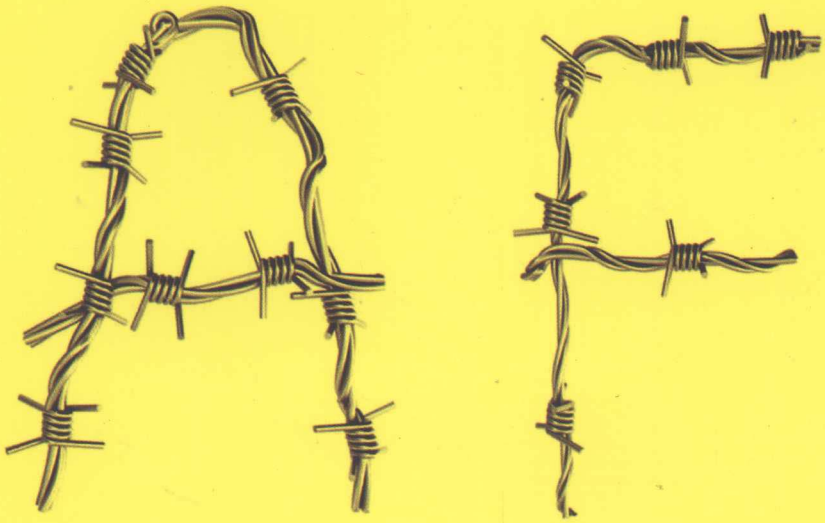
HZ BOOKS
华章科技

ELSEVIER
爱思唯尔

**Android取证领域广受好评的经典著作，资深取证技术专家撰写，世界顶级取证专家审校，理论指导与实用性兼备**

从Android的硬件设备、应用开发环境、系统原理多角度剖析Android系统的安全原理，结合实用的工具和案例系统讲解Android取证的技术、策略、方法和步骤

安全技术大系
SECURITY



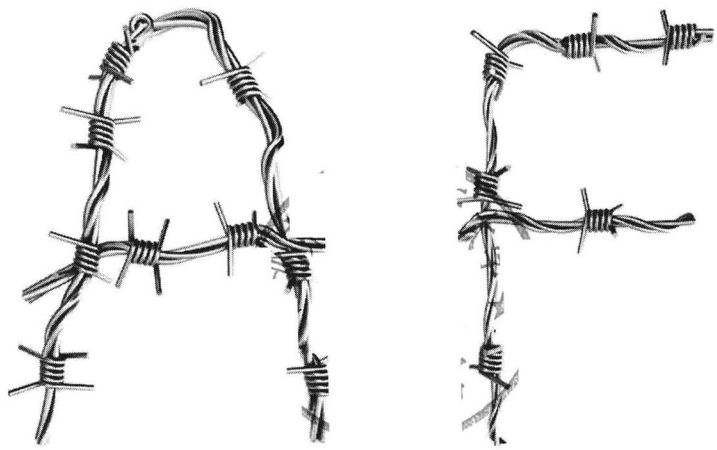
Android Forensics
Investigation, Analysis and Mobile Security for Google Android

# Android取证实战

## 调查、分析与移动安全

（美） Andrew Hoog 著
何泾沙 等译

机械工业出版社
China Machine Press



Android Forensics

Investigation, Analysis and Mobile Security for Google Android

# Android取证实战

## 调查、分析与移动安全

（美） Andrew Hoog 著

何泾沙 等译

机械工业出版社
China Machine Press

**图书在版编目（CIP）数据**

Android取证实战：调查、分析与移动安全/（美）胡格（Hoog, A.）著；何泾沙等译. —北京：机械工业出版社，2013.5
（华章程序员书库）
书名原文：Android Forensics: Investigation, Analysis and Mobile Security for Google Android

ISBN 978-7-111-42199-3

Ⅰ. A… Ⅱ. ① 胡… ② 何… Ⅲ. 移动终端－应用程序－程序设计 Ⅳ. TN929.53

中国版本图书馆CIP数据核字（2013）第077825号



**本书版权登记号：图字：01-2012-5192**

本书是Android取证领域广受好评的经典著作，也是国内第一本关于Android取证的著作，由资深取证技术专家撰写，世界顶级取证专家审校，权威性毋庸置疑！从Android的硬件设备、应用开发环境、系统原理等多角度剖析了Android系统的安全原理，结合实用的取证分析工具和经典案例，讲解了Android取证的原理、技术、策略、方法和步骤。

全书一共7章：第1章介绍了Android平台的概况和特点、Linux与Android，Android与取证，并讲解如何创建基于Ubuntu的虚拟机；第2章讲解了Android所支持的各种类型的硬件和终端设备，为取证和安全分析做好准备。第3章讲解了软件开发套件、Android虚拟终端的安装，以及取证技术的一些重要概念，涵盖Davlik虚拟机、Android程序调试桥、USB调试设置等；第4章分析了Android系统的数据存储方式、涉及的内存类型，以及Android中常见的各类文件系统；第5章分析了Android终端设备成为泄漏数据以及用于作为主动攻击源的原因，并为个人、企业安全总监和应用开发者提供了一些非常具体的建议；第6章深入讲解了规避密码的几个不同策略和多种逻辑获取技术和物理获取技术（如adb pull、备份分析、AFLogical、JTAG、芯片摘取、AFPhysical等）；第7章介绍了一些具体的策略和Android文件的目录（文件夹）结构，并深入分析了11个可以用于获取Android终端设备中主要数据的应用程序。



机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）
责任编辑：高婧雅
三河市杨庄长鸣印刷装订厂印刷
2013年6月第1版第1次印刷
186mm×240mm·20.25印张
标准书号：ISBN 978-7-111-42199-3
定价：69.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991 88361066 投稿热线：（010）88379604
购书热线：（010）68326294 88379649 68995259 读者信箱：hzjsj@hzbook.com

# 译 者 序

从2008年10月第一部Android智能手机诞生至今，在短短不到五年的时间内，Android移动平台已经快速成长为全球最流行的、用于移动应用开发的操作系统，在2011年就已经以27%的份额占据智能手机操作系统的首位。虽然目前关于Android系统应用方面的统计数据基本上都来源于智能手机和平板电脑，然而因其在移动终端设备市场中所具有的强大竞争力以及在系统功能方面所具有的优越性，相信在不久的将来，Android操作系统将会在其他各种类型的移动终端设备中得到更加广泛的应用，诸如汽车电子、智能电视、全球定位系统（GPS）终端、游戏机、笔记本电脑以及其他电子产品。因此，学习和掌握Android操作系统及其在移动系统中的应用对跟踪当今最新信息技术的发展趋势至关重要。

伴随着信息技术的快速发展，信息已经成为人们工作和生活中的重要资源。尤其是近年来移动通信技术的飞速发展以及智能手机应用的日益普及，信息在各个层面（国家、社会、团体、个人）更加紧密地联系在一起，各类信息无所不在、触手可及。然而，以移动通信技术为代表的信息技术在给人们的工作和生活带来极大便利的同时，也不可避免地引发了各种负面问题，尤其是利用网络和信息而引发的各类非法或犯罪行为，如窃取国家机密和个人隐私信息、网络诈骗、网上非法交易、在线间谍、黑客攻击、网上刺探等犯罪行为不断出现，而且呈现出高速增长的势头。利用智能手机或其他无线移动终端设备进行犯罪是一种典型的高科技犯罪，亟待设计出相应的对策加以防范、监控和打击，以确保信息技术与应用的持续快速发展。打击利用信息技术进行犯罪所面临的挑战之一就是在犯罪实施后如何按照法律、法规的要求对犯罪事实进行认定，而认定犯罪事实的关键就在于获取有效证据。因此，计算机取证（数字取证），即从信息系统中获取与犯罪事实相关的数据，并使其成为法律上可采纳的有效证据，这在近年来已经成为信息系统安全研究领域中的一个热点问题。然而，与传统的信息安全问题不同，计算机取证不仅仅是一个技术问题，它还涉及诸如法律法规、社会道德规范、个人隐私权利等众多有关其他技术和人文因素的考虑，属于交叉学科问题，这就给计算机取证带来了一定程度的复杂性。

鉴于基于Android的无线移动终端设备应用的日益广泛，对这些终端设备中的数据进行提取、处理和分析以获得司法证据也变得越来越迫切，成为一个不可忽略的途径。公安机关、法院等各级侦探和执法部门急需在案件的侦探和审理过程中获取涉案人员的智能手机或其他移动终端设备中存有的通讯录、通话记录、来往信息、数码照片、各类文件等用户信息和数据，并尽可能对已经删除的以上信息和数据进行恢复，以推进案件的调查和审理。因此移动取证技术成为打击网络犯罪、保护合法信息的重要技术手段。然而，面向移动终端设备进行取证所涉及的信息采集和分析具有较高的技术难度，同时也受到系统和应

用的影响。因此，针对不同的系统，深入分析系统的内部体系结构、掌握取证的原理和方法对实现移动取证至关重要。

本书就是在这一背景下，针对上述需求而撰写完成的，在对 Android 操作系统的相关部分进行深入分析的基础上，系统地介绍了如何从基于 Android 操作系统的移动终端中获取数据的手段和技术，是一本较完整的学习和研究 Android 取证技术的技术参考书。学习和掌握 Android 取证技术，一方面能够增强人们对相关信息和数据的保护意识，并可利用更加有效的手段来保护这些信息和数据的安全（如及时进行迁移或删除而不被犯罪分子所窃取），另一方面也能够帮助各级执法部门获取网络犯罪的有效证据，打击网络犯罪，保障国家安全和个人隐私权利。

本书由北京工业大学教授、博士生导师、北京市特聘教授何泾沙博士负责翻译，北京工业大学博士研究生赵斌、国家软件产品质量监测检验中心朱娜斐博士参与了部分章节的翻译工作。北京工业大学博士研究生张玉强、中国科学院信息工程研究所徐菲博士，以及张航、张伊璇、刘公政、万雪姣、张伯雍、潘力斌等参与了翻译过程中举办的相关技术研讨，并协助了部分章节的翻译工作。全书最后由何泾沙博士进行统稿及审校。由于译者的水平有限，再加上时间上的限制，全书的翻译中难免存在不妥之处，敬请广大读者批评指正，译者在此深表谢意。

何泾沙

# 前　言

从2008年10月第一部Android手机的诞生到2011年年初，Android移动平台迅速成长为全球最流行的移动操作系统。对消费者来说，Android平台的爆炸性成长在竞争和功能方面都是一个巨大的胜利。同时，由于缺乏用于调查相应设备和手持终端的知识以及工具，取证分析师和信息安全工程师遇到了巨大的难题。本书试图解决这些问题，不仅详细介绍了Android的软件、硬件和文件系统，而且分享了计算机取证获取技术以及随后所需的设备分析工作。对于缺乏计算机取证方面知识的读者，本书将提供基于免费、开放的代码库编写的实例，而且读者也可以亲身参与到这些实例的编写中。因为免费的Android开发套件能够提供一个完整的Android仿真器，所以读者不需要实际拥有任何Android终端设备。

随着Android终端设备数量的快速增加，用户对于这些终端设备中存储着数据的意识也在相应增强。然而遗憾的是，大多数对这些数据感兴趣的却是网络犯罪团伙，他们更清楚地知道这些终端设备中存储着大量的个人信息和商业信息，而对Android平台的成功攻击会为其带来巨大的“收益”。如果要应对这种威胁，就需要深入地了解Android平台，不但对于Android系统开发者和制造商如此，对于Android应用开发者和企业中的信息安全管理者也是如此。更加安全的应用将有助于防止敏感信息泄露，也会帮助信息安全管理者为系统制订更加有效的安全策略。

目前很多关于Android的统计数据都是针对智能手机以及平板电脑的，在不久的将来，Android将会在更多的终端设备中得到应用，如汽车、电视、全球定位系统（GPS）终端、游戏机、笔记本电脑以及其他电子产品。对于取证分析师和安全工程师来说，针对Android的取证分析将会有一个很大比例的增长。最后，Android的魅力不只绽放于某些特定的国家或地区，它将会对全球的个人、企业和机构产生巨大的影响。

下面将对本书中各章的内容进行简要介绍。

**第1章**

该章在介绍Android平台的发展史后，还将讨论Android开放源码项目（Android Open Source Project，AOSP）、平台国际化、Android市场，同时提供有关Linux的一些简单辅导信息，并对Android取证进行简要说明。本章还将逐步讲解如何创建一个基于Ubuntu的虚拟机，其后在全书的实例中都将会用到。本书极力推荐Ubuntu虚拟机，它还可以应用到本书以外的其他Android取证实例中。

**第2章**

该章介绍Android所支持的各种类型的硬件和终端设备。虽然硬件的兼容性对制造商来说非常重要，最终也会使消费者受益，但是对大量硬件和终端设备的广泛支持却给取证

分析师和安全工程师带来了巨大的挑战。因此，对硬件组件、终端设备类型以及 Android 启动过程的清楚了解非常有助于对整个 Android 的了解，也对取证和安全分析具有很大帮助。

**第 3 章**

该章讨论 Android 系统的不同版本、Android 软件开发套件（Software Development Kit，SDK）、Davlik 虚拟机、Android 安全的核心组件以及其他与 Android 取证相关的重要概念，如 Android 程序调试桥（adb）、USB 调试设置等。本章还将提供一些详细的实例，包括如何在 Linux、OS X 和 Windows 上安装软件开发套件，以及如何创建一个 Android 虚拟终端用以测试取证技术。

**第 4 章**

该章介绍如何在 Android 终端设备上存储数据，内容包括数据存储方式（共享参考、文件、SQLite 及网络）以及 Android 终端设备所使用的内存类型，如 RAM 以及十分重要的 NAND 闪存。该章也会详细介绍读者在 Android 终端设备中经常会遇到的各类文件系统，如 YAFFS2、EXT、FAT32/FAT16 及各类底层文件系统。

**第 5 章**

该章讨论 Android 终端设备、数据和应用的安全。首先回顾了 Android 终端设备如何泄露数据及其如何被用做一个主动攻击源。在讨论一些重要的安全概念后，该章将给个人、企业安全管理者和应用开发者这三类主要读者提供一些非常具体的建议。随着 Android 持续快速增长，数据和信息的安全问题将变得日益严峻。因此，该章对这个重要的问题进行了深入且切合实际的快速讨论。

**第 6 章**

该章介绍具体且十分有用的从 Android 终端设备获得取证信息的一些技术。在介绍了不同类型的获取方法以及如何对 Android 终端设备进行操控后，本章还讨论了规避密码的 7 个不同策略。随后，本章介绍一些具体的获取 SD 卡以及任何插入的内置多媒体卡（Embedded Multi Media Card）的技术以及相对应的代码。在此基础上，该章介绍一些逻辑获取技术，包括一些已经包含在 Android 和软件开发套件（SDK）里的技术以及一个称为 AFLogical 的可以供执法者和政府机构免费使用的技术，并简单描述了 6 个商用取证软件。最后，本章详细介绍了获取 NAND 闪存物理映像的技术，包括 6 个如何获得超级用户权限的方法以及由 viaForensics 公司开发的 AFPhysical 技术。

**第 7 章**

该章是最后一章，将介绍一些具体的策略以及相应的应用程序，使取证分析师和安全工程师可以对得到的 Android 终端设备进行分析。虽然很多传统的取证技术仍然适用于 Android 取证分析，但是 Android 中新的文件系统以及硬件的特殊性要求更多的新技术。没有这些新技术，从 Android 终端设备中实际获取的数据只能够得到极少有价值的内容和信息。除了提供背景信息以及实用的应用软件，该章还将给出 Android 文件的目录（文件夹）结构，并深入分析 11 个可以用于获取 Android 终端设备中主要数据的应用程序。具备了以上知识，取证分析师和安全工程师可以对任何可以获得的 Android 终端设备进行取证分析。

## 网站

访问以下网站可以获得与本书相配套的其他资料，如代码、程序及随后的更新等：http://viaforensics.com/education/android-forensics-mobile-security-book/。

## 致谢

我现在真正理解“举全村之力”（It takes a village）的深刻含义了，它不但适用于描述抚养孩子，也同样适用于撰写书籍。因此，我要衷心感谢“整个村庄”：

- 感谢我的家庭成员：妻子和女儿们。
- 感谢 Lee Haas 为本书所做的出色的文本编辑工作，并时刻督促我按照原定计划完成此书的撰写。
- 感谢 Ted Eull 为读者提供的出色服务，时常帮助我将头脑里激荡的想法用清晰的言语和文字表达出来。同时 Ted 也是我的好朋友。衷心感谢他的妻子，为他在创业过程中长时间工作所给予的耐心和支持。
- 感谢 Chris Triplett 率先开始对 Android 的研究及其所进行的出色工作。Chris 在将通俗的英语应用到数字取证，以弥补语言描述上的欠缺，以及提供喜剧性疏解方面十分有天分。
- 感谢 Katie Strzempka 负责另外一本书的撰写（“iPhone and iOS Forensics”）。在此郑重地向读者推荐这本书。
- 感谢我的父母 Stevie 和 Al。他们从人生的开始就为我制定了一条正确的发展道路，并且能够在我稍有偏差时及时提醒。
- 感谢 Harmonee 和 Hadabogee 照顾我的女儿们、准备晚餐以及提供的其他很多方面的帮助。
- 感谢众多在地方、州、联邦政府的法律部门及其他部门中为公共事业提供服务的勇敢的人们，感谢他们为我们的社会和国家所做的一切。
- 感谢 Google（谷歌）认识到 Android 的价值，并且为移动终端设备创造了一个新的开放平台。
- 感谢苹果公司提供了另外一个开发平台。
- 最后，感谢所有的读者。我衷心希望本书可以为读者带来价值，并赞赏他们给予的任何支持。

# 推荐阅读


**黑客大曝光：Web应用程序安全（原书第3版）**

作者：（美）Joel Scambray 等 译者：姚军 等 ISBN：978-7-111-35662-2 定价：65.00元

**黑客大曝光：恶意软件和Rootkit安全**

作者：（美）Michael A. Davis 等 译者：姚军 等 ISBN：978-7-111-34034-8 定价：55.00元

**黑客大曝光：无线网络安全（原书第2版）**

作者：（美）Johnny Cache 等 译者：李瑞民 等 ISBN：978-7-111-37248-6 定价：69.00元

**C++反汇编与逆向分析技术揭秘**

作者：钱林松 等 ISBN：978-7-111-35633-2 定价：69.00元

**网络扫描技术揭秘：原理、实践与扫描器的实现**

作者：李瑞民 ISBN：978-7-111-36532-7 定价：79.00元

**BackTrack 4：利用渗透测试保证系统安全**

作者：Shakeel Ali 等 译者：陈雪斌 等 ISBN：978-7-111-36643-0 定价：59.00元

**Windows PE权威指南**

作者：戚利 ISBN：978-7-111-35418-5 定价：89.00元

**内核漏洞的利用与防范**

作者：Enrico Perla 等 译者：吴世忠 等 ISBN：978-7-111-37429-9 定价：79.00元

**Java加密与解密的艺术**

作者：梁栋 ISBN：978-7-111-29762-8 定价：69.00元

**云计算安全与隐私**

作者：Tim Mather 等 译者：刘戈舟 等 ISBN：978-7-111-34525-1 定价：65.00元

**安全之美**

作者：Andy Oram 等 译者：徐波 等 ISBN：978-7-111-33477-4 定价：65.00元

# 目　录

# 第 1 章

# Android 与移动取证

**本章要点**

- Android 平台
- Linux、开源软件与取证
- Android 开放源码项目
- Android 平台的国际化
- Android 市场
- Android 取证

## 1.1 绪论

数字取证是一个令人兴奋且高速发展的技术领域，可对诸如公司内部调查分析、民事诉讼、刑事调查、情报收集以及涉及国家安全等众多方面产生巨大的影响。作为快速发展及变化的领域，移动取证给人们带来了巨大的商机以及严峻的挑战。虽然 Android 取证所涉及的从移动终端设备中获取数据并对其加以分析本身非常有趣，但是首先对 Android 平台以及取证分析需要使用的工具进行全面了解尤为重要。全面掌握此方面的知识能够使取证分析师和安全工程师成功地对 Android 终端设备进行取证分析。

> **提示：针对本书内容所做的更正、更新以及相关软件**
>
> 所有针对本书内容所做的更正、更新，甚至软件实例都将在线提供，通过以下网址进行访问：http://viaforensics.com/education/android-forensics-mobile-security-book/。希望读者经常访问以上网站，随着时间推移，它会给读者提供更多有价值的信息。除了内容上的更正与更新，本书中用到的某些软件也可以通过此网站进行下载。

## 1.2 Android 平台

Android 是一个基于 Linux 2.6 内核的开源移动终端设备平台，并通过电信服务提供商、移动设备和元部件制造商以及软件开发商联合成立的开放手机联盟（Open Handset Alliance）进行管理。

Android 已经对智能手机市场产生了巨大影响，对于取证领域来说也将如此。在第一部 Android 终端设备于 2008 年 10 月推出的两年零一个月之后，Android 就成为全球第二大智能手机平台，占领了美国 6.15 亿部智能手机市场中 26% 的份额（comScore 报告）。表 1.1 是由 comScore 公司提供的 2010 年 11 月美国智能手机市场占有份额数据。

**表 1.1 2010 年 11 月美国智能手机占用份额（13 周岁及以上用户）**

| 平　台 | 智能手机用户占有市场份额（%） |
|---|---|
| RIM | 33.5 |
| 谷歌（Google） | 26.0 |
| 苹果（Apple） | 25.0 |
| 微软（Microsoft） | 9.0 |
| 奔迈（Palm） | 3.9 |

然而，Android 的影响力已不仅限于美国市场。根据高德纳咨询公司（Gartner, Inc.）的市场分析报告，Android 操作系统（OS）在 2010 年第三季度已经成为第二最受欢迎的操作系统，在全球智能手机市场占有 25.5% 的份额（Gartner says, n.d.），如表 1.2 所示。

**表 1.2 2009—2010 年第三季度全球的智能手机销售量，按照操作系统分类**

| 公　司 | 2010 年第三季度销售量（千台） | 2010 年第三季度市场占有率（%） | 2009 年第三季度销售量（千台） | 2009 年第三季度市场占有率（%） |
|---|---|---|---|---|
| 塞班（Symbian） | 29 480.1 | 36.6 | 18 314.8 | 44.6 |
| Android | 20 500.0 | 25.5 | 1424.5 | 3.5 |
| iOS | 13 484.4 | 16.7 | 7040.4 | 17.1 |
| Research in motion | 11 908.3 | 14.8 | 8522.7 | 20.7 |
| 微软（Microsoft） | | | | |
| Windows mobile | 2247.9 | 2.8 | 3259.9 | 7.9 |
| Linux | 1697.1 | 2.1 | 1918.5 | 4.7 |
| 其他操作系统 | 1214.8 | 1.5 | 612.5 | 1.5 |
| 总计 | 80 532.6 | 100.0 | 41 093.3 | 100.0 |

引用 Google Investor 网站上所发布的谷歌首席执行官 Eric Schmidt 的报告，2011 年 2 月每天就有超过 350 000 部 Android 终端设备投入使用（Google investor, n.d.）。以上数据只是智能手机市场的情况，而智能手机仅仅是市场上应用 Android 系统的众多终端设备中的一类。

Android 的开放源码特性不但为工业界开辟了一个新的发展方向，而且能够让开发者、精通代码的取证分析师以及高水平的犯罪团伙（非常不幸）对终端设备进行深入透彻的了解。随着核心的平台技术快速成熟（同时可以继续免费使用），网络服务提供商及各类硬件生产商能够把更多的精力放在如何提供专门的、个性化的服务和功能上，以留住他们所拥有的客户。

### 1.2.1　Android 的发展历程

在过去 30 年间，企业在手持计算设备的研发上投入了巨资，希望培育出新的市场。与传统计算机的发展情况相似，用于制造手持计算设备的核心硬件元部件在技术上取得了巨大的进步，为手持计算设备提供了一个体积虽小但功能强大的移动平台。

对 Android 的发展起到关键作用的核心人物当属 Andy Rubin，他曾经任职于几家研发机器人的公司，还有苹果公司、WebTV 及 Danger Inc. 公司。其在任职 Danger Inc. 公司期间开发出了一款智能手机以及相应的操作系统，即人们熟知的 T-Mobile Sidekick。这个叫做 DangerOS 的操作系统使用 Java 进行开发，提供软件开发套件，并具有现代智能手机的部分功能。2004 年，Rubin 离开了 Danger Inc. 公司，在尝试了几个新的想法后，又回到了智能手机开发行业，与几个志同道合的工程师进行合作，于 2003 年成立了 Android 公司（Android, Inc.）。

在合作团队进行开发的同时，Rubin 积极地向潜在的投资人和无线通信服务提供商宣传 Android，其中就包括谷歌公司，随后谷歌公司在 2005 年 7 月收购了 Android 公司。对 Android 公司的收购以及随之而来的申请专利、提供涉及移动通信的服务以及投标获得无线通信频谱使市场推测谷歌正在开发属于自己的智能手机并有可能将公司发展成为一个无线通信服务提供商。

然而，2007 年 11 月 5 日，Andy Rubin 在谷歌官方博客上宣布了一个更加宏伟的计划（Official Google blog, n.d.）：

> Android 是第一款真正开放的综合移动开发平台，包含一个操作系统、用户界面以及应用程序，即包括运行移动电话所需要的所有软件，但却不会是一个阻碍移动创新的私有财产。Android 由我们与开放手机联盟（Open Handset Alliance）合作开发，该联盟由 30 多家高科技公司和主要移动通信服务公司组成，包括摩托罗拉公司（Motorola）、美国高通公司（Qualcomm）、宏达国际电子股份有限公司（HTC，High Tech Computer Corporation）和 T Mobile。通过与无线通信服务提供商、设备制造商、开发商及其他相关公司建立全面的合作伙伴关系，我们希望推出一个标准的、开放的移动软件平台，为移动通信界打造一个基于开放的生态系统。我们相信最终结果将会更好地加快创新的步伐，给移动通信用户提供超乎想象的应用和性能。

一周后，谷歌向开发商发布了早期版的 Android 软件开发套件（SDK）。此次发布也让谷歌在 2008 年的 1 月至 4 月间发起了第一波 Android 开发挑战（Android Developer Challenge）。谷歌为此投入了 100 万美元，奖励最具创新的 Android 应用。50 个获得此荣誉的 Android 应用登载在以下网站：http://code.google.com/android/adc/adc_gallery/。

2008 年 8 月，谷歌宣布推出 Android 市场（Android Market），任何应用开发商都可以将自己为移动终端设备开发的软件上传到 Android 市场，供移动用户浏览、下载及安

装。最初的版本不支持对下载的应用程序进行收费。随后，在 2009 年年初，谷歌为 Android 市场增加了收费功能。最后，2008 年 10 月，谷歌正式发布了官方版本的 Android 开放源码项目（AOSP）（Bort, n.d.），并正式向市场推出第一款 Android 智能手机 T-Mobile G1。

一经推出，Android 生态系统就经历了一个高速的增长，目前拥有来自于众多领域的贡献者。表 1.3 总结了 Android 平台的重要发展里程碑。

**表 1.3 Android 的发展里程碑**

| 时　间 | 事　件 |
|---|---|
| 2005 年 7 月 1 日 | 谷歌收购 Android 公司 |
| 2007 年 11 月 12 日 | Android 系统正式推出 |
| 2008 年 8 月 28 日 | Android 市场正式推出 |
| 2008 年 9 月 23 日 | Android 1.0 平台正式推出 |
| 2008 年 10 月 21 日 | Android 正式成为开放源码软件 |
| 2009 年 2 月 13 日 | Android 市场：美国开始接受收费应用 |
| 2009 年 3 月 12 日 | Android 市场：英国开始接受收费应用 |
| 2009 年 4 月 15 日 | Android 1.5 (Cupcake) 平台正式推出 |
| 2009 年 9 月 16 日 | Android 1.6 (Donut) 平台正式推出 |
| 2009 年 10 月 5 日 | Android 2.0/2.1 (Eclair) 平台正式推出 |
| 2010 年 5 月 20 日 | Android 2.2 (Froyo) 平台正式推出 |
| 2010 年 5 月 23 日 | Android 2.2 Nexus One 版手机正式推出 |
| 2010 年 12 月 6 日 | Android 2.3 (Gingerbread) 平台正式推出 |
| 2011 年 2 月 2 日 | Android 3.0 (Honeycomb) 预览版正式推出 |

### 1. 开放手机联盟

开放手机联盟（Open Handset Alliance，OHA）是一个由移动技术公司组成的共同合作实体，包括无线通信服务提供商、手机和零部件制造商、软件开发商及其他技术支持商和系统集成商。此联盟成立于 2007 年 11 月 5 日，最初有 34 个成员。然而，到 2011 年 1 月，此联盟已经发展到拥有近 80 个成员。

开放手机联盟（OHA）的宗旨是“加速移动技术创新，为消费者提供功能丰富、价格低廉、服务优质的移动体验”（Alliance FAQ，n.d.），其工作重点是协调、开发及推出 Android 终端设备。谷歌是 OHA 和 AOSP 的主要幕后推动者。因此，有人抱怨说此联盟只不过是一个市场销售机制，没有为联盟成员和消费者提供任何实质性的价值。然而，在 2010 年，新的成员继续加入此联盟，OHA 毫无疑问将继续存在。表 1.4 列出截至 2011 年 2 月 3 日 OHA 成员的名单，按照移动通信服务提供商、手机制造商、半导体生产商、软件开发公司、市场推广公司进行分类（联盟成员 Alliance members，n.d.）。

表 1.4　开放手机联盟成员

| 成员类型 | 公　司 |
| --- | --- |
| 移动通信服务提供商 | Bouygues Telecom |
| | 中国移动通信公司 |
| | 中国电信公司 |
| | 中国联通 |
| | 日本 KDDI 公司 |
| | 日本 NTT DoCoMo 公司 |
| | 软银移动公司（Softbank Mobile Corp.） |
| | Sprint Nextel |
| | T-Mobile |
| | 意大利电信（Telecom Italia） |
| | Telefo' nica |
| | Telus |
| | 沃达丰（Vodafone） |
| 手机制造商 | 宏碁公司（Acer Inc.） |
| | 阿尔卡特移动电话（Alcatel Mobile Phones） |
| | 华硕电脑（ASUSTeK Computer Inc.） |
| | CCI |
| | 戴尔公司（Dell） |
| | 富士康国际（FIH） |
| | 海尔电信（青岛）有限责任公司 |
| | 宏达国际电子股份有限公司（HTC Corporation） |
| | 华为科技公司 |
| | 京瓷株式会社（Kyocera） |
| | 联想移动通信技术公司 |
| | LG |
| | 摩托罗拉公司（Motorola） |
| | 日本 NEC 公司 |
| | 三星电子（Samsung） |
| | 夏普公司（Sharp Corporation） |
| | 索尼爱立信公司（Sony Ericsson） |
| | 东芝公司（Toshiba Corporation） |
| | 中兴通讯股份有限公司（ZTE Corporation） |
| 半导体生产商 | AKM Semiconductor Inc. |
| | 听众（Audience） |
| | ARM |
| | Atheros Communications |
| | 博通公司（Broadcom Corporation） |