Die fbox Familie

- Hardware
- Firmware
- Firmware-Update und Modifikation
- DONE
- TODO
- Mitmachen

Hardware

- Prozessor: TI AR7 Dual Core
  - MIPS R4K Prozessor
  - TI DSP
- Flash 4MB
- SDRAM 8/16/32 MB je nach Modell
- Infineon ISDN/POTS/ab Chipset
- WLAN TI VLYNQ
- serielle Konsole auf Hauptplatine
- MIPS EJTAG

Firmware

- TI Platform Bootloader ADAM2
- Linux Kernel
- Treiber
- Linux Userland
- AVM Userland

ADAM2

- serieller Prompt
- recovery über Netz via modifiziertem FTP
- environment Variablen zur Konfiguration
  - auch vom Linux-Kernel aus les-/schreibbar

Linux Kernel

- Montavista Linux 2.4.17
- TI “NSP”
  - TI-Anpassungen für Prozessor
  - TI USB-Slave-Treiber
  - TI WLAN-Treiber
  - TI DSL/ATM-Treiber
- Unsaubere Copyrights, die AVM noch teilweise zu klären hat

Treiber

- WLAN und DSL
  - proprietäre TI-Binärtreiber
- USB-Slave
  - proprietärer TI-Slavelayer
  - AVM CDC-Ethernettreiber (Source?)
- CAPI
  - 1 Interface für ISDN-Anschluss
  - 1 Interface für POTS-Anschluss
  - 1 Interface für die ab-Ports
  - 1 Pseudo-Interface als VOIP-Schnittstelle
  - kein Fax-Support auf der Box

Treiber

- TFFS (AVM Tiny Flash File System)
  - erweitert TI ADAM2 environment
  - stellt Konfigdateien als character device zur Verfügung
    - keine Seeks
    - Dateien können nur komplett geschrieben werden
  - arbeitet auf zwei mtd-Partitionen
    - Transaktionsicherheit auch bei Überlauf
  - Source zugesagt
  - Struktur ist aber bereits reverse engineered

Userland

- uClibc 0.9.26 unbekannter Konfiguration
  - anscheinend kompatibles buildroot existiert aber
- busybox
  - Version ist alt genug, um einen Bug in tar zu haben, der es erfordert, eigene Firmware-Images mit altem busybox-tar zu packen

AVM Userland

- dsld
  - DSL-Verbindung inkl. ATM autoconfig
  - PPPOE
  - auf BSD basierender IP-Filter
  - NAT
  - Portforwarding
  - Anbindung an TI-Treiber über ATM-Interface
  - Anbindung an Linux-Stack über TAP-Device

AVM Userland

- multid
  - DHCP-Server
  - DHCP-Client
  - DNS-Proxy
  - DDNS-Client (noch inoffiziell)
  - konfiguriert beim Start das Netzwerk auf Grundlage der ar7.cfg

AVM Userland

- telefon
  - Telefonanlagensoftware aus der Fritz!X
  - auf Linux portiert
  - greift über CAPI auf Interfaces inkl. VOIP zu
- voipd
  - SIP Implementierung
  - basiert u.a. auf libosip
  - stellt Services über virtuelles CAPI-Interface zur Verfügung

AVM Userland

- ctlmgr
  - zentrale Schnittstelle für
    - Konfig (ar7.cfg, void.cfg etc.)
    - Status (DSL-Parameter, SIP-Registrierung)
    - Management (reboot)
- webcm
  - CGI inkl. einfachem Skripting
  - nutzt ctlmgr zur Statusabfrage und Konfigmanipulation
- websrv
  - einfacher httpd

AVM Userland

- capiovertcp_server
  - stellt das ISDN-CAPI-Interface über Netz zur Verfügung
  - benutzt das bei Bluetooth für CAPI genutzte Protokoll CMTP über TCP
  - Proof-of-Concept Client existiert
- run_clock
  - Betriebstundenzähler (?)
- sntpclient

Firmware Upgrade und Modifikation

- Updates sind tar-Dateien
  - müssen wegen busybox-Fehler auch mit altem busybox-tar gepackt werden
- Bestandteile
  - eigentliches Updateskript liegt im tar!
  - ermöglicht Pseudoupdates, die z.B. telnetd nur starten
  - Flashinhalt liegt als kernel.image und filesystem.image (squashfs-Image) im tar
  - einfach Modifikation möglich

DONE

- kompatibles uClibc-buildroot
  - Konfiguration geraten und durch Vergleich von vorhandenen Symbolen bestätigt
- damit eigene Binaries möglich
- strace, capi Tracer etc.
- nfs-Module für den AVM-Kernel
  - mittles pivot_root aus frühem Startskript ist ein quasi-nfsroot möglich

TODO

1. DSL + Netzwerk ohne dsld
   - netfilter in den Kernel
   - wie geht das mit ATM?
2. Zugriff auf Telefonie-Hardware
   - CAPI-Erweiterungen reverse engineering
   - eigener Treiber
3. freie Telefonie/VOIP-Software portieren
4. eigenes Konfigurationssystem

Mitmachen

- WIKI
  - http://www.wehavemorefun.de/fritzbox
- Mailinglist
  - http://lists.trilos.net/mailman/listinfo/fritz
- VOIP Webforum
  - http://www.ip-phone-forum.de/forum/index.php?c=31
- Nutznetz
  - de.comm.technik.dsl