Android (operating system)

10.1 Introduction: Android is a mobile operating system (OS) based on the Linux kernel and currently developed by Google. With a user interface based on direct manipulation, Android is designed primarily for touchscreen mobile devices such as smartphones and tablet computers, with specialized user interfaces for televisions (Android TV), cars (Android Auto), and wrist watches (Android Wear). The OS uses touch inputs that loosely correspond to real-world actions, like swiping, tapping, pinching, and reverse pinching to manipulate on-screen objects, and a virtual keyboard. Despite being primarily designed for touchscreen input, it also has been used in game consoles, digital cameras, and other electronics.

Android is the most popular mobile OS. As of 2013, Android devices sell more than Windows, iOS, and Mac OS devices combined,[14][15][16][17] with sales in 2012, 2013 and 2014[18] close to the installed base of all PCs.[19] As of July 2013 the Google Play store has had over 1 million Android apps published, and over 50 billion apps downloaded.[20] A developer survey conducted in April–May 2013 found that 71% of mobile developers develop for Android.[21] At Google I/O 2014, the company revealed that there were over 1 billion active monthly Android users (that have been active for 30 days), up from 538 million in June 2013.[22]

Android's source code is released by Google under open source licenses, although most Android devices ultimately ship with a combination of open source and proprietary software.[3] Initially developed by Android, Inc., which Google backed financially and later bought in 2005,[23] Android was unveiled in 2007 along with the founding of the Open Handset Alliance—a consortium of hardware, software, and telecommunication companies devoted to advancing open standards for mobile devices.[24]

Android is popular with technology companies which require a ready-made, low-cost and customizable operating system for high-tech devices.[25] Android's open nature has encouraged a large community of developers and enthusiasts to use the open-source code as a foundation for community-driven projects, which add new features for advanced users[26] or bring Android to devices which were officially released running other operating systems. The operating system's success has made it a target for patent litigation as part of the so-called "smartphone wars" between technology companies.

10.2 History: Android, Inc. was founded in Palo Alto, California in October 2003 by Andy Rubin (co-founder of Danger),[29] Rich Miner (co-founder of Wildfire Communications, Inc.),[30] Nick Sears[31] (once VP at T-Mobile), and Chris White (headed design and interface development at WebTV)[23] to develop, in Rubin's words "smarter mobile devices that are more aware of its owner's location and preferences".[23] The early intentions of the company were to develop an advanced operating system for digital cameras, when it was realized that the market for the devices was not large enough, and diverted their efforts to producing a smartphone operating system to rival those of Symbian and Windows Mobile.[32] Despite the past accomplishments of the founders and early employees, Android Inc. operated secretly, revealing only that it was working on software for mobile phones.[23] That same year, Rubin ran out of money. Steve Perlman, a close friend of Rubin, brought him $10,000 in cash in an envelope and refused a stake in the company.[33]

Google acquired Android Inc. on August 17, 2005; key employees of Android Inc., including Rubin, Miner, and White, stayed at the company after the acquisition.[23] Not much was known about Android Inc. at the time, but many assumed that Google was planning to enter the mobile phone market with this move.[23] At Google, the team led by Rubin developed a mobile device platform powered by the Linux kernel. Google marketed the platform to handset makers and carriers on the promise of providing a flexible, upgradable system. Google had lined up a series of hardware component and software partners and signaled to carriers that it was open to various degrees of cooperation on their part.[34][35][36]

Speculation about Google's intention to enter the mobile communications market continued to build through December 2006.[37] An earlier prototype codenamed "Sooner" had a closer resemblance to a BlackBerry phone, with no touchscreen, and a physical, QWERTY keyboard, but was later re-engineered to support a touchscreen, to compete with other announced devices such as the 2006 LG Prada and 2007 Apple iPhone.[38][39] In September 2007, *InformationWeek* covered an Evalueserve study reporting that Google had filed several patent applications in the area of mobile telephony.[40][41]

Eric Schmidt, Andy Rubin and Hugo Barra at a press conference for the Google's Nexus 7 tablet.

On November 5, 2007, the Open Handset Alliance, a consortium of technology companies including Google, device manufacturers such as HTC, Sony and Samsung, wireless carriers such as Sprint Nextel and T-Mobile, and chipset makers such as Qualcomm and Texas Instruments, unveiled itself, with a goal to develop

open standards for mobile devices.[24] That day, Android was unveiled as its first product, a mobile device platform built on the Linux kernel version 2.6.25.[24][42] The first commercially available smartphone running Android was the HTC Dream, released on October 22, 2008.[43]

10.3 Features:

Interface

Android's default user interface is based on direct manipulation,[53] using touch inputs, that loosely correspond to real-world actions, like swiping, tapping, pinching, and reverse pinching to manipulate on-screen objects, and a virtual keyboard.[53] The response to user input is designed to be immediate and provides a fluid touch interface, often using the vibration capabilities of the device to provide haptic feedback to the user. Internal hardware such as accelerometers, gyroscopes and proximity sensors[54] are used by some applications to respond to additional user actions, for example adjusting the screen from portrait to landscape depending on how the device is oriented, or allowing the user to steer a vehicle in a racing game by rotating the device, simulating control of a steering wheel.[55]

Android devices boot to the homescreen, the primary navigation and information point on the device, which is similar to the desktop found on PCs. Android homescreens are typically made up of app icons and widgets; app icons launch the associated app, whereas widgets display live, auto-updating content such as the weather forecast, the user's email inbox, or a news ticker directly on the homescreen.[56] A homescreen may be made up of several pages that the user can swipe back and forth between, though Android's homescreen interface is heavily customisable, allowing the user to adjust the look and feel of the device to their tastes.[57] Third-party apps available on Google Play and other app stores can extensively re-theme the homescreen, and even mimic the look of other operating systems, such as Windows Phone.[58] Most manufacturers, and some wireless carriers, customise the look and feel of their Android devices to differentiate themselves from their competitors.[59]

Present along the top of the screen is a status bar, showing information about the device and its connectivity. This status bar can be "pulled" down to reveal a notification screen where apps display important information or updates, such as a newly received email or SMS text, in a way that does not immediately interrupt or inconvenience the user.[60] Notifications are persistent until read (by tapping, which opens the relevant app) or dismissed by sliding it off the screen. Beginning on

Android 4.1, "expanded notifications" can display expanded details or additional functionality; for instance, a music player can display playback controls, and a "missed call" notification provides buttons for calling back or sending the caller an SMS message.[61]

Android provides the ability to run applications which change the default launcher and hence the appearance and externally visible behaviour of Android. These appearance changes include a multi-page dock or no dock, and many more changes to fundamental features of the user interface.[62]

Hardware

The main hardware platform for Android is the 32-bit ARMv7 architecture. The Android-x86 project provides support for the x86 architecture,[9] and Google TV uses a special x86 version of Android. In 2012, Intel processors began to appear on more mainstream Android platforms, such as phones.[80] In 2013, Freescale announced support for Android on its i.MX processor, specifically the i.MX5X and i.MX6X series.[81]

As of November 2013, Android 4.4 recommends at least 512 MB of RAM,[82] while for "low RAM" devices 340 MB is the required minimum amount that does not include memory dedicated to various hardware components such as the baseband processor.[83] Android 4.4 requires a 32-bit ARMv7, MIPS or x86 architecture processor (latter two through unofficial ports),[9][84] together with an OpenGL ES 2.0 compatible graphics processing unit (GPU).[85] Android supports OpenGL ES 1.1, 2.0 and 3.0. Some applications explicitly require a certain version of the OpenGL ES, thus suitable GPU hardware is required to run such applications.[85]

In addition to running directly on x86-based hardware, Android can also be run on x86 architecture by using an Android emulator which is part of the Android SDK, or by using third-party emulators such as BlueStacks,[86][87] GenyMotion or Andy.[88]

Android devices incorporate many optional hardware components, including still or video cameras, GPS, orientation sensors, dedicated gaming controls, accelerometers, gyroscopes, barometers, magnetometers, proximity sensors, pressure sensors, thermometers, and touchscreens. Some hardware components are not required, but became standard in certain classes of devices, such as smartphones, and additional requirements apply if they are present. Some other hardware was initially required, but those requirements have been relaxed or

eliminated altogether. For example, as Android was developed initially as a phone OS, hardware such as microphones were required, while over time the phone function became optional.[66] Android used to require an autofocus camera, which was relaxed to a fixed-focus camera[66] if it is even present at all, since the camera was dropped as a requirement entirely when Android started to be used on set-top boxes.

Development

Android is developed in private by Google until the latest changes and updates are ready to be released, at which point the source code is made available publicly.[89] This source code will only run without modification on select devices, usually the Nexus series of devices. The source code is, in turn, adapted by OEMs to run on their hardware.[90] Android's source code does not contain the often proprietary device drivers that are needed for certain hardware components.[91]

The green Android logo was designed for Google in 2007 by graphic designer Irina Blok. The design team was tasked with a project to create a universally identifiable icon with the specific inclusion of a robot in the final design. After numerous design developments based on science-fiction and space movies, the team eventually sought inspiration from the human symbol on restroom doors and modified the figure into a robot shape. As Android is open-sourced, it was agreed that the logo should be likewise, and since its launch the green logo has been reinterpreted into countless variations on the original design.

10.4 **Linux kernel**

Android consists of a kernel based on the Linux kernel long-term support (LTS) branch. As of January 2014, current Android versions are built upon Linux kernel 3.4 or newer,[101][102] but the specific kernel version number depends on the actual Android device and chipset.[103][104][105] Android has used various kernels since its first 2.6.25.[42]

Android's Linux kernel has further architectural changes that are implemented by Google outside the typical Linux kernel development cycle, such as the inclusion of components like Binder, ashmem, pmem, logger, wakelocks, and different out-of-memory (OOM) handling.[106][107][108] Certain features that Google contributed back to the Linux kernel, notably a power management feature called "wakelocks", were rejected by mainline kernel developers partly because they felt that Google did not show any intent to maintain its own code.[109][110][111] Google announced in April 2010 that they would hire two employees to work with the Linux kernel

community,[112] but Greg Kroah-Hartman, the current Linux kernel maintainer for the stable branch, said in December 2010 that he was concerned that Google was no longer trying to get their code changes included in mainstream Linux.[110] Some Google Android developers hinted that "the Android team was getting fed up with the process," because they were a small team and had more urgent work to do on Android.[113]

In August 2011, Linus Torvalds said that "eventually Android and Linux would come back to a common kernel, but it will probably not be for four to five years".[114] In December 2011, Greg Kroah-Hartman announced the start of Android Mainlining Project, which aims to put some Android drivers, patches and features back into the Linux kernel, starting in Linux 3.3.[115] Linux included the autosleep and wakelocks capabilities in the 3.5 kernel, after many previous attempts at merger. The interfaces are the same but the upstream Linux implementation allows for two different suspend modes: to memory (the traditional suspend that Android uses), and to disk (hibernate, as it is known on the desktop).[116] Google maintains a public code repository that contains their experimental work to re-base Android off the latest stable Linux versions.[117][118]

The flash storage on Android devices is split into several partitions, such as /system for the operating system itself, and /data for user data and application installations.[119] In contrast to desktop Linux distributions, Android device owners are not given root access to the operating system and sensitive partitions such as /system are read-only. However, root access can be obtained by exploiting security flaws in Android, which is used frequently by the open-source community to enhance the capabilities of their devices,[120] but also by malicious parties to install viruses and malware.[121]

Android is a Linux distribution according to the Linux Foundation,[122] Google's open-source chief Chris DiBona,[123] and several journalists.[124][125] Others, such as Google engineer Patrick Brady, say that Android is not Linux in the traditional Unix-like Linux distribution sense; Android does not include the GNU C Library and some of other components typically found in Linux distributions

10.5 **Security and privacy**

Permissions are used to control a particular application's access to system functions. Android applications run in a sandbox, an isolated area of the system that does not have access to the rest of the system's resources, unless access permissions are explicitly granted by the user when the application is installed.

Before installing an application, Play Store displays all required permissions: a game may need to enable vibration or save data to an SD card, for example, but should not need to read SMS messages or access the phonebook. After reviewing these permissions, the user can choose to accept or refuse them, installing the application only if they accept.[143] The sandboxing and permissions system lessens the impact of vulnerabilities and bugs in applications, but developer confusion and limited documentation has resulted in applications routinely requesting unnecessary permissions, reducing its effectiveness.[144] Google has now pushed an update to Android Verify Apps feature, which will now run in background to detect malicious processes and crack them down.[145]

The "App Ops" privacy and application permissions control system, used for internal development and testing by Google, was introduced in Google's Android 4.3 release for the Nexus devices. Initially hidden, the feature was discovered publicly; it allowed users to install a management application and approve or deny permission requests individually for each of the applications installed on a device.[146] Access to the App Ops was later restricted by Google starting with Android 4.4.2 with an explanation that the feature was accidentally enabled and not intended for end-users; for such a decision, Google received criticism from the Electronic Frontier Foundation.[147][148][149] Individual application permissions management, through the App Ops or third-party tools, is currently only posssible with root access to the device.[150][151]

Research from security company Trend Micro lists premium service abuse as the most common type of Android malware, where text messages are sent from infected phones to premium-rate telephone numbers without the consent or even knowledge of the user.[152] Other malware displays unwanted and intrusive adverts on the device, or sends personal information to unauthorised third parties.[152] Security threats on Android are reportedly growing exponentially; however, Google engineers have argued that the malware and virus threat on Android is being exaggerated by security companies for commercial reasons,[153][154] and have accused the security industry of playing on fears to sell virus protection software to users.[153] Google maintains that dangerous malware is actually extremely rare,[154] and a survey conducted by F-Secure showed that only 0.5% of Android malware reported had come from the Google Play store.[155]

Google currently uses Google Bouncer malware scanner to watch over and scan the Google Play store apps.[156] It is intended to flag up suspicious apps and warn users of any potential threat with an application before they download it.[157] Android version 4.2 *Jelly Bean* was released in 2012 with enhanced security

features, including a malware scanner built into the system, which works in combination with Google Play but can scan apps installed from third party sources as well, and an alert system which notifies the user when an app tries to send a premium-rate text message, blocking the message unless the user explicitly authorises it.[158] Several security firms, such as Lookout Mobile Security,[159] AVG Technologies,[160] and McAfee,[161] have released antivirus software for Android devices. This software is ineffective as sandboxing also applies to such applications, limiting their ability to scan the deeper system for threats.[162]

Android smartphones have the ability to report the location of Wi-Fi access points, encountered as phone users move around, to build databases containing the physical locations of hundreds of millions of such access points. These databases form electronic maps to locate smartphones, allowing them to run apps like Foursquare, Google Latitude, Facebook Places, and to deliver location-based ads.[163] Third party monitoring software such as TaintDroid,[164] an academic research-funded project, can, in some cases, detect when personal information is being sent from applications to remote servers.[165] In August 2013, Google released Android Device Manager (ADM), a component that allows users to remotely track, locate, and wipe their Android device through a web interface.[100][166] In December 2013, Google released ADM as an Android application on the Google Play store, where it is available to devices running Android version 2.2 and higher.[167][168]

The open-source nature of Android allows security contractors to take existing devices and adapt them for highly secure uses. For example Samsung has worked with General Dynamics through their Open Kernel Labs acquisition to rebuild *Jelly Bean* on top of their hardened microvisor for the "Knox" project.[169][170]

As part of the broader 2013 mass surveillance disclosures it was revealed in September 2013 that the American and British intelligence agencies, the National Security Agency (NSA) and Government Communications Headquarters (GCHQ) respectively, have access to the user data on iPhone, BlackBerry, and Android devices. They are reportedly able to read almost all smartphone information, including SMS, location, emails, and notes.[171] Further reports in January 2014 revealed the intelligence agencies capabilities to intercept the personal information transmitted across the internet by social networks and other popular apps such as Angry Birds, which collect personal information of their users for advertising and other commercial reasons. GCHQ has, according to The Guardian, a wiki-style guide of different apps and advertising networks, and the different data that can be siphoned from each.[172] Later that week, the Finnish Angry Birds developer Rovio

announced that it was reconsidering its relationships with its advertising platforms in the light of these revelations, and called upon the wider industry to do the same.[173]

The documents revealed a further effort by the intelligence agencies to intercept Google Maps searches and queries submitted from Android and other smartphones to collect location information in bulk.[172] The NSA and GCHQ insist their activities are in compliance with all relevant domestic and international laws, although the Guardian stated "the latest disclosures could also add to mounting public concern about how the technology sector collects and uses information, especially for those outside the US, who enjoy fewer privacy protections than Americans."[172