

A

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

**KHOA AN TOÀN THÔNG TIN**

Bộ môn: **An toàn hệ điều hành**

BÀI BÁO CÁO:

**Tìm hiểu hệ điều hành cho các thiết bị di động Google Android**

**Giảng viên giảng dạy:** TS. Hoàng Xuân Dậu

**Sinh viên thực hiện:** Nhóm 01

Đặng Việt Anh B21DCAT023 Hoàng Việt Anh B21DCAT025 Hồ Phan Đức Anh B21DCAT024 Lê Đức Anh B21DCAT026

Lý Đức Anh B21DCAT030

***Hà Nội - 02/2024***

MỤC LỤC

1. [GIỚI THIỆU CHUNG 1](#_TOC_250025)
2. [KIẾN TRÚC CỦA HỆ ĐIỀU HÀNH 1](#_TOC_250024)
3. [CÁC THÀNH PHẦN CỦA HỆ ĐIỀU HÀNH 2](#_TOC_250023)
   1. [Tầng LINUX KERNEL 2](#_TOC_250022)
   2. [Tầng LIBRARIES và ANDROID RUNTIME 2](#_TOC_250021)
   3. [Tầng APPLICATION FRAMEWORK 3](#_TOC_250020)
   4. [Tầng APPLICATION 3](#_TOC_250019)
4. [CÀI ĐẶT HỆ ĐIỀU HÀNH CHO ĐIỆN THOẠI 3](#_TOC_250018)
5. [CÁC TÍNH NĂNG NỔI BẬT 11](#_TOC_250017)
   1. [Giao tiếp trường gần (NFC) 11](#_TOC_250016)
   2. [Bàn phím thay thế 11](#_TOC_250015)
   3. [Truyền hồng ngoại 11](#_TOC_250014)
   4. [Điều khiển không chạm 11](#_TOC_250013)
   5. [Tự động hóa 12](#_TOC_250012)
   6. [Tải xuống ứng dụng không dây 12](#_TOC_250011)
   7. [Bộ nhớ và hoán đổi pin 13](#_TOC_250010)
   8. [Màn hình chính tùy chỉnh 13](#_TOC_250009)
   9. [Giao diện linh hoạt 14](#_TOC_250008)
   10. [ROM tùy chỉnh 14](#_TOC_250007)
6. [CÁC VẤN ĐỀ AN NINH 15](#_TOC_250006)

* Các thành phần chính của An ninh, an toàn Android gồm 15
* [Các nguyên nhân ảnh hưởng đến vấn đề an ninh, an toàn Android 15](#_TOC_250005)

1. [AN TOÀN CỦA GOOGLE ANDROID 15](#_TOC_250004)

* [Các tính năng bảo mật của Android 15](#_TOC_250003)
* [Phương pháp bảo mật 16](#_TOC_250002)
* [Dịch vụ bảo mật của Google 17](#_TOC_250001)

1. [TỔNG KẾT 18](#_TOC_250000)

# GIỚI THIỆU CHUNG

* 1. **Android là gì?**

Android là một hệ điều hành được cài đặt trên một số phần cứng riêng biệt mà ở đây chủ yếu là cài đặt trên các thiết bị Smartphone như Samsung, Huawei, LG, …

# Lịch sử

Hệ điều hành Android có nguồn gốc tên từ Android, Inc. – công ty cha đẻ của Android. Công ty được thành lập tại Palo Alto, California vào tháng 10 năm 2003 do Andy Rubin – đồng sáng lập công ty Danger, Rich Miner – đồng sáng lập công ty viễn thông Winldfire, Nick Sears – cựu Phó giám đốc T- Moblie, và Chris White – trưởng khiết kế và giao diện tại WebTV.

# Phát triển

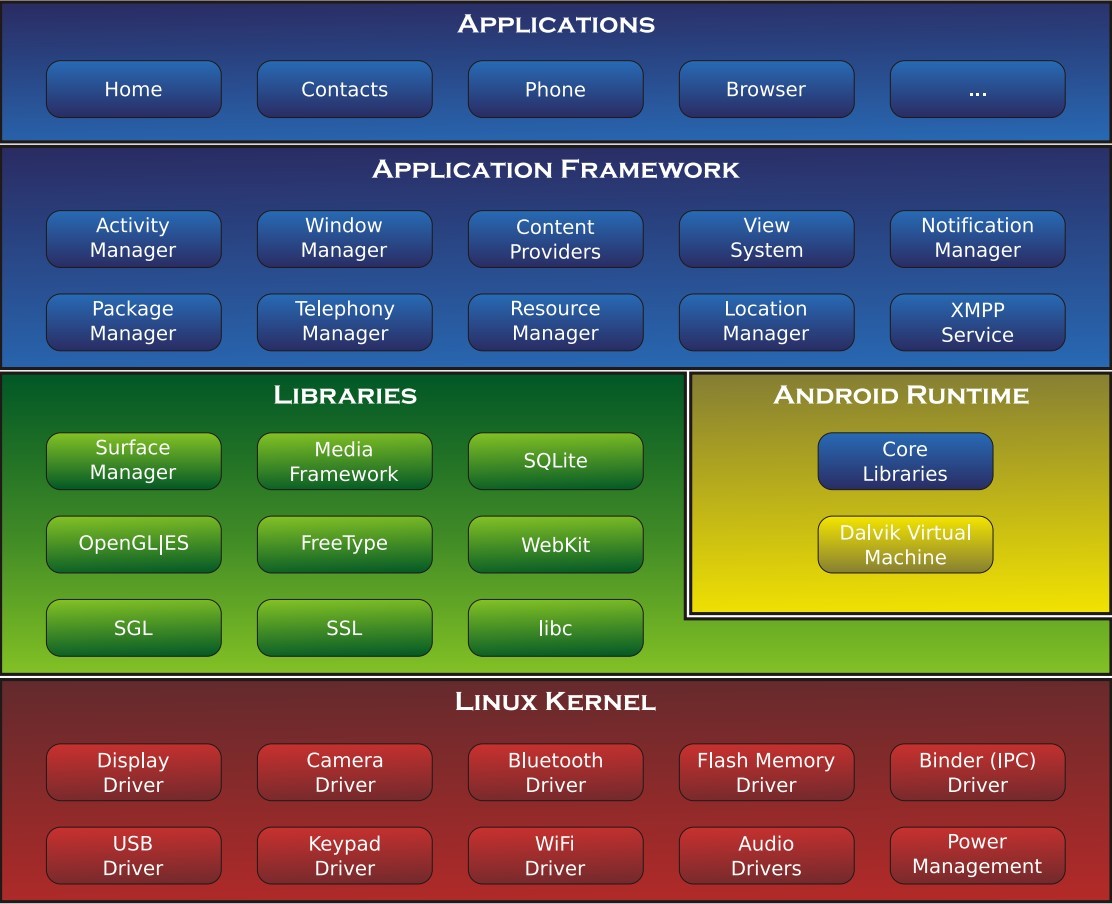
Google mua lại Android, Inc vào ngày 17 tháng 8 năm 2005, biến nó thành một bộ phận trực thuộc Google. Tại Google, nhóm phát triển đã phát triển một nền tảng di động phát triển trên nền tảng Linux được thiết kế dành cho các thiết bị di động có màn hình cảm ứng như điện thoại di động và máy tính bảng. Android có mã nguồn mở và Google phát hành mã nguồn theo Giấy phép Apache. Ngoài ra, Android còn có một cộng đồng lập trình viên đông đảo chuyên viết các ứng dụng để mở rộng chức năng của thiết bịm bằng một loại ngôn ngữ lập trình Java có sửa đổi.

# Thành công

Đến nay, Andorid trở thành một trong những nền tảng điện thoại di động thông minh phổ biến nhất thế giới. Android chiếm 87,7% thị phần điện thoại thông minh trên toàn thế giới vào thời điểm quý 2 năm 2017, với tổng cộng 2 tỷ thiết bị đã được kích hoạt và 1,3 triệu lượt kích hoạt mỗi ngày.

# KIẾN TRÚC CỦA HỆ ĐIỀU HÀNH

Android được chia thành 5 phần và 4 tầng chính từ dưới lên trên là tầng hạt nhân Linux, Tầng Libraries & Android Runtime, Tầng Application Framework và Tầng Applications.



*Mô hình kiến trúc nền tảng của Android*

# CÁC THÀNH PHẦN CỦA HỆ ĐIỀU HÀNH

# Tầng LINUX KERNEL

Hệ điều hành Android được phát triển dựa trên hạt nhân Linux, cụ thể hạt nhân Linux phiên bản 2.6, điều đó được thể hiện ở mức dưới cùng. Tất cả mọi hoạt động của điện thoại muốn thi hành được thì đều được thực hiện ở mức cấp thấp ở lớp này bao gồm Quản lý bộ nhớ (Memory Management), Giao tiếp với phần cứng (Driver Model), Thực hiện bảo mật (Security), Quản lý tiến trình (Process).

Tầng Kernel: Là nhân lõi của hệ điều hành, chứa các tập lệnh, driver giao tiếp giữa phần cứng và phần mềm của Android. Tuy được phát triển dựa vào nhân Linux nhưng thực ra nhân Linux đã được nâng cấp và sửa đổi rất nhiều để phù hợp với tính chất của những thiết bị cầm tay như hạn chế về bộ vi xử lý, dung lượng bộ nhớ, kích thước màn hình, nhu cầu kết nối mạng không dây, …

Tầng này gồm các thành phần chủ yếu:

* + **Display Driver:** Điều khiển việc hiển thị lên màn hình cũng như thu nhanh chứng điều khiển của người dùng lên màn hình như di chuyển, cảm ứng, …
  + **Camera Driver:** Điều khiển hoạt động của camera, nhận luồng dữ liệu từ camera trả về.
  + **Bluetooth Driver:** Điều khiển thiết bị phát và thu sóng Bluetooth.
  + **Flash Memory Driver:** Quản lý việc đọc ghi … lên các thiết bị nhớ như thẻ SD, Flash.
  + **Binder (IPC) Driver:** Chịu trách nhiệm về việc kết nối và liên lạc với mạng vô tuyến như CDMA, GSM, 3G, 4G, TLE, để đảm bảo những chức năng truyền thông được thực hiện.
  + **USB Driver:** Quản lý hoạt động của các cổng giao tiếp USB.
  + **Keypad Driver:** Điều khiển bàn phím.
  + **Wifi Driver:** Chịu trách nhiệm về việc thu phát sóng Wifi.
  + **Audio Driver:** Điều khiển các bộ thu phát âm thanh, giải mã các tín hiệu dạng audio thành tín điệu và ngược lại.
  + **Power Management:** Giám sát việc tiêu thụ điện năng.

# Tầng LIBRARIES và ANDROID RUNTIME

* 1. **Phần Libraries**

Phần Libraries: chứa các thư viện, API gần như cốt lõi của Android. Phần này có nhiều thư viện được viết bằng C/C++ để các phần mềm có thể sử dụng, các thư viện đó được tập hợp thành một nhóm như:

* + - **Surface Manager:** Quản lý truy cập vào các hệ thống hiển thị con (subsystem) và lớp đồ họa 2D, 3D từ nhiều ứng dụng.
    - **Media Framework:** Cung cấp hỗ trợ để phát và ghi lại các định dạng âm thanh và video
    - **SQLite:** Hệ cơ sở dữ liệu để các ứng dụng có thể sử dụng.
    - **OpenGL|ES:** Giao diện lập trình ứng dụng đa ngôn ngữ, nền tảng (API) để hiển thị đồ họa vector 2D và 3D
    - **FreeType:** Thư viện phần mềm có sẵn miễn phí để hiển thị phông chữ
    - **WebKit:** Tập hợp các lớp cho phép xây dựng khả năng duyệt web.
    - **SGL:** Thư viện gồm các công cụ đồ họa 2D
    - **SSL:** Công nghệ bảo mật để thiết lập liên kết được mã hóa giữa máy chủ web và trình duyệt web.
    - **Libc:** Cung cấp các API cơ bản để tương tác hệ điều hành

# Phần Android Runtime

Phần này chứa các thư viện mà một chương trình viết bằng ngôn ngữ Java có thể hoạt động. Phần này có 2 bộ phân tương tự như mô hình chạy Java trên máy tính thường.

* + - **Core Libraries**: Chứa các lớp như Java IO, Collection, File Access.
    - **Dalvik Virtual Machine-máy ảo Java đặc biệt**: Sử dụng các tính năng cốt lõi của Linux như quản lý bộ nhớ, đa luồng, những thứ đã có sẵn trong Java.

# Tầng APPLICATION FRAMEWORK

Tầng này xây dựng bộ công cụ - các phần tử ở mức cao để các lập trình viên có phát triển nhanh chóng xây dựng ứng dụng. Nó được viết bằng Java, có khả năng sử dụng chung để tiết kiệm tài nguyên.

Đây là một nền mở, có ưu điểm:

* **Với các hãng sản xuất điện thoại:** Có thể tùy biến để phù hợp với cấu hình điện thoại mà họ sản xuất như để có nhiều mẫu mã, style phù hợp thị hiếu người dùng
* **Với lập trình viên:** Cho phép lập trình viên có thể sử dụng các API ở tầng trên mà không cần phải hiểu rõ cấu trúc bên dưới, tạo điều kiện cho lập trình viên tự do sáng tạo bởi vì chỉ cần quan tâm đến nội dung mà ứng dụng mà học làm việc. Một tập hợp API rất hữu ích được xây dựng sẵn như hệ thống định vị, các dịch vụ chạy nền, liên lạc giữa các ứng dụng, các thành phần giao diện cao cấp …

Một số thành phần của tầng:

* + **Activity Manager:** Quản lý các chu kỳ sống của một ứng dụng cũng như cung cấp công cụ điều khiển các Activity.
  + **Window Manager:** Quản lý việc xây dựng và hiển thị các giao diện người dùng cũng như tổ chức quản lý các giao diện giữa các ứng dụng.
  + **Content Providers:** Cho phép các ứng dụng chia sẻ dữ liệu với các ứng dụng khác.
  + **View System:** Tập các thành phần giao diện (view) được sử dụng để tạo giao diện người dùng.
  + **Notification Manager:** Quản lý việc hiển thị các thông báo như báo có tin nhắn, có tin nhắn mới,

…

* + **Package Manager:** Một tập hợp các phần mềm dùng để quản lý và tự động hóa việc cài đặt, nâng cấp, gỡ bỏ các phần mềm/thư viện (package).
  + **Telephony Manager:** Cung cấp công cụ để thực hiện liên lạc như gọi điện thoại.
  + **Resource Manager:** Quản lý tài nguyên tĩnh của các ứng dụng bao gồm các file hình ảnh, âm thanh, layout, string.
  + **Location Manager:** Cho phép xác định vị trí điện thoại dựa vào hệ thống định vị toàn cầu GPS và Google Maps.
  + **XMPP Service:** Cung cấp công cụ để liên lạc trong thời gian thực.

# Tầng APPLICATION

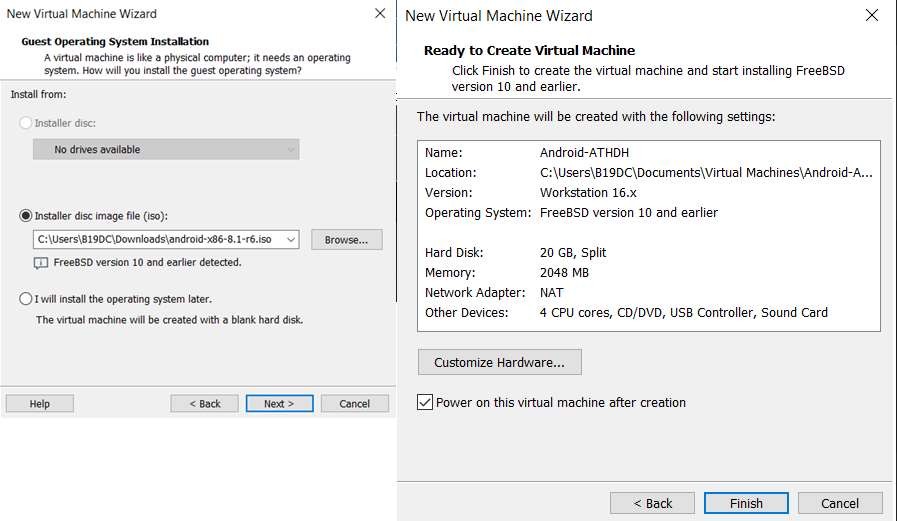
Đây là lớp ứng dụng giao tiếp với người dùng, bao gồm các ứng dụng. Các ứng dụng cơ bản, được cài đặt đi liền với hệ điều hành như:

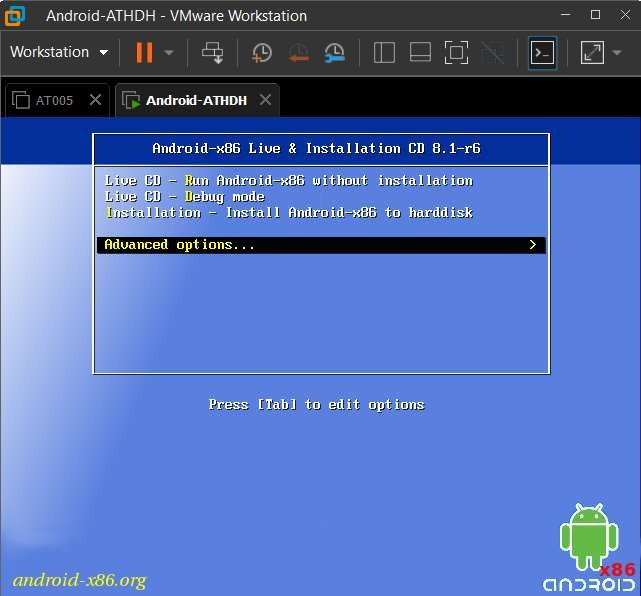
* + Phone: Gọi điện
  + Contacts: Quản lý danh bạ
  + Browser: Trình duyệt Web
  + SMS: Nhắn tin
  + Calendar: Lịch
  + …

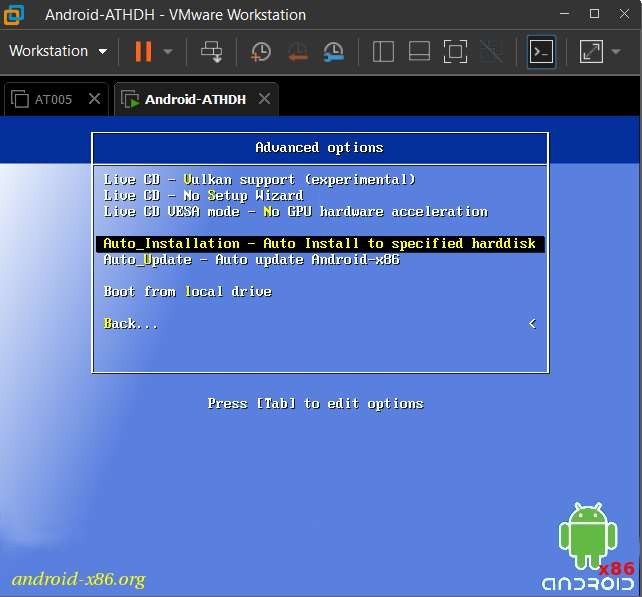
# CÀI ĐẶT HỆ ĐIỀU HÀNH CHO ĐIỆN THOẠI

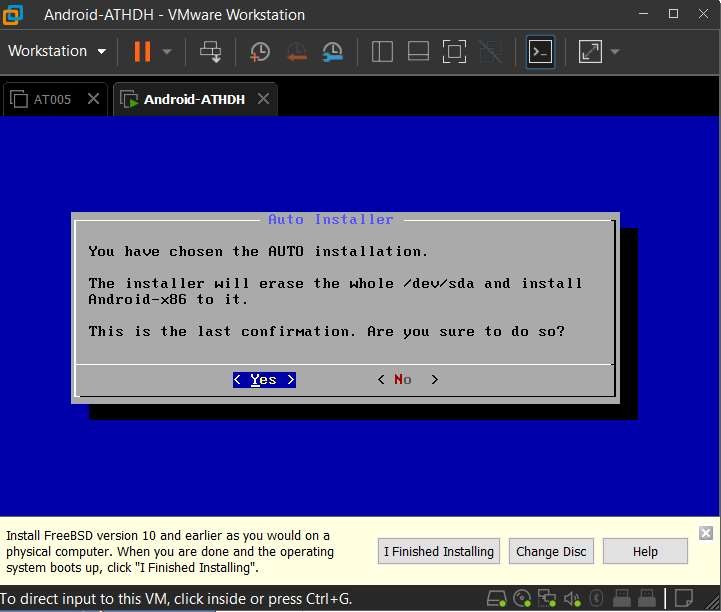
Hầu hết các bản cập nhập cho Android đều có sẵn trên mạng, không cần phải chép vào máy vi tính, USB hoặc kết nối qua cáp để truyền qua, … Nhà phát hành đưa ra các phiên bản Android mới tùy thuộc vào nhu cầu của người dùng. Thông thường, sẽ có một bản thông báo ở trên hệ điều hành có sẵn và kèm

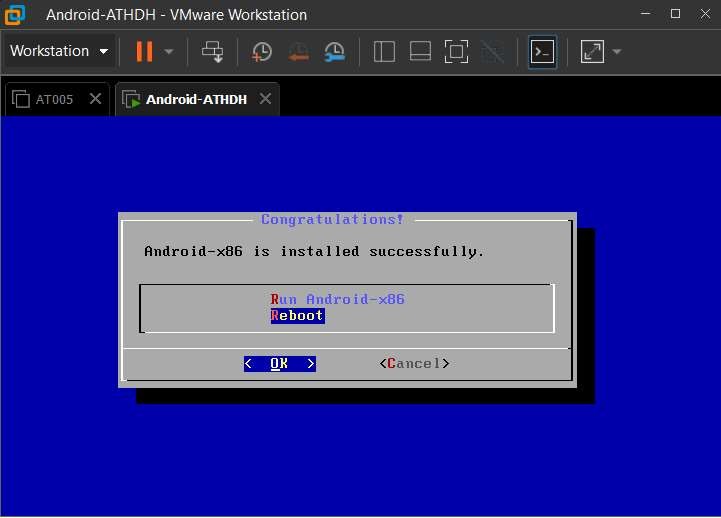
theo cập nhập tự động trong Smartphone hoặc máy tính bảng, trong trường hợp không có thông báo, chúng ta có thể xem thông tin qua mạng và tải chúng về máy.

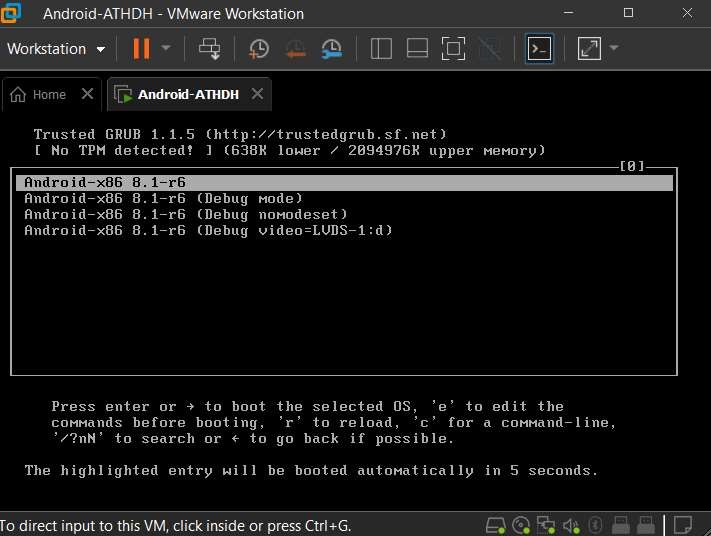
1. **Chuẩn bị**
   * Phần mềm VMware Workstation
   * Bộ cài Android x86 ( file ISO )
2. **Thiết lập trên Vmware**
   * Cấu hình máy ảo Android
   * Chọn **Advanced options…**

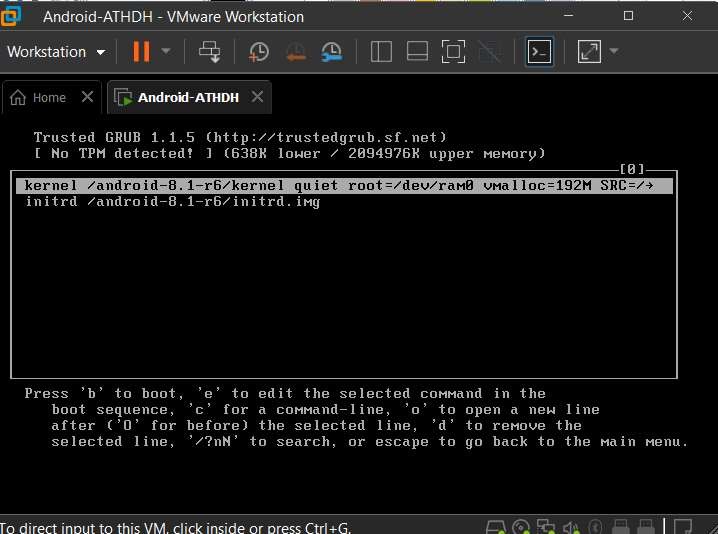


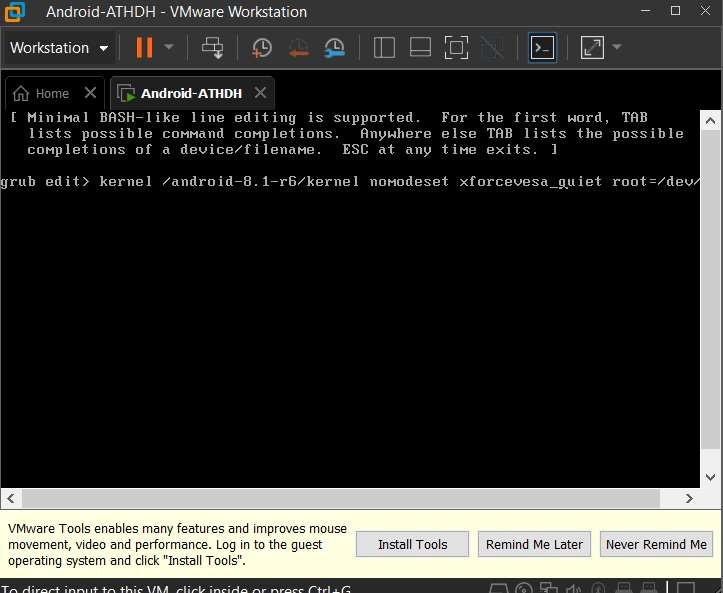
* + Chọn **Auto Installation – Auto Install to specified harddisk**.
  + Chọn **Yes**

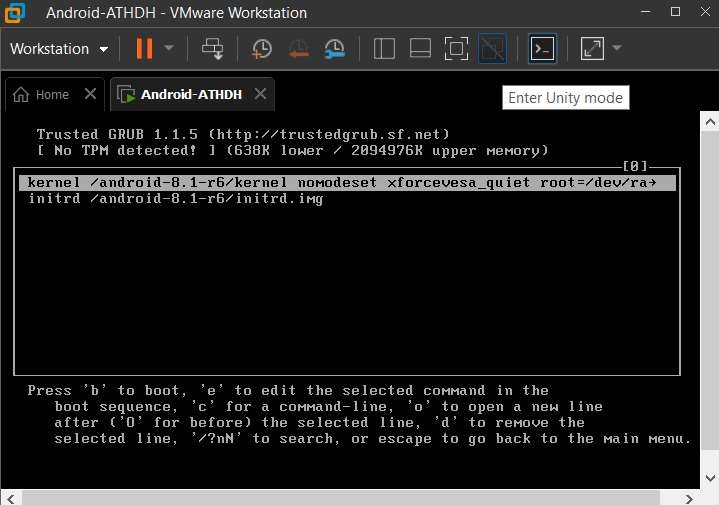


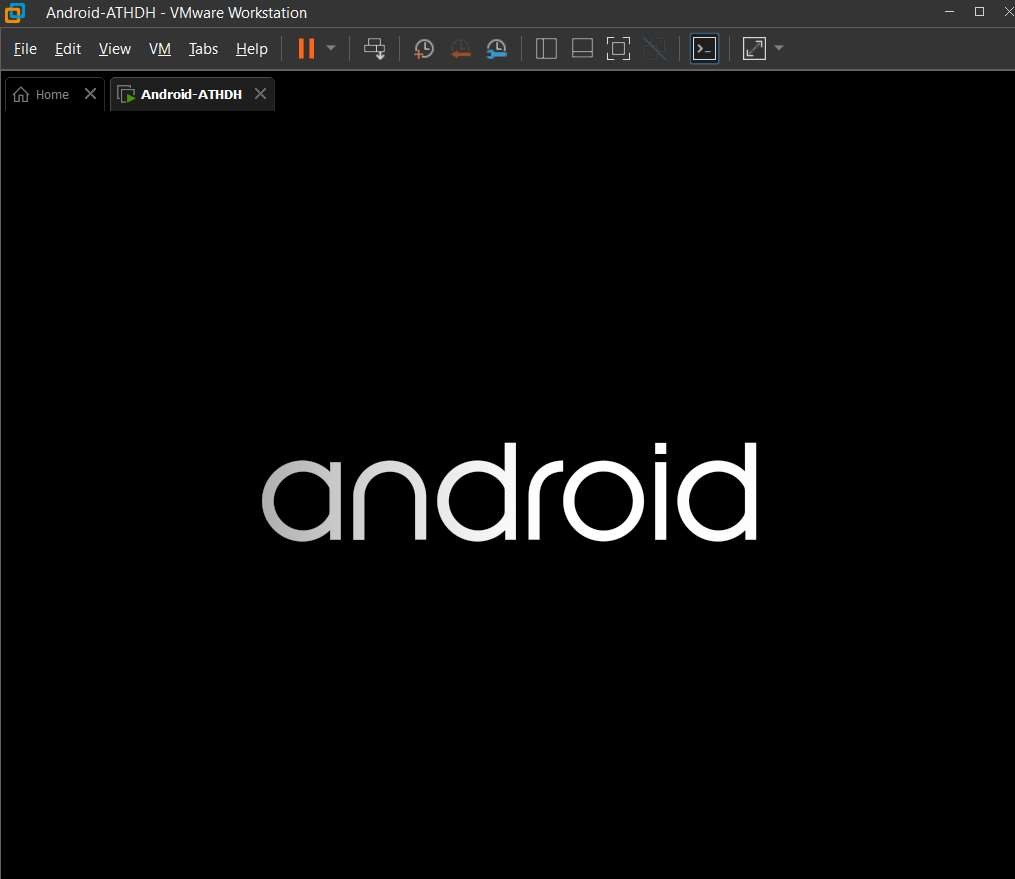
* + **Reboot -> OK**
  + Sau khi khởi động lại và vào menu boot, ấn phím **E** để chỉnh sửa menu boot đầu tiên.

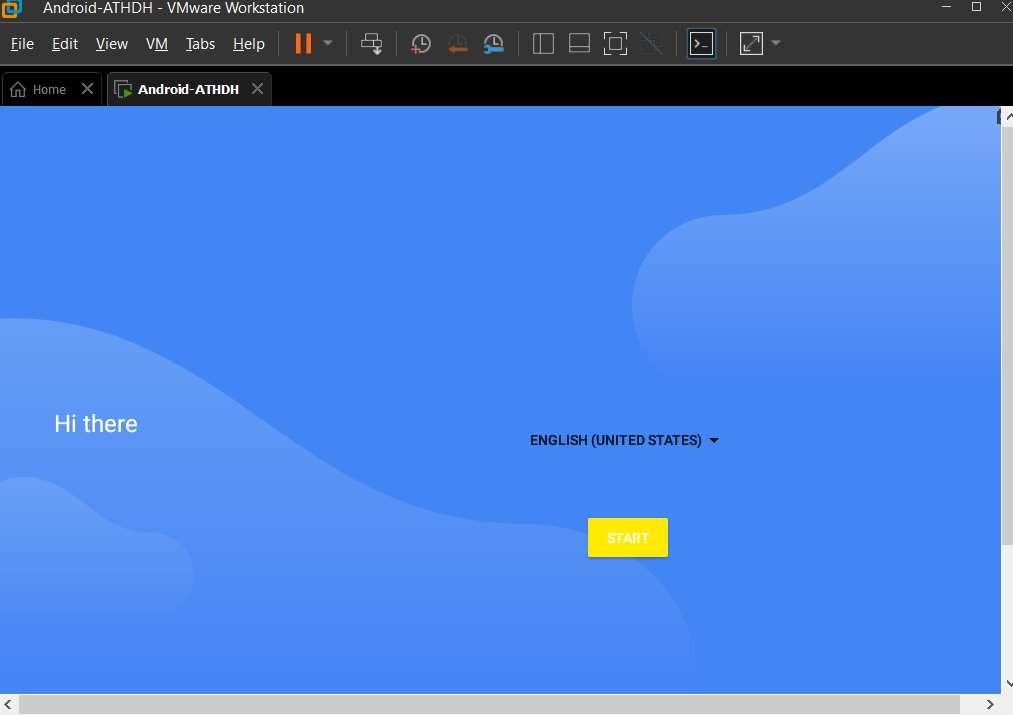


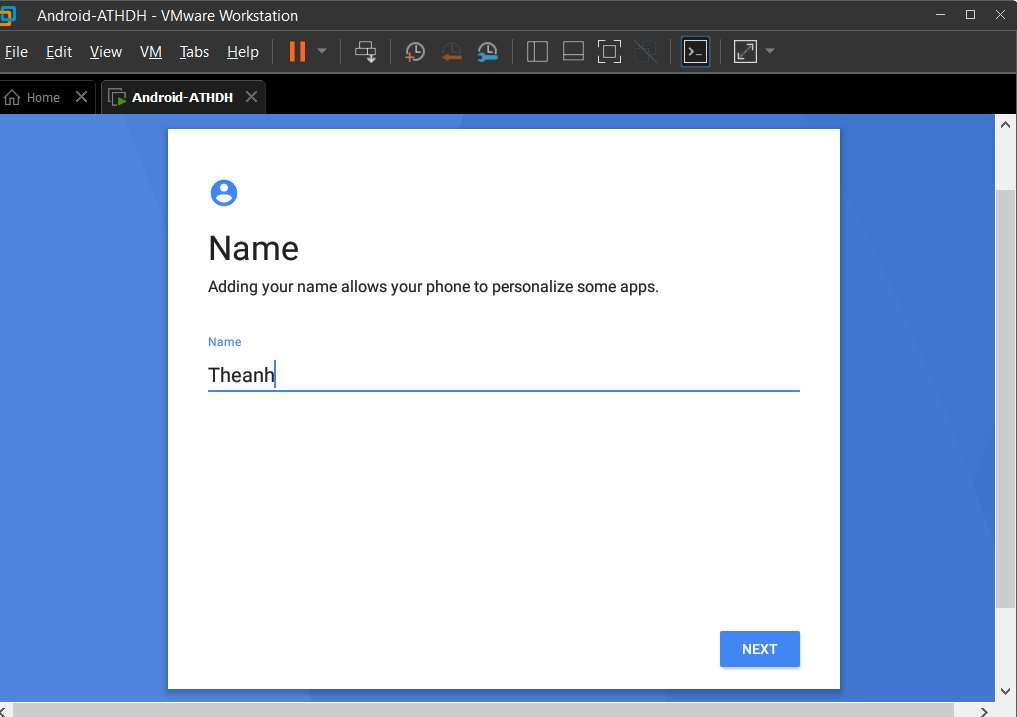
* + Sau đó, ấn phím **E** lần nữa để chỉnh sửa.
  + Sửa lệnh thành **kernel nomodeset xforcevesa\_quiet**.- > Enter

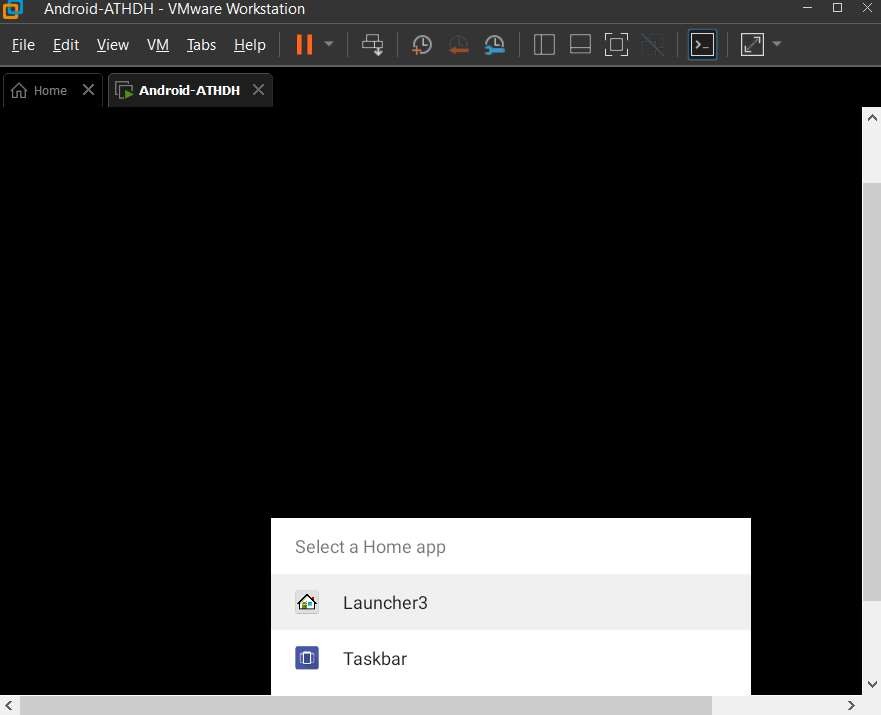


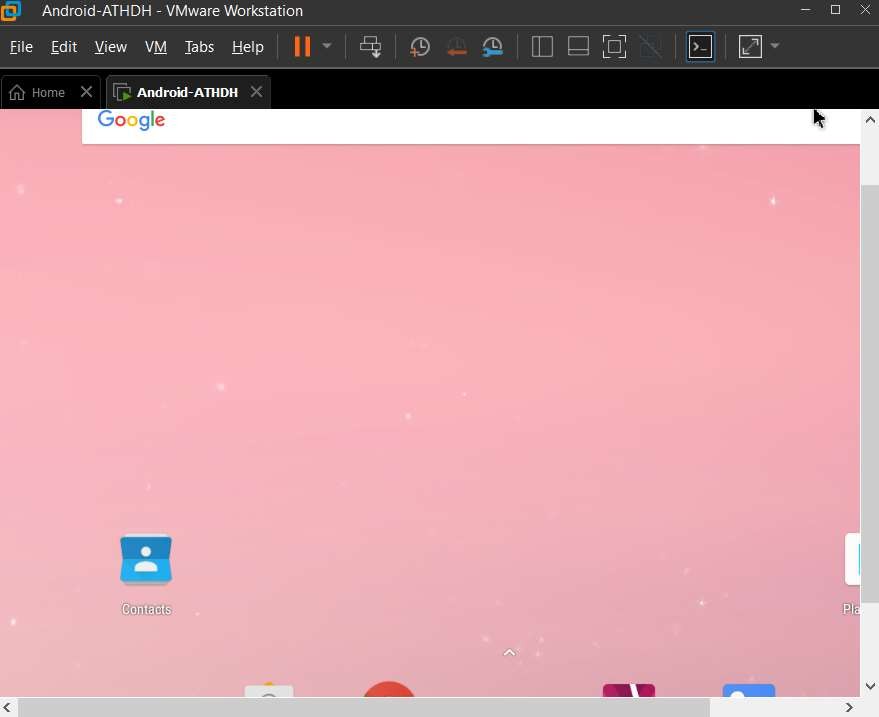
* + Ấn **B** để quay lại mục trước
  + Sau khi quay lại mục trước, dòng lệnh sẽ tự chạy và chờ menu boot Android xuất hiện là thành công.



* + Ấn **Start** để bắt đầu
  + Đặt tên người dùng



* + Chọn **Launcher3**
  + Cài đặt thành công



# CÁC TÍNH NĂNG NỔI BẬT

# Giao tiếp trường gần (NFC)

Hầu hết các thiết bị Android đều hỗ trợ NFC, cho phép các thiết bị điện tử dễ dàng tương tác trong khoảng cách ngắn. Mục đích chính ở đây là tạo ra một lựa chọn thanh toán đơn giản hơn so với việc mang theo thẻ tín dụng hoặc tiền mặt, và trong khi thị trường chưa bùng nổ như nhiều chuyên gia đã dự đoán, có thể có một giải pháp thay thế đang hoạt động, dưới dạng Bluetooth Low Energy (BLE).

# Bàn phím thay thế

Android hỗ trợ nhiều bàn phím và dễ cài đặt chúng; các ứng dụng SwiftKey, Skype và 8pen đều cung cấp các cách để nhanh chóng thay đổi kiểu bàn phím của bạn. Các hệ điều hành di động khác hoặc hoàn toàn không cho phép bàn phím phụ, hoặc quá trình cài đặt và sử dụng chúng rất tẻ nhạt và tốn thời gian.

# Truyền hồng ngoại

Hệ điều hành Android hỗ trợ bộ phát hồng ngoại tích hợp, cho phép bạn sử dụng điện thoại hoặc máy tính bảng làm điều khiển từ xa.



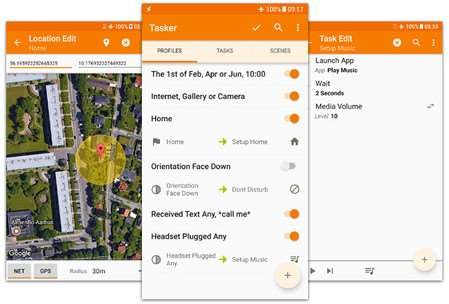
# Điều khiển không chạm

Sử dụng các ứng dụng Android như Wave Control , người dùng có thể điều khiển điện thoại không cần chạm, chỉ bằng cử chỉ. Bạn có đôi tay lộn xộn nhưng cần phải tắt màn hình hoặc thay đổi một bài hát? Giản dị. Điều này có thể đặc biệt hữu ích nếu bạn đang lái xe, vì vậy bạn có thể quan sát đường đi của cả hai.



# Tự động hóa

Ứng dụng Tasker cho phép bạn không chỉ kiểm soát các quyền của ứng dụng mà còn tự động hóa chúng. Bạn chỉ muốn các dịch vụ vị trí của mình hoạt động trong ngày? Bạn muốn tạo một cách tùy chỉnh để bắt đầu âm nhạc của mình — ví dụ: bằng lệnh thoại và ở một âm lượng nhất định? Tasker có thể giúp bạn.



# Tải xuống ứng dụng không dây

Việc truy cập các cửa hàng ứng dụng trên bất kỳ thiết bị di động nào có thể khiến bạn khó chịu, nhưng iOS sẽ khiến việc này khó khăn hơn một chút — tải xuống một ứng dụng trên máy tính của bạn và ứng dụng đó sẽ không đồng bộ hóa với thiết bị di động của bạn cho đến khi bạn cắm và truy cập iTunes. Trong khi đó, bằng cách sử dụng Android Market hoặc các tùy chọn của bên thứ ba như AppBrain, cho phép bạn tải xuống ứng dụng trên PC và sau đó tự động đồng bộ hóa chúng với Droid của bạn mà không cần cắm.



# Bộ nhớ và hoán đổi pin

Điện thoại Android cũng có khả năng phần cứng độc đáo. Hệ điều hành của Google giúp bạn có thể tháo và nâng cấp pin hoặc thay thế pin không còn sạc được nữa. Ngoài ra, điện thoại Android đi kèm với khe cắm thẻ SD để mở rộng dung lượng lưu trữ.



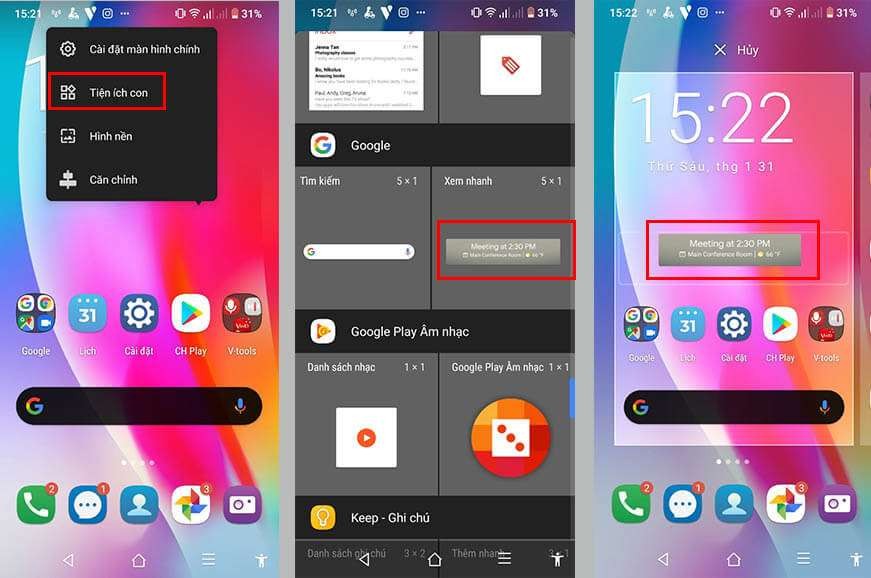
# Màn hình chính tùy chỉnh

Mặc dù có thể hack một số điện thoại nhất định để tùy chỉnh màn hình chính, nhưng Android đi kèm với khả năng này ngay từ đầu. Tải xuống trình khởi chạy của bên thứ ba như Nova, Apex hoặc Slide và bạn có thể thêm cử chỉ, phím tắt mới hoặc thậm chí cải tiến hiệu suất cho các thiết bị kiểu cũ hơn.



# Giao diện linh hoạt

Các ứng dụng rất linh hoạt, nhưng đôi khi bạn muốn có thông tin trong nháy mắt thay vì phải mở một ứng dụng và đợi nó tải. Các tiện ích Android cho phép bạn hiển thị bất kỳ tính năng nào bạn chọn, ngay trên màn hình chính — bao gồm các ứng dụng thời tiết, tiện ích âm nhạc hoặc các công cụ năng suất giúp nhắc nhở bạn một cách hữu ích về các cuộc họp sắp tới hoặc thời hạn sắp tới.



# ROM tùy chỉnh

Đây là một vấn đề lớn. Bởi vì hệ điều hành Android là mã nguồn mở, các nhà phát triển có thể điều chỉnh hệ điều hành hiện tại và xây dựng các phiên bản của riêng họ, người dùng có thể tải xuống và cài đặt thay thế cho hệ điều hành gốc. Một số có đầy đủ các tính năng, trong khi những người khác thay đổi giao diện của thiết bị. Rất có thể nếu có một tính năng bạn muốn, ai đó đã tạo sẵn một bản ROM tùy chỉnh cho nó.

# CÁC VẤN ĐỀ AN NINH

* **Các thành phần chính của An ninh, an toàn Android**

## Thiết kế đánh giá

Quá trình bảo mật Android bắt đầu sớm trong vòng đời phát triển với việc tạo ra một mô hình cấu hình bảo mật và phong phú. Mỗi tính năng chính của nền tảng này được xem xét bởi kỹ thuật và các nguồn lực an ninh, với kiểm soát an ninh thích hợp vào kiến trúc của hệ thống.

## Kiểm tra thâm nhập và xem xét lại mã

Trong sự phát triển của nền tảng này, Android được tạo ra và các thành phần mã nguồn mở có thể đánh giá là có an ninh vững chắc. Những đánh giá này được thực hiện bởi đội an ninh Android, đội ngũ an ninh thông tin kỹ thuật của Google, và các chuyên gia tư vấn an ninh độc lập. Mục tiêu của những đánh giá này là để xác định các điểm yếu và lỗ hổng có thể có trước khi nền tảng là mã nguồn mở, và để mô phỏng các loại phân tích sẽ được thực hiện bởi các chuyên gia an ninh bên ngoài khi phát hành.

## Mã nguồn mở và đánh giá cộng đồng

Dự án mã nguồn mở Android cho phép mở rộng an ninh xem xét lại bởi bất kỳ bên nào quan tâm đến dự án này. Android cũng sử dụng công nghệ mã nguồn mở đã trải qua nhiều cuộc rà soát an ninh từ bên ngoài, chẳng hạn như hạt nhân Linux. Các thị trường Android cung cấp một diễn đàn cho người sử dụng và các công ty cung cấp thông tin về các ứng dụng cụ thể, trực tiếp đến người sử dụng.

## Trả lời sự cố

Khi phát hiện các vấn đề hợp pháp, nhóm nghiên cứu Android có một quá trình phản ứng cho phép giảm thiểu nhanh chóng các lỗ hổng để đảm bảo rằng rủi ro tiềm ẩn cho tất cả người sử dụng Android được giảm thiểu.

# Các nguyên nhân ảnh hưởng đến vấn đề an ninh, an toàn Android :

* + Mã độc ồ ạt tấn công Android
  + Kho ứng dụng Android Market (thật và giả)
  + Ứng dụng có chèn mã độc và được cung cấp miễn phí
  + Cài trực tiếp tập tin APK

# AN TOÀN CỦA GOOGLE ANDROID

# Các tính năng bảo mật của Android

# Hộp kín ứng dụng (App sandbox)

Nền tảng Android tận dụng tính năng bảo vệ dựa trên người dùng Linux để xác định và cô lập các tài nguyên ứng dụng. Để thực hiện việc này, Android chỉ định một ID người dùng (UID) duy nhất cho từng ứng dụng Android và chạy ứng dụng đó trong quy trình riêng của ứng dụng đó. Android sử dụng UID này để thiết lập Hộp kín ứng dụng cấp nhân.

# Đăng ký ứng dụng (App signing)

Tính năng đăng ký ứng dụng cho phép các nhà phát triển xác định tác giả của ứng dụng và cập nhật ứng dụng của họ mà không cần tạo giao diện và quyền phức tạp. Mọi ứng dụng chạy trên nền tảng Android phải có chữ ký của nhà phát triển.

# Xác thực (Authentication)

Android sử dụng khái niệm khóa mật mã được xác thực bởi người dùng yêu cầu lưu trữ khóa mật mã và nhà cung cấp dịch vụ cũng như trình xác thực người dùng.

Trên các thiết bị có cảm biến vân tay, người dùng có thể đăng ký một hoặc nhiều dấu vân tay và sử dụng các dấu vân tay đó để mở khóa thiết bị và thực hiện các tác vụ khác. Hệ thống

con Gatekeeper thực hiện xác thực mẫu thiết bị / mật khẩu trong Môi trường thực thi tin cậy (TEE).

Android 9 trở lên có thêm xác nhận được bảo vệ (Protected Confirmation), cung cấp cho người dùng một cách để xác nhận chính thức các giao dịch quan trọng, chẳng hạn như thanh toán.

# Sinh trắc học (Biometrics)

Sinh trắc học cung cấp cách xác nhận danh tính của người sở hữu thiết bị thuận tiện hơn nhưng có khả năng kém an toàn hơn. Trong mô hình xác thực phân cấp, xác thực chính (chẳng hạn như các phương thức dựa trên yếu tố đã biết như mã PIN, hình mở khóa và mật khẩu) cung cấp mức độ bảo mật cao nhất. Sinh trắc học ở cấp độ xác thực thứ cấp, cung cấp sự cân bằng giữa sự tiện lợi và bảo mật. CDD (Compatibility Definition Document) của Android xác định ba lớp độ mạnh sinh trắc học: Lớp 3 (Mạnh), Lớp 2 (Yếu) và Lớp 1 (Thuận tiện). Mỗi lớp có một tập hợp các điều kiện tiên quyết, đặc quyền và ràng buộc. Tất cả ba lớp đều được phép tích hợp với màn hình khóa, nhưng chỉ các trình xác thực Mạnh và Yếu mới được phép tích hợp với các API android.hardware.biometrics.

# Mã hóa (Encryption)

Sau khi thiết bị được mã hóa, tất cả dữ liệu do người dùng tạo sẽ tự động được mã hóa trước khi đưa nó vào đĩa và tất cả các lần đọc tự động giải mã dữ liệu trước khi trả lại cho quá trình gọi. Mã hóa đảm bảo rằng ngay cả khi một bên trái phép cố gắng truy cập vào dữ liệu, họ sẽ không thể đọc được dữ liệu đó.

# Kho khóa (Keystore)

Android cung cấp kho khóa được hỗ trợ bởi phần cứng cung cấp tính năng tạo khóa, nhập và xuất khóa bất đối xứng, nhập khóa đối xứng thô, mã hóa và giải mã bất đối xứng với các chế độ đệm thích hợp, v.v.

# Linux tăng cường bảo mật (Security-Enhanced Linux)

Là một phần của mô hình bảo mật Android, Android sử dụng Linux được tăng cường bảo mật (SELinux) để thực thi kiểm soát truy cập bắt buộc (MAC) trên tất cả các quy trình, ngay cả các quy trình chạy với đặc quyền root / superuser (khả năng của Linux).

# Môi trường thực thi đáng tin cậy Trusty (TEE)

Trusty là một hệ điều hành (OS) an toàn cung cấp Môi trường thực thi đáng tin cậy (TEE) cho Android. Hệ điều hành Trusty chạy trên cùng một bộ xử lý với hệ điều hành Android, nhưng Trusty bị cô lập với phần còn lại của hệ thống bởi cả phần cứng và phần mềm.

# Khởi động đã được xác minh (Verified Boot)

Verified Boot cố gắng đảm bảo tất cả mã được thực thi đến từ một nguồn đáng tin cậy (thường là nhà sản suất phụ tùng gốc của thiết bị), chứ không phải từ kẻ tấn công hoặc bên không đáng tin. Nó thiết lập một chuỗi tin cậy đầy đủ, bắt đầu từ gốc tin cậy được bảo vệ bằng phần cứng đến bộ nạp khởi động, đến phân vùng khởi động và các phân vùng đã được xác minh khác.

# Phương pháp bảo mật

Các phương pháp bao gồm:

1. **Bảo mật tổ chức và hoạt động -** Tạo ra các phương pháp bảo mật mạnh mẽ trong nhóm và tổ chức của bạn:
   * Tạo một nhóm bảo mật và quyền riêng tư chuyên dụng và thiết lập một nhà lãnh đạo cho tổ chức này
   * Xây dựng quy trình xác minh
   * Theo dõi thay đổi mã nguồn
   * Xác thực tính toàn vẹn của mã nguồn và phả hệ
2. **Bảo mật hệ thống -** Rà soát và cải thiện hệ điều hành cốt lõi và bảo mật thiết bị.
   * Xác thực sinh trắc học (Biometric authentication)
   * SELinux
   * Cửa hậu (Backdoors)
   * Công cụ phát triển (Development tools)
   * Chức năng nhúng trong AOSP
   * Cập nhật bảo mật
   * Quản lý khóa (Key management)
   * Hệ thống ký hình ảnh (System image signing)
   * Bộ nạp khởi động có thể mở khóa (Unlockable bootloaders)
   * Thiết bị kiểm tra thử xâm nhập (Device pentesting)

# Bảo mật ứng dụng

Xem xét và cải thiện bảo mật của các ứng dụng trên thiết bị.

* + Xem xét mã nguồn (Source code review)
  + Kiểm tra tự động (Automated testing)
  + Quét lỗ hổng bảo mật (Vulnerability scanning)
  + Các ứng dụng có khả năng gây hại (Potentially Harmful Applications)
  + Quyền và cài đặt ứng dụng (App installation and permissions)
  + Đăng ký ứng dụng (App signing)
  + Cô lập ứng dụng và tiến trình (Isolating apps and processes)

# An ninh mạng

Xem xét và cải thiện tính bảo mật của truyền thông mạng từ thiết bị.

* + Bảo mật ổ cắm tai nghe
  + Tắt ADB (Android debug bridge)

1. **Bảo mật phần cứng** - Xem xét các lựa chọn phần cứng để cải thiện bảo mật thiết bị.
   * Bộ nhớ thiết bị
   * StrongBox Keymaster
2. **Bảo mật quyền riêng tư** - Cho phép người dùng kiểm soát việc xử lý dữ liệu của họ.
   * Ghi dữ liệu
   * Bộ sưu tầm số liệu
   * Phần mềm gián điệp

# Dịch vụ bảo mật của Google

Google cung cấp một tập hợp các dịch vụ dựa trên đám mây có sẵn cho các thiết bị Android tương thích với dịch vụ di động của Google. Mặc dù các dịch vụ này không phải là một phần của Dự án nguồn mở Android (Android Open Source Project - AOSP), nhưng chúng được hỗ trợ trên nhiều thiết bị Android.

Các dịch vụ bảo mật chính của Google là:

1. **Google Play:** Google Play là một tập hợp các dịch vụ cho phép người dùng khám phá, cài đặt và mua ứng dụng từ điện thoại Android của họ hoặc web. Google Play giúp các nhà phát triển dễ dàng tiếp cận người dùng Android và khách hàng tiềm năng. Google Play cũng cung cấp xem xét cộng đồng, ứng dụng xác minh giấy phép , quét an ninh ứng dụng, và các dịch vụ bảo mật khác.
2. **Các bản cập nhật Android:** Các dịch vụ cập nhật Android mang lại khả năng mới và cập nhật bảo mật cho thiết bị Android được lựa chọn, bao gồm bản cập nhật thông qua web hoặc qua vô tuyến (OTA).
3. **Dịch vụ ứng dụng:** Frameworks cho phép các ứng dụng Android với khả năng sử dụng điện toán đám mây như (sao lưu) dữ liệu ứng dụng, các thiết lập và Thông báo từ đám mây tới thiết bị (cloud-to-device messaging - C2DM) để thông báo đẩy (messaging push).
4. **Xác minh ứng dụng:** Cảnh báo hoặc tự động chặn việc cài đặt các ứng dụng độc hại và các ứng dụng liên tục quét trên thiết bị, cảnh báo hoặc loại bỏ các ứng dụng độc hại .
5. **SafetyNET:** Hệ thống phát hiện xâm nhập bảo vệ quyền riêng tư để hỗ trợ Google theo dõi, giảm thiểu các mối đe dọa bảo mật đã biết và xác định các mối đe dọa bảo mật mới.
6. **SafetyNET Xác nhận (SafetyNET Attestation):** API (Application Programming Interface - Phương thức trung gian kết nối các ứng dụng và thư viện khác nhau) của bên thứ ba để xác định xem thiết bị có tương thích với CTS (Common Type System - Loại hệ thống chung ) hay không. SafetyNet Attestation cũng có thể xác định ứng dụng Android đang giao tiếp với máy chủ ứng dụng.
7. **Android Device Manager:** Một ứng dụng web và ứng dụng Android để xác định vị trí thiết bị bị mất hoặc bị đánh cắp.

# TỔNG KẾT

Hệ điều hành Android trở thành nền tảng điện thoại di dộng điện thoại thông minh phổ biến nhất thế giới với nhiều tính năng, một hệ điều hành không nặng nề, có khả năng tinh chỉnh và giá rẻ chạy trên các thiết bị công nghệ cao.

Về vấn đề an ninh, an toàn so với các hệ điều hành khác hiện nay như IOS, Balackberry OS, Symbian OS thì Android là hệ điều hành có độ an toàn, an ninh và bảo mật kém nhất, nhưng nhờ vào việc phát triển ứng dụng bảo mật ngày càng mạnh đã phần nào giảm đi sự nguy hiểm cho người dùng.