



# Von schlaunen Telefonen und kleinen Robotern

Dr. Christoph Zimmermann

27.6.2023

# cat /etc/motd

- Historie
- Architektur
- Sicherheit
- Basics
- Interessantes
- Richtig Interessantes
- Q & A

# Historie

- 2003: Gründung (A. Rubin, R. Miner, N. Sears, C. White)
- 2005: Akquisition durch Google
- 2008: HTC Dream
- 2013: A. Rubin => S. Pichai
- 2019: Android Q(10) != Nachtsch
- 2019: Java => Koitlin
- 2023: Container, k8s & Android :-)

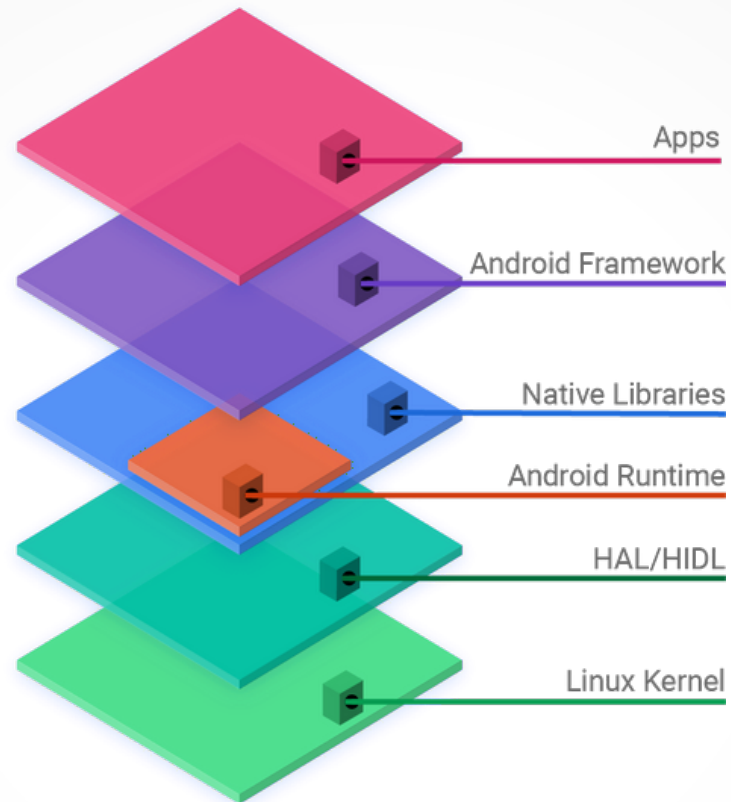
# Historie (ff.)

- 1.0 (2008): OS + initiale Gapps
- 2.0 (2009): Exchange-Unterstützung, Auto-Rotate
- 3.0 (2011): Multicore CPUs/FUSE, User-Data Verschlüsselung
- 4.0 (2011): Foto-Editor, WebP, SELinux Default (4.3)
- 5.0 (2014): Dalvik=>ART, 64 bit CPUs, Material Design, 4k
- 6.0 (2015): USB-C, Unicode
- 7.0 (2016): JIT-Compiler+Profiling
- 8.0 (2017): Play-Protect, Treble, herunterladbare Fonts

# Historie (ff.)

- 9.0 (2018): Android Dashboard, Gesten-basiertes UI
- 10.0 (2019): WPA3, biometrische Authentifizierung, TLS 1.3
- 11.0 (2020): Enterprise Profile, einmalige Berechtigungen
- 12.0 (2021): präzise / ungefähre Position, Privacy-Dashbord
- 13.0 (2022): ART-Optimierung (GC, JIT), Bluetooth LE Audio
- 14.0 (2023): Superskalierbare Fonts (200%), Cloned Apps

# Architektur



# Sicherheit (Übersicht)

- SafetyNet / Play Integrity API
- Apps:
  - Eigene User ID pro App => Kernel-Level Sandbox
  - Play Store: Ausschließlich signierte Apps
  - Vetting:
    - Vor Play Store Deployment
    - Geräte-basiert: Play Protect
- SELinux (bzw. Enklaven wie Samsung Knox)

# Basics

- Partitionen (Übersicht):
  - boot / init\_boot: Kernel, initrd
  - system: AOSP
  - odm: SoC-Blobs, etc.
  - recovery: In boot-Partition bei A/B-Devices!
  - userdata: Apps + Daten
  - vendor: Binaries die nicht zu AOSP gehören
  - Android 11: Single-System Image



# Basics (ff.)

- Android SDK:
  - Fastboot: Interaktion mit Bootloader
  - Android Debugging Bridge (ADB): Interaktion mit AOSP+Recovery
- Rooting
- OTA:
  - Slots (aka Seamless Updates, A/B):
  - OTA => Transaktionen
  - Zwei Partitionen-Sätze

# Interessantes

- `github.com/Genymobile/scrcpy`
- `fastboot boot <image_name>`
- OTA: `adb sideload via recovery (zip != img)`
- recovery: adb-Unterstützung
- Boot Loop:
  1. `adb logcat`
  2. Reset via recovery (`wipe != format!`)

# Richtig Interessantes

<https://termux.dev>

# Links

- Android Dev Docs: <https://developer.android.com>
- SafetyNet:  
<https://developer.android.com/training/safetynet>
- Play Integrity API:  
<https://developer.android.com/google/play/integrity/overview>
- SafetyNet-Umgehung: <https://www.xda-developers.com/how-to-pass-safetynet-android>
- k8s & Android:  
<https://cfp.tuebix.org/tuebix-2023/talk/DYUZFB>

# Q & A

# Danke!

© 2023 CC-BY

Dr. Christoph Zimmermann

monochrome at <ignore>space</ignore>gmail<dot></dot>com