with the absolute radio frequency localization. Indoor Geolocation Science and Technology is a multidisciplinary book that presents the fundamentals of opportunistic localization and navigation science and technology used in different platforms such as: smart devices, unmanned ground and flying vehicles, and existing cars operating as a part of intelligent transportation systems. Material presented in the book is beneficial for Electrical and Computer Engineering, Computer Science, Robotics Engineering, Biomedical Engineering or other disciplines who are interested in integration of navigation into their multi-disciplinary projects. The book provides examples with supporting MATLAB codes and hands-on projects throughout to improve the ability of the readers to understand and implement variety of algorithms. It can be used for both academic education, as a textbook with problem sets and projects, and industrial training, as a practical reference book for professionals involved in design and performance evaluation. The author of this book has pioneering research experience and industrial exposure in design and performance evaluation of indoor geolocation based on empirical measurement and modeling of the behavior of the radio propagation in indoor areas and inside the human body. The presentation of the material is based on examples of research and development that his students have performed in his laboratory, his teaching experiences as a professor, and his experiences as a technical consultant to successful startup companies.

Fundamentals of Digital Communication Systems John Wiley & Sons

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

Field Expedient SDR: Basic Digital Communications (black and White Version) Packt Publishing Ltd

An “ingenious, horrifying” (The Guardian) first contact story by one of the twentieth century’s most brilliant—and neglected—science fiction and horror writers, whom Stephen King called “the best writer of science fiction that England has ever produced.” “Few books capture the obscure, elliptical way that threats move from the background to the foreground of reality like The Kraken Wakes. . . . Feels all too familiar in today’s age of anti-vaxxer disinformation and QAnon conspiracists.” —Alexandra Kleeman, from the Introduction What if aliens invaded and colonized Earth’s oceans rather than its land? Britain, 1953: It begins with red dots appearing across the sky and crashing to the oceans’ deeps. At first, many people believe that these aliens are interested in only what’s down below. But when the polar ice-caps begin to melt, it becomes clear that these beings are not interested in sharing the Earth and that humankind might just be on the brink of extinction. . . .

The LabVIEW Style Book John Wiley & Sons

A hands-on introduction to microcontroller project design with dozens of example circuits and programs. Presents practical designs for use in data loggers, controllers, and other small-computer applications. Example circuits and programs in the book are based on the popular 8052-BASIC microcontroller, whose on-chip BASIC programming language makes it easy to write, run, and test your programs. With over 100 commands, instructions, and operators, the BASIC-52 interpreter can do much more than other single-chip BASICs. Its abilities include floating-point math, string handling, and special commands for storing programs in EPROM, EEPROM, or battery-backed RAM.

Multirate Signal Processing For Communication Systems Apress

bull; Demonstrates how real-time audio and video is packetized for transmission. bull; Explains the details of the RTP standards and related concepts. bull; How to implement RTP to work around network problems and limitations

Security and Privacy for Implantable Medical Devices Addison-Wesley Professional

An engineer's introduction to concepts, algorithms, and advancements in Digital Signal Processing. This lucidly written resource makes extensive use of real-world examples as it covers all the important design and engineering references.

Practical recipes on implementing information gathering, network security, intrusion detection, and post-exploitation Pearson Education India

This is the eBook version of the print title. The illustrations are in color for this eBook version. Drawing on the experiences of a world-class LabVIEW development organization, The LabVIEW Style Book is the definitive guide to best practices in LabVIEW development. Leading LabVIEW development

manager Peter A. Blume presents practical guidelines or “rules” for optimizing every facet of your applications: ease of use, efficiency, readability, simplicity, performance, maintainability, and robustness. Blume explains each style rule thoroughly, presenting realistic examples and illustrations. He even presents “nonconforming” examples that show what not to do—and why not. While the illustrations in the print book are in black and white, you can download full-color versions from the publisher web site for free.

Have Fun while Voiding your Warranty McGraw Hill Professional

Note: There are two versions of this book, one with full-color illustrations, the other with interior images in black and white. This is the black and white edition. Software Defined Radios are revolutionizing wireless communications, but getting started can be a challenge. Much of the available SDR training veers either towards highly mathematical engineering classes or radio cookbooks with little explanation for the steps taken. Basic Digital Communications steers between these two extremes by leveraging knowledge you already have but didn't know was applicable to radio technology. Through a series of hands-on exercises, you'll learn: the key components of digital transmissions like preambles, payloads and error checking how to build transmitters using OOK and FSK how to build more advanced radios with PSK and QPSK the best techniques for viewing digitally modulated signals how to model noise and other system imperfections When you complete this third volume of our Field Expedient SDR series, you'll know enough to venture into the wild and start exploring the RF spectrum. Many of the online SDR tutorials and walkthroughs will make much more sense, allowing you to build more advanced radios and perform more advanced activities like reverse engineering and RF security research.

Basic Electronics and Linear Circuits Createspace Independent Publishing Platform

The book starts with a completely fresh perspective on introduction to signals and continues to dealing with complex numbers without any complicated mathematics. The only skills you require are addition, multiplication and knowing what cos and sin are! The topics of discrete domains - both time and frequency - are explained in an intuitive manner such that traveling between the two through Discrete Fourier Transform (DFT) becomes quite natural. Furthermore, the concepts needed to implement modern digital communication systems such as convolution, filters and multirate signal processing are illustrated through the help of beautiful figures. Next, the book demystifies modulation and demodulation in a way easy to grasp even for a non-technical reader. The focus is on linear modulations, particularly Pulse Amplitude Modulation (PAM), Quadrature Amplitude Modulation (QAM) and Phase Shift Keying (PSK). Matched filtering is clarified in time, frequency and mathematical details in a story-like development. In addition, the topic of pulse shape filtering is covered in a depth and from angles never

described anywhere before. The book continues with stethoscopes of a communication system, namely eye diagrams and scatter plots and towards the error rates of various modulation schemes along with the energy scaling factors of respective blocks. Finally, their spectral efficiencies are described taking into account the bandwidth, signal-to-noise ratio and data rates. This text is a simple way for you to enter at the beginner level and make your way up to wireless system design. Mathematics is included at a school level. I rely more on visualizing equations through beautiful figures. Therefore, you will encounter numerous figures throughout the text with logical and intuitive explanations. But you will not encounter any integrals, probability theory and detection/estimation theory. You will not even find any e or j of complex numbers either. The most complicated notation I have used is "sum everything from N1 to N2."

Communication System Design Using DSP Algorithms Packt Publishing Ltd

This book provides a new perspective on modeling cyber-physical systems (CPS), using a data-driven approach. The authors cover the use of state-of-the-art machine learning and artificial intelligence algorithms for modeling various aspect of the CPS. This book provides insight on how a data-driven modeling approach can be utilized to take advantage of the relation between the cyber and the physical domain of the CPS to aid the first-principle approach in capturing the stochastic phenomena affecting the CPS. The authors provide practical use cases of the data-driven modeling approach for securing the CPS, presenting novel attack models, building and maintaining the digital twin of the physical system. The book also presents novel, data-driven algorithms to handle non- Euclidean data. In summary, this book presents a novel perspective for modeling the CPS.

Signaling System No. 7 (SS7/C7) Springer Nature

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.

Afternoons with Mr. Hogan Cambridge University Press

Software-Defined Radio for EngineersArtech House

Galactic Radio Astronomy Cisco Press

Explore embedded systems pentesting by applying the most common attack techniques and patterns Key Features Learn various pentesting tools and techniques to attack and secure your hardware infrastructure Find the glitches in your hardware that can be a possible entry point for attacks Discover best practices for securely designing products Book Description

Hardware pentesting involves leveraging hardware interfaces and communication channels to find vulnerabilities in a device. Practical Hardware Pentesting will help you to plan attacks, hack your embedded devices, and secure the hardware infrastructure. Throughout the book, you will see how a specific device works, explore the functional and security aspects, and learn how a system senses and communicates with the outside world. You will start by setting up your lab from scratch and then gradually work with an advanced hardware lab. The book will help you get to grips with the global architecture of an embedded system and sniff on-board traffic. You will also learn how to identify and formalize threats to the embedded system and understand its relationship with its ecosystem. Later, you will discover how to analyze your hardware and locate its possible system vulnerabilities before going on to explore firmware dumping, analysis, and exploitation. Finally, focusing on the reverse engineering process from an attacker point of view will allow you to understand how devices are attacked, how they are compromised, and how you can harden a device against the most common hardware attack vectors. By the end of this book, you will be well-versed with security best practices and understand how they can be implemented to secure your hardware. What you will learn Perform an embedded system test and identify security critical functionalities Locate critical security components and buses and learn how to attack them Discover how to dump and modify stored information Understand and exploit the relationship between the firmware and hardware Identify and attack the security functions supported by the functional blocks of the device Develop an attack lab to support advanced device analysis and attacks Who this book is for This book is for security professionals and researchers who want to get started with hardware security assessment but don't know where to start. Electrical engineers who want to understand how their devices can be attacked and how to protect against these attacks will also find this book useful.

Data-Driven Modeling of Cyber-Physical Systems using Side-Channel Analysis Pearson Education

Cutting-edge techniques for finding and fixing critical security flaws Fortify your network and avert digital catastrophe with proven strategies from a team of security experts. Completely updated and featuring 13 new chapters, Gray Hat Hacking, The Ethical Hacker’s Handbook, Fifth Edition explains the enemy’s current weapons, skills, and tactics and offers field-tested remedies, case studies, and ready-to-try testing labs. Find out how hackers gain access, overtake network devices, script and inject malicious code, and plunder Web applications and browsers. Android-based exploits, reverse engineering techniques, and cyber law are thoroughly covered in this state-of-the-art resource. And the new topic of exploiting the Internet of things is introduced in this edition. •Build and launch spoofing exploits with Ettercap •Induce error conditions and crash software using fuzzers •Use advanced reverse engineering to exploit Windows and Linux

software •Bypass Windows Access Control and memory protection schemes •Exploit web applications with Padding Oracle Attacks •Learn the use-after-free technique used in recent zero days •Hijack web browsers with advanced XSS attacks •Understand ransomware and how it takes control of your desktop •Dissect Android malware with JEB and DAD decompilers •Find one-day vulnerabilities with binary diffing •Exploit wireless systems with Software Defined Radios (SDR) •Exploit Internet of things devices •Dissect and exploit embedded devices •Understand bug bounty programs •Deploy next-generation honeypots •Dissect ATM malware and analyze common ATM attacks •Learn the business side of ethical hacking

Practical Hardware Pentesting Createspace Independent Publishing Platform

Outlines a revisionist approach to management while arguing against common perceptions about the inevitability of startup failures, explaining the importance of providing genuinely needed products and services as well as organizing a business that can adapt to continuous customer feedback.

Inside Radio: An Attack and Defense Guide Springer

'Galactic Radio Astronomy' was chosen as the subject of this Symposium, which was held in conjunction with the IAU General Assembly that took place in Sydney in August 1973, largely because it is a very suitable Southern Hemisphere topic. This results in part from the advantages of a southern location in studying the Galaxy and in part from the long association of Australia with radio astronomy. Following the General Assembly, the Symposium was held at the Surf air Inter national Hotel in Maroochydore, Queensland, from 3 to 7 September, 1973. The conference participants were effectively isolated from the rest of the world during the Symposium, and the excellent spring weather and geographical situation led to the development of an unusually good rapport. The Symposium was sponsored by Commissions 40, 33, and 34. The Organizing Committee was composed of A. H. Barrett (chairman), J. E. Baldwin, D. S. Heeschen, F. J. Kerr, J. Lequeux, S. W. McCuskey, P. G. Mezger, B. Y. Mills, Yu. N. Parijskij, B. J. Robinson, H. van der Laan, and H. F. Weaver. The Local Committee, consisting ofB. J. Robinson, N. G. Seddon, and P. J. Kelly, looked after the arrangements in very fine style. The Symposium was supported financially by the IAU, the Australian Academy o~ Science, the CSIRO Division of Radiophysics, Union Carbide Australia Limited, and the Science Foundation for Physics within the University of Sydney.