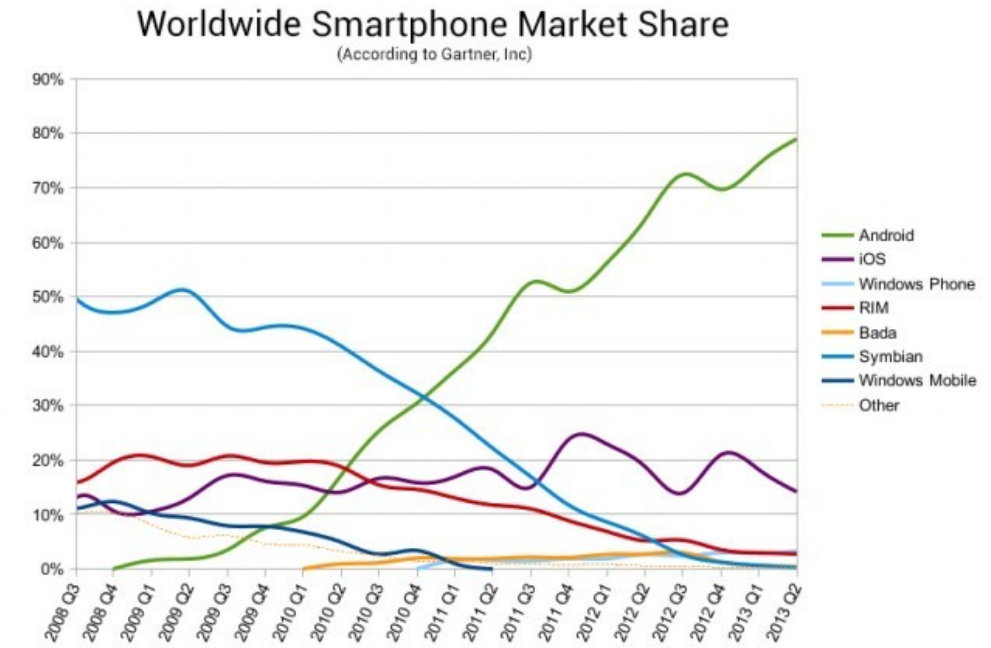
# Android ohne Google

Don't be evil.



# Agenda

- Android Ökosystem
- Google Cloud → vertrauens^Weigener Server
- Demo
- VPN
- Gerät rooten/Cyanogenmod

# Was Google bietet

- Playstore
- Kalender/Kontakte/GMail
- ~~Talk~~Hangouts/Google+
- Youtube/Picasa/Maps
- Backup/Google Drive
- Sprachsuche/-erkennung

# Was Google dem Entwickler bietet

- Google Play services
  - In-App-Bezahlung
  - Werbung
- Google analytics
- Google Cloud Messaging

# Was daran problematisch ist

- GApps sind nicht frei
- Schnittstellen/TOS der Clouddienste
- Bedingungen der Open Handset Alliance
- AOSP Apps verwaisen, Ersatz durch Gapps
  - Email → Gmail
  - Gallery → Picasa/Google+
  - SMS → Hangouts
  - Browser → Chrome

# Warum ohne Google?

- Google will Deine Daten.
- NSA
- Google will die Herrschaft über Android
- Cyanogenmod wegen
  - Datenschutz (Pdroid)
  - Kein Facebook/Whatsapp/$Datenkrake vorinstalliert

# Möglichkeiten ohne Root oder Custom ROM

- Anderer App-Store
- Eigene Cloud-Dienste
  - Kontakte
  - Kalender
  - Storage
  - Mail
  - Chat
- VPN (ipsec)

# F-Droid

- Appstore der FSF
- Eigenes Repository möglich
  - Buildsystem zur Erstellung von APKs aus Quellen
- Installation:
  - aus fremden  Quellen erlauben
  - Von http://f-droid.org herunterladen

# Kontakte/Kalender

- Schnittstelle: Sync Adapter (ab Android 2.2)
- ActiveSync
  - MS Standard, Patente
  - Basiert auf WebDAV
- CardDAV/CalDAV
  - Apple Vorschlag, Standardisierung über RFC
  - Basiert auf WebDAV
- Localprovider

# Eigener Server

- OwnCloud (Files, CalDAV/CardDAV)
- Tine 2.0 (Files, CalDAV/CardDAV, ActiveSync)
- Seafile (Files, proprietäres Protokoll)
- Jabber Server (RFC 6120-6122, 3923,...)
- SIP Server
- Racoon/StrongSwan/OpenSwan, OpenVPN

# Storage

- OwnCloud/Tine 2.0
  - Apache + PHP → WebDAV
- Seafile
  - Python + C
- Android Clients sind ()/“§&$(/“§$&(„§/$&

# Funktionierende Kombinationen

- Kalender, Kontakte:
  - Tine2.0 + Active Sync
  - OwnCloud + CardDAV Sync + CardDAV Sync Adapter
- Dateien
  - OwnCloud + Client
  - Seafile + Client

# Demo

- Xperia Pro in Auslieferungszustand
  - F-Droid
  - CA installieren
  - Kalender + Kontakte sync
- Tine 2.0
- OwnCloud

# VPN

- IPSEC
  - Fritzbox
  - Linuxkiste mit racoon
- OpenVPN
- Server: statische IP oder dyndns o.ä.

# IPSec zu FritzBox

- Bei AVM gut dokumentiert, siehe Links
- Config-Datei erstellen mit Windows-Programm, läuft problemlos in wine
- Hochladen und Aktivieren
- Android ab 4.0.x
  - Ipsec Xauth PSK
  - Ipsec-Id=“Gruppenname“, PSK abtippen/einfügen

# IPsec zu Linuxserver

- Racoon installieren
- Server(pem)- und Clientzertifikat(p12) erstellen
- Ggf Ports 4500 und 500 UDP weiterleiten
- Netfilter Regeln eintragen:

```
iptables -t nat -A POSTROUTING ! -p esp -s $SHADOWNET/24 -j SNAT --to-source $SERVER_IP

iptables -t mangle -A FORWARD -p tcp --tcp-flags SYN,RST SYN -j TCPMSS --set-mss 552
```

# Ipsec zu Linuxserver IP 1.2.3.4

```
path certificate "/etc/racoon/certs";
log debug;
timer {
        natt_keepalive 45 sec;
}
listen {
        lsakmp 1.2.3.4[500];
        isakmp_natt 1.2.3.4[4500];
}
remote anonymous {
        exchange_mode aggressive,main;
        support_proxy on;
        ike_frag on;
        my_identifier fqdn "myserver.dyndns.org";
        certificate_type x509
            "myserver.dyndns.org_ipsec.crt"
            "myserver.dyndns.org_ipsec.pem";
        ca_type x509 "myserver_ca.crt";
        passive on;
        proposal_check strict;
        generate_policy on;
        nat_traversal force;
        dpd_delay 20;
        esp_frag 552;
        proposal {
                encryption_algorithm aes256;
                hash_algorithm sha1;
                authentication_method xauth_rsa_server;
                dh_group modp1024;
        }
}

sainfo anonymous {
        encryption_algorithm aes256;
        authentication_algorithm hmac_sha1;
        compression_algorithm deflate;
}

mode_cfg {
        auth_source system;
        conf_source local;
        accounting system;
        network4 $SHADOWNET;
        netmask4 255.255.255.0;
        dns4 $MYDNSSERVER;
}
```

# OpenVPN

- Verschlüsselter IP über UDP/TCP-Tunnel
- Server einfach aufzusetzen
- Android ab 4.0.x ziemlich einfach
- OpenVPN-Client aus F-Droid-Store
- Auth über Zertifikat
  - Als .p12 in root der sdcard legen
  - Einstellungen → Sicherheit → Von SD-Karte inst.
- Evtl. Problem: tun.ko

# Demo

- Motorola Defy zum „freien“ Smartphone machen
  - Rooten
  - Second init
  - CM flashen
  - F-Droid installieren
  - Apps

# Rooten (Defy)

- Mehrere Varianten:
  - SuperOneClick.exe, braucht Windows+Motorola-Treiber
  - Gingerbreak.apk
  - Manuell
    - Benötigt adb aus Android-SDK-Tools
    - Binaries (psneuter, busybox, su, SuperUser.apk) aus SuperOneClick-Installer
    - http://www.pocketables.com/2011/06/how-to-manually-root-almost-any-android-device.html

# Cyanogenmod installieren (Defy)

- Anleitung dreimal gründlich durchlesen
- Akku >70%
- SndInit.apk und cm10 besorgen
- SndInit.apk installieren und ausführen, reboot
- Reboot in recovery (Leiser-T. bei blauer LED)
- Backup, Wipe (Factory Reset)
- Zip von SD-Card installieren

# Gute freie Apps

- K9 Mail
- OSM And (Ofllinekarte + Navi)
- Ghost commander (Filemanager)
- Wordpress Client
- (VX)Connectbot (SSH Client)
- Firefox
- Cool Reader (Ebook reader)
- APV PDF Viewer
- AntennaPOD (Podcast)
- Apollo (mp3 player, in CM dabei)
- VIM
- XBMC Remote
- Zxing (Barcode scanner)
- Yaaic (irc)
- Xabber (XMPP)

# Ohne Ersatz

- Google Cloud Messaging
- APIs
- App-Backup
- Spracherkennung (On-/Offline)

# Links

- http://arstechnica.com/gadgets/2013/10/ googles-iron-grip-on-android-controlling-open-source-by-any-means-necessary/
- https://prism-break.org/
- http://f-droid.org
- http://www.cyanogenmod.org
- http://www.avm.de/de/Service/Service-Portale/Service-Portal/VPN_Interoperabilitaet/16518.php