Replicant

Zum Stand der Entwicklung von ”freien” Betriebssystemen für Smartphones

Orhan Kemal Yüksel

Zusammenfassung
Eine Übersicht zur Verwendbarkeit von Replicant 6.0* unter einem Samsung Galaxy S3 Smartphone (i9300). Ein von Android und proprietärer Software befreitetes Betriebssystem für Smartphones.

Unterstützte Geräte: Galaxy S2 - i9100, Galaxy Note 2 - n7000/n7100, Galaxy S3 - i9300/i9305, Galaxy Nexus - i9250, Galaxy Tab 2 - 7.0 (p31xx)/10.1 (p51xx), Galaxy Note - 8.0 (n51xx)

https://www.replicant.us

Inhaltsverzeichnis

1. Einleitung

Im März 2011 wird eine Anwendung die gegen die Nutzungsbedingungen von Google verstösst per Fernwartung von ca. 260000 Smartphones entfernt [1]. Dieses massenhafte und ungefragte Löschen einer Software führte schon damals vielen vor Augen was durch die vorgegebenen Firmen-AGBs von all seinen_ihren Nutzer_innen akzeptiert wird [2]: die Zustimmung für einem permanenten Zugriff auf persönliche Informationen und deren Verwertung durch kommerzielle Firmen (Google). Das zuvor genannte Beispiel macht vor allem eines deutlich: Dass die Option zu einem ungehinderteren Zugriff auf Daten, die in Android Betriebssystemen hinterlegt sind[1], vorhanden ist. [3]. Das wird noch nicht einmal von Google selbst bestritten [4][5]. Ein Grund mehr nach alternativen Betriebssystemen Ausschau zu halten, um Firmen wie Google oder Apple dauerhaft den Zugriff auf unsere Daten zu entziehen.

[1] Inwiefern diese Hintertüre bereits von Google selbst oder nur im Rahmen von Amtshilfeersuchen staatlicher Behörden genutzt wird, soll nicht Bestandteil dieses Beitrags sein. Es reicht völlig aus das die Schnittstelle existiert und sich ausnutzen lässt.

2. Funktionsweise von Smartphones

Smartphones setzen sich aus verschiedenen Hardware Komponenten zusammen (Mikrofon, Kamera, GPS, . . .), die über Hersteller eigene Software (Firmware, Treiber) angesprochen werden. Hierzu zählt der Grossteil von Programm-Funktionen, die bei einem Bootvorgang eines Smartphones zum Ansprechen der Hardware verwendet werden. Da sich dieser Programmcode innerhalb kleiner Adapterplatinen auf einem „Ein-Chip-System“ befindet wird ihre Funktionaliät als System-On-a-Chip (SoC) bezeichnet [6].

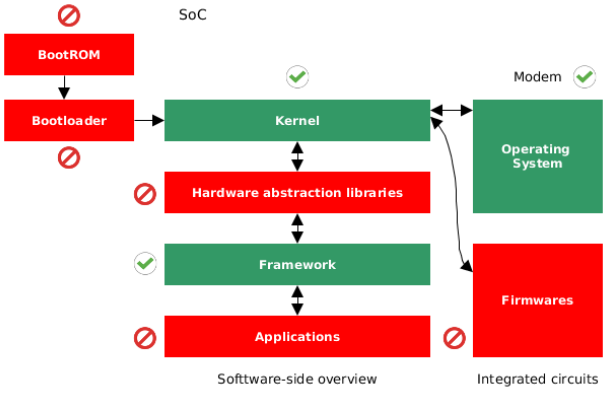

Abbildung 1. Samsung Galaxy S3 ohne Replicant.

An das SoC ist der Hauptprozessor des Smartphones angebunden. Das SoC hat nach einem erfolgreichen Bootvorgang des Smartphones Zugriff auf weitere Hardware Komponenten wie der Kamera, dem Mikrofon oder dem GPS. Der Bootvorgang wird über unveränderliche Befehle, die von der BootROM an das SoC gesendet werden initiiert. In einem zweiten Schritt wird der Bootloader gestartet. Die Firmware zum Steuern der

einzelnen Hardware Komponenten sowie die BootROM und der Bootloader bestehen aus proprietärer Software [7]. Software über die wir keine Kontrolle haben und von der wir auch nicht Wissen was sie genau macht, da ihr Quellcode nicht öffentlich zugänglich ist. Für einen Teil der bisher erwähnten Hardware Komponenten existiert bereits freie Firmware [8] - zumindest für einige Smartphone-Modelle. Davon ausgeschloßen ist die BootROM, da sie sich in einem Speicherbereich befindet, der nur über die Hardware gelesen werden kann und daher auch nicht veränderbar ist. Unter Abbildung 1 ist die System-Arichitektur eines Samsung Galaxy S3 (i9300) in seinem ursprünglichen Zustands dargestellt (die roten / heller gekennzeichneten Bereiche mit dem Einbahnstrassen-Symbol enthalten proprietäre Software. Dazu zählt auch das Modem. Die grünen Bereiche, welche mit einem OK-Symbol markiert sind, enthalten freie Software).

Ein Modem[2] übernimmt vor einer „Telefonverbindung“ die Einwahl bei einem Netzanbieter, in dem es das zuvor beschriebene SoC anspricht. Es enthält ebenfalls einen Prozessor, hat Zugriff auf den Speicher des Hauptprozessors und wird über proprietäre Software ausgeführt. Da das Modem in der Regel durchgehend über das GSM-Netz (Mobiltelefon-Netz) mit dem jeweiligen Netzanbieter verbunden ist, muss es gut isoliert werden, um es vor einem Zugriff auf Hardware Komponenten wie der Kamera, GPS oder dem Mikrofon zu schützen (siehe Abbildung 2).

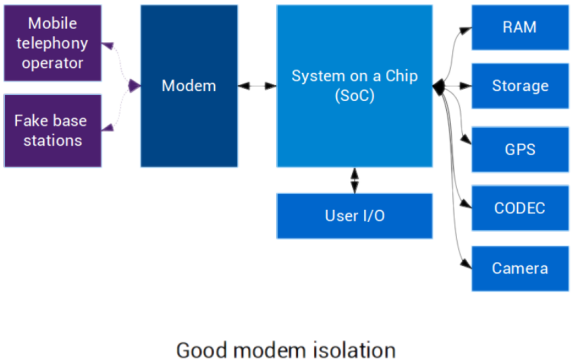

Abbildung 2. Isoliertes Modem

Da Modems aufgrund schlechter Isolierung oft Zugriff auf Hard- und Software Komponenten eines Betriebssystems erhalten stellen sie das Haupt-Einfallstor bzgl. der Sicherheit von Smatphones dar (siehe Abbildung 3).

Obwohl viele der aktuellen Smartphone-Betriebssysteme wie Android, Firefox OS, Ubuntu Touch oder Tizen ihren Quellcode veröffentlicht haben und einen Linux Kernel verwenden sind trotzdem noch viele proprietäre Treiber darin enthalten. Einige dieser Komponenten besitzen nachweißlich Hintertüren für einen Zugriff von außen [9][3].

[2]Oft auch als Baseband oder Radio bezeichnet.

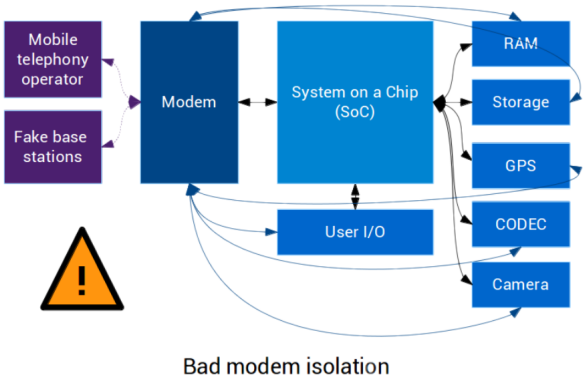

Abbildung 3. Schlecht isoliertes Modem

Neben der Problematik von proprietärer Software haben vorinstallierte Programme wie sie z.B. unter Android eingebunden sind weiterhin eine grosse Bedeutung in der alltäglichen Überwachung von Smartphone-Benutzer_innen [10].

Auch sollte die Rolle der zuvor angesprochenen Netzanbierter nicht unterschätzt werden: viele speichern die genauen Zeitpunkte von Textnachrichten / Gesprächen und orten oft die Standpunkte der jeweiligen Smartphones. Außerdem ermöglichen sie staatlichen Behörden einen Zugriff auf die genutzten Geräte, falls dies nicht schon eigenständig durch IMSI-Catcher betrieben wird [11].

3. Replicant als alternatives Betriebssystem

Replicant ist ein von Android befreites „freies“ Betriebssystem für Smartphones. Unter Version 6.0 wird nur eine begrenzte Anzahl an Geräten unterstützt [12]. Es basiert auf der Grundlage von LineageOS [13] und ersetzt bzw. greift nicht auf proprietäre Komponenten des Systems zu [14]. Zudem enthält es keine Software die nach der Freien-Software-Definition als „unfrei“ gilt [15][16]. Unter Abbildung 4 ist die Systemarchitektur eines Samsung Galaxy S3 (i9300) mit installierten Replicant zu sehen, in der nur noch im BootROM und Bootloader proprietäre Software enthalten ist (die rot / heller gekennzeichneten Architektur-Bereiche enthalten proprietäre Software. Die in grün markierten Bereiche mit dem Ok-Symbol enthalten freie Software. Der Firmware-Bereich ist in Orange hinterlegt, da sich Teile von proprietärer Firmware noch auf dem Smartphone befinden, die allerdings nicht genutzt werden).

4. Replicant 6.0: Installation und Setup

Voraussetzung:
Linux oder Mac OS X Betriebssystem.
Ein von Replicant 6.0 unterstütztes Smartphone [12].

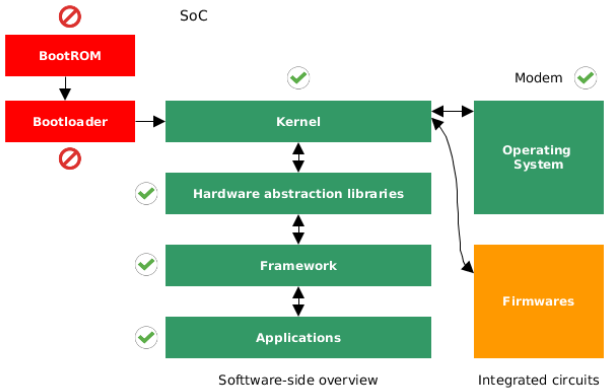

Abbildung 4. Samsung Galaxy S3 mit Replicant

Installationsanleitung (Replicant Wiki)[17]:

Um sicher zugehen das uns keine veränderte Verion der benötigten Replicant Dateien beim Download zugeschickt werden, benötigen wir den Pubklic-Key von einem der Replicant Entwicklern (Wolfgang Wiedmeyer). Damit lässt sich die Signatur der über das Internet besorgten Dateien überprüfen. Mit folgendem Terminal-Befehl kann der öffentliche Schlüssel besorgt und der Fingerabdruck des Schlüssel abgeglichen werden:

$ gpg –recv-key 5816A24C10757FC4
$ gpg –fingerprint 5816A24C10757FC4

Fingerprint:
0F30 D1A0 2F73 F70A 6FEE 048E 5816 A24C 1075 7FC4

Anschließend müssen noch die für eine Replicant Installation benötigten Dateien und Programme besorgt werden.

System
replicant-6.0-i9300.zip [18]
replicant-6.0-i9300.zip.asc [19]

Abgleichen der Prüfsumme, verifizieren der GPG-Signatur:

$ shasum -a 256 /pfad/replicant-6.0-i9300.zip
025d38a42223314042dd8ffabf0275530d0e15df9f1c739e5ae32b469585dcff

$ gpg –verify /pfad/replicant-6.0-i9300.zip.asc /pfad/replicant-6.0-i9300.zip
gpg: Good signature from ”Wolfgang Wiedmeyer . . . ”[unknown]
. . .
gpg: WARNING: This key is not certified with a trusted signature!
. . .

Der Abgleich der Prüfsummen und das Verifizieren mit dem Keyfile sollte auch für die folgenden Dateien und Programme durchgeführt werden:

Recovery
recovery-i9300.img [20]
recovery-i9300.img.asc [21]

sha-256 Prüfsumme (recovery-i9300.img):
a37be3020a594796e2f0a4ba4c4a7d070926cd2b23dc83667a8c2458aada74ce

Programme (nur unter Linux lauffähig)
adb [22]
adb.asc [23]

sha-256 Prüfsumme (adb):
324f4f8d66498644becc80e4032c1331d5f6c1032193d4a17ace6d5f44a41cfe

heimdall [24]
heimdall.asc [25]

sha-256 Prüfsumme (heimdall):
547ff8b08845351c57d45958bb5e8d949397ee9a0e369047f1f70c78f25bb534

Falls die digitalen Unterschriften (Prüfsummen und Keyfiles) übereinstimmen muss das Gerät in den Download-Modus gesetzt werden. Nachdem das Smartphone heruntergefahren und von einer USB-Verbindung getrennt wurde muss es **mit gehaltener Einschalt-Taste, Lautstärke-Leiser Taste und der Auswahl-Taste neu** gestartet werden (siehe Abbildung 5).
Nach kurzer Zeit sollte eine Warn-Hinweis Meldung erscheinen (Confirm that you want to download a custom OS), die bestätigt werden muss (Laustärke-Lauter Taste). Anschließend befindet sich das Smartphone im Download-Modus und das USB-Kabel muss wieder an dem Computer angeschloßen werden.

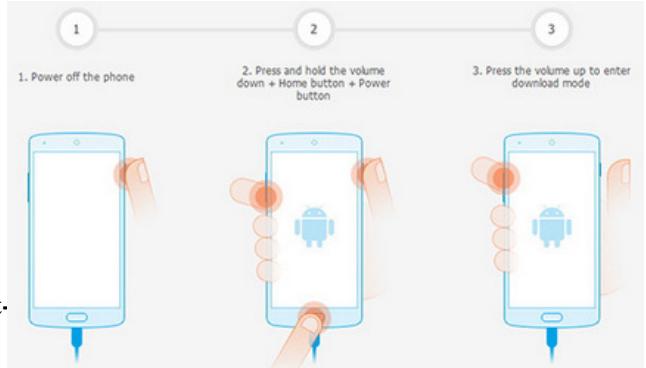

Abbildung 5. Tastenkombination: Download Modus

Nun muss das zuvor per Download besorgte Recovery-Image mit Heimdall über das Terminal installiert werden:

$ heimdall flash –BOOT /pfad/recovery-i9300.img –RECOVERY /pfad/recovery-i9300.img

Das Smartphone sollte nun von selbst in den Wiederherstellungsmodus booten (recovery mode). Falls eine Neuinstalation gewünscht ist muss der Menü-Punkt „Factory reset“ und anschließend „Wipe data“ ausgewählt und bestätigt werden. Bei einem Upgrade[3] sollten die beiden zuvor genannten Schritte nicht ausgeführt werden, da ansonsten sämtliche Smartphone Einstellungen und Daten verloren gehen. Danach muss noch der Menü-Punkt „Apply update“ gewählt werden und folgender Befehl über das Terminal ausgeführt werden[4]:

$ adb sideload /pfad/replicant-6.0-i9300.zip

Nachdem das System-Image erfolgreich übertragen wurde kann über die Zurück-Taste ins Recovery-Hauptmenü gewechselt werden. Hier muss der Punkt „Reboot system now“ ausgewählt werden und das Smartphone sollte unter Replicant 6.0 starten.

5. Replicant 6.0: Was läuft, was nicht . . . ?

Unter der am 17. September 2017 veröffentlichten zweiten Version von Replicant 6.0 können die grundlegenden Funktionen eines Smartphones genutzt werden. Dazu zählt die Verwendung von beliebigen SIM-Karten und die damit mögliche Nutzung des GSM-Netzes unterschiedlicher Anbieter zum Telefonieren, wie auch das Surfen im Internet über UMTS. Zusätzlich kann die Rückkamera verwendet werden, ohne dafür auf proprietäre Software zurückgreifen zu müssen [12][26]. Aufgrund nicht vorhandener freier Treiber kann 3D-Grafik, Wlan (Workaround: siehe Punkt 6), Bluetooth, Frontkamera und die Hardware Kodierung von Medien aktuell nicht verwendet werden. Das betrifft auch die Funktionalität des GPS. Zudem ist die Darstellungsgeschwindigkeit des Displays nicht mit jener von aktuellen Android-Systemen vergleichbar und Anwendungen die einen Zugriff auf die GPU des Smartphones benötigen sind unter Replicant-6.0 leider nicht lauffähig (das betrifft z.B. Orfox - eine Art Torbrowser für Smartphones) [27]. Ein möglicher Workaround ist die Aktivierung von llvmpipe was allerdings ein langsameres Rendern der Darstllungen im Displays zu Folge hat [28].

2D-Grafik[5]	3D-Grafik	Audio
funktioniert	fehlt	funktioniert

[6]

Telefonieren	Mobile Daten	Wlan
funktioniert	funktioniert	fehlt (Workaround: siehe Punkt 6)

Bluetooth	NFC	GPS
fehlt	funktioniert	fehlt

Sensoren	Kamera	Medienkodierung[7]
funktioniert	Rückkamera funktioniert, Frontkamera nicht	fehlt

Damit Replicant 6.0 in der aktuellen Version lauffähig ist wurde einiges an Code umgeschrieben oder durch freie Firmware ersetzt. Das betrifft Beispielweise auch das unter Punkt 2 beschriebene Modem und dem Problem des oft nicht bekannten Isolierung-Grades[8]. Der ursprüngliche Code wurde hier durch das freie Radio Interface Samsung-RIL und dem IPC Modem Protokoll ersetzt [29][30]. Für alle die der Modem-Isolierung trotzdessen nicht trauen: seit dem zweiten Image von Replicant 6.0 kann [31] das Modem über ein Skript deaktiviert werden [32]. Eine weitere Möglchkeit ist die Nutzung eines der drei von Replicant unterstützten Tablets ohne GSM-Unterstützung (nur Wlan) [12].

6. Replicant 6.0: Freies Wlan über USB

Da aktuell kein freier Treiber für das eingebundene Wlan Modul existiert (Broadcom BCM 4334), kann unter Replicant 6.0 kein Wlan genutzt werden (Samsung Galaxy S3 i9300 Smartphone).
Es besteht allerdings die Möglichkeit sich über einen USB Wlan Adapter (AR9271 Chipsatz) mit dem Internet zu verbinden, was einen erhöhten Akku-Verbrauch zu Folge hat[9]. Einen passender USB Wlan Adapter kann z.B. über Technoethical bezogen werden [33]. Zusätzlich wird noch ein USB OTG Y-Kabel oder ein Micro-USB OTG Konverter benötigt.
Für eine erfolgreiche Verbindung kann das Programm RepWifi verwendet werden. Hierfür muss noch der Root-Zugriff für Anwendungen unter den „Entwickleroptionen“ zugelassen werden. Über die Anwendung RepWifi ist es möglich nach offenen Wlan Netzen zu suchen und sich über WPA/WPA2 mit ihnen zu verbinden. Alle Verbindungen werden dauerhaft gespeichert, um zu einem späteren Zeitpunkt eine erneute Verbindung zu ermöglichen.
Die MAC-Addresse lässt sich temporär über folgenden Replicant Terminal-Befehl[10] ändern:
$ su; ip link set wlan0 address xx:xx:xx:xx:xx:xx

[3] Ein Backup kann davor über die im App-Store von F-Droid erhältliche App oandbckup erstellt werden.

[4] Falls adb nicht funktioniert kann es daran liegen das keine Verbindung zum Rechner erkannt wurde. Oft hilft ein erneutes anschließen des Smartphones über USB. Außerdem muss dem USB Debugging nach entsprechender Aufforderung auf dem Smartphone zugestimmt werden. Mit dem Befehl „adb devices“ kann zudem überprüft werden ob das Gerät erkannt wird.

[6] Da die Grafikdarstellung über freie Software umgesetzt wird ist die Darstellungsgeschwindigkeit nicht mit eines Android-Betriebssystem vergleichbar.

[7] Hardware

[8] Auch wenn die Replicant-Entwickler_innen bereits bei der Auswahl der Hardware auf eine möglichst gute Isolierung des Modems achten, kann dies nicht mit 100% Gewissheit überprüft werden.

[9] Im Falle eines schwachen Akkus kann es passieren das der Wlan Adapter nicht mehr mit Strom versorgt wird.

[10] Das Terminal kann über Einstellungen ¿ Entwickleroptionen ¿ Debugging ¿ Lokales Terminal aktiviert werden.

Eine aktuellere Version von RepWifi kann über folgende URL bezogen werden:

RepWifiApp_v0.5.apk [34]
RepWifiApp_v0.5.apk.sig [35]

Nach dem Überprüfen der Signatur (siehe Punkt 4) kann die Anwendung über adb installiert werden[11]:

$ adb install /pfad/RepWifiApp_v0.5.apk

F-Droid [36], ein alternativer App-Store für freie Software, funktioniert mit dem USB Wlan-Adapter erst seit dem zweiten Image von Replicant 6.0 [31]. Es ist auch möglich Apps und deren GPG-Signaturen direkt über die Seite von F-Droid [37] zu beziehen und anschließend per adb zu installieren[12].

Mit Relplicant 6.0 [31] ist es nicht möglich einen Internet-Hotspot einzurichten.

7. Replicant 6.0: Offline Karten (OsmAnd)

Über die Anwendung OsmAnd ist es möglich weltweites Kartenmaterial offline zu nutzen und sich somit einem Tracking von Firmen wie Google oder einer staatlichen Überwachnung zu entziehen. Das Kartenmaterial kann anonym per Tails [38] besorgt werden [39] und anschließend auf ein Smartphone oder Tablet übertragen werden, das z.B. auschließlich für eine Offline Nutzung angeschafft wurde.

$ unzip /pfad/map.obf.zip
$ adb push /pfad/map.obf.zip
/storage/emulated/0/Android/data/net.osmand.plus/files/

8. Replicant 6.0: Verschlüsselte Telefonate (Mumble)

Mit Plumble können verschlüsselte Gespräche über frei wählbare Mumble-Server geführt werden (VOIP)[13]. Die Anwendung kann über F-Droid installiert werden.
In fast allen Städten existieren mittlerweile Freifunk-Knoten [40] was die Möglichkeit eröffnet Telefonate über einen zuvor aufgesetzten Mumble-Server Kanal zu führen:

- Aufsetzen eines passwortgeschützten Mumble Server Kanals[14].
- Notieren der Freifunk-Knoten Adressen für unterwegs.
- Deaktivien des Replicant Modem[32].
- Verbindung mit einem Freifunk-Knoten.
- Über die Plumble App kann nun eine Verbindung zu dem Mumble-Server hergestellt und verschlüsselt telefoniert werden.
- Es besteht die Möglichkeit Plumble über Tor zu tunneln[15].
- Bei bedarf kann das Modem zu jderzeit wieder aktiviert werden [32].

9. Nützliche Software & Resourcen

Bei der Vielzahl an freien Anwendungen die über F-Droid angeboten werden [37] solltet ihr euch so wenig Apps wie möglich auf eurem Smartphone installieren und deren Zugriffe soweit es geht einschränken[16]: Umso weniger Apps installiert sind umso weniger Schwachstellen können auch ausgenutzt werden. Wichtig ist das die Anwendungen über F-Droid installiert. Nur dann werden sie mit Updates versorgt.
Als Grundvoraussetzung für die allgemeine Datensicherheit sollte das System über Einstellungen
¿ Sicherheit ¿ Verschlüsselung ¿ Telefon verschlüsseln verschlüsselt werden (durch eine gute separate Passphrase [41]).

Orfox, Orweb, Lighning
Orfox läuft nur über den bereits angesprochenen Workaround [28] und ist der aktuell sinnvollste Ansatz um sich „anonym“ im www zu bewegen. Alternativ kann auch Orweb oder Lighning genutzt werden[17]. Falls Lightning über Tor verwendet werden soll muss unter den Allgemeinen-Einstellungen der HTTP-Proxy auf Orbot geändert werden.

Signal[18]
Signal ist leider nicht im AppStore von F-Droid enthalten. Falls ihr trotzdem eine Version auf eurem Replicant-Smartphone installieren wollt kann ein Apk von deren Webseite besorgt werden:

Signal-4.10.12.apk [42]

Abgleichen der Prüfsumme (apksigner):

$ apksigner verify –print-certs Downloads/Signal-website-release-4.10.12.apk

[11] Was in den Entwickleroptionen zugelassen werden muss.
[12] Ihr erhaltet dann keine Aktualisierungen über F-Droid und müsst euch um neue Software-Versionen eigenständig kümmern
[13] Die Gespräche werden über TLS und OCB-AES128 verschlüsselt
[14] Z.B. mit einem vertrauswürdigen Server: talk.systemli.org, Port: 64738. Hinweis: Der Server befindet sich in Deutschland - einem Land das wahrscheinlich bald wieder Provider dazu verpflichtet sämtliche Verbindungsdaten mindestens sechs Monate zu speichern (Vorratsdatenspeicherung).
[15] Einstellungen ¿ Allgemein ¿ Über Tor verbinden / Erzwinge TCP
[16] ¿ Settings ¿ Apps
[17] Unter den Einstellungen von Lightning lassen sich diverse Sicherheitseinstellungen wie z.B. Einstellungen zu User-Ageng, Javascript, Standort, Cache oder Cookies festlegen.
[18] Aufgrund der fehlenden Google-Dienste kann es zu einigen Einschränkungen bei der Verwendung von Signal kommen.

Fingerprint (certificate SHA-256 digest):
29f34e5f27f211b424bc5bf9d67162c0eafba2da35af35c16416fc44d2176b26

Orbot
Orbot ist eine Proxy-Anwendung über die sämtliche Verbindungen ins Internet durch Tor [43] getunnelt werden können[19]:

Orbot Einstellungen[20]:

- Anftage auf Root-Zugriff: aktivieren
- Transparenten Vermittlung: aktivieren
- Alles durch Tor leiten: aktivieren

Um Orbot über F-Droid installieren zu können muss „Guardian Project Official Releases“ unter den Paketquellen in den Einstellungen von F-Droid aktiviert werden.

Plumble
Mit Plumble können verschlüsselte Gespräche über frei wählbare Mumble-Server geführt werden (VOIP)[21]. Die Anwendung kann über F-Droid installiert werden.
In fast allen Städten existieren mittlerweile Freifunk-Knoten [40] was die Möglichkeit eröffnet Telefonate über einen zuvor aufgesetzten Mumble-Server Kanal zu führen:

- Aufsetzen eines passwortgeschützten Mumble Server Kanals[22].
- Notieren der Freifunk-Knoten Adressen für unterwegs.
- Deaktivien des Replicant Modems [32].
- Verbindung zu einem Freifunk-Knoten.
- Über die Plumble App kann nun eine Verbindung zu dem Mumble-Server hergestellt und verschlüsselt telefoniert werden.
- Es besteht die Möglichkeit Plumble über Tor zu tunneln[23].
- Bei bedarf kann das Modem zu jderzeit wieder aktiviert werden [32].

Nützlich für das zuvor dargestellte Unterfangen wäre eine Offline Karte wie Osmand (siehe 7), die sich die Standorte von Freifunk-Knoten merkt[24].

[19] Vorrausgesetzt die App erlaubt eine Proxy-Unterstützung.
[20] Es ist auch möglich die Apps für eine Tor-Tunneling einzeln auszuwählen.
[21] Die Gespräche werden über TLS und OCB-AES128 verschlüsselt.
[22] Z.B. unter einem vertauswürdigen Server: talk.systemli.org, Port: 64738. Der Server befindet sich in Deutschland - einem Land das wahrscheinlich bald wieder Provider dazu verpflichtet sämtliche Verbindungsdaten mindestens sechs Monate zu speichern (Vorratsdatenspeicherung)
[23] Einstellungen ¿ Allgemein ¿ Über Tor verbinden / Erzwinge TCP
[24] Die Freifunk-App welche in F-Droid zu finden ist mit Replicant nicht benutzbar und sollte nicht installiert werden, da sie System-Konflikte verursacht.

Obscure, CameraV
Mit ObsuraCam lassen sich Gesichter in Bildern durch Pixel unkenntlich machen. Die kann auf fotografierte Bilder oder auf Bilder aus Gallarien angewendet werden. Neben diesem Feature entfernt die App auch Metadaten [44] wie GPS oder die Modellnummer des Smartphones über welches das Bild erstellt wurde.
CameraV bietet einen verschlüsselten Bereich in dem die gemachten Bilder abgelegt werden können. Dafür muss die Einstellung „Üse External Camera Apps’ deaktiviert werden. Zusätzlich bietet die Anwendung Möglichkeiten zum Austausch von Bildern über das Internet sowie das hinzufügen von eigenen Metadaten an. Neben diesen, nicht wirklich auf Sicherheit ausgelegten Optionen, enthält die App einen Panic-Button mit dem sämtlchier Inhalt oder die ganze Anwendung gelöscht werden kann.
Falls das Aufnehmen von Bildern über die Rückkamera nicht mehr funktioniert kann es an einem Ëinfrieren”der App liegen, was wie folgt behoben werden kann: Replicant Einstellungen ¿ Apps ¿ Kamera (zweite) ¿ Speicher ¿ Daten Löschen.
Um ObsuraCam oder CameraV über F-Droid installieren zu können muss „Guardian Project Official Releases“ unter den Paketquellen in den Einstellungen von F-Droid aktiviert werden.

AIMSICD (IMSI-Catcher Schutz)
AIMSICD ist eine App in der Alpha-Phase die vorgibt IMSI-Catcher zu entdecken. Inwieweit die Anwendung dies auch zuverlässig umsetzt kann hier nicht überprüft werden. Eine Möglichkeit sich zuverlässig vor IMSI-Catchern zu schützen ist ein Deaktivieren des Modems [32].

Weitere empfehlenswerte Software:

- AdAway - Unterbindet Werbung
- APG - OpenPGP Port
- DuckDuckGo - Auf privatsphäre bedachte Suchmaschine
- K-9 Mail - EMail Programm mit OpenPGP unterstützung
- Wi-Fi Privacy Police - unterbindet das unötige senden von WLAN-Verbindungsinformationen.

Alternative Betriebssysteme und Projekte:

- https://wiki.debian.org/Mobile
- http://maemo.org/intro/
- https://copperhead.co/android/
- https://blog.torproject.org/mission-improbable-hardening-android-security-and-privacy

10. Ausblick

Da sich Replicant 6.0 in einem laufendem Entwicklungsprozeß befindet wären monatliche Veröffentlichungen von Replicant Images hilfreich[25].
Die Entwicklung quelloffener BIOS Firmware macht auch für Smartphone SoC ihre Forschritte und könnte schon bald in greifbare nähe rücken [46][47]. Damit ließen sich grosse Teile ersetzen. Evtl. wäre dies auch für den gesamten Bootloader möglich. Dadurch würde ein Betriebssystem für Smartphones existieren, welches bis auf die BootROM auf freier Software basiert [8].
Eine weitere sinnvolle Anwendung könnte eine für ARM-Architekturen [48] optimierte Version von Tails, die über eine MicroSD des Samasung Galaxy S3 genutzt werden könnte [49].
Auf längere Sicht ist eine Portierung von Debian für ARM-Architekturen der vielversprechenste Ansatz [50][51]. Solange sich hier nichts grundlegenderes bewegt ist Replicant das am weitesten von proprietärer Firmware befreite Betriebssystem - zumindest was der Autor dieses Beitrags gefunden hat.
Aktuell hat Purism eine Crowdfunding-Kampagne zur Entwicklung eines angeblich freien Smartphonesërfolgreich beendet [52]. Laut der Webseite der Hersteller_innen soll das Smartphone einen freien Bootloader enthalten und neben einem ”befreiten”GPS auch Debian als Betriebssystem unterstützen. Es bleibt abzuwarten was an den Versprechungen dran ist, da Purism schon einmal ihre Nutzer_innen zu Gunsten einer Vermarktung ihrer Produkte belogen hat [53][54].
Interessant ist auch ein Kommentar von Seiten eines Replicant-Entwicklers dazu:
I’m maybe wrong, but ... Purism’s only interest to my eyes is into collecting bucks with found raising. They claim to be building the libre-est”hw available, but it has long revealed to be much less free than what we currently have already. And much more expensive. (see: found raising to build a librecomputer from scratch ... with i5s and i7s.. in it). Apart from that ... It could be interesting in a way ... But just like with fairphone, I believe that if their interest was really into making libre systems, the should’ve contacted the Replicant project to join efforts from the beginning, before the found-raising campaign. To me, purismßtands for pure (and expensive) lies”. Period. I wouldn’t bother too much about their proclaims ....

Literatur

[1] KÖGLER, N. F.: *Wenn Google das Smartphone fernsteuert*. http://www.zeit.de/digital/mobil/2011-03/Google-Android-Smartphone, 2011

[2] INC., Google: *Google Nutzungsbedingungen*. https://www.google.de/intl/de/policies/terms/regional.html, 2013

[3] K., Paul: *Replicant developers find and close Samsung Galaxy backdoor*. https://www.fsf.org/blogs/community/replicant-developers-find-and-close-samsung-ga 2014

[4] INC., Google: *An Update on Android Market Security*. https://googlemobile.blogspot.de/2011/03/update-on-android-market-security.html, 2011

[5] INC., Google: *Exercising Our Remote Application Removal Feature*. https://android-developers.googleblog.com/2010/06/exercising-our-remote-application.html, 2010

[6] WIKIPEDIA: *System-on-a-Chip*. https://de.wikipedia.org/wiki/System-on-a-Chip, 2017

[7] GNU: *Proprietäre Software*. https://www.gnu.org/philosophy/categories.de.html#ProprietarySoftware, 2017

[8] GNU: *Freie Software*. https://www.gnu.org/philosophy/categories.de.html#FreeSoftware, 2017

[9] FSF, Gnu: *Malware in Mobile Devices*. https://www.gnu.org/philosophy/malware-mobiles.html, 2017

[10] GOLEM: *Google sammelt Telefonprotokolle von Android-Geräten*. https://www.golem.de/news/ueberwachung-google-sammelt-gespraechsprotokoll html, 2016

[11] WIKIPEDIA: *IMSI-Catcher*. https://de.wikipedia.org/wiki/IMSI-Catcher, 2017

[12] REPLICANT: *Replicant status (Replicant 6.0)*. https://redmine.replicant.us/projects/replicant/wiki/ReplicantStatus#Replicant-60, 2017

[13] PROJECT, The L.: *LineageOS Android Distribution*. https://lineageos.org, 2017

[14] REPLICANT: *Freedom and privacy/security issues*. https://www.replicant.us/freedom-privacy-security-issues.php, 2017

[15] GNU: *Unfreie Software*. https://www.gnu.org/philosophy/categories.de.html#non-freeSoftware, 2017

[16] GNU, Fsf: *Freie Software. Was ist das?* https://www.gnu.org/philosophy/free-sw.de.html, 2017

[17] REPLICANT: *Galaxy S 3 (I9300) Installation*. https://redmine.replicant.

[25] da ein eigenständiges kompilieren des 60-70 GB grossen Quellcodes nur bedingt Replicant Nutzer_innen zumutbar ist [45].

us/projects/replicant/wiki/GalaxyS3I9300Installation, 2017

[18] REPLICANT: *replicant-6.0-i9300.zip*. https://ftp-osl.osuosl.org/pub/replicant/images/replicant-6.0/0002/images/i9300/replicant-6.0-i9300.zip, 2017

[19] REPLICANT: *replicant-6.0-i9300.zip.asc*. https://ftp-osl.osuosl.org/pub/replicant/images/replicant-6.0/0002/images/i9300/replicant-6.0-i9300.zip.asc, 2017

[20] REPLICANT: *recovery-i9300.img*. https://ftp-osl.osuosl.org/pub/replicant/images/replicant-6.0/0002/images/i9300/recovery-i9300.img, 2017

[21] REPLICANT: *recovery-i9300.img.asc*. https://ftp-osl.osuosl.org/pub/replicant/images/replicant-6.0/0002/images/i9300/recovery-i9300.img.asc, 2017

[22] REPLICANT: *adb*. https://ftp-osl.osuosl.org/pub/replicant/images/replicant-6.0/0002/tools/adb, 2017

[23] REPLICANT: *adb.asc*. https://ftp-osl.osuosl.org/pub/replicant/images/replicant-6.0/0002/tools/adb.asc, 2017

[24] REPLICANT: *heimdall*. https://ftp-osl.osuosl.org/pub/replicant/images/replicant-6.0/0002/tools/heimdall, 2017

[25] REPLICANT: *heimdall.asc*. https://ftp-osl.osuosl.org/pub/replicant/images/replicant-6.0/0002/tools/heimdall.asc, 2017

[26] REPLICANT: *Replicant Hardware*. https://redmine.replicant.us/projects/replicant/wiki/GalaxyS3I9300, 2017

[27] REPLICANT: *Graphics*. https://redmine.replicant.us/projects/replicant/wiki/Graphics, 2017

[28] REPLICANT: *Graphics*. https://redmine.replicant.us/projects/replicant/wiki/Graphics#Enabling-llvmpipe-as-software-renderer, 2017

[29] REPLICANT: *Samsung-RIL*. https://redmine.replicant.us/projects/replicant/wiki/Samsung-RIL, 2017

[30] REPLICANT: *libsamsung-ipc*. https://redmine.replicant.us/projects/replicant/wiki/Libsamsung-ipc, 2017

[31] REPLICANT: *A new Replicant 6.0 release*. https://blog.replicant.us/2017/09/a-new-replicant-6-0-release/, 2017

[32] REPLICANT: *Disabling the Modem*. https://redmine.replicant.us/projects/replicant/wiki/ModemDisable, 2017

[33] TECHNOETHICAL: *Technoethical N150 Mini Wireless USB Adapter for GNU/Linux-libre*. https://tehnoetic.com/adapters/tehnoetic-wireless-adapter-gnu-linux-libre-tet- 2017

[34] REPLICANT: *RepWifiApp_v0.5.apk*. https://redmine.replicant.us/attachments/download/1520/RepWifiApp_v0.5.apk, 2017

[35] REPLICANT: *RepWifiApp_v0.5.apk.sig*. https://redmine.replicant.us/attachments/download/1519/RepWifiApp_v0.5.apk.sig, 2017

[36] REPLICANT: *F-Droid*. https://redmine.replicant.us/projects/replicant/wiki/FDroid, 2017

[37] FOSS: *F-Droid*. https://f-droid.org/, 2017

[38] TAILS: *Privacy for anyone anywhere*. https://tails.boum.org/, 2017

[39] OSMAND: *OsmAnd Karten*. http://download.osmand.net/rawindexes/, 2017

[40] FREIFUNK: *Freifunk*. https://freifunk.net, 2017

[41] WIKIPEDIA: *Passwort*. https://de.wikipedia.org/wiki/Passwort, 2017

[42] SYSTEMS, Whisper: *Signal Download*. https://signal.org/android/apk/, 2017

[43] TORPROJECT: *Anonymity Online*. https://www.torproject.org, 2017

[44] WIKIPEDIA: *Metadaten digitaler Bilder*. https://de.wikipedia.org/wiki/Metadaten#Metadaten_digitaler_Bilder, 2017

[45] REPLICANT: *Replicant source code*. https://redmine.replicant.us/projects/replicant/wiki/ReplicantSourceCode, 2017

[46] COREBOOT: *ARM*. https://www.coreboot.org/ARM, 2017

[47] COREBOOT: *Exynos5*. https://www.coreboot.org/Exynos5, 2017

[48] WIKIPEDIA: *ARM-Architektur*. https://de.wikipedia.org/wiki/ARM-Architektur, 2017

[49] TAILS: *ARM Platform*. https://tails.boum.org/blueprint/ARM_platforms/, 2017

[50] DEBIAN: *Debian on mobile devices*. https://wiki.debian.org/Mobile, 2017

[51] DEBIAN: *ARM Ports*. https://www.debian.org/ports/arm/, 2017

[52] PURISM: *English 5 – A Security and Privacy Focused Phone*. https://puri.sm/shop/librem-5/, 2017

[53] SELF.LINUX reddit: *On the LibreM laptop; Purism doesn't believe in user freedom, and doesn't care about your privacy.* https://www.reddit.com/r/linux/comments/3anjgm/on_the_librem_laptop_purism_doesnt_believe_in/, 2015

[54] DEVELOPER phoronix c.: *Coreboot Developer: Purism Doesn't Deliver On Libre Firmware*. https://www.phoronix.com/scan.php?page=news_item&px=Coreboot-Dev-Purism, 2015