Repurposing Gadgets

Daniel Maslowski
Agenda

- Introduction
- Gadgets and Ideas
- Tools and Utilities
- Tinkering
Introduction
Hello, I am Daniel :-)

Work and education
- IT security and computer science
- software engineer
- infrastructure and web
- apps, UIs, ecommerce

Open Source contributions
- hardware and firmware
- operating systems
- software distributions
- reverse engineering
Gadgets and Ideas
Wireless Storages

... are just networked devices with storage

old ideas
- MCU running a small application, sometimes RTOS
- SoC, Arm or MIPS, running Linux
- built-in SD card reader

new ideas
- access point for devices in your NoT (Network of Things)
- MQTT broker for controlling things, e.g., via SUSI AI
Network Video Recorders (NVRs)

old ideas
- essentially storage with more connectors
  - USB, HDMI, ethernet
  - built-in network switch
  - analog video input
- SoC, mostly Arm, running Linux

new ideas
- little general purpose computer with web browser
- home theatre / movie player
IP cameras

Essentially, these are just camera sensors attached to some SoC that is running Linux, with Wi-Fi and/or ethernet modules and often SD card readers.

They typically feature two motors to rotate and tilt, sometimes a speaker and a microphone for two-way audio communication.

OpenIPC project - https://openipc.org/
Tools and Utilities
Hardware

- network cables and switch
- wireless access point
- SPI flash programmer
- USB serial converter
- dupont wires and probes
- soldering equipment
- screwdrivers
u-root

A universal root filesystem

- many small tools
- all open, meant for studying and understanding
- easily portable
- written in Go

https://u-root.org/
Welcome to u-root!

u-root

4.214060 | cgroup: Unknown subsys name 'net_cls'
4.214060 | cgroup: Unknown subsys name 'net_cls'
4.217296 | cgroup: Unknown subsys name 'hugeltb'
4.217296 | cgroup: Unknown subsys name 'hugeltb'

Framebuffer resolution: 640 480 640 3

spring();
break;
centre

- DHCP server
- TFTP server
- simple binary, written in Go
- easy to run on your laptop

https://github.com/Harvey-OS/go/tree/main/cmd/centre
Tinkering
IP Camera Teardown
Astronaut Teardown
NVRs from inside
PSLab as a Logic Analyzer
Adding Missing Components
Serial and U-Boot

0 Storage Device(s) found
i:0, No usb storage device found!
Press CTRL-C to abort autoboot in 0 seconds
16384 KiB hi_fmc at 0:0 is now current device
CFG_BOOT ADDR:0x0 argc 2 argv[0] logload
### h264dvr.jpg UbootLogload complete:bytes oadaddr0x84000000 loaded to
0x8dc00000
### h264dvr.jpg UbootLogload complete: 32878 bytes loaded to 0x8dc00000
jpeg decoding ...
<<addr=0x8dc00000, size=0xb5f9, vbuf=0x8dd00000>>
PicType: 3 ,Output Addr, Y: 8dd00000,UV: 8dd7b800
<<1mgwidth=800, imgheight=600, linebytes=832>>
decode success!!!!
decode jpeg success.
decode jpeg!
srcAddr 0x82000000, dstAddr 0x81000000
find squashfs file: name bin, start block 0, offset 2653, type 1
find squashfs file: name boot, start block 0, offset 2757, type 1
read inode: name boot, sb 0, of 2757, type 1
find squashfs file: name zImage.img, start block 0, offset 2685, type 2
read inode: name zImage.img, sb 0, of 2685, type 2
### FS load complete: 2454195 bytes loaded to 0x81000000
## Booting kernel from Legacy Image at 81000000 ...
  Image Name: Linux-4.9.37
  Image Type: ARM Linux Kernel Image (uncompressed)
  Data Size: 2454131 Bytes = 2.3 MiB
  Load Address: 80000000
  Entry Point: 80000000
  Loading Kernel Image ... OK
OK
Starting kernel ...
U-Boot Shell

System startup............
System startup


Check Flash Memory Controller v100 ... Found
SPI Nor(cs 0) ID: 0xef 0x40 0x18
eFlashType: 3.
Flash Name: XM W25Q128FV, W25Q128JV{0xEF4018}, 0x10000000.
@ifmc_spi_nor_probe(), XmSpiNor ProtMgr probe(): OK.
@ifSpiNor_enableQuadMode(), Disable Quad Failed, SRx: [2, 0x3F].
@ifSpiNor_enable4ByteAddrMode(), isn't support 4-byte mode.
Block:64KB Chip:16MB Name:"XM W25Q128FV,W25Q128JV"
CONFIG CLOSE_SPI .BPIN 4IO = y.
read->iftype[0: STD, 1: DUAL, 2: DIO, 3: QUAD, 4: QIO]: 1.
Current level[0], lock_level_max:7.
unlock all.
SRx val: {{1, 0x2}, [1, 0x3F], [1, 0xE0], [0, 0x0]}.
SPI Nor total size: 16MB
In:  serial
Out: serial
Err: serial
USB: scanning bus for devices... 1 USB Device(s) found
  Storage Device(s) found
USB: scanning bus for devices... 1 USB Device(s) found
  Storage Device(s) found
i:0, No usb storage device found!
Press CTRL-C to abort autoboot in 2 secondshisilicon # <INTERRUPT>
hisilicon # <INTERRUPT>
hisilicon # whee :)
CTRL-A Z for help | 115200 8N1 | NOR | Minicom 2.7.1 | VT102 | Online 0:0 | ttyUSB0
U-Boot TFTP

hisilicon # sf read 0x82000000 0x0 0x1000000
hisilicon # tftp 0x82000000 firmware.bin 0x1000000
Hisilicon ETH net controller
MAC: 00-0B-3F-00-00-01
eth0 : phy status change : LINK=DOWN : DUPLEX=FULL : SPEED=100M
eth0 : phy status change : LINK=UP : DUPLEX=FULL : SPEED=100M
TFTP to server 192.168.1.12; our IP address is 192.168.1.10
Upload Filename 'firmware.bin'.
Upload from address: 0x82000000, 16.000 MB to be send ...
Uploading: # [ Connected ]
************************************************************************** [ 2.888 MB]
************************************************************************** [ 5.752 MB]
************************************************************************** [ 8.616 MB]
U-Boot Kernel Commandline

anyka$ setenv bootargs 'console=ttySAK0,115200n8 root=/dev/mtdblock4 rootfstype=squashfs
init=/sbin/init mem=64M memsize=64M single'

anyka$ printenv
    backuppage=ffffffff
    baudrate=115200
    boot_normal=readcfg; run read kernel; bootm ${loadaddr}
    bootargs=console=ttySAK0,115200n8 root=/dev/mtdblock4 rootfstype=squashfs
    init=/sbin/init mem=64M memsize=64M single

... Environment size: 979/4088 bytes

anyka$ saveenv

Saving Environment to SPI Flash...
Env save done OK

anyka$ reset
    resetting...
    heartbeat = 1

... Starting kernel ...

Uncompressing Linux... done, booting the kernel.
Anyka Linux Kernel Version: 2.6.02
Booting Linux on physical CPU 0
Linux version 3.4.35 (maema-PC) (gcc version 4.8.5 (anyka (gcc-4.8.5 + binutils-2.24 + ulclibc-0.9.33.2)(28170223))) #19 Fri Oct 18 11:21:47 CST 2019
CPU: ARM926EJ-S [41069265] revision 5 (ARMv5TEJ), cr=80053177

... Freeing init memory: 100K
-/bin/sh: id: not found
welcome to file system
[root@(none) ~]# ls
bin  dev  etc  ext  init  lib  mnt  mvs  proc  sbin  sys  tmp  usr  var
[root@(none) ~]#
No init, just insmod

[root@(none) ~]# insmod /ext/modules/b188fu.ko
RTL871X: module init start
RTL871X: rlt8188fu v4.3.23.1 16377.20151216
RTL871X: build time: May 31 2018 17:23:04
usbscore: registered new interface driver rlt8188fu
RTL871X: module init ret=0
[root@(none) ~]# insmod /mvs/modules/otg-hs.ko
usbs-host usbs-host: Anyka usbs host controller
usbs-host usbs-host: new USBS bus registered, assigned bus number 1
usbs-host usbs-host: lrd 18, lo mem 0x28200000
usbs usbs1: New USBS device found, idVendor=1d6b, idProduct=0002
usbs usbs1: New USBS device strings: Mfr=3, Product=2, SerialNumber=1
usbs usbs1: Product: Anyka usbs host controller
usbs usbs1: Manufacturer: Linux 3.4.35 usbs-host
usbs usbs1: SerialNumber: Anyka usbs host controller
hub 1-0:1.0: USB hub found
hub 1-0:1.0: 1 port detected
usbs otg-hs controller driver initialized
usbs 1-1: new high-speed USBS device number 2 using usbs-host
usbs 1-1: New USBS device found, idVendor=0bda, idProduct=179
usbs 1-1: New USBS device strings: Mfr=1, Product=2, SerialNumber=3
usbs 1-1: Product: 802.11n
usbs 1-1: Manufacturer: Realtek
usbs 1-1: SerialNumber: 00084c000001
RTL871X: hal com config channel plan chplan:9x20
RTL871X: rtw_ndev_init[wlan0] ifmac_addr=7c:a7:b0:55:5a:f8
[root@(none) ~]# ifconfig -a
  lo    Link encap:Local Loopback
        LOOPBACK    MTU:16436    Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
  wlan0  Link encap:Ethernet  HWaddr 7c:a7:b0:55:5a:f8
        BROADCAST MULTICAST    MTU:1500    Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
u-root on a Wireless Storage

```
root@airdisk:~# chroot mipsle/ /bin/sh
/# ls -l
Exception: exec: "ls": executable file not found in $PATH
[TTY], line 1: ls -l
/# paths=/bin $@paths
/# ls -l
drwxr-xr-x 1001 1001 0 Sep 15 20:26 bbin
drwxr-xr-x 1001 1001 0 Sep 15 20:18 bin
drwxr-xr-x 1001 1001 0 Apr 22 18:02 dev
drwxr-xr-x 1001 1001 0 Sep 15 20:18 etc
Lrwxrwxrwx root 0 9 Sep 15 20:18 init -> bbin/init
drwxr-xr-x 1001 1001 0 Apr 22 18:02 lib64
drwx------ root 0 0 Sep 15 19:50 root
drwxr-xr-x 1001 1001 0 Apr 22 18:02 tcz
drwxrwxrwx 1001 1001 0 Apr 22 18:02 tmp
drwxr-xr-x 1001 1001 0 Apr 22 18:02 ubin
drwxr-xr-x 1001 1001 0 Apr 22 18:02 usr
drwxr-xr-x 1001 1001 0 Apr 22 18:02 var
/# cat /etc/resolv.conf
nameserver 8.8.8.8
/# uname -a
Linux airdisk 3.10.14+ #2 Tue Sep 15 20:03:49 CST 2015 mips (none)
/#
```
u-root on an NVR
Thanks! Questions?
Extras
Fun

astronaut protocol

SanDisk Media Drive disco