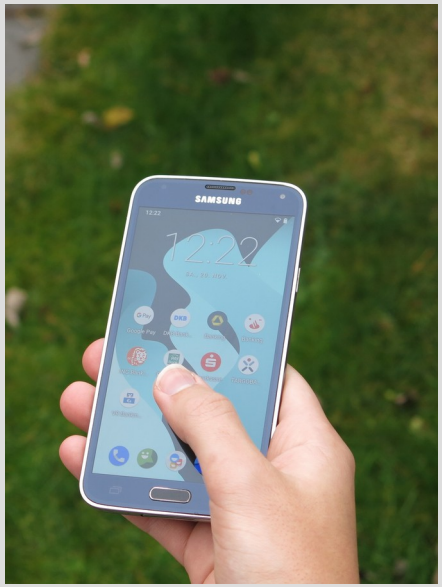
Freies Handy-Betriebssystem und Mobile Banking – geht das?

Markus Oppmann
KNF Kongress, 2021

https://www.franken.de/veranstaltungen/kongress/knf-kongress-2021

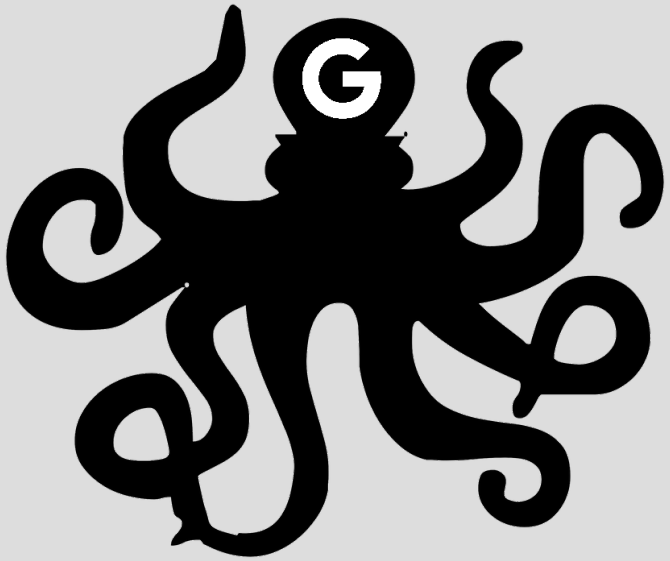
Übersicht

- Was ist ein „Freies Betriebssystem“ und wieso sollte ich das wollen?
- Wieso funktionieren manche Apps nicht mehr?
- Gibt es eine Lösung? Wenn ja, wie funktioniert das?
- Fazit



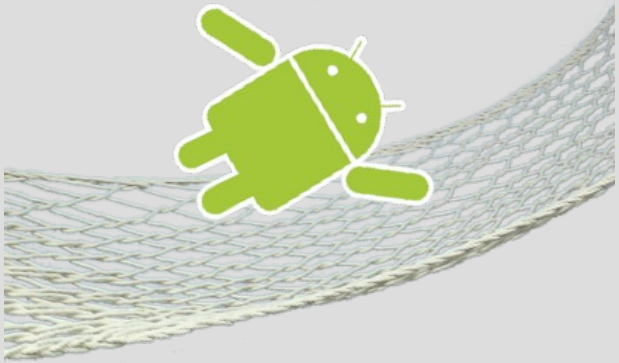
„Freies Betriebssystem“

- Betriebssystem unabhängig von „Datenkrake Google“
- Auch: „Custom ROM“
- Beispiel: LINEAGE
- Vorteile:
  - Längerer Support alter Geräte
  - Mehr Kontrolle



Wieso gehen manche Apps nicht?

- Apps nutzen Googles SafetyNet-API
- 2 Prüfungen:
  - Basis-Integrität
  - CTS-Kompabilität
- Custom ROM verändert System und lässt CTS-Kompabilitätsprüfung fehlschlagen.



Gibt es eine Lösung?

- Ja:  Magisk

  The Magic Mask for Android

- Ändert das System, ohne das System zu ändern

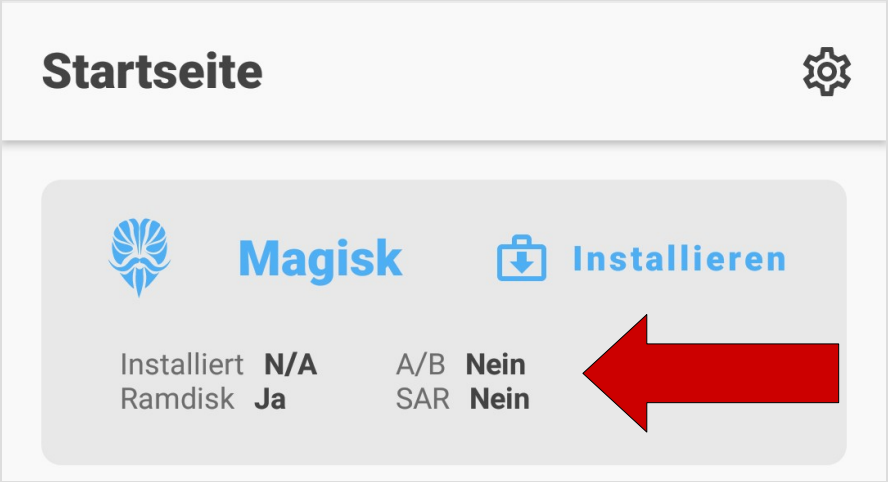
- Weiterführende Informationen

Root – Nachteil oder Vorteil?

- Vorteile:
  - Volle Hoheit über Gerät
- Nachteile:
  - Fehler können gravierende Folgen haben
  - Bösartige Apps könnten erheblichen Schaden anrichten

Wie funktioniert das im Detail?

- Schritt 1: Magisk-App installieren: https://github.com/topjohnwu/Magisk/releases/latest
- Parameter „Ramdisk“, „A/B“ und „SAR“ merken
  - Ramdisk Ja: Boot-Partition. Nein: Recovery-Partition



Wie funktioniert das im Detail?

- Schritt 2: Bootloader entsperren falls nötig (Internetrecherche)

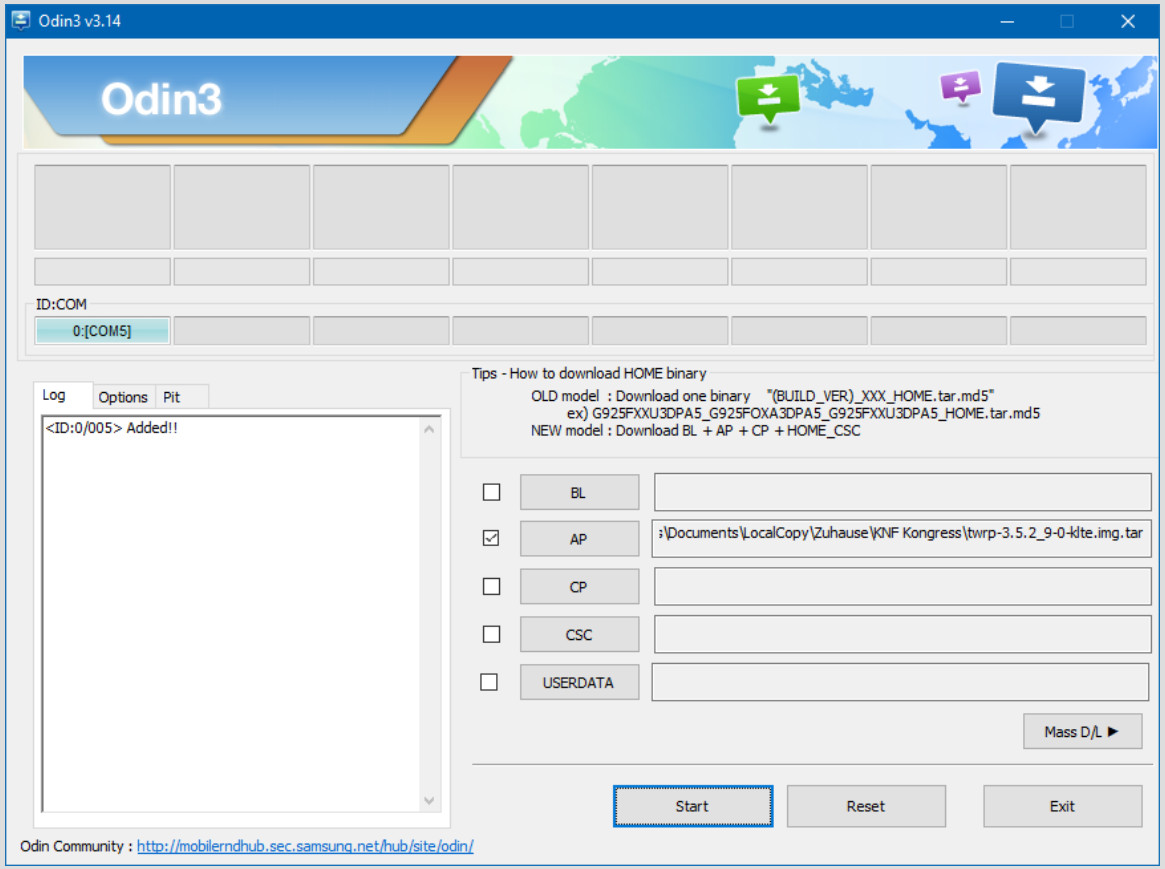
Achtung! Garantieverlust!

- Schritt 3: Nötige Tools installieren
  - Samsung: Odin (z.b. https://odindownloader.com) + USB-Treiber (https://developer.samsung.com/android-usb-driver)
  - oder Heimdall

Wie funktioniert das im Detail?

- Schritt 4: TWRP installieren
  - Für Gerät passende Version herunter laden: https://twrp.me/Devices
  - Gerät in Download-Modus booten (Tastenkombination recherchieren)
  - An PC anschließen und Flashen (AP)

Wie funktioniert das im Detail?



Wie funktioniert das im Detail?

- Schritt 5: Backup erstellen
  - SD-Karte einlegen
  - In Recovery-Modus starten (Tastenkombination recherchieren)
  - In TWRP „Sichern“ wählen
  - Mindestens Boot, Recovery, System und Data sichern.

Wie funktioniert das im Detail?

Wie funktioniert das im Detail?

- Schritt 6: Zu patchendes Image extrahieren:
  - Passendes Custom ROM herunterladen (z.B. https://wiki.lineageos.org/devices)
  - Je nach „Ramdisk“-Wert boot.img oder recovery.img extrahieren.
- Schritt 7: Image patchen
  - Image auf Smartphone kopieren
  - Magisk-App öffnen und bei „Magisk“ auf „Installieren“ tippen.
  - Bei „Methode“ „Eine Datei auswählen und patchen“ anwählen, dann das Image auswählen.
  - „Los Geht’s“

Wie funktioniert das im Detail?

- Das gepatchte Image ist unter `storage/emulated/0/Download/magisk_patched-`[zufälliger Text]`.img` zu finden.
- Gepatchtes Image auf PC kopieren.

- Schritt 8: Original-Image ersetzen
  - Gepachtes Image nach `boot.img` / `recovery.img` umbenennen und originales Image in Zip-Datei dadurch ersetzen.

Wie funktioniert das im Detail?

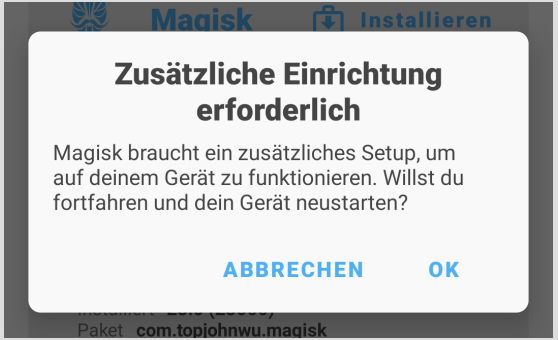
- Schritt 9: Google-Paket auswählen
  - z.B. von OpenGApps (https://opengapps.org)
  - Architektur z.B. auf LineageOS-Geräteseite
  - Android-Version des LineageOS-Builds wählen
  - Empfohlene Variante: Nano
  - Zip-Datei herunterladen
- Schritt 10: Dateien auf Gerät kopieren
  - Gepatchtes LineageOS-zip und OpenGApps-zip auf Gerät übertragen.

Wie funktioniert das im Detail?

- Schritt 11: Dateien installieren
  - In Recovery Mode booten
  - In TWRP „Installieren“ wählen, dann LineageOS-zip auswählen.
  - „Mehr ZIPs hinzufügen“ wählen und OpenGApps-zip auswählen.
  - „ZIP-Signaturprüfung“ und „Automatischer Neustart“ deaktivieren
  - Installation bestätigen
  - Nach Abschluss auf TWRP-Hauptseite „Löschen“ wählen und bestätigen
  - Danach System neustarten

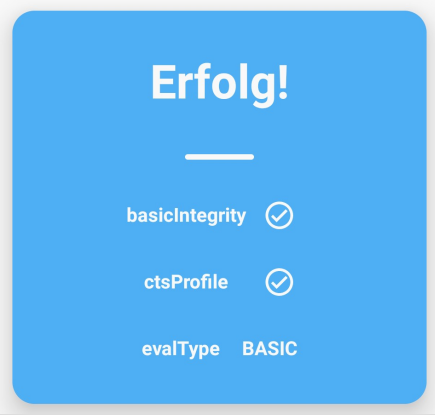
Wie funktioniert das im Detail?

- Schritt 12: zusätzliches Setup
  - Nach Systemeinrichtung die Magisk-App starten (noch kein App-Icon)
  - Jetzt wird die Vollversion der App heruntergeladen und installiert (Berechtigung „Apps aus unbekannter Quelle installieren“ erteilen)
  - Zusätzliche Einrichtung erforderlich, Gerät wird neu gestartet.
  - Nach Neustart ist Magisk einsatzbereit



Wie funktioniert das im Detail?

- Schritt 13: Magisk Konfigurieren
  - Optional: Verstecke die Magisk-App in Einstellungen
  - In Magisk-Einstellungen MagiskHide aktivieren
  - Auf der Magisk-Startseite das Schild anwählen, dann MagiskHide.
  - Dort alle Apps wählen vor denen Magisk und Root versteckt werden soll.
- Schritt 14: SafetyNet-Test machen
  - Handy neu starten
  - Auf Magisk-Startseite „SafetyNet überprüfen“ wählen, proprietären Code herunterladen lassen



Fazit

- Noch offene Punkte:
  - OTA-Update von LineageOS
  - Rechtliche Bedenken
- SafetyNet und Magisk wird ein Katz- und Mausspiel bleiben

Fazit

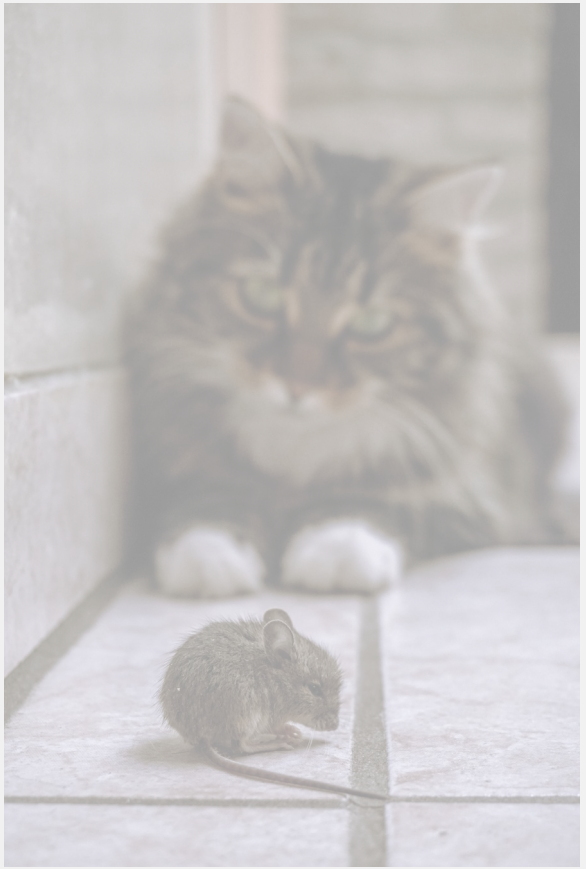
- Noch offene Punkte:
  - OTA-Update von Lir
  - Rechtliche Bedenke
- SafetyNet und Magisk
  und Mausspiel bleibe

13:35

Jailbreak oder Root eines Geräts

Eingriffe wie "Jailbreaken" oder "Rooten" haben ernsthafte Auswirkungen auf die Sicherheit von mobilen Geräten. "Jailbreak" bezeichnet das Entfernen von Nutzungsbeschränkungen bei Geräten mit dem Betriebssystem iOS, da bestimmte, in der Regel sicherheitsrelevante Funktionen serienmäßig durch den Hersteller gesperrt sind. Dadurch wird sichergestellt, dass im Serienzustand auf dem Gerät nur Software aus dem App Store des Herstellers installiert werden kann. Unter dem "Rooten" eines Geräts mit einem auf Linux basierenden Betriebssystem, insbesondere von Geräten mit dem Betriebssystem Android, versteht man das Verschaffen von erweiterten Rechten für und durch einen Benutzer. Diese Rechte werden auch als "Root-Rechte" oder "Administratorrechte" bezeichnet. Die Nutzung der App auf Geräten mit dergestalt verändertem Betriebssystem ist aus Sicherheitsgründen nicht erlaubt. Die TARGOBANK behält sich vor, die Nutzung der App auf solchen Geräten - sofern technisch umsetzbar - zu unterdrücken. Die Bank übernimmt keine Haftung, wenn der Teilnehmer sein Gerät unter Verletzung der iOS-Softwarelizenzbedingungen von Apple Inc. oder der Google-Nutzungsbedingungen nutzt oder die Software des verwendeten Betriebssystems (iOS oder Android) verändert wurde und dadurch Fehler in der App entstehen oder eine missbräuchliche Nutzung der App ermöglicht wird.

BESTÄTIGEN



Fazit

- Noch offene Punkte:
  - OTA-Update von LineageOS
  - Rechtliche Bedenken
- SafetyNet und Magisk wird ein Katz- und Mausspiel bleiben

Ende

Danke für Eure Aufmerksamkeit!

Markus Oppmann

markus@memotech.franken.de

Weiterführende Links

- Allgemeine Installationsanleitung Magisk: https://topjohnwu.github.io/Magisk/install.html
- Tutorial von XDA Developers: https://www.xda-developers.com/how-to-install-magisk
- Magisk Troubleshhot Wiki: https://www.didgeridoohan.com/magisk/HomePage
- Installation von TWRP: https://www.xda-developers.com/how-to-install-twrp
- Infos zu Heimdall: https://glassechidna.com.au/heimdall

Bildquellen

- Folie 3: LineageOS-Logo (LineageOS Project, Brand Guidelines)
- Folie 3: Eigenes Werk aus Google-Logo (Google Inc., Public domain, via Wikimedia Commons) und Krake (pngimg.com, CC BY-NC 4.0)
- Folie 4: Eigenes Werk aus Android-Bot (Bersam, CC BY 3.0, via Wikimedia Commons) und Hängematte (pngimg.com, CC BY-NC 4.0)
- Folie 5: Magisk Logo (topjohnwu, GPLv3)
- Folie 6: Eigenes Werk aus Android Robot (Google Inc., CC BY 3.0, via Wikimedia Commons) und Wappen Lindau (See page for author, Public domain, via Wikimedia Commons)
- Folie 9 und 11: TWRP Logo
- Folie 15: Google-Logo (Google Inc., Public domain, via Wikimedia Commons)
- Folie 19, 20, 21: Katz und Maus (Katherine Mihailova, Pexels-Lizenz, via Pexels)
- Folie 22: Glocke (Micrografx Inc., Micrografx GraphicsSuite 2)
- Sonstige Bilder: Eigene Aufnahmen