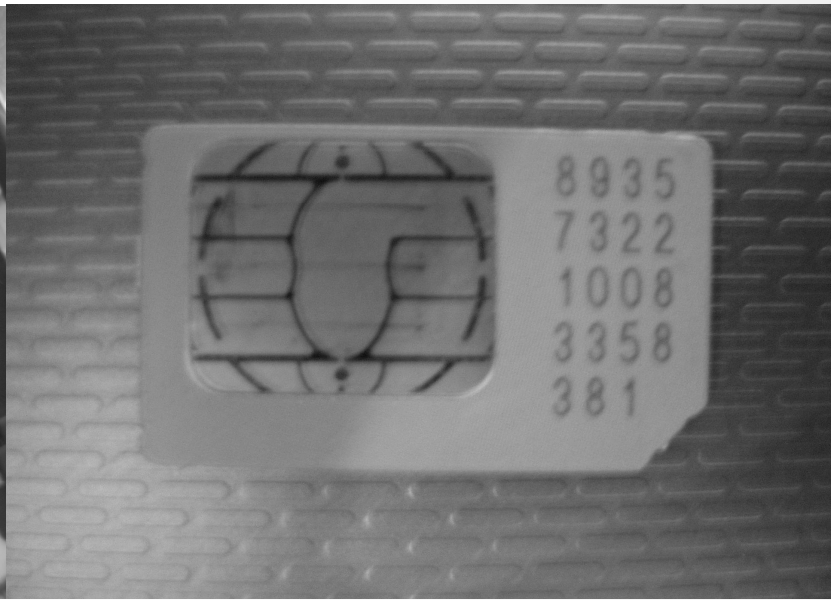
Handy-Verschlüsselung

Lineage OS Supported Devices

Tracking: IMEI und IMSI

Seriennummern von *Telefon* und *SIM-Karte* werden gemeinsam gesendet und sind verknüpft

- ***Handy und SIM-Karte gleichzeitig tauschen***



Überwachung

Position

- GPS *(unwahrscheinlich)*
- Handy-Masten ***(wahrscheinlich)***
- W-LAN-Netze

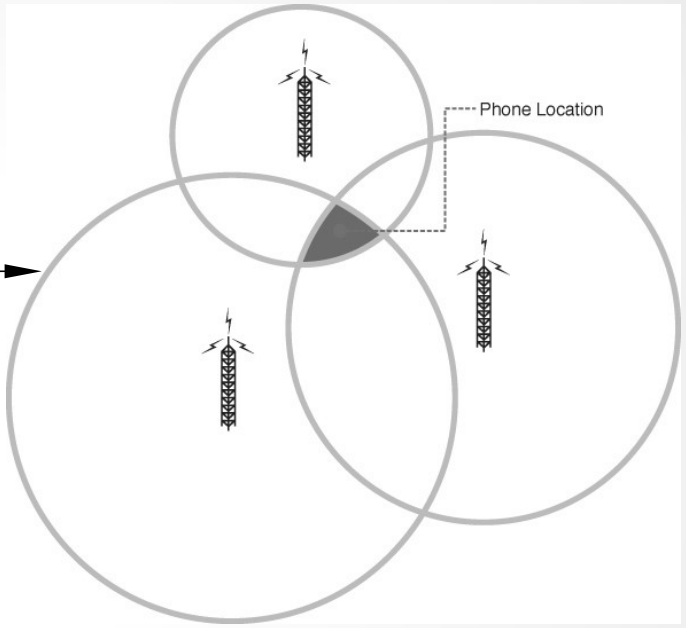
Verbindungsdaten ***(wahrscheinlich)***

- Wer? Wann? Wo? Mit Wem?

Inhalt *(in Sonderfällen)*

- Telefonate
- SMS

Gespeicherte Daten (Browser- & Chatverläufe)



Staatstrojaner

Kann alles ausspähen, was am und ums Handy passiert.

Wie kommt dieser aufs Handy?

- Durch (unbemerkte) *Beschlagnahmung* des Geräts
- Online durch Ausnutzen von *Fehlern* (Sicherheitslücken) in der Software
  - ➔ ***Updates, Updates, Updates!***
- Online durch Ausnutzen von *Hintertüren* in der Software
  - ➔ ***Eigenes Betriebssystem installieren***
- Phishing

Welches Gerät?
Tasten oder Touchscreen

Software ist verantwortlich für
Funktionsumfang & Komplexität

- Software entscheidet über Aktivierung von GPS, Mikrofon, …
- Sicherheit steht und fällt mit dem Betriebssystem

Kein Tasten-Handy hat einsehbare Software

- ***Potenziell alle verwanzt***

Warum nur Smartphone?

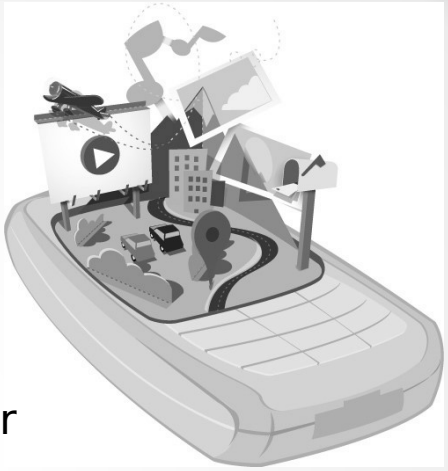
Betriebssystem

- Verschiedene unbekannte
- Geheimer Source Code
- Keine Fehlerbehebung
- Nicht austauschbar

Betriebssystem

- Android
- Open Source
- Sicherheits-Updates
- Austauschbar

Warum Android?



Entwickelt von der *Open Handset Alliance*
(84 Unternehmen)

Geprüft von vielen Seiten
(Industrie & Community)

- OPEN SOURCE: Funktionsweise für alle einsehbar

Apple iPhone hat iOS statt Android

- ***Geheimer Source Code***
- ***Nicht austauschbar***

Open Source: Freie Software

> Um das Konzept zu verstehen sollte man an *frei* wie in *Redefreiheit* denken, nicht wie in *Freibier*.
>
> – gnu.org

Strategie
Eigenes Betriebssystem

Austausch des Betriebssystems durch ein vertrauenswürdiges mit möglichst minimalem Funktionsumfang

Lineage OS

- Minimales Android
- Open Source Community
- Ohne Google-Apps wie *Play Store, Gmail* etc.
- Telefon verschlüsselbar
- Lokale Offline-Kontakte

Voraussetzung

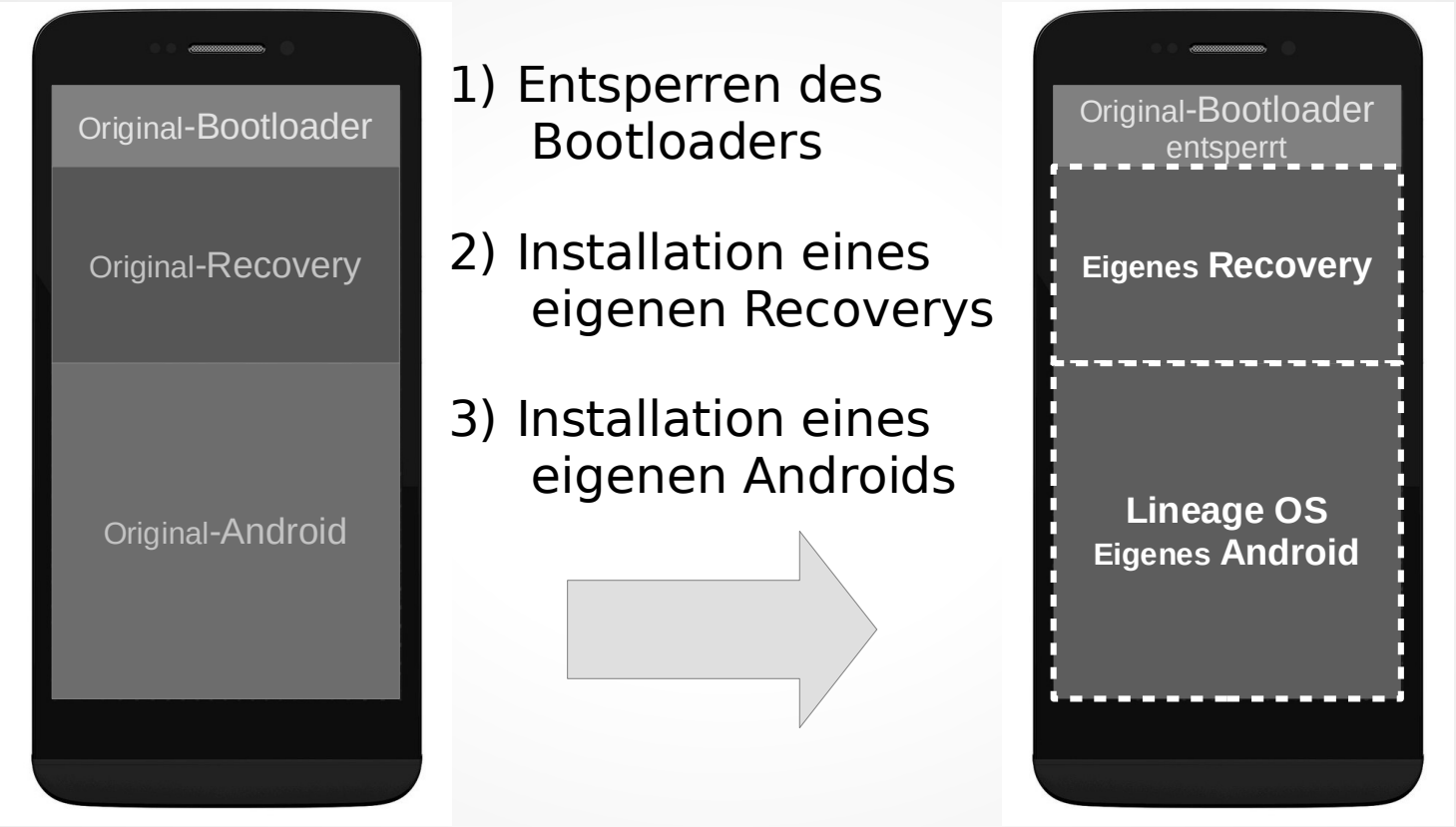
Gerät muss (offiziell oder inoffiziell) von Lineage OS unterstützt werden

Internet-Recherche vor Kauf:

- Internet-Suche: Handymodell Lineage
- wiki.lineageos.org/devices
- forum.xda-developers.com

Auf exakte Modellbezeichnung achten!

Austausch des Betriebssystems



1) Entsperren des Bootloaders

Bootloader startet das Betriebssystem

- Wenn noch gesperrt nur Installation von Original-Betriebssystemen des Herstellers möglich
- Nicht alle Handymodelle haben gesperrten Bootloader
- Verlust der Garantie durch Entsperrung
  - Gesetzliche Gewährleistung von 2 Jahren unberührt (z.B. defektes Display)
- Bei *Beschlagnahmung* können auch Behörden leichter Software auf entsperrten Geräten installieren
  - ➔ ***Nicht einschalten! Sondern austauschen oder neu aufsetzen!***

2) Installation eines eigenen Recoverys

Recovery ist der Installations- und Wartungsmodus für das eigentliche Betriebssystem. Beispiele:

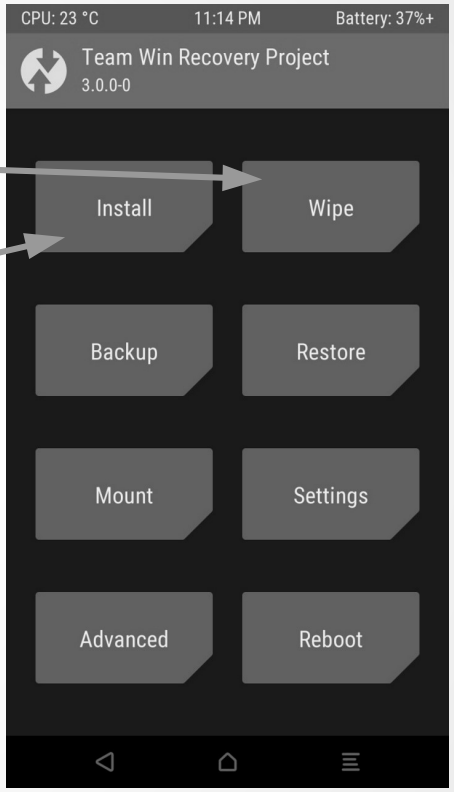
- Team Win Recovery Project (TWRP)
- ClockworkMod (CWM)

- Installation mittels Bootloader im „Download-Modus“ und USB-Verbindung
- Oder Installation mittels Original-Recovery (je nach Modell)

3) Installation eines eigenen Androids

Installation mittels eigenem Recoverys

- Zuerst Cache, Daten und System löschen
- Installation von Speicherkarte (.*zip*-Datei)



Regelmäßig Updates installieren!

→ bei Updates nur Cache löschen

Verschlüsselung Interner Speicher

Enthält u.a.

- Kontakte
- Dateien & Fotos
- installierte Apps
- Einstellungen
- Browser-, SMS- & Chatverläufe

Einstellungen > Sicherheit > Gerät verschlüsseln

- Passwort oder Entsperrcode muss eingestellt sein
- ***Vorgang ist nicht umkehrbar!***

Speicherkarte verschlüsseln

Enthält u.a.

- Dateien & Fotos
- Daten von Apps

Einstellungen > Speicher >
Speicherkarte als internen Speicher verwenden

- ***Speicherkarte kann nur mehr von diesem Gerät gelesen werden***

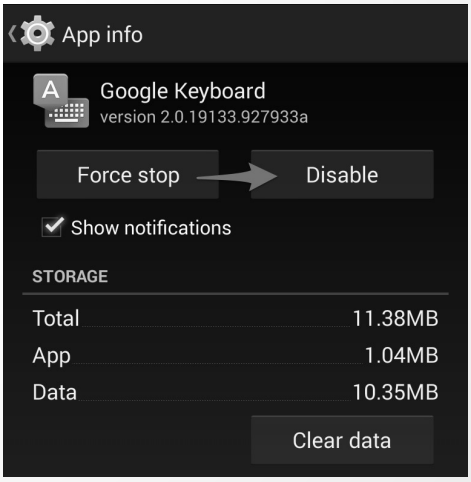
Software einschränken
Integrierte Apps deaktivieren

Je weniger Software, desto weniger Fehler
= geringere Angriffsfläche

- Wichtig bei Original-Betriebssystemen,
  bei Lineage OS nicht unbedingt notwendig

Einstellungen > Apps >
Menü > Systemanwendungen anzeigen

- Apps und Dienste einzeln deaktivieren
  bis auf die notwendigsten
- Unnötige Berechtigungen entziehen
- Im Zweifel Internet fragen



App: „F-Droid“

- Vergleichbar mit *App Store* oder *Google Play*
- Enthält nur Open Source Apps
- Nur Apps, die Privatsphäre respektieren

➔ Download: f-droid.org

App: „Yalp Store“

- Ermöglicht Installation von Apps, die nur in *Google Play* aber nicht in *F-Droid* sind
- YALP ist PLAY rückwärts geschrieben

➔ Installation via F-Droid

Verschlüsselte Kommunikation mit App: „Signal“

Durchgehende (Gerät-zu-Gerät) Verschlüsselung für *Nachrichten* und *Telefonate*

- Verschlüsseltes wird durch das Internet geleitet
- Normale SMS werden verschlüsselt gespeichert

➔ Installation via Yalp-Store

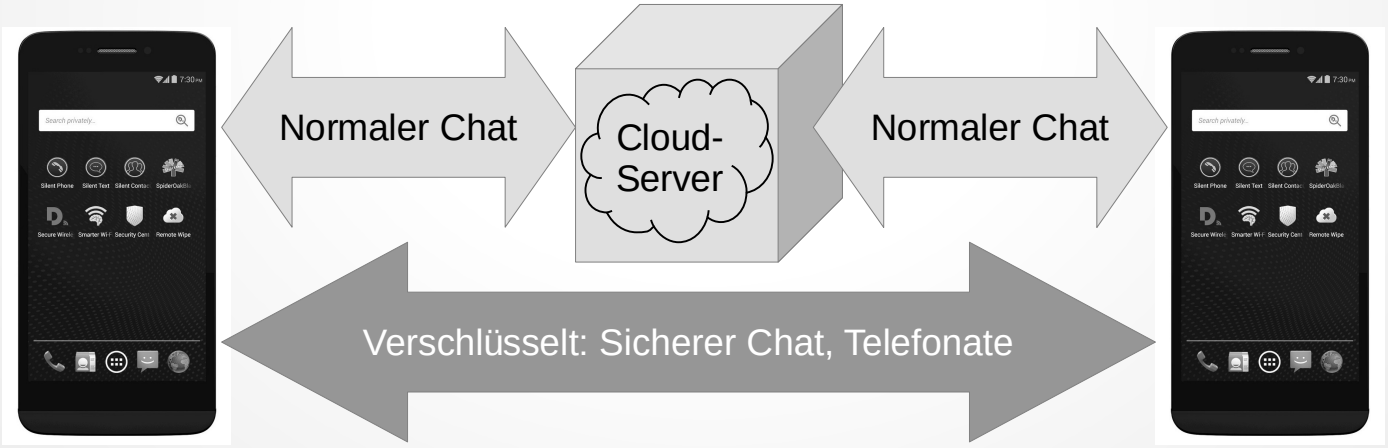
App: „Telegram“

Cloud-basierter Internet-Messenger
für *Nachrichten* und *Telefonate*

- Normaler Chat wird in der Cloud gespeichert
- ***Optionale*** Gerät-zu-Gerät-Verschlüsselung

  Nicht als sicherer Messenger voreingestellt

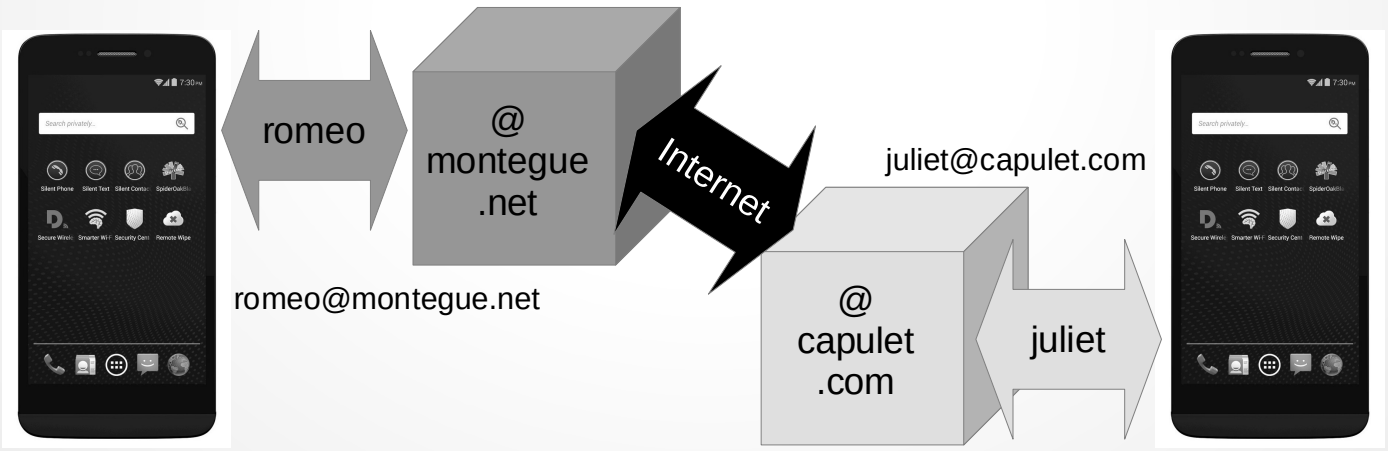
➔ Installation via F-Droid



Jabber (XMPP)

Messenger vergleichbar mit E-Mail (benötigt Server)

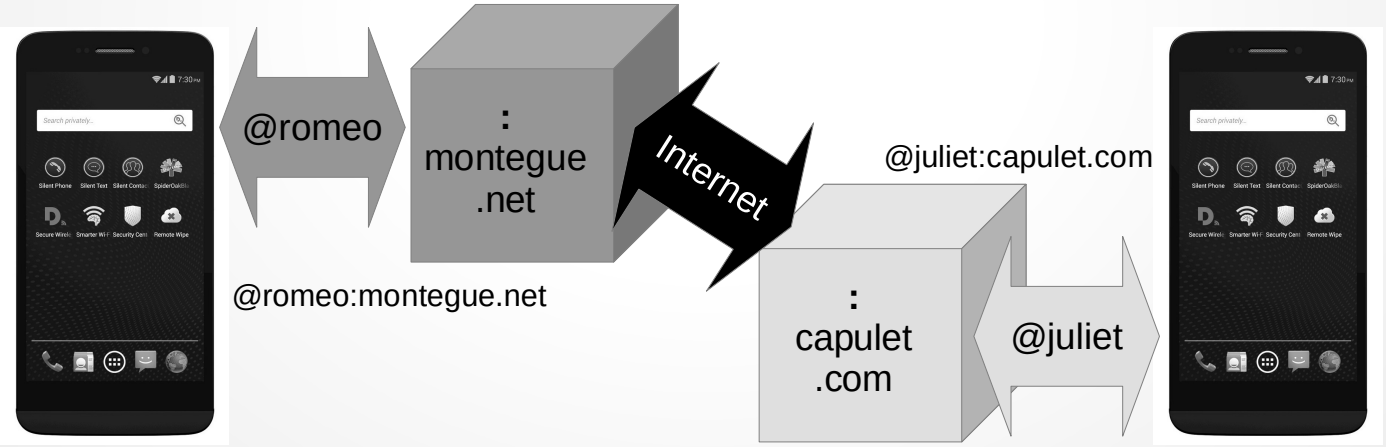
- ***Optionale*** Gerät-zu-Gerät-Verschlüsselung OMEMO
- App: z.B. Conversations



Riot.im (matrix.org)

Dezentraler Messenger mit (Video-)Telefonie

- ***Optionale*** Ende-zu-Ende-Verschlüsselung
- Integration mit anderen Diensten
- App: z.B. Riot.im



App: „Fennec F-Droid“

- Vom F-Droid-Projekt bereinigter *Firefox*
- Browser statt Apps verwenden wenn möglich
  - Funktion „Zum Startbildschirm hinzufügen“
- Besser als vorinstallierter Browser weil via F-Droid updatebar
  - ***Browser-Updates sind sicherheitsrelevant!***

„Orbot“ und „Orfox“

Tor-Anonymisierungs-Netzwerk

Installation via Yalp Store:

- *Orbot* (Tor)
- *Orfox* (Browser)