

Dalvik And Art Android Internals Newandroidbook

This book constitutes the refereed proceedings of the 10th International IFIP WG 2.13 Conference on Open Source Systems, OSS 2014, held in San José, Costa Rica, in May 2014. The 16 revised full papers and 16 short papers presented together with 5 poster papers were carefully reviewed and selected from 61 submissions. They have been organized in the following topical sections: open source visualization and reporting; open source in business modeling; open source in mobile and web technologies; open source in education and research; development processes of open source products; testing and assurance of open source projects; and global impact on open source communities and development. The last section consists of five case studies and demonstrations of open source projects.

Explore real-world threat scenarios, attacks on mobile applications, and ways to counter them About This Book Gain insights into the current threat landscape of mobile applications in particular Explore the different options that are available on mobile platforms and prevent circumventions made by attackers This is a step-by-step guide to setting up your own mobile penetration testing environment Who This Book Is For If you are a mobile application evangelist, mobile application developer, information security practitioner, penetration tester on infrastructure web applications, an application security professional, or someone who wants to learn mobile application security as a career, then this book is for you. This book will provide you with all the skills you need to get started with Android and iOS pen-testing. What You Will Learn Gain an in-depth understanding of Android and iOS architecture and the latest changes Discover how to work with different tool suites to assess any application Develop different strategies and techniques to connect to a mobile device Create a foundation for mobile application security principles Grasp techniques to attack different components of an Android device and the different functionalities of an iOS device Get to know secure development strategies for both iOS and Android applications Gain an understanding of threat modeling mobile applications Get an in-depth understanding of both Android and iOS implementation vulnerabilities and how to provide counter-measures while developing a mobile app In Detail Mobile security has come a long way over the last few years. It has transitioned from "should it be done?" to "it must be done!" Alongside the growing number of devices and applications, there is also a growth in the volume of Personally identifiable information (PII), Financial Data, and much more. This data needs to be secured. This is why Pen-testing is so important to modern application developers. You need to know how to secure user data, and find vulnerabilities and loopholes in your application that might lead to security breaches. This book gives you the necessary skills to security test your mobile applications as a beginner, developer, or security practitioner. You'll start by discovering the internal components of an Android and an iOS application. Moving ahead, you'll understand the inter-process working of these applications. Then you'll set up a test environment for this application using various tools to identify the loopholes and vulnerabilities in the structure of the applications. Finally, after collecting all information about these security loop holes, we'll start securing our applications from these threats. Style and approach This is an easy-to-follow guide full of hands-on examples of real-world attack simulations. Each topic is explained in context with respect to testing, and for the more inquisitive, there are more details on the concepts and techniques used for different platforms.

Google Android dominates the mobile market, and by targeting Android, your apps can run on most of the phones and tablets in the world. This new fourth edition of the #1 book for learning Android covers all modern Android versions from Android 4.1 through Android 5.0. Freshly added material covers new Android features such as Fragments and Google Play Services. Android is a platform you can't afford not to learn, and this book gets you started. Android is a software toolkit for mobile phones and tablets, created by Google. It's inside more than a billion devices, making Android the number one platform for application developers. Your own app could be running on all those devices! Getting started developing with Android is easy. You don't even need access to an Android phone, just a computer where you can install the Android SDK and the emulator that comes with it. Within minutes, Hello, Android gets you creating your first working application: Android's version of "Hello, World." From there, you'll build up a more substantial example: an Ultimate Tic-Tac-Toe game. By gradually adding features to the game, you'll learn about many aspects of Android programming, such as creating animated user interfaces, playing music and sound effects, building location-based services (including GPS and cell-tower triangulation), and accessing web services. You'll also learn how to publish your applications to the Google Play Store. This fourth edition of the bestselling Android classic has been revised for Android 4.1-4.3 (Jelly Bean), 4.4 (KitKat), and Android 5.0 (Lollipop). Topics have been streamlined and simplified based on reader feedback, and every page and example has been reviewed and updated for compatibility with the latest versions of Android. If you'd rather be coding than reading about coding, this book is for you.

MQ Telemetry Transport (MQTT) is a messaging protocol that is lightweight enough to be supported by the smallest devices, yet robust enough to ensure that important messages get to their destinations every time. With MQTT devices such as smart energy meters, cars, trains, satellite receivers, and personal health care devices can communicate with each other and with other systems or applications. This IBM® Redbooks® publication introduces MQTT and takes a scenario-based approach to demonstrate its capabilities. It provides a quick guide to getting started and then shows how to grow to an enterprise scale MQTT server using IBM WebSphere® MQ Telemetry. Scenarios demonstrate how to integrate MQTT with other IBM products, including WebSphere Message Broker. This book also provides typical usage patterns and guidance on scaling a solution. The intended audience for this book ranges from new users of MQTT and telemetry to those readers who are looking for in-depth knowledge and advanced topics.

There are many Android programming guides that give you the basics. This book goes beyond simple apps into many areas of Android development that you simply will not find in competing books. Whether you want to add home screen app widgets to your arsenal, or create more complex maps, integrate multimedia features like the camera, integrate tightly with other applications, or integrate scripting languages, this book has you covered. Moreover, this book has over 50 pages of Honeycomb-specific material, from dynamic fragments, to integrating navigation into the action bar, to creating list-based app widgets. It also has a chapter on using NFC, the wireless technology behind Google Wallet and related services. This book is one in CommonsWare's growing series of Android related titles, including "The Busy Coder's Guide to Android Development," "Android Programming Tutorials," and the upcoming "Tuning Android Applications." Table of Contents WebView, Inside and Out Crafting Your Own Views More Fun With ListViews Creating Drawables Home Screen App Widgets Interactive Maps Creating Custom Dialogs and Preferences Advanced Fragments and the Action Bar Animating Widgets Using the Camera Playing Media Handling System Events Advanced Service Patterns Using

System Settings and Services Content Provider Theory Content Provider Implementation Patterns The Contacts ContentProvider Searching with SearchManager Introspection and Integration Tapjacking Working with SMS More on the Manifest Device Configuration Push Notifications with C2DM NFC The Role of Scripting Languages The Scripting Layer for Android JVM Scripting Languages Reusable Components Testing Production

The rapid growth and development of Android-based devices has resulted in a wealth of sensitive information on mobile devices that offer minimal malware protection. This has created an immediate need for security professionals that understand how to best approach the subject of Android malware threats and analysis. In *Android Malware and Analysis*, K Build Android N applications using modern techniques and libraries to get your own high-quality apps published on Google Play in no time About This Book Get started with Android development, from the installation of required tools to publishing to the market Make your applications Android N ready—Android has evolved quite a lot since the very beginning and so has their Software Development Kit—so get up to speed Save time and improve the quality of your applications with widely used open source libraries and dependency management Who This Book Is For Want to get started with Android development? Start here. What You Will Learn Get to know how to use popular open source libraries to reduce time to market and avoid re-inventing the wheel Automate your application's testing phase to avoid last minute crashes Use dependency management to properly keep dependencies and updates under control Efficiently show huge amounts of items in a list Forget about memory and speed concerns Publish and monetize your Android applications on Google Play Persist your application data so it can continue working in offline mode Don't let the UX break because of network issues In Detail The mobile app market is huge. But where do you start? And how you can deliver something that takes Google Play by storm? This guide is the perfect route into Android app development – while it's easy for new apps to sink without a trace, we'll give you the best chance of success with practical and actionable guidance that will unlock your creativity and help you put the principles of Android development into practice. From the fundamentals and getting your project started to publishing your app to a huge market of potential customers, follow this guide to become a confident, creative and reliable mobile developer. Get to grips with new components in Android 7 such as RecyclerView, and find out how to take advantage of automated testing, and, of course, much, much more. What are you waiting for? There's never been a better time – or a better way – to get into Android app development. Style and approach More than just a manual, this is an accessible route into Android development. Packed with examples that demonstrate how to put key concepts and ideas into practice, this guide isn't just about learning, it's about immediate development.

The book examines how Fog will change the information technology industry in the next decade. Fog distributes the services of computation, communication, control and storage closer to the edge, access and users. As a computing and networking architecture, Fog enables key applications in wireless 5G, the Internet of Things, and big data. The authors cover the fundamental tradeoffs to major applications of fog. The book chapters are designed to motivate a transition from the current cloud architectures to the Fog (Chapter 1), and the necessary architectural components to support such a transition (Chapters 2-6). The rest of the book (Chapters 7-xxx) are dedicated to reviewing the various 5G and IoT applications that will benefit from Fog networking. This volume is edited by pioneers in Fog and includes contributions by active researchers in the field. Covers fog technologies and describes the interaction between fog and cloud Presents a view of fog and IoT (encompassing ubiquitous computing) that combines the aspects of both industry and academia Discusses the various architectural and design challenges in coordinating the interactions between M2M, D2D and fog technologies "Fog for 5G and IoT" serves as an introduction to the evolving Fog architecture, compiling work from different areas that collectively form this paradigm

Mobile devices, such as smart phones, have achieved computing and networking capabilities comparable to traditional personal computers. Their successful consumerization has also become a source of pain for adopting users and organizations. In particular, the widespread presence of information-stealing applications and other types of mobile malware raises substantial security and privacy concerns. *Android Malware* presents a systematic view on state-of-the-art mobile malware that targets the popular Android mobile platform. Covering key topics like the Android malware history, malware behavior and classification, as well as, possible defense techniques.

Android on x86: an Introduction to Optimizing for Intel® Architecture serves two main purposes. First, it makes the case for adapting your applications onto Intel's x86 architecture, including discussions of the business potential, the changing landscape of the Android marketplace, and the unique challenges and opportunities that arise from x86 devices. The fundamental idea is that extending your applications to support x86 or creating new ones is not difficult, but it is imperative to know all of the technicalities. This book is dedicated to providing you with an awareness of these nuances and an understanding of how to tackle them. Second, and most importantly, this book provides a one-stop detailed resource for best practices and procedures associated with the installation issues, hardware optimization issues, software requirements, programming tasks, and performance optimizations that emerge when developers consider the x86 Android devices. Optimization discussions dive into native code, hardware acceleration, and advanced profiling of multimedia applications. The authors have collected this information so that you can use the book as a guide for the specific requirements of each application project. This book is not dedicated solely to code; instead it is filled with the information you need in order to take advantage of x86 architecture. It will guide you through installing the Android SDK for Intel Architecture, help you understand the differences and similarities between processor architectures available in Android devices, teach you to create and port applications, debug existing x86 applications, offer solutions for NDK and C++ optimizations, and introduce the Intel Hardware Accelerated Execution Manager. This book provides the most useful information to help you get the job done quickly while utilizing best practices. What you'll learn The development-relevant differences between Android on ARM and Android on Intel x86 How to set up the SDK for an emulated Intel Android device How to build the Android OS for the Intel Mobile Processor How to create new x86 based Android applications, set up testing and performance tuning, and port existing Android applications to work with the x86 processor How to debug problems they encounter when working on the x86 Android test platform Intricacies of the Intel Hardware Accelerated Execution Manager. The reader will also gain significant insight into the OpenGL Android support. Who this book is for Android developers Hardware designers who need to understand how Android will work on their processors CIOs and CEOs of technology-based companies IT staff who may encounter or need to understand the issues New startup founders and entrepreneurs Computer science students Table of Contents Chapter 1: History & Evolution of Android OS Chapter 2: Mobile Device Applications – Uses and Trends Chapter 3: Why x86 on Android? Chapter 4: Android Development – Business Overview and Considerations Chapter 5: Android Devices with Intel Processors Chapter 6: Installing the Android SDK for Intel Application Development Chapter 7: The Intel Mobile Processor Chapter 8: Creating and Porting NDK-based Android Applications Chapter 9: Debugging Android Chapter 10: Performance Optimization for Android Applications on x86 Chapter 11: x86 NDK and C++ Optimizations Chapter 12: Intel Hardware Accelerated Execution Manager Appendix: References

Explore every nook and cranny of the Android OS to modify your device and guard it against security threats About This Book Understand and counteract against offensive security threats to your applications

Maximize your device's power and potential to suit your needs and curiosity See exactly how your smartphone's OS is put together (and where the seams are) Who This Book Is For This book is for anyone who wants to learn about Android security. Software developers, QA professionals, and beginner- to intermediate-level security professionals will find this book helpful. Basic knowledge of Android programming would be a plus. What You Will Learn Acquaint yourself with the fundamental building blocks of Android Apps in the right way Pentest Android apps and perform various attacks in the real world using real case studies Take a look at how your personal data can be stolen by malicious attackers Understand the offensive maneuvers that hackers use Discover how to defend against threats Get to know the basic concepts of Android rooting See how developers make mistakes that allow attackers to steal data from phones Grasp ways to secure your Android apps and devices Find out how remote attacks are possible on Android devices In Detail With the mass explosion of Android mobile phones in the world, mobile devices have become an integral part of our everyday lives. Security of Android devices is a broad subject that should be part of our everyday lives to defend against ever-growing smartphone attacks. Everyone, starting with end users all the way up to developers and security professionals should care about android security. Hacking Android is a step-by-step guide that will get you started with Android security. You'll begin your journey at the absolute basics, and then will slowly gear up to the concepts of Android rooting, application security assessments, malware, infecting APK files, and fuzzing. On this journey you'll get to grips with various tools and techniques that can be used in your everyday pentests. You'll gain the skills necessary to perform Android application vulnerability assessment and penetration testing and will create an Android pentesting lab. Style and approach This comprehensive guide takes a step-by-step approach and is explained in a conversational and easy-to-follow style. Each topic is explained sequentially in the process of performing a successful penetration test. We also include detailed explanations as well as screenshots of the basic and advanced concepts.

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.

Smartphones from an Applied Research Perspective highlights latest advancements of research undertaken in multidisciplinary fields where the smartphone plays a central role. Smartphone is synonymous to innovation in today's society. Very few visionaries predicted its social, cultural, technological and economic impacts, although the usage of smartphone is almost pervasive and transcendental. This book is meant for researchers and postgraduate students looking forward for hot topics for their final year projects, doctoral or even postdoctoral studies. Practitioners too will find food for thought and will surely be amazed by the broadness of the topics presented.

If you are a forensic analyst or an information security professional wanting to develop your knowledge of Android forensics, then this is the book for you. Some basic knowledge of the Android mobile platform is expected.

Android Application Security Essentials is packed with examples, screenshots, illustrations, and real world use cases to secure your apps the right way. If you are looking for guidance and detailed instructions on how to secure app data, then this book is for you. Developers, architects, managers, and technologists who wish to enhance their knowledge of Android security will find this book interesting. Some prior knowledge of development on the Android stack is desirable but not required.

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 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.

Embedded Android is for Developers wanting to create embedded systems based on Android and for those wanting to port Android to new hardware, or creating a custom development environment. Hackers and moders will also find this an indispensable guide to how Android works.

This book presents state-of-the-art intelligent methods and techniques for solving real-world problems and offers a vision of future research. Featuring 143 papers from the 4th Future Technologies Conference, held in San Francisco, USA, in 2019, it covers a wide range of important topics, including, but not limited to, computing, electronics, artificial intelligence, robotics, security and communications and their applications to the real world. As such, it is an interesting, exciting and inspiring read.

Provides information on Android programming, covering such topics as creating an Android application, using the Eclipse Workbench, Java, XML, broadcast receivers, and the Android Market. These Proceedings are the work of researchers contributing to the 10th International Conference on Cyber Warfare and Security ICCWS 2015, co hosted this year by the University of Venda and The Council for Scientific and Industrial Research. The conference is being held at the Kruger National Park, South Africa on the 24-25 March 2015. The Conference Chair is Dr Jannie Zaaiman from the University of Venda, South Africa, and the Programme Chair is Dr Louise Leenen from the Council for Scientific and Industrial Research, South Africa.

The two-volume set, LNCS 9878 and 9879 constitutes the refereed proceedings of the 21st European Symposium on Research in Computer Security, ESORICS 2016, held in Heraklion, Greece, in September 2016. The 60 revised full papers presented were carefully reviewed and selected from 285 submissions. The papers cover a wide range of topics in security and privacy, including data protection: systems security, network security, access control, authentication, and security in such emerging areas as cloud computing, cyber-physical systems, and the Internet of Things.

Learn Android Studio covers Android Studio and its rich tools ecosystem, including Git and Gradle: this book covers how Android Studio works seamlessly with Git, for source control, and Gradle, a build and test tool. In addition, this book demonstrates how to develop/collaborate with remote Git web-hosting services such as GitHub and Bitbucket. Four complete Android projects accompany this volume and are available for download from a public Git repository. With this book, you learn the latest and most productive tools in the Android tools ecosystem, and the best practices for Android app development. You will be able to take away the labs' code as templates or frameworks to re-use and customize for your own similar apps. Android Studio is an intuitive, feature-rich, and extremely forgiving Integrated Development Environment (IDE). This IDE is more productive and easier to use for your Android app creations than Eclipse. With this book you will quickly master Android Studio and maximize your Android development time. Source code on the remote web-hosting service is targeted to the latest Android Studio release, version 1.2.

An in-depth look into Mac OS X and iOS kernels Powering Macs, iPhones, iPads and more, OS X and iOS are becoming ubiquitous. When it comes to documentation, however, much of them are shrouded in mystery. Cocoa and Carbon, the application frameworks, are neatly described, but system programmers find the rest lacking. This indispensable guide illuminates the darkest corners of those systems, starting with an architectural overview, then drilling all the way to the core. Provides you with a top down view of OS X and iOS Walks you through the phases of system startup—both Mac (EFI) and mobile (iBoot) Explains how processes, threads, virtual memory, and filesystems are maintained Covers the security architecture Reviews the internal APIs used by the system—BSD and Mach Dissects the kernel, XNU, into its sub components: Mach, the BSD Layer, and I/O kit, and explains each in detail Explains the inner workings of device drivers From architecture to implementation, this book is essential reading if you want to get serious about the internal workings of Mac OS X and iOS.

Build fast and efficient Android apps that run as reliably as clockwork in a multi-device world About This Book Wide coverage of various topics that help in developing optimal applications Explore the concepts of Advanced Native Coding in depth A must-have for professional-standard Android developers for whom performance failures and the sloppy use of resources are simply unacceptable Who This Book Is For This book is aimed at developers with an advanced knowledge of Android and who want to test their skills and learn new techniques to increase the performance of their applications. We assume they are comfortable working with the entire Android SDK, and have been doing it for a few years. They need to be familiar with frameworks such as NDK to use native code, which is crucial for app performance What You Will Learn Create Android applications that squeeze the most from the limited resource capacity of devices Swap code that isn't performing Efficient memory management by identifying problems such as leaks Reap the benefits of multithreaded and asynchronous programming Maximize the security and encryption mechanisms natively provided by Android Perform efficient network operations and techniques to retrieve data from servers Master the NDK to write native code that can perform faster operations In Detail Performant applications are one of the key drivers of success in the mobile world. Users may abandon an app if it runs slowly. Learning how to build applications that balance speed and performance with functionality and UX can be a challenge; however, it's now more important than ever to get that balance right. Android High Performance will start you thinking about how to wring the most from any hardware your app is installed on, so you can increase your reach and engagement. The book begins by providing an introduction to state-of-the-art Android techniques and the importance of performance in an Android application. Then, we will explain the Android SDK tools regularly used to debug and profile Android applications. We will also learn about some advanced topics such as building layouts, multithreading, networking, and security. Battery life is one of the biggest bottlenecks in applications; and this book will show typical examples of code that exhausts battery life, how to prevent this, and how to measure battery consumption from an application in every kind of situation to ensure your apps don't drain more than they should. This book explains techniques for building optimized and efficient systems that do not drain the battery, cause memory leaks, or slow down with time. Style and approach The book follows a tutorial-based approach to take the reader from the basic fundamentals of debugging to advanced performance-improvement concepts.

The two-volume set, LNCS 9326 and LNCS 9327 constitutes the refereed proceedings of the 20th European Symposium on Research in Computer Security, ESORICS 2015, held in Vienna, Austria, in September 2015. The 59 revised full papers presented were carefully reviewed and selected from 298 submissions. The papers address issues such as networks and Web security; system security; crypto application and attacks; risk analysis; privacy; cloud security; protocols and attribute-based encryption; code analysis and side-channels; detection and monitoring; authentication; policies; and applied security.

There are more than one billion Android devices in use today, each one a potential target. Unfortunately, many fundamental Android security features have been little more than a black box to all but the most elite security professionals—until now. In Android Security Internals, top Android security expert Nikolay Elenkov takes us under the hood of the Android security system. Elenkov describes Android security architecture from the bottom up, delving into the implementation of major security-related components and subsystems, like Binder IPC, permissions, cryptographic providers, and device administration. You'll learn: –How Android permissions are declared, used, and enforced –How Android manages application packages and employs code signing to verify their authenticity –How Android implements the Java Cryptography Architecture (JCA) and Java Secure Socket Extension (JSSE) frameworks –About Android's credential storage system and APIs, which let applications store cryptographic keys securely –About the online

account management framework and how Google accounts integrate with Android –About the implementation of verified boot, disk encryption, lockscreen, and other device security features –How Android’s bootloader and recovery OS are used to perform full system updates, and how to obtain root access With its unprecedented level of depth and detail, Android Security Internals is a must-have for any security-minded Android developer.

See your app through a hacker's eyes to find the real sources of vulnerability The Mobile Application Hacker's Handbook is a comprehensive guide to securing all mobile applications by approaching the issue from a hacker's point of view. Heavily practical, this book provides expert guidance toward discovering and exploiting flaws in mobile applications on the iOS, Android, Blackberry, and Windows Phone platforms. You will learn a proven methodology for approaching mobile application assessments, and the techniques used to prevent, disrupt, and remediate the various types of attacks. Coverage includes data storage, cryptography, transport layers, data leakage, injection attacks, runtime manipulation, security controls, and cross-platform apps, with vulnerabilities highlighted and detailed information on the methods hackers use to get around standard security. Mobile applications are widely used in the consumer and enterprise markets to process and/or store sensitive data. There is currently little published on the topic of mobile security, but with over a million apps in the Apple App Store alone, the attack surface is significant. This book helps you secure mobile apps by demonstrating the ways in which hackers exploit weak points and flaws to gain access to data. Understand the ways data can be stored, and how cryptography is defeated Set up an environment for identifying insecurities and the data leakages that arise Develop extensions to bypass security controls and perform injection attacks Learn the different attacks that apply specifically to cross-platform apps IT security breaches have made big headlines, with millions of consumers vulnerable as major corporations come under attack. Learning the tricks of the hacker's trade allows security professionals to lock the app up tight. For better mobile security and less vulnerable data, The Mobile Application Hacker's Handbook is a practical, comprehensive guide.

Android Programming Unleashed is the most comprehensive and technically sophisticated guide to best-practice Android development with today's powerful new versions of Android: 4.1 (Jelly Bean) and 4.0.3 (Ice Cream Sandwich). Offering the exceptional breadth and depth developers have come to expect from the Unleashed series, it covers everything programmers need to know to develop robust, high-performance Android apps that deliver a superior user experience. Leading developer trainer Bintu Harwani begins with basic UI controls, then progresses to more advanced topics, finally covering how to develop feature rich Android applications that can access Internet-based services and store data. He illuminates each important SDK component through complete, self-contained code examples that show developers the most effective ways to build production-ready code. Coverage includes: understanding the modern Android platform from the developer's standpoint... using widgets, containers, resources, selection widgets, dialogs, and fragments... supporting actions and persistence... incorporating menus, ActionBars, content providers, and databases... integrating media and animations... using web, map, and other services... supporting communication via messaging, contacts, and emails... publishing Android apps, and much more.

An in-depth exploration of the inner-workings of Android: In Volume I, we take the perspective of the Power User as we delve into the foundations of Android, filesystems, partitions, boot process, native daemons and services.

This is an easy-to-follow guide, full of hands-on and real-world examples of applications. Each of the vulnerabilities discussed in the book is accompanied with the practical approach to the vulnerability, and the underlying security issue. This book is intended for all those who are looking to get started in Android security or Android application penetration testing. You don't need to be an Android developer to learn from this book, but it is highly recommended that developers have some experience in order to learn how to create secure applications for Android.

Create the perfectly customized system by unleashing the power of Android OS on your embedded device About This Book Understand the system architecture and how the source code is organized Explore the power of Android and customize the build system Build a fully customized Android version as per your requirements Who This Book Is For If you are a Java programmer who wants to customize, build, and deploy your own Android version using embedded programming, then this book is for you. What You Will Learn Master Android architecture and system design Obtain source code and understand the modular organization Customize and build your first system image for the Android emulator Level up and build your own Android system for a real-world device Use Android as a home automation and entertainment system Tailor your system with optimizations and add-ons Reach for the stars: look at the Internet of Things, entertainment, and domotics In Detail Take a deep dive into the Android build system and its customization with Learning Embedded Android Programming, written to help you master the steep learning curve of working with embedded Android. Start by exploring the basics of Android OS, discover Google's "repo" system, and discover how to retrieve AOSP source code. You'll then find out to set up the build environment and the first AOSP system. Next, learn how to customize the boot sequence with a new animation, and use an Android "kitchen" to "cook" your custom ROM. By the end of the book, you'll be able to build customized Android open source projects by developing your own set of features. Style and approach This step-by-step guide is packed with various real-world examples to help you create a fully customized Android system with the most useful features available.

Multithreading is essential if you want to create an Android app with a great user experience, but how do you know which techniques can help solve your problem? This practical book describes many asynchronous mechanisms available in the Android SDK, and provides guidelines for selecting the ones most appropriate for the app you're building. Author Anders Goransson demonstrates the advantages and disadvantages of each technique, with sample code and detailed explanations for using it efficiently. The first part of the book describes the

building blocks of asynchronous processing, and the second part covers Android libraries and constructs for developing fast, responsive, and well-structured apps. Understand multithreading basics in Java and on the Android platform Learn how threads communicate within and between processes Use strategies to reduce the risk of memory leaks Manage the lifecycle of a basic thread Run tasks sequentially in the background with HandlerThread Use Java's Executor Framework to control or cancel threads Handle background task execution with AsyncTask and IntentService Access content providers with AsyncQueryHandler Use loaders to update the UI with new data

Summary Android in Action, Third Edition is a comprehensive tutorial for Android developers. This fast-paced book puts you in the driver's seat -- you'll master the SDK, build WebKit apps using HTML 5, and even learn to extend or replace Android's built-in features by building useful and intriguing examples. About the Technology When it comes to mobile apps, Android can do almost anything, and with this book, so can you! Android, Google's popular mobile operating system and SDK for tablets and smart phones, is the broadest mobile platform available. It is Java-based, HTML5-aware, and loaded with the features today's mobile users demand. About this Book Android in Action, Third Edition takes you far beyond "Hello Android." You'll master the SDK, build WebKit apps using HTML 5, and even learn to extend or replace Android's built-in features. You'll find interesting examples on every page as you explore cross-platform graphics with RenderScript, the updated notification system, and the Native Development Kit. This book also introduces important tablet concepts like drag-and-drop, fragments, and the Action Bar, all new in Android 3. Purchase of the print book comes with an offer of a free PDF, ePub, and Kindle eBook from Manning. Also available is all code from the book. What's Inside Covers Android 3.x SDK and WebKit development from the ground up Driving a robot with Bluetooth and sensors Image processing with Native C code This book is written for hobbyists and developers. A background in Java is helpful. No prior experience with Android is assumed. ===== Table of Contents PART 1 WHAT IS ANDROID? THE BIG PICTURE Introducing Android Android's development environment PART 2 EXERCISING THE ANDROID SDK User interfaces Intents and Services Storing and retrieving data Networking and web services Telephony Notifications and alarms Graphics and animation Multimedia 1Location, location, location PART 3 ANDROID APPLICATIONS Putting Android to work in a field service application Building Android applications in C PART 4 THE MATURING PLATFORM Bluetooth and sensors Integration Android web development AppWidgets Localization Android Native Development Kit Activity fragments Android 3.0 action bar Drag-and-drop

Malware analysis is a powerful investigation technique widely used in various security areas including digital forensics and incident response processes. Working through practical examples, you'll be able to analyze any type of malware you may encounter within the modern world.

In 2004, Android was two people who wanted to build camera software. But they couldn't get investors interested. Today, Android is a large team at Google, shipping an operating system (including camera software) to over three billion devices worldwide. This is the inside story, told by the people who made it happen. "What are the essential ingredients that lead a small team to build software at the sheer scale and impact of Android? We may never fully know, but this first person account is probably the closest set of clues we have." –Dave Burke, VP of Android Engineering "Androids captures a strong picture of what the early development of Android, as well as the Android team, was like." –Dianne Hackborn, Android Framework Engineer "Androids is the engaging tale of a motley group of coders with a passion to make insanely great products who banged out the operating system when that idea seemed nuts. True to his geek genes, Chet Haase tells this remarkable tale of technical and business success from the trenches, an inspiring, massive collective effort of dozens of programmers who flipped their seemingly late timing to their advantage, and presaged a generation of platform builders. Read Androids to discover what it takes to create a hot tech team that shipped a product running today on more than 3 billion devices." –Jonathan Littman, co-author of The Entrepreneurs Faces: How Makers, Visionaries and Outsiders Succeed, and author of The Fugitive Game All profits from the book will be donated to charity.

This is the eBook version of the print title. Note that the eBook does not provide access to the practice test software that accompanies the print book. Learn, prepare, and practice for CompTIA Pentest+ PT0-001 exam success with this CompTIA Cert Guide from Pearson IT Certification, a leader in IT Certification. Master CompTIA Pentest+ PT0-001 exam topics Assess your knowledge with chapter-ending quizzes Review key concepts with exam preparation tasks Practice with realistic exam questions Get practical guidance for next steps and more advanced certifications CompTIA Pentest+ Cert Guide is a best-of-breed exam study guide. Leading IT security experts Omar Santos and Ron Taylor share preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. The book presents you with an organized test preparation routine through the use of proven series elements and techniques. Exam topic lists make referencing easy. Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. Review questions help you assess your knowledge, and a final preparation chapter guides you through tools and resources to help you craft your final study plan. Well regarded for its level of detail, assessment features, and challenging review questions and exercises, this study guide helps you master the concepts and techniques that will allow you to succeed on the exam the first time. The CompTIA study guide helps you master all the topics on the Pentest+ exam, including: Planning and scoping: Explain the importance of proper planning and scoping, understand key legal concepts, explore key aspects of compliance-based assessments Information gathering and vulnerability identification: Understand passive and active reconnaissance, conduct appropriate information gathering and use open source intelligence (OSINT); perform vulnerability scans; analyze results; explain how to leverage gathered information in exploitation; understand weaknesses of specialized systems Attacks and exploits: Compare and contrast social engineering attacks; exploit network-based, wireless, RF-based, application-based, and local host vulnerabilities; summarize physical security attacks; perform post-exploitation techniques Penetration testing tools: Use numerous tools to perform reconnaissance, exploit vulnerabilities and perform post-exploitation activities; leverage the Bash shell, Python, Ruby, and PowerShell for basic scripting Reporting and communication: Write reports containing effective findings and recommendations for mitigation; master best practices for reporting and communication; perform post-engagement activities such as cleanup of tools or shells

Decompiling Android looks at the the reason why Android apps can be decompiled to recover their source code, what it means to Android developers and how you can protect your code from prying eyes. This is also a good way to see how good and bad Android apps are constructed and how to learn from them in building your own apps. This is becoming an increasingly important

topic as the Android marketplace grows and developers are unwittingly releasing the apps with lots of back doors allowing people to potentially obtain credit card information and database logins to back-end systems, as they don't realize how easy it is to decompile their Android code. In depth examination of the Java and Android class file structures Tools and techniques for decompiling Android apps Tools and techniques for protecting your Android apps

[Copyright: ca6287275883d292cc7c283ab98322f7](#)