

Asus Beta Firmware Rt

This book constitutes the proceedings of the 7th International Conference on Mobile Computing, Applications, and Services (MobiCASE 2015) held in Berlin, Germany, in November 2015. The 16 full and 4 poster papers were carefully reviewed and selected from 43 submissions, and are presented together with 4 papers from the First Workshop on Situation Recognition by Mining Temporal Information (SIREMETI 2015). The conference papers cover the following topics: intelligent caching, activity recognition and crowdsourcing, mobile frameworks, middleware, interactive applications and mobility.

Cloud Computing: Theory and Practice provides students and IT professionals with an in-depth analysis of the cloud from the ground up. Beginning with a discussion of parallel computing and architectures and distributed systems, the book turns to contemporary cloud infrastructures, how they are being deployed at leading companies such as Amazon, Google and Apple, and how they can be applied in fields such as healthcare, banking and science. The volume also examines how to successfully deploy a cloud application across the enterprise using virtualization, resource management and the right amount of networking support, including content delivery networks and storage area networks.

Developers will find a complete introduction to application development provided on a variety of platforms. Learn about recent trends in cloud computing in critical areas such as: resource management, security, energy consumption, ethics, and complex systems Get a detailed hands-on set of practical recipes that help simplify the deployment of a cloud based system for practical use of computing clouds along with an in-depth discussion of several projects Understand the evolution of cloud computing and why the cloud computing paradigm has a better chance to succeed than previous efforts in large-scale distributed computing One problem with helicoptering is that there are virtually no flying clubs, at least of the sort that exist for fixed wing, so pilots get very little chance to swap stories, unless they meet in a muddy field somewhere, waiting for their passengers. As a result, the same mistakes are being made and the same lessons learnt separately instead of being shared - it's comforting sometimes to know that you're not the only one to inflate the floats by accident! Even when you do get into a school, there are still a couple of things they don't teach you, namely that aviation runs on paperwork, and how to get a job, including interview techniques, etc - flying the aircraft is actually less than a third of the job. Another is that nobody really tells you anything, either about the job you have to do (from the customer) or how to do it (the company) - you will always be up against the other guy who managed to do it last week! Sure, there will be training, but, even in the best companies, this will be relatively minimal. This book is an attempt to correct the above situations by gathering together as much information as possible for helicopter pilots, old and new, professional and otherwise, in an attempt to explain the why, so the how will become easier (you will be so much more useful

if you know what the customer is trying to achieve). In short, this is all the stuff nobody taught me - every tip and trick I have learnt has been included. Kismet is the industry standard for examining wireless network traffic, and is used by over 250,000 security professionals, wireless networking enthusiasts, and WarDriving hobbyists. Unlike other wireless networking books that have been published in recent years that geared towards Windows users, Kismet Hacking is geared to those individuals that use the Linux operating system. People who use Linux and want to use wireless tools need to use Kismet. Now with the introduction of Kismet NewCore, they have a book that will answer all their questions about using this great tool. This book continues in the successful vein of books for wireless users such as WarDriving: Drive, Detect Defend. *Wardrive Running Kismet from the BackTrack Live CD *Build and Integrate Drones with your Kismet Server *Map Your Data with GPSTMap, KisMap, WiGLE and GpsDrive

This book constitutes the refereed proceedings of the 21st International Symposium on Research in Attacks, Intrusions, and Defenses, RAID 2018, held in Heraklion, Crete, Greece, in September 2018. The 32 revised full papers were carefully reviewed and selected from 145 submissions. They are organized in the following topical sections: attacks; intrusion detection and prevention; DDoS attacks; passwords, accounts, and users; machine learning for computer security; hardware-assisted security; software security; malware; IoT/CPS security; security measurements; and defenses.

The 3-volume set CCIS 1422, CCIS 1423 and CCIS 1424 constitutes the refereed proceedings of the 7th International Conference on Artificial Intelligence and Security, ICAIS 2021, which was held in Dublin, Ireland, in July 2021. The total of 131 full papers and 52 short papers presented in this 3-volume proceedings was carefully reviewed and selected from 1013 submissions. The papers were organized in topical sections as follows: Part I: artificial intelligence; Part II: artificial intelligence; big data; cloud computing and security internet; Part III: cloud computing and security; encryption and cybersecurity; information hiding; IoT security. .

Windows 8 SecretsJohn Wiley & SonsAdvances in Artificial Intelligence and Security7th International Conference, ICAIS 2021, Dublin, Ireland, July 19-23, 2021, ProceedingsSpringer Nature

This 2nd edition textbook has been expanded to include of 175 additional pages of additional content, created in response to readers feedback, as well as to new hardware and software releases. The book presents foundational robotics concepts using the ROBOTIS BIOLOID and OpenCM-904 robotic systems, and is suitable as a curriculum for a first course in robotics for undergraduate students or a self-learner. It covers wheel-based robots, as well as walking robots. Although it uses the standard "Sense, Think, Act" approach, communications (bot-to-bot and PC-to-bot) programming concepts are treated in more depth (wired and wireless ZigBee/Bluetooth). Algorithms are developed

and described via ROBOTIS' proprietary RoboPlus IDE, as well as the more open Arduino-based Embedded C environments. Additionally, a vast array of web-based multimedia materials are used for illustrating robotics concepts, code implementations and videos of actual resulting robot behaviors. Advanced sensor interfacing for gyroscope, inertial measuring unit, foot pressure sensor and color camera are also demonstrated.

Written as a tutorial to explore and understand the power of R for machine learning. This practical guide that covers all of the need to know topics in a very systematic way. For each machine learning approach, each step in the process is detailed, from preparing the data for analysis to evaluating the results. These steps will build the knowledge you need to apply them to your own data science tasks. Intended for those who want to learn how to use R's machine learning capabilities and gain insight from your data. Perhaps you already know a bit about machine learning, but have never used R; or perhaps you know a little R but are new to machine learning. In either case, this book will get you up and running quickly. It would be helpful to have a bit of familiarity with basic programming concepts, but no prior experience is required.

Using the new OpenCL (Open Computing Language) standard, you can write applications that access all available programming resources: CPUs, GPUs, and other processors such as DSPs and the Cell/B.E. processor. Already implemented by Apple, AMD, Intel, IBM, NVIDIA, and other leaders, OpenCL has outstanding potential for PCs, servers, handheld/embedded devices, high performance computing, and even cloud systems. This is the first comprehensive, authoritative, and practical guide to OpenCL 1.1 specifically for working developers and software architects. Written by five leading OpenCL authorities, OpenCL Programming Guide covers the entire specification. It reviews key use cases, shows how OpenCL can express a wide range of parallel algorithms, and offers complete reference material on both the API and OpenCL C programming language. Through complete case studies and downloadable code examples, the authors show how to write complex parallel programs that decompose workloads across many different devices. They also present all the essentials of OpenCL software performance optimization, including probing and adapting to hardware. Coverage includes Understanding OpenCL's architecture, concepts, terminology, goals, and rationale Programming with OpenCL C and the runtime API Using buffers, sub-buffers, images, samplers, and events Sharing and synchronizing data with OpenGL and Microsoft's Direct3D Simplifying development with the C++ Wrapper API Using OpenCL Embedded Profiles to support devices ranging from cellphones to supercomputer nodes Case studies dealing with physics simulation; image and signal processing, such as image histograms, edge detection filters, Fast Fourier Transforms, and optical flow; math libraries, such as matrix multiplication and high-performance sparse matrix multiplication; and more Source code for this book is available at <https://code.google.com/p/opencv-book-samples/>

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. So, you've created a few projects with Arduino, and now it's time to kick it up a notch. Where do you go next? With **Pro Arduino**, you'll learn about new tools, techniques, and frameworks to make even more ground-breaking, eye-popping projects. You'll discover how to make Arduino-based gadgets and robots interact with your mobile phone. You'll learn all about the changes in Arduino 1.0, you'll create amazing output with **openFrameworks**, and you'll learn how to make games with the **Gameduino**. You'll also learn advanced topics, such as modifying the Arduino to work with non-standard Atmel chips and Microchip's PIC32. Rick Anderson, an experienced Arduino developer and instructor, and Dan Cervo, an experienced Arduino gadgeteer, will give you a guided tour of advanced Arduino capabilities. If it can be done with an Arduino, you'll learn about it here. This book constitutes the revised selected papers from the 13th International Conference on Risks and Security of Internet and Systems, **CRISIS 2018**, held in Arcachon, France, in October 2018. The 12 full papers and 6 short papers presented in this volume were carefully reviewed and selected from 34 submissions. They cover diverse research themes that range from classic topics, such as vulnerability analysis and classification; apps security; access control and filtering; cloud security; cyber-insurance and cyber threat intelligence; human-centric security and trust; and risk analysis. This is the origin story of technology super heroes: the creators and founders of ARM, the company that is responsible for the processors found inside 95% of the world's mobile devices today. This is also the evolution story of how three companies - Apple, Samsung, and Qualcomm - put ARM technology in the hands of billions of people through smartphones, tablets, music players, and more. It was anything but a straight line from idea to success for ARM. The story starts

with the triumph of BBC Micro engineers Steve Furber and Sophie Wilson, who make the audacious decision to design their own microprocessor - and it works the first time. The question becomes, how to sell it? Part I follows ARM as its founders launch their own company, select a new leader, a new strategy, and find themselves partnered with Apple, TI, Nokia, and other companies just as digital technology starts to unleash mobile devices. ARM grows rapidly, even as other semiconductor firms struggle in the dot com meltdown, and establishes itself as a standard for embedded RISC processors. Apple aficionados will find the opening of Part II of interest the moment Steve Jobs returns and changes the direction toward fulfilling consumer dreams. Samsung devotees will see how that firm evolved from its earliest days in consumer electronics and semiconductors through a philosophical shift to innovation. Qualcomm followers will learn much of their history as it plays out from satellite communications to development of a mobile phone standard and emergence as a leading fabless semiconductor company. If ARM could be summarized in one word, it would be "collaboration." Throughout this story, from Foreword to Epilogue, efforts to develop an ecosystem are highlighted. Familiar names such as Google, Intel, Mediatek, Microsoft, Motorola, TSMC, and others are interwoven throughout. The evolution of ARM's first 25 years as a company wraps up with a shift to its next strategy: the Internet of Things, the ultimate connector for people and devices. Research for this story is extensive, simplifying a complex mobile industry timeline and uncovering critical points where ARM and other companies made fateful and sometimes surprising decisions. Rare photos, summary diagrams and tables, and unique perspectives from insiders add insight to this important telling of technology history.

This book outlines innovative processes used to research, conceive and develop innovations in the Customer eXperience (CX) space for both large and small companies.

The open source nature of the platform has not only established a new direction for the industry, but enables a developer or forensic analyst to understand the device at the most fundamental level. Android Forensics covers an open source mobile device platform based on the Linux 2.6 kernel and managed by the Open Handset Alliance. The Android platform is a major source of digital forensic investigation and analysis. This book provides a thorough review of the Android platform including supported hardware devices, the structure of the Android development project and implementation of core services (wireless communication, data storage and other low-level functions). Finally, it will focus on teaching readers how to apply actual forensic techniques to recover data. Ability to forensically acquire Android devices using the techniques outlined in the book Detailed information about Android applications needed for forensics investigations Important information about SQLite, a file based structured data storage relevant for both Android and many other platforms.

The revised and extended papers collected in this volume represent the cutting-

edge of research at the nexus of electrical engineering and intelligent systems. They were selected from well over 1000 papers submitted to the high-profile international World Congress on Engineering held in London in July 2011. The chapters cover material across the full spectrum of work in the field, including computational intelligence, control engineering, network management, and wireless networks. Readers will also find substantive papers on signal processing, Internet computing, high performance computing, and industrial applications. The Electrical Engineering and Intelligent Systems conference, as part of the 2011 World Congress on Engineering was organized under the auspices of the non-profit International Association of Engineers (IAENG). With more than 30 nations represented on the conference committees alone, the Congress features the best and brightest scientific minds from a multitude of disciplines related to engineering. These peer-reviewed papers demonstrate the huge strides currently being taken in this rapidly developing field and reflect the excitement of those at the frontiers of this research.

Optimizing Network Traffic is a valuable technical resource that outlines the best practices for managing enterprise-scale network traffic on a Microsoft Windows NT Server 4.0 network. Based on the real-world experiences and projects of Microsoft Consulting Services (MCS), this guide helps IT professionals plan, increase, and manage network communications systemwide. Referring to Optimizing Network Traffic is like having an MCS consultant right there to help you determine the best approach to your network traffic needs. You'll learn how other organizations have wrestled with and resolved similar issues in capturing, benchmarking, and analyzing network traffic data to resolve systemwide problems and scalability issues.

Briefly, a boot loader is the first software program that runs when a computer starts. It is responsible for loading and transferring control to an operating system kernel software (such as Linux or GNU Mach). The kernel, in turn, initializes the rest of the operating system (e.g. a GNU system). GNU GRUB is a very powerful boot loader, which can load a wide variety of free operating systems, as well as proprietary operating systems with chain-loading. GRUB is designed to address the complexity of booting a personal computer; both the program and this manual are tightly bound to that computer platform, although porting to other platforms may be addressed in the future. One of the important features in GRUB is flexibility; GRUB understands filesystems and kernel executable formats, so you can load an arbitrary operating system the way you like, without recording the physical position of your kernel on the disk. Thus you can load the kernel just by specifying its file name and the drive and partition where the kernel resides. This manual is available online for free at gnu.org. This manual is printed in grayscale. For over a decade, Andrew "bunnie" Huang, one of the world's most esteemed hackers, has shaped the fields of hacking and hardware, from his cult-classic book *Hacking the Xbox* to the open-source laptop Novena and his mentorship of various hardware startups and developers. In *The Hardware Hacker*, Huang

shares his experiences in manufacturing and open hardware, creating an illuminating and compelling career retrospective. Huang's journey starts with his first visit to the staggering electronics markets in Shenzhen, with booths overflowing with capacitors, memory chips, voltmeters, and possibility. He shares how he navigated the overwhelming world of Chinese factories to bring chumby, Novena, and Chibitronics to life, covering everything from creating a Bill of Materials to choosing the factory to best fit his needs. Through this collection of personal essays and interviews on topics ranging from the legality of reverse engineering to a comparison of intellectual property practices between China and the United States, bunnieweaves weaves engineering, law, and society into the tapestry of open hardware. With highly detailed passages on the ins and outs of manufacturing and a comprehensive take on the issues associated with open source hardware, *The Hardware Hacker* is an invaluable resource for aspiring hackers and makers.

This book sheds light on all aspects of earnings claims, including defining what an earnings claim really is, the origins of its regulation under the franchise disclosure laws, how a franchisor should prepare an earnings claim, how a franchisee should use an earnings claim, how a franchisee may attack lawful and unlawful earnings claims, how a franchisor may defend against such attacks, and how the government franchise enforcement authorities investigate unlawful earnings claim activity.

Bring life to your robot using ROS robotic applications About This Book This book will help you boost your knowledge of ROS and give you advanced practical experience you can apply to your ROS robot platforms This is the only book that offers you step-by-step instructions to solidify your ROS understanding and gain experience using ROS tools From eminent authors, this book offers you a plethora of fun-filled examples to make your own quadcopter, turtlebot, and two-armed robots Who This Book Is For If you are a robotics developer, whether a hobbyist, researchers or professional, and are interested in learning about ROS through a hands-on approach, then this book is for you. You are encouraged to have a working knowledge of GNU/Linux systems and Python. What You Will Learn Get to know the fundamentals of ROS and apply its concepts to real robot examples Control a mobile robot to navigate autonomously in an environment Model your robot designs using URDF and Xacro, and operate them in a ROS Gazebo simulation Control a 7 degree-of-freedom robot arm for visual servoing Fly a quadcopter to autonomous waypoints Gain working knowledge of ROS tools such as Gazebo, rviz, rqt, and Move-It Control robots with mobile devices and controller boards In Detail The visionaries who created ROS developed a framework for robotics centered on the commonality of robotic systems and exploited this commonality in ROS to expedite the development of future robotic systems. From the fundamental concepts to advanced practical experience, this book will provide you with an incremental knowledge of the ROS framework, the backbone of the robotics evolution. ROS standardizes many layers of robotics functionality from low-level device drivers to process control to message passing to software package management. This book provides step-by-step examples of mobile, armed, and flying robots, describing the ROS implementation as the basic model for other robots of these types. By controlling these robots, whether in simulation or in reality, you will use ROS to drive, move, and fly robots using ROS control. Style and approach This is an easy-to-follow guide with hands-on examples of ROS robots, both real and in simulation.

This book constitutes the refereed proceedings of the 36th IFIP TC 11 International Conference on Information Security and Privacy Protection, SEC 2021, held in Oslo, Norway, in June 2021.* The 28 full papers presented were carefully reviewed and selected from 112 submissions. The papers present novel research on theoretical and practical aspects of security and privacy protection in ICT systems. They are organized in topical sections on digital signatures; vulnerability management; covert channels and cryptography; application and system security; privacy; network security; machine learning for security; and security management. *The conference was held virtually.

This book constitutes revised papers from the nine workshops and one accompanying event which took place at the 22nd International Conference on Business Information Systems, BIS 2019, held in Seville, Spain, in June 2019. There was a total of 139 submissions to all workshops of which 57 papers were accepted for publication. The workshops included in this volume are: AKTB 2019: 11th Workshop on Applications of Knowledge-Based Technologies in Business BITA 2019: 10th Workshop on Business and IT Alignment BSCT 2019: Second Workshop on Blockchain and Smart Contract Technologies DigEX 2019: First International Workshop on transforming the Digital Customer Experience iCRM 2019: 4th International Workshop on Intelligent Data Analysis in Integrated Social CRM iDEATE 2019: 4th Workshop on Big Data and Business Analytics Ecosystems ISMAD 2019: Workshop on Information Systems and Applications in Maritime Domain QOD 2019: Second Workshop on Quality of Open Data SciBOWater 2019: Second Workshop on Scientific Challenges and Business Opportunities in Water Management

This book constitutes the refereed proceedings of the 24th Nordic Conference on Secure IT Systems, NordSec 2019, held in Aalborg, Denmark, in November 2019. The 17 full papers presented in this volume were carefully reviewed and selected from 32 submissions. They are organized in topical sections named: privacy; network security; platform security and malware; and system and software security.

With the Supreme Court likely to reverse *Roe v. Wade*, the landmark abortion decision, American debate appears fixated on clashing rights. The first comprehensive legal history of a vital period, *Abortion and the Law in America* illuminates an entirely different and unexpected shift in the terms of debate. Rather than simply championing rights, those on opposing sides battled about the policy costs and benefits of abortion and laws restricting it. This mostly unknown turn deepened polarization in ways many have missed. Never abandoning their constitutional demands, pro-choice and pro-life advocates increasingly disagreed about the basic facts. Drawing on unexplored records and interviews with key participants, Ziegler complicates the view that the Supreme Court is responsible for the escalation of the conflict. A gripping account of social-movement divides and crucial legal strategies, this book delivers a definitive recent history of an issue that transforms American law and politics to this day.

Learn how to write high-quality kernel module code, solve common Linux kernel programming issues, and understand the fundamentals of Linux kernel internals Key Features Discover how to write kernel code using the Loadable Kernel Module framework Explore industry-grade techniques to perform efficient memory allocation and data synchronization within the kernel Understand the essentials of key internals topics such as kernel architecture, memory management, CPU scheduling, and kernel synchronization Book Description Linux Kernel Programming is a comprehensive introduction for those new to Linux kernel and module development. This easy-to-follow guide will have you up and running with writing kernel code in next-to-no time. This book uses the latest 5.4 Long-Term Support (LTS) Linux kernel, which will be maintained from November 2019 through to December 2025. By working with the 5.4 LTS kernel throughout the book, you can be confident that your knowledge will continue to be valid for years to come. This Linux book begins by showing you how to build the kernel from the source. Next, you'll learn how to write your first kernel module using the powerful Loadable

Kernel Module (LKM) framework. The book then covers key kernel internals topics including Linux kernel architecture, memory management, and CPU scheduling. Next, you'll delve into the fairly complex topic of concurrency within the kernel, understand the issues it can cause, and learn how they can be addressed with various locking technologies (mutexes, spinlocks, atomic, and refcount operators). You'll also benefit from more advanced material on cache effects, a primer on lock-free techniques within the kernel, deadlock avoidance (with lockdep), and kernel lock debugging techniques. By the end of this kernel book, you'll have a detailed understanding of the fundamentals of writing Linux kernel module code for real-world projects and products. What you will learn Write high-quality modular kernel code (LKM framework) for 5.x kernels Configure and build a kernel from source Explore the Linux kernel architecture Get to grips with key internals regarding memory management within the kernel Understand and work with various dynamic kernel memory alloc/dealloc APIs Discover key internals aspects regarding CPU scheduling within the kernel Gain an understanding of kernel concurrency issues Find out how to work with key kernel synchronization primitives Who this book is for This book is for Linux programmers beginning to find their way with Linux kernel development. Linux kernel and driver developers looking to overcome frequent and common kernel development issues, as well as understand kernel internals, will benefit from this book. A basic understanding of Linux CLI and C programming is required.

This book constitutes the refereed proceedings of the 13th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2016, held in San Sebastián, Spain, in July 2016. The 19 revised full papers and 2 extended abstracts presented were carefully reviewed and selected from 66 submissions. They present the state of the art in intrusion detection, malware analysis, and vulnerability assessment, dealing with novel ideas, techniques, and applications in important areas of computer security including vulnerability detection, attack prevention, web security, malware detection and classification, authentication, data leakage prevention, and countering evasive techniques such as obfuscation.

"If I had this book 10 years ago, the FBI would never have found me!" -- Kevin Mitnick This book has something for everyone---from the beginner hobbyist with no electronics or coding experience to the self-proclaimed "gadget geek." Take an ordinary piece of equipment and turn it into a personal work of art. Build upon an existing idea to create something better. Have fun while voiding your warranty! Some of the hardware hacks in this book include: * Don't toss your iPod away when the battery dies! Don't pay Apple the \$99 to replace it! Install a new iPod battery yourself without Apple's "help" * An Apple a day! Modify a standard Apple USB Mouse into a glowing UFO Mouse or build a FireWire terabyte hard drive and custom case * Have you played Atari today? Create an arcade-style Atari 5200 paddle controller for your favorite retro videogames or transform the Atari 2600 joystick into one that can be used by left-handed players * Modern game systems, too! Hack your PlayStation 2 to boot code from the memory card or modify your PlayStation 2 for homebrew game development * Videophiles unite! Design, build, and configure your own Windows- or Linux-based Home Theater PC * Ride the airwaves! Modify a wireless PCMCIA NIC to include an external antenna connector or load Linux onto your Access Point * Stick it to The Man! Remove the proprietary barcode encoding from your CueCat and turn it into a regular barcode reader * Hack your Palm! Upgrade the available RAM on your Palm m505 from 8MB to 16MB · Includes hacks of today's most popular gaming

systems like Xbox and PS/2. · Teaches readers to unlock the full entertainment potential of their desktop PC. · Frees iMac owners to enhance the features they love and get rid of the ones they hate.

This book will teach the reader how to make the most of their WRT54G series hardware. These handy little inexpensive devices can be configured for a near endless amount of networking tasks. The reader will learn about the WRT54G's hardware components, the different third-party firmware available and the differences between them, choosing the firmware that is right for you, and how to install different third-party firmware distributions. Never before has this hardware been documented in this amount of detail, which includes a wide-array of photographs and complete listing of all WRT54G models currently available, including the WRTSL54GS. Once this foundation is laid, the reader will learn how to implement functionality on the WRT54G for fun projects, penetration testing, various network tasks, wireless spectrum analysis, and more! This title features never before seen hacks using the WRT54G. For those who want to make the most out of their WRT54G you can learn how to port code and develop your own software for the OpenWRT operating system. Never before seen and documented hacks, including wireless spectrum analysis Most comprehensive source for documentation on how to take advantage of advanced features on the inexpensive wrt54g platform Full coverage on embedded device development using the WRT54G and OpenWRT

This IBM® Redbooks® publication documents and addresses topics to provide step-by-step customizable application and programming solutions to tune application and workloads to use IBM Power Systems™ hardware architecture. This publication explores, tests, and documents the solution to use the architectural technologies and the software solutions that are available from IBM to help solve challenging technical and business problems. This publication also demonstrates and documents that the combination of IBM high-performance computing (HPC) solutions (hardware and software) delivers significant value to technical computing clients who are in need of cost-effective, highly scalable, and robust solutions. First, the book provides a high-level overview of the HPC solution, including all of the components that makes the HPC cluster: IBM Power System S822LC (8335-GTB), software components, interconnect switches, and the IBM Spectrum™ Scale parallel file system. Then, the publication is divided in three parts: Part 1 focuses on the developers, Part 2 focuses on the administrators, and Part 3 focuses on the evaluators and planners of the solution. The IBM Redbooks publication is targeted toward technical professionals (consultants, technical support staff, IT Architects, and IT Specialists) who are responsible for delivering cost-effective HPC solutions that help uncover insights from vast amounts of client's data so they can optimize business results, product development, and scientific discoveries.

The definitive guide to penetrating and defending wireless networks. Straight from the field, this is the definitive guide to hacking wireless networks. Authored

by world-renowned wireless security auditors, this hands-on, practical guide covers everything you need to attack -- or protect -- any wireless network. The authors introduce the 'battlefield,' exposing today's 'wide open' 802.11 wireless networks and their attackers. One step at a time, you'll master the attacker's entire arsenal of hardware and software tools: crucial knowledge for crackers and auditors alike. Next, you'll learn systematic countermeasures for building hardened wireless 'citadels' including cryptography-based techniques, authentication, wireless VPNs, intrusion detection, and more. Coverage includes: Step-by-step walkthroughs and explanations of typical attacks Building wireless hacking/auditing toolkit: detailed recommendations, ranging from discovery tools to chipsets and antennas Wardriving: network mapping and site surveying Potential weaknesses in current and emerging standards, including 802.11i, PPTP, and IPSec Implementing strong, multilayered defenses Wireless IDS: why attackers aren't as untraceable as they think Wireless hacking and the law: what's legal, what isn't If you're a hacker or security auditor, this book will get you in. If you're a netadmin, sysadmin, consultant, or home user, it will keep everyone else out.

Learn how to set up and configure networks to create robust connections, and how to quickly diagnose and repair problems should something go wrong. Whatever version of Windows you are using, you will need a stable Internet connection and access to your company network and its shared files and resources. When a network connection fails, it can result in an expensive loss of productivity. What You'll Learn Set up and manage different types of network connections Use and configure Windows TCP/IP stack Determine the common causes of networking problems and how to avoid them Troubleshoot network connection problems Manage networking for Windows virtual machines Keep the mobile or BYOD worker connected to your company network Who This Book Is For IT pros, Windows expert and power users, and system administrators The number of Android devices running on Intel processors has increased since Intel and Google announced, in late 2011, that they would be working together to optimize future versions of Android for Intel Atom processors. Today, Intel processors can be found in Android smartphones and tablets made by some of the top manufacturers of Android devices, such as Samsung, Lenovo, and Asus. The increase in Android devices featuring Intel processors has created a demand for Android applications optimized for Intel Architecture: Android Application Development for the Intel® Platform is the perfect introduction for software engineers and mobile app developers. Through well-designed app samples, code samples and case studies, the book teaches Android application development based on the Intel platform—including for smartphones, tablets, and embedded devices—covering performance tuning, debugging and optimization. This book is jointly developed for individual learning by Intel Software College and China Shanghai JiaoTong University.

[Copyright: 05f72f2e5ff75eac9dda5c32fceb2257](http://05f72f2e5ff75eac9dda5c32fceb2257)