www.crysys.hu

Mobile Security – Android With a focus on the system

Gergő Ládi
Laboratory of Cryptography and System Security
Department of Networked Systems and Services
Gergo.Ladi@CrySyS.hu

Previously, on IT Security (BSc studies)

- System & Application Security
  - Android Platform Architecture & Security
  - The Android Permission Model
  - The application installation process
  - How system updates work
- Device Security
  - Screen Lock, Trust Agents
  - Default USB behaviour

- These topics will not be on the exam, but you are generally expected to have an understanding of these in order to understand today's topics

Previously, on Software Security (MSc studies)

- Detection of tampering and hostile environments
  - Emulators, emulator detection
  - Rooting, root detection
  - Installer detection, signature checks
- Protecting Android applications
  - Reverse engineering and obfuscation
  - The use of cryptography
  - Secure data storage

- These topics will not be on the exam, but you are generally expected to have an understanding of these in order to understand today's topics

SYSTEM & DEVICE SECURITY (CONTINUED)

Application Signing (reminder)

- All apps must be digitally signed in order to be installed
- The signing certificate does **not** need to be issued by a trusted CA
  - That is, the certificate may be self-signed
  - This also means that we can't find out much (if anything) about the developer (based on the certificate)
- However, the choice of certificates is important
  - Updates to apps may only be installed if the update is signed by the same key as the previous version
  - Apps signed by the same key may request to be put in the same sandbox
  - Google requires that any app published to the Play Store be signed with a certificate that is valid at least until 22 October 2033

Application Signing

- There are three (four) different signature schemes
- v1 scheme – a standard JAR signing method
  - A hash is computed for each file separately, and the list of hashes is signed
  - Verification is slow and more resource intensive as the entire package must be decompressed, files must be checked one-by-one, and unsigned files need to be skipped over
  - Some parts of the application can not be protected (e.g. ZIP metadata)

- v2 scheme (APK Signature Scheme)
  - The entire APK is treated as one data blob
  - Faster and less resource intensive to validate
  - Protects against more kinds of tampering
  - Supported in Android 7 or better
  - Required from Android 11

Application Signing

- v3 scheme
  - New in Android 9
  - Very similar to v2
  - Adds support for the rotation of signing keys

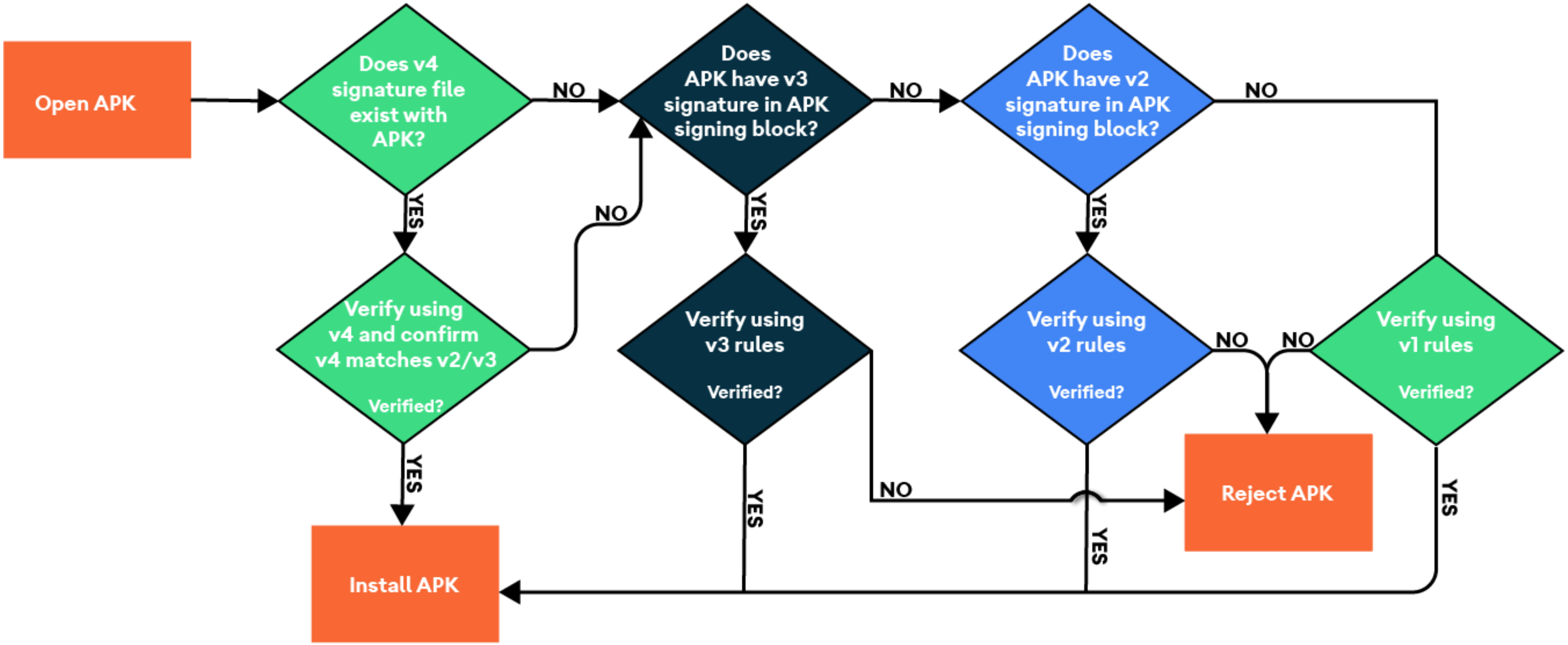
- v4 scheme
  - New in Android 11
  - Stored in <apk>.idsig instead of the .apk file
  - Requires a complementary v2 or v3 signature
  - Supports incremental downloads (streaming)
    - To be used with big (2 GB+) applications, e.g. games

Application Signing

- The same application may contain multiple signatures of multiple versions
  - I.e. an app may have a v1, a v2, a v3, and a v4 signature at the same time
- Devices verify the highest version of signature that they understand
  - If verification fails, the app is rejected (lower versions are not tried)
  - Except for v4; verification continues even if a v4 check fails

- In theory, there may be multiple signatures of the same version as well (with different certificates), however, Google does not allow such applications in the Play Store

Application Signing


Open APK
Does v4 signature file exist with APK?
NO
YES
Verify using v4 and confirm v4 matches v2/v3
Verified?
NO
YES
Install APK
Does APK have v3 signature in APK signing block?
NO
YES
Verify using v3 rules
Verified?
YES
NO
Does APK have v2 signature in APK signing block?
NO
YES
Verify using v2 rules
Verified?
NO
YES
Reject APK
Verify using v1 rules
Verified?
NO
YES

Source: Android Developer Guide

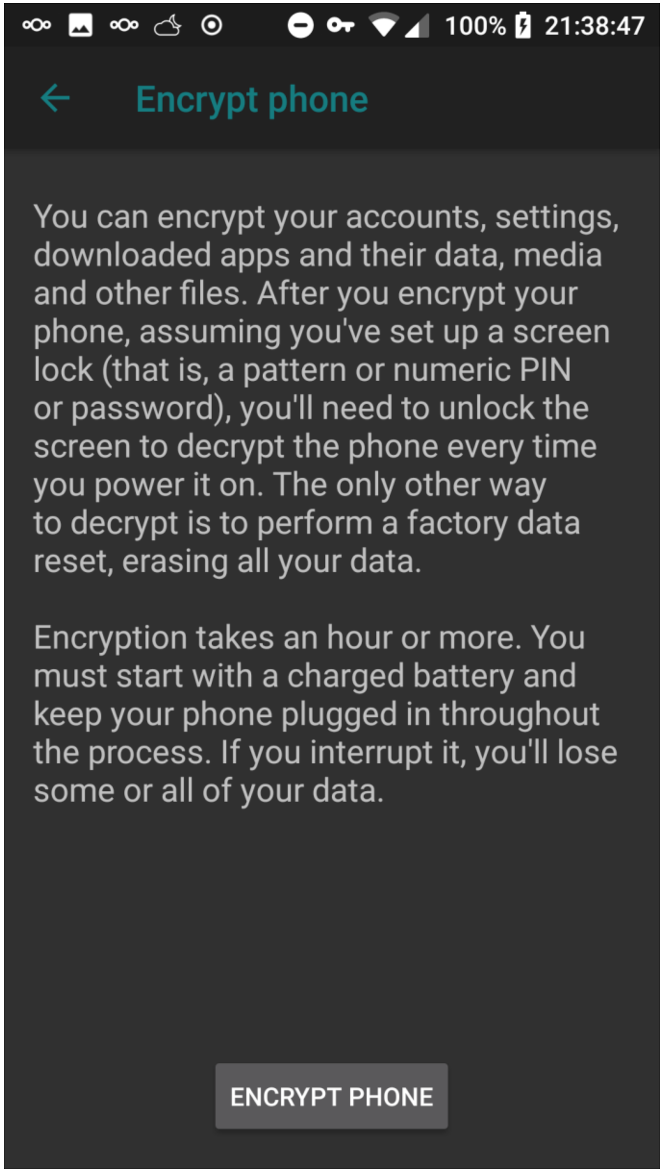
Device Encryption

- Supported since Android 2.3
  - Automatically enabled on some phones starting from Android 5.0
- Superseded by file-based encryption in Android 10

- The contents of the phone may be encrypted so that a password is needed to boot the phone (or read any file stored on it)
  - Based on dm-crypt, a Linux full-disk encryption module
  - Uses AES in CBC mode with a 128-bit key which is derived from the password using PBKDFv2
  - Starting from Android 5.1, PINs and patterns may be used instead of a password, but this is less secure
    - The fingerprint reader cannot be used at this point as this would need access to the fingerprint database, which is also stored encrypted on the phone

Device Encryption

- If the device is stolen, it is reasonably impossible for thieves to access the data on it
- Encryption is a one-way process, it can only be turned off by a factory reset
  - The SD card can be decrypted later, though
- The encryption adds some overhead (CPU, battery consumption)
- Your mileage may vary
  - Feature set and inner workings changed a lot since 2.3
  - Supported in different ways by different ROMs
  - Not available on Android 10 or newer devices



You can encrypt your accounts, settings, downloaded apps and their data, media and other files. After you encrypt your phone, assuming you've set up a screen lock (that is, a pattern or numeric PIN or password), you'll need to unlock the screen to decrypt the phone every time you power it on. The only other way to decrypt is to perform a factory data reset, erasing all your data.

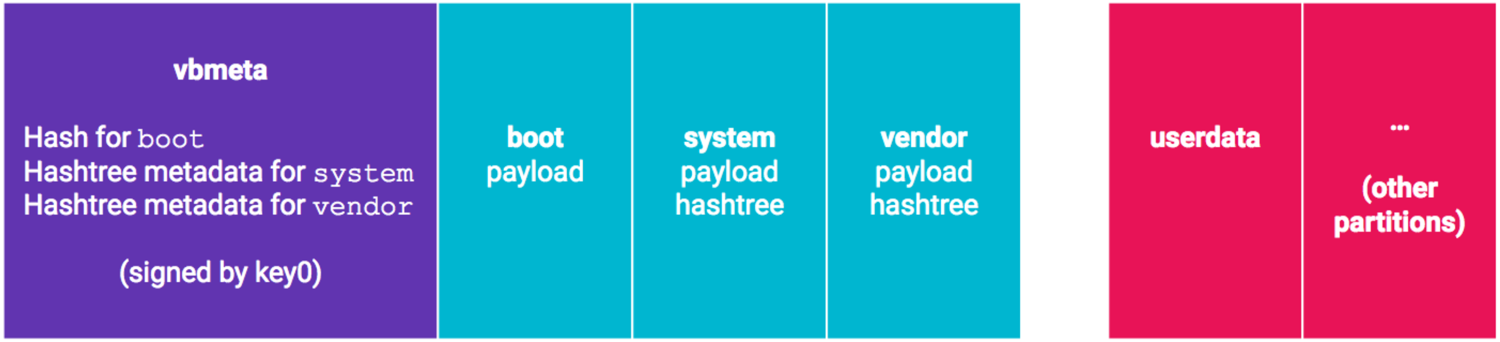
Encryption takes an hour or more. You must start with a charged battery and keep your phone plugged in throughout the process. If you interrupt it, you'll lose some or all of your data.

File-Based Encryption

- Supported since Android 7, mandatory starting from Android 10
- Instead of encrypting the entire storage like with Device Encryption, individual files are encrypted (with possibly different keys)
  - Device Encrypted storage – encrypted with a device-specific key, available after boot
  - Credential Encrypted storage – encrypted with a user's key, available after the user has unlocked the phone
- The system can boot without having to enter a master key
  - Some functionality (such as Alarms) now work after a reboot
- Uses AES or Adiantum (Android 10)

Verified Boot

- Provides a means of verifying whether anything from the boot loader to the operating system was tampered with
  - Similar to Secure Boot in today's UEFI systems
- Relies on hashes and digital signatures
- Uses a hardware root of trust
  - The root key is generally supplied by the vendor
  - Some vendors allow a user-specified key to be installed as well (for customization)



vbmeta

Hash for `boot`
Hashtree metadata for `system`
Hashtree metadata for `vendor`

(signed by key0)

boot payload

system payload hashtree

vendor payload hashtree

userdata

...

(other partitions)

Verified Boot

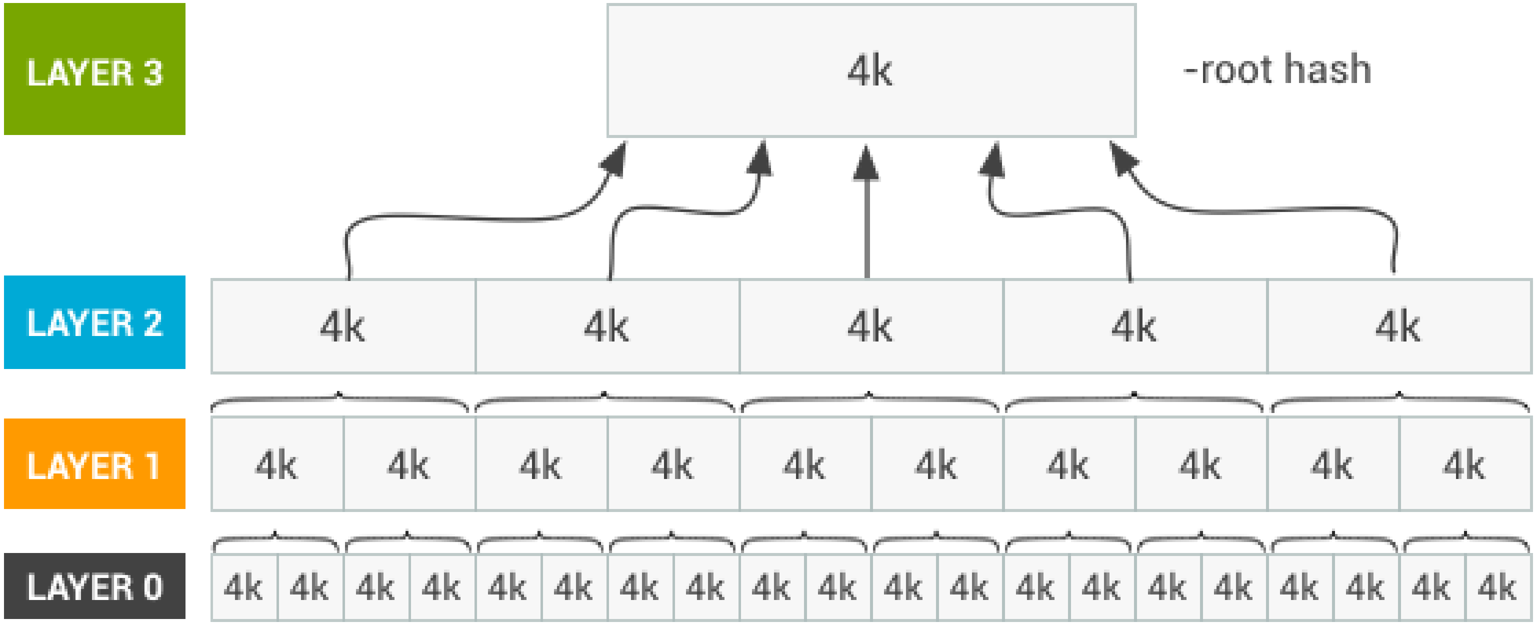
- Makes it possible to detect changes to critical parts of the system
  - By malicious software (e.g. rootkits)
  - From "natural" data corruption

- Rollback protection
  - An attacker cannot downgrade to older versions of the system

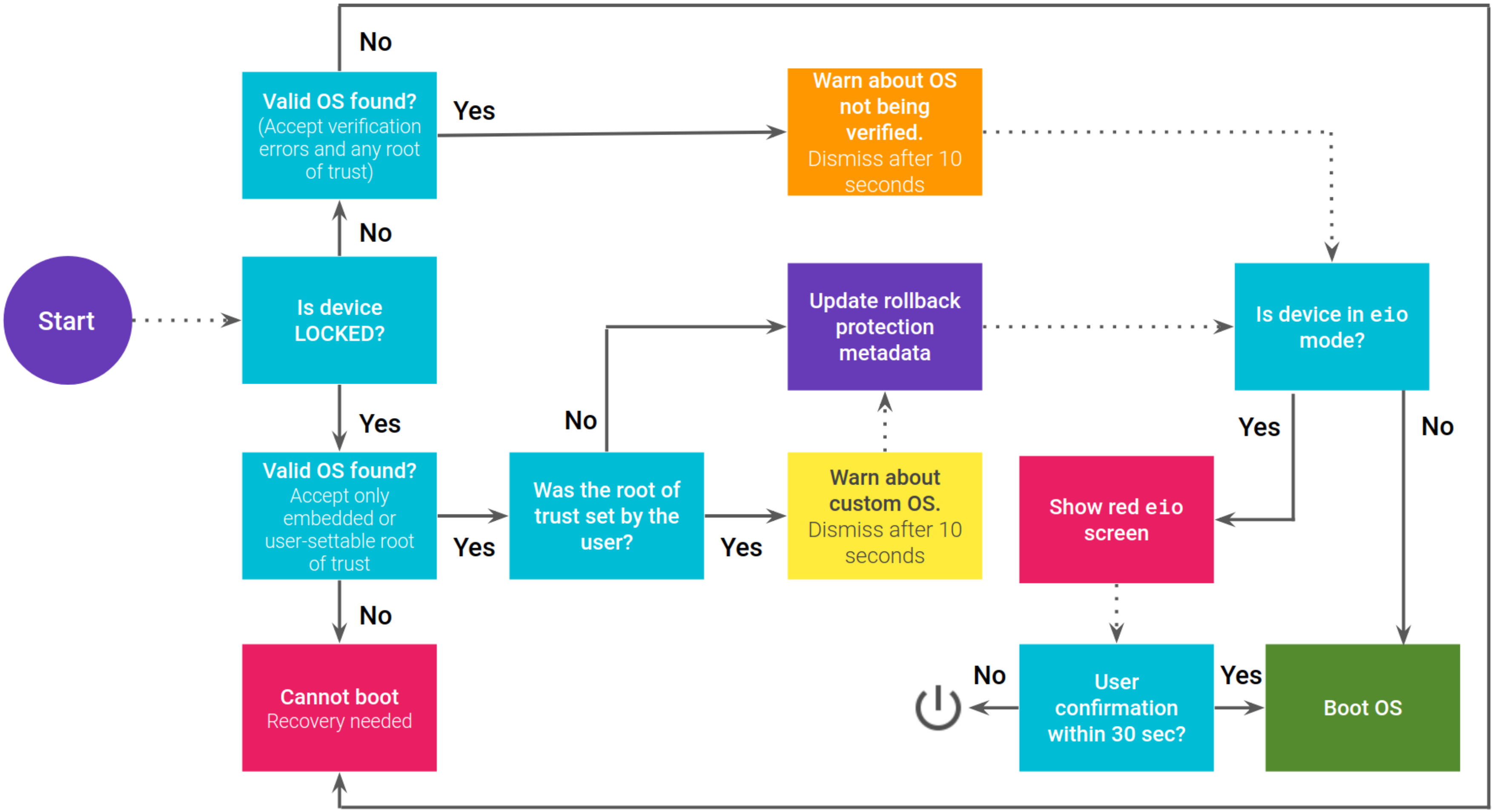
- Introduced in Android 4.4 (KitKat) – Verified Boot 1
- Android 8.0+ – Android Verified Boot (Verified Boot 2)
  - Now compatible with Project Treble

Verified Boot

- Relies on dm-verity, a standard Linux kernel feature
  - Large partitions are divided into blocks
  - Blocks are hashed individually
  - Hashes are then combined into a tree
  - It is easy to check any part of the tree while only trusting the root hash

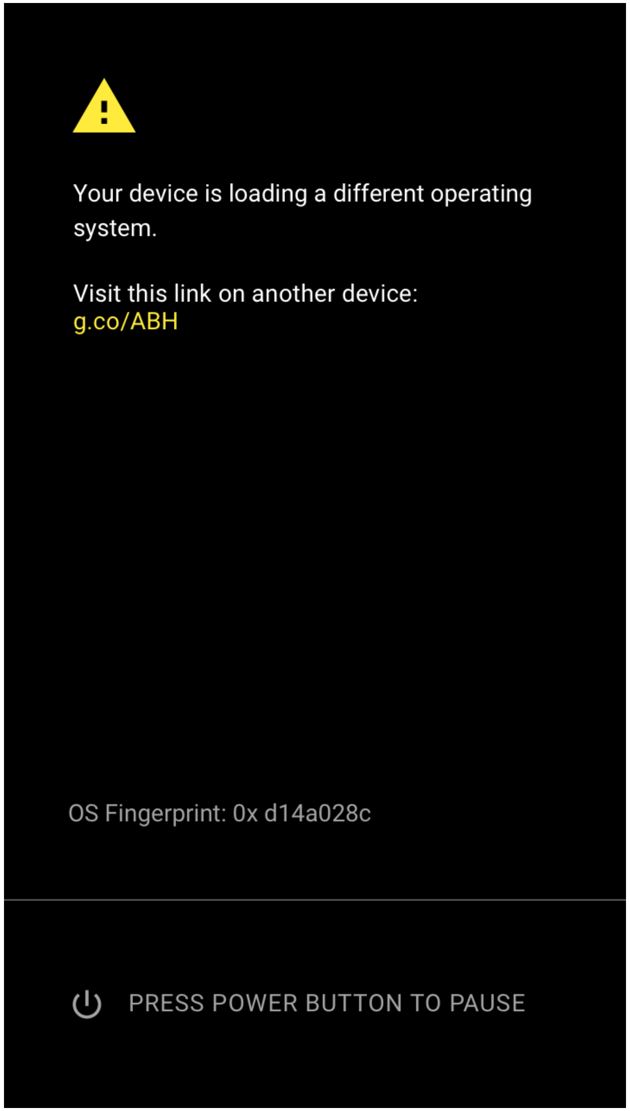

LAYER 3
4k
-root hash
LAYER 2
4k 4k 4k 4k 4k
LAYER 1
4k 4k 4k 4k 4k 4k 4k 4k 4k 4k
LAYER 0
4k 4k 4k 4k 4k 4k 4k 4k 4k 4k 4k 4k 4k 4k 4k 4k 4k 4k 4k 4k

The Android Boot Process


Start
Is device LOCKED?
No
Valid OS found? (Accept verification errors and any root of trust)
No
Yes
Warn about OS not being verified. Dismiss after 10 seconds
Yes
Valid OS found? Accept only embedded or user-settable root of trust
Yes
Was the root of trust set by the user?
No
Yes
Warn about custom OS. Dismiss after 10 seconds
Update rollback protection metadata
Is device in eio mode?
Yes
No
Show red eio screen
No
Cannot boot Recovery needed
User confirmation within 30 sec?
No
Yes
Boot OS

Source: AOSP

The Android Boot Process – Example Screens

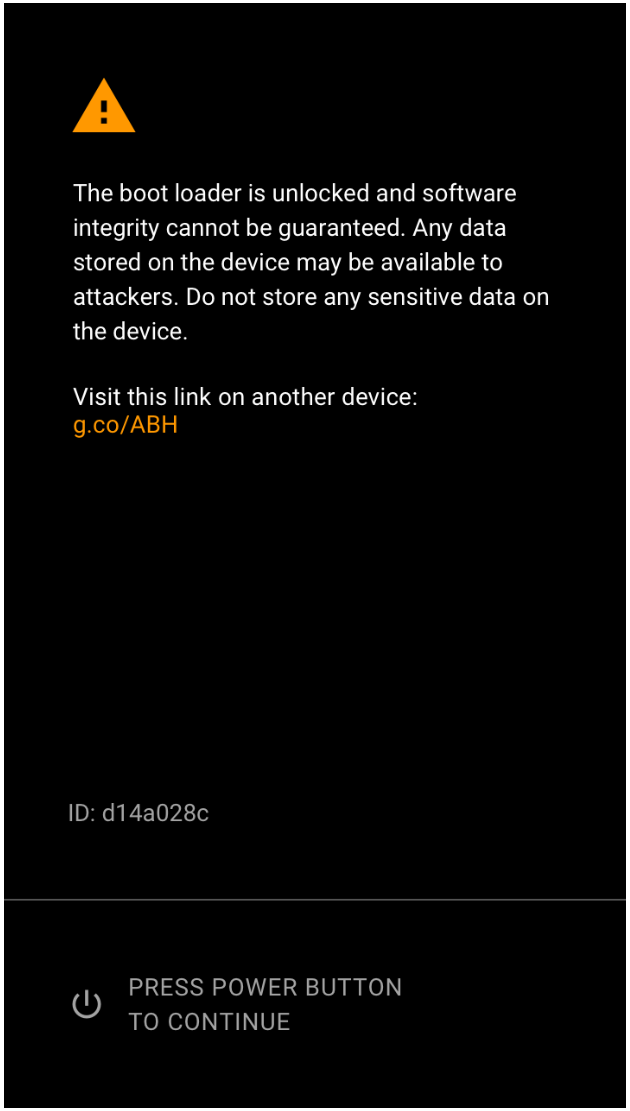


Your device is loading a different operating system.

Visit this link on another device:
g.co/ABH

OS Fingerprint: 0x d14a028c

⏻ PRESS POWER BUTTON TO PAUSE

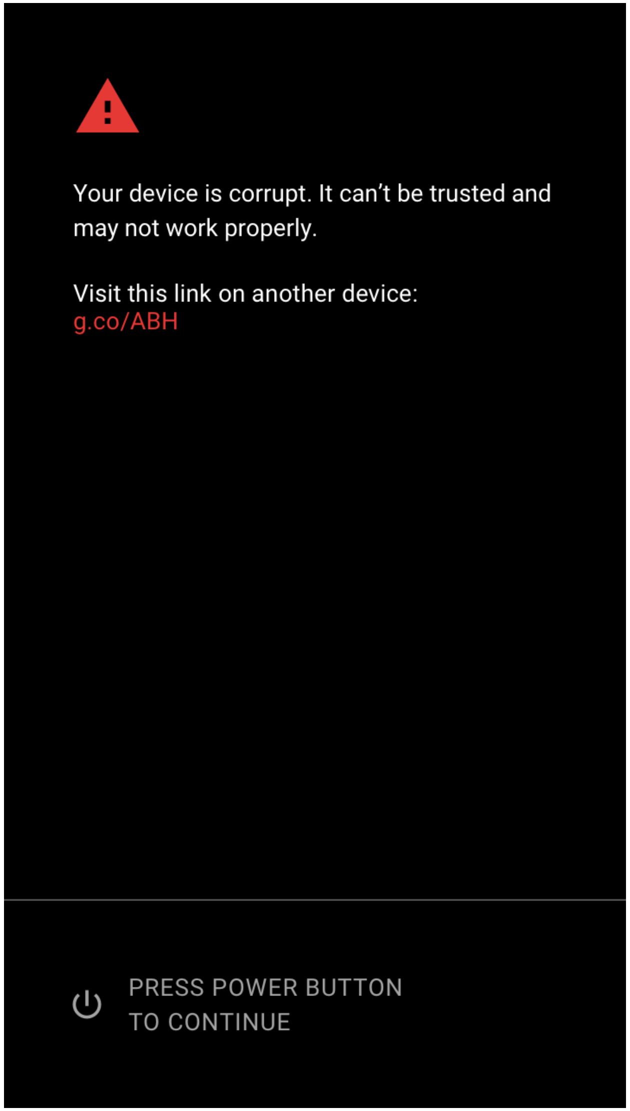


The boot loader is unlocked and software integrity cannot be guaranteed. Any data stored on the device may be available to attackers. Do not store any sensitive data on the device.

Visit this link on another device:
g.co/ABH

ID: d14a028c

⏻ PRESS POWER BUTTON
TO CONTINUE

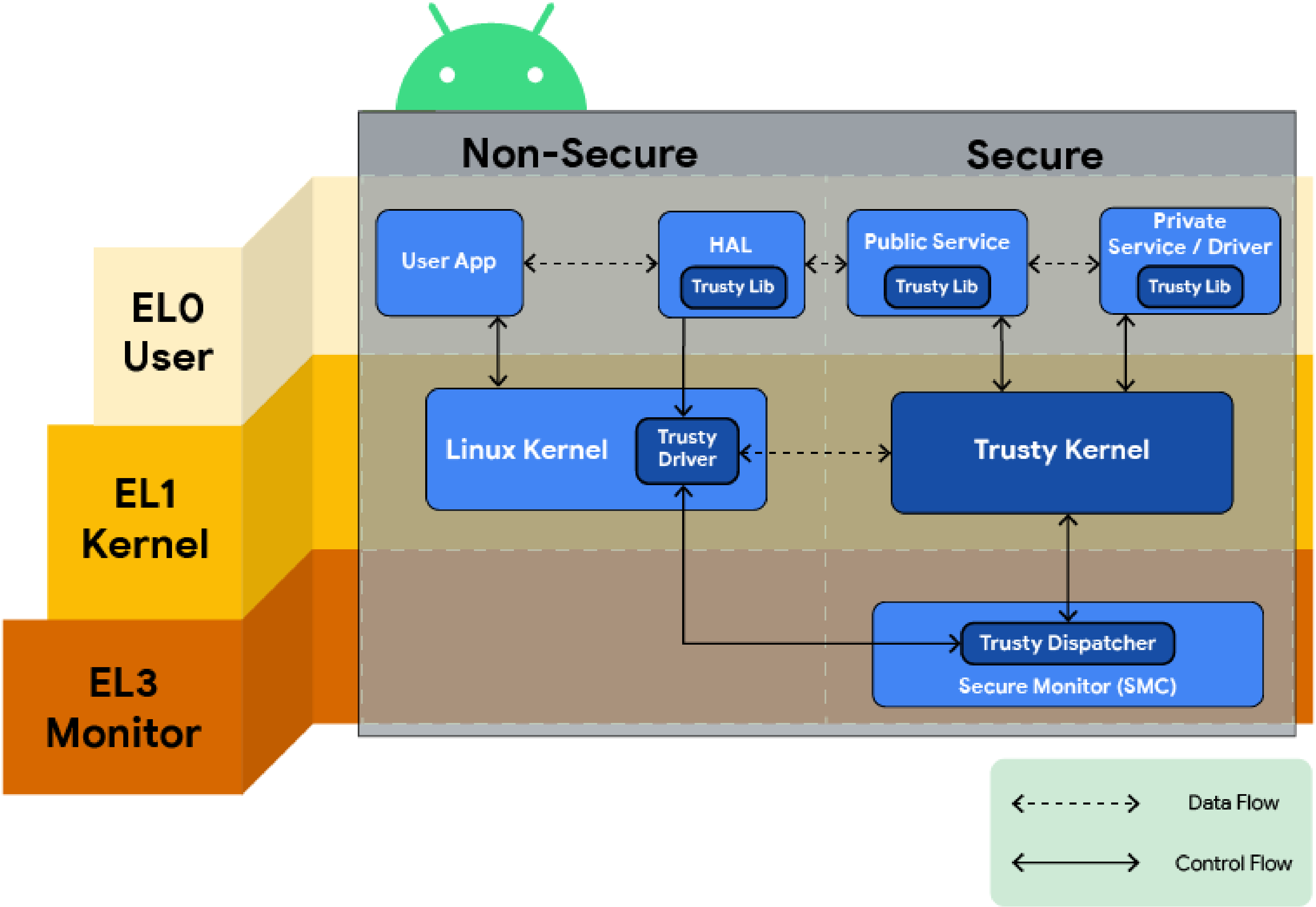


Your device is corrupt. It can’t be trusted and may not work properly.

Visit this link on another device:
g.co/ABH

⏻ PRESS POWER BUTTON
TO CONTINUE

Trusty


Non-Secure
Secure
EL0
User
EL1
Kernel
EL3
Monitor
User App
HAL
Trusty Lib
Public Service
Trusty Lib
Private
Service / Driver
Trusty Lib
Linux Kernel
Trusty
Driver
Trusty Kernel
Trusty Dispatcher
Secure Monitor (SMC)
Data Flow
Control Flow

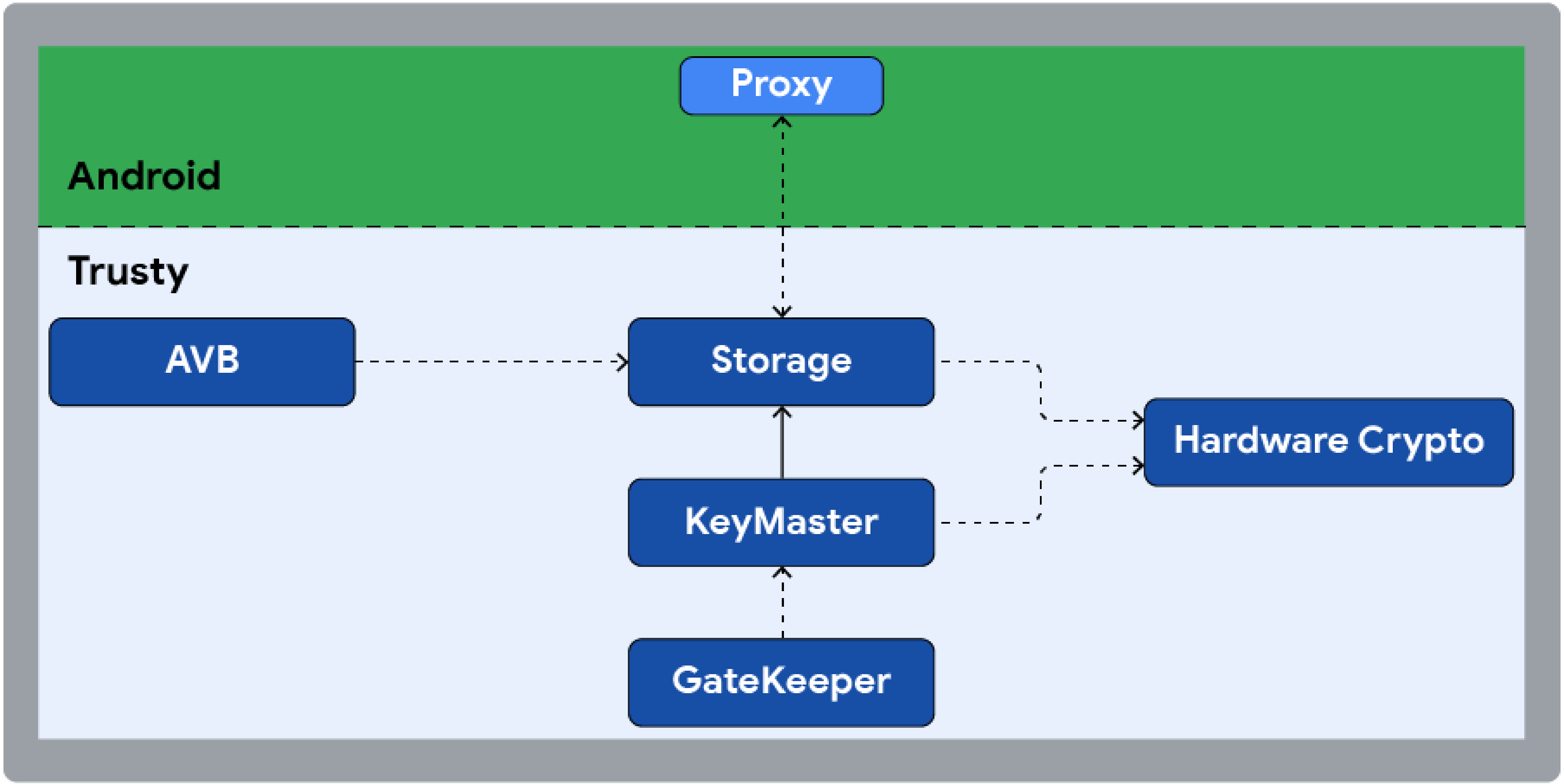
Trusty

- A Trusted Execution Environment (TEE)
- Free and open source, available by default for vendors
  - But vendors may choose to implement their own TEEs

- Runs alongside Android as a second operating system
  - Isolated using ARM TrustZone or Intel virtualization tech.

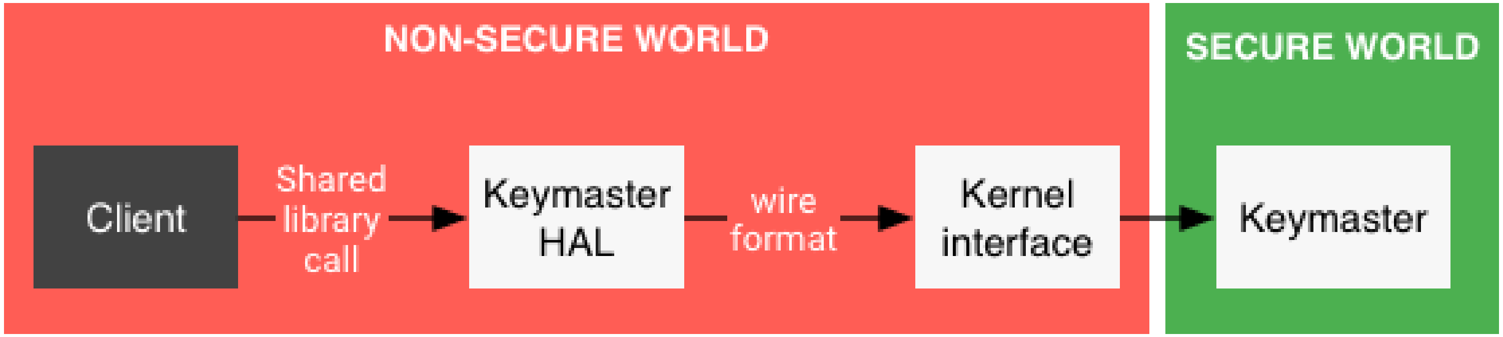
- Plays a role in several security-related features
- Runs Trusted Apps (TAs)

Trusty


Proxy
Android
Trusty
AVB
Storage
Hardware Crypto
KeyMaster
GateKeeper

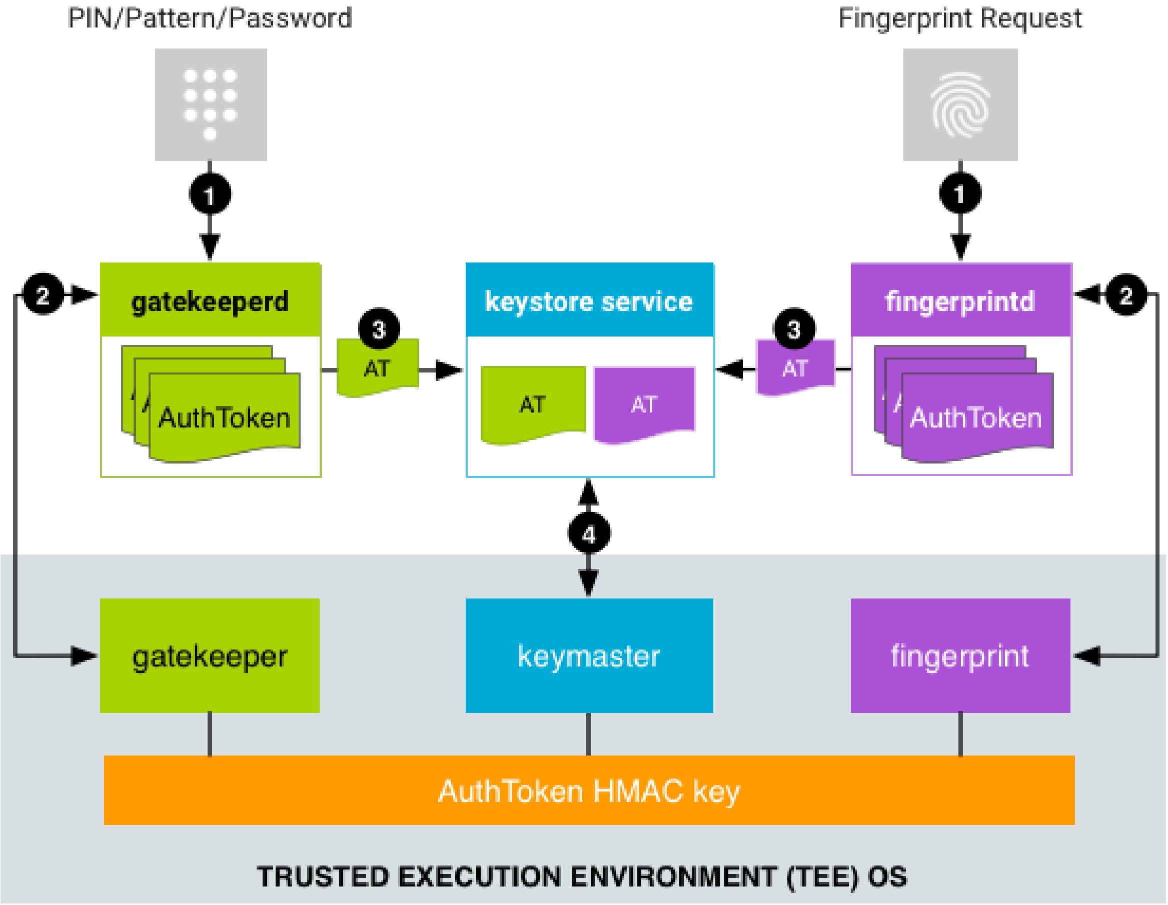
KeyMaster

- Provides cryptography-related services
  - Key generation, import/export
  - Encryption, decryption
  - Digital signature generation and verification
  - Message authentication
- Makes use of hardware-backed features as much as possible



GateKeeper

- Responsible for authentication-related functions

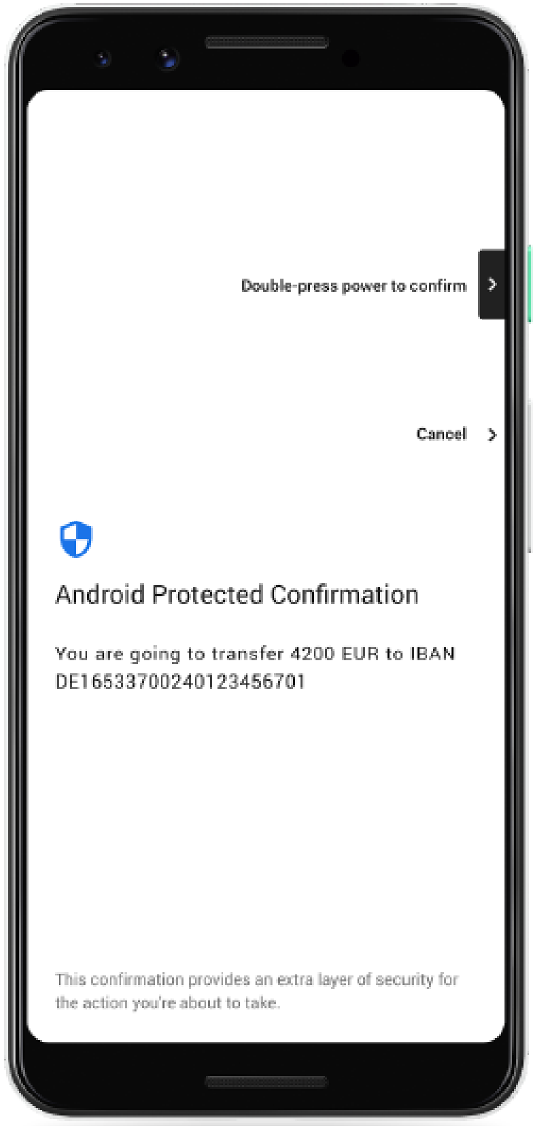


Biometrics

- Built-in support for fingerprint readers and face identification devices, but the API allows for custom implementations
- Classification of authenticators, based on architectural and biometric security performance
  - Class 3 – Strong
    - 0-7% SAR, 1:50000 FAR, max. 10% FRR
    - 72 hours before fallback
  - Class 2 – Weak
    - 7-20% SAR, 1:50000 FAR, max. 10% FRR
    - 24 hours total OR 4-hour idle timeout OR 3 incorrect attempts before fallback
  - Class 1 – Convenience
    - 20+% SAR, 1:50000 FAR, max. 10% FRR
    - 24 hours total OR 4-hour idle timeout OR 3 incorrect attempts before fallback
    - May be removed in the future

Protected Confirmation

- Apps may invoke a trusted UI when asking for confirmation for high-risk or otherwise critical actions (e.g. bank transactions)
- Apps running on the phone cannot see or interact with this prompt in any way
  - Not even if the OS is compromised
- Requires Android 9 or higher



Android Protected Confirmation

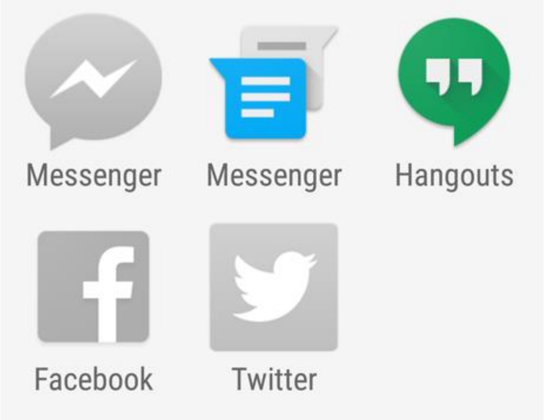
You are going to transfer 4200 EUR to IBAN DE16533700240123456701

This confirmation provides an extra layer of security for the action you're about to take.

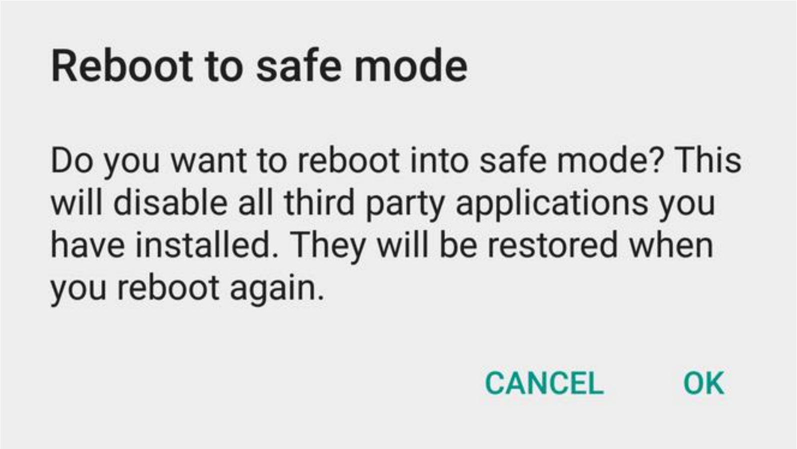
MISCELLANEOUS

Safe Mode

- Android can be rebooted into a Safe Mode
  - The exact key combination varies, so check the manual of your ROM for details
  - The text 'Safe Mode' is usually displayed on the screen
- In the Safe Mode, only core applications are available
  - No third-party apps can be started in this mode (they are greyed out)
  - Apps can still be uninstalled
  - If you're having issues, you can find out if they are being caused by apps or not
- A reboot takes you back to 'normal' mode



Source: https://www.cultofandroid.com

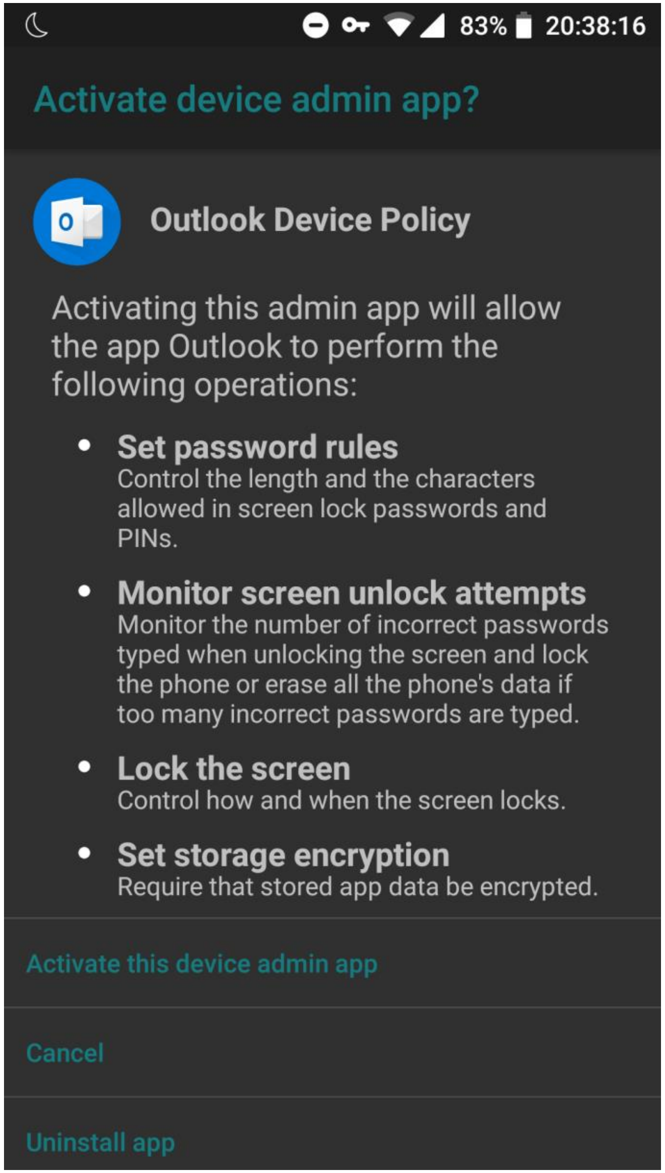


Reboot to safe mode

Do you want to reboot into safe mode? This will disable all third party applications you have installed. They will be restored when you reboot again.

Device Administrators

- Apps with Device Administrator permissions have the ability to
  - Set rules regarding how the lock screen works
  - Require strong passwords
  - Require that storage be encrypted
  - Disable the camera
  - Wipe the device after X failed login attempts
  - Remotely wipe the device
- Typically used in enterprise environments on the employees' phones as a data loss prevention countermeasure



Activate device admin app?

Outlook Device Policy

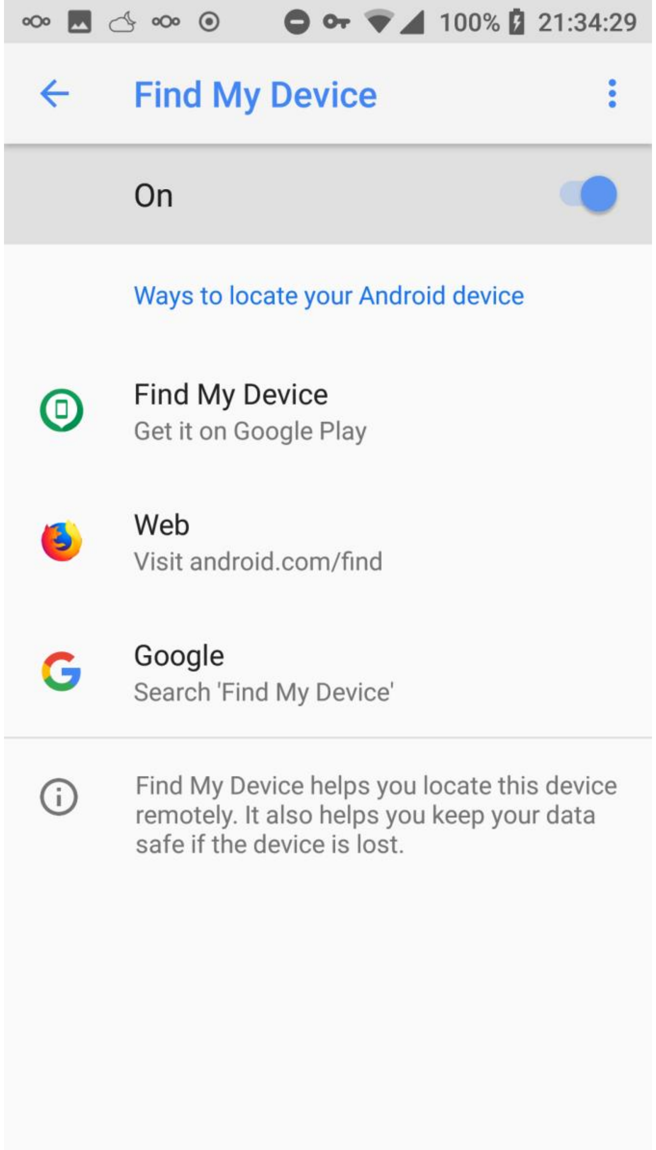
Activating this admin app will allow the app Outlook to perform the following operations:

- **Set password rules**
  Control the length and the characters allowed in screen lock passwords and PINs.
- **Monitor screen unlock attempts**
  Monitor the number of incorrect passwords typed when unlocking the screen and lock the phone or erase all the phone's data if too many incorrect passwords are typed.
- **Lock the screen**
  Control how and when the screen locks.
- **Set storage encryption**
  Require that stored app data be encrypted.

Find My Device

- Lets you
  - See where your phone was seen last
  - Ring your phone
    - Full volume beeping, even if set to silent
  - Lock your phone
    - Set a pattern/PIN/password if one is not set
    - Add a lock screen message to help someone return your device
  - Remotely wipe the device

- For it to work, the phone
  - Must be turned on with the feature enabled
  - Must be linked to a Google Account
  - Needs internet and GPS access



100% 21:34:29

Find My Device

On

Ways to locate your Android device

Find My Device
Get it on Google Play

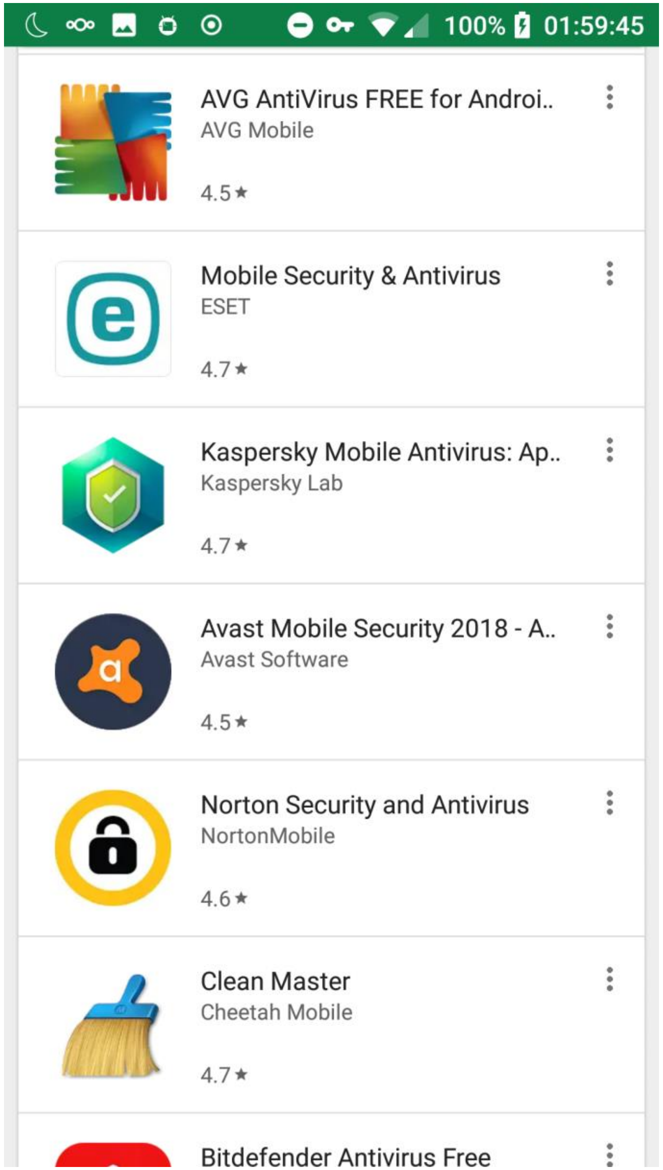
Web
Visit android.com/find

Google
Search 'Find My Device'

Find My Device helps you locate this device remotely. It also helps you keep your data safe if the device is lost.

Food For Thought: Antivirus For Android?

- A search in the Play Store for 'Antivirus' yields several tens of results
  - Results include some of the big names
- But can these actually detect malware?
  - Remember, apps have no access to each other's data... unless the phone is rooted and root permissions are given to the AV...
- Key features typically are
  - Call blocking (in/out)
  - "Secure" VPN
  - Phishing protection
  - Device tracking & remote wipe
  - Password-protected access to selected apps



100% 01:59:45

AVG AntiVirus FREE for Androi..
AVG Mobile
4.5★

Mobile Security & Antivirus
ESET
4.7★

Kaspersky Mobile Antivirus: Ap..
Kaspersky Lab
4.7★

Avast Mobile Security 2018 - A..
Avast Software
4.5★

Norton Security and Antivirus
NortonMobile
4.6★

Clean Master
Cheetah Mobile
4.7★

Bitdefender Antivirus Free

THANK YOU FOR YOUR ATTENTION!

Control Questions

- Why must Android applications be signed?
- How can Android applications be signed?
  What schemes are used? Explain and compare them.
- What is Device Encryption? How does it work?
- What is File-Based Encryption? How does it work?
- Compare Device Encryption and File-Based Encryption.
- Explain the concept and purpose of Verified Boot. How is it implemented in Android systems?
- Explain the Android boot process.

Control Questions

- What is Trusty? How does it relate to Android? What services does it provide?
- What support does Android provide for biometric authentication?
- What is Protected Confirmation? What is its purpose?

- What is Safe Mode (in Android)? What is its purpose?
- Explain the concept of Device Administrators (in Android).