Kindle3 hacking

Pavel Růžička <ruza@ruza.eu>

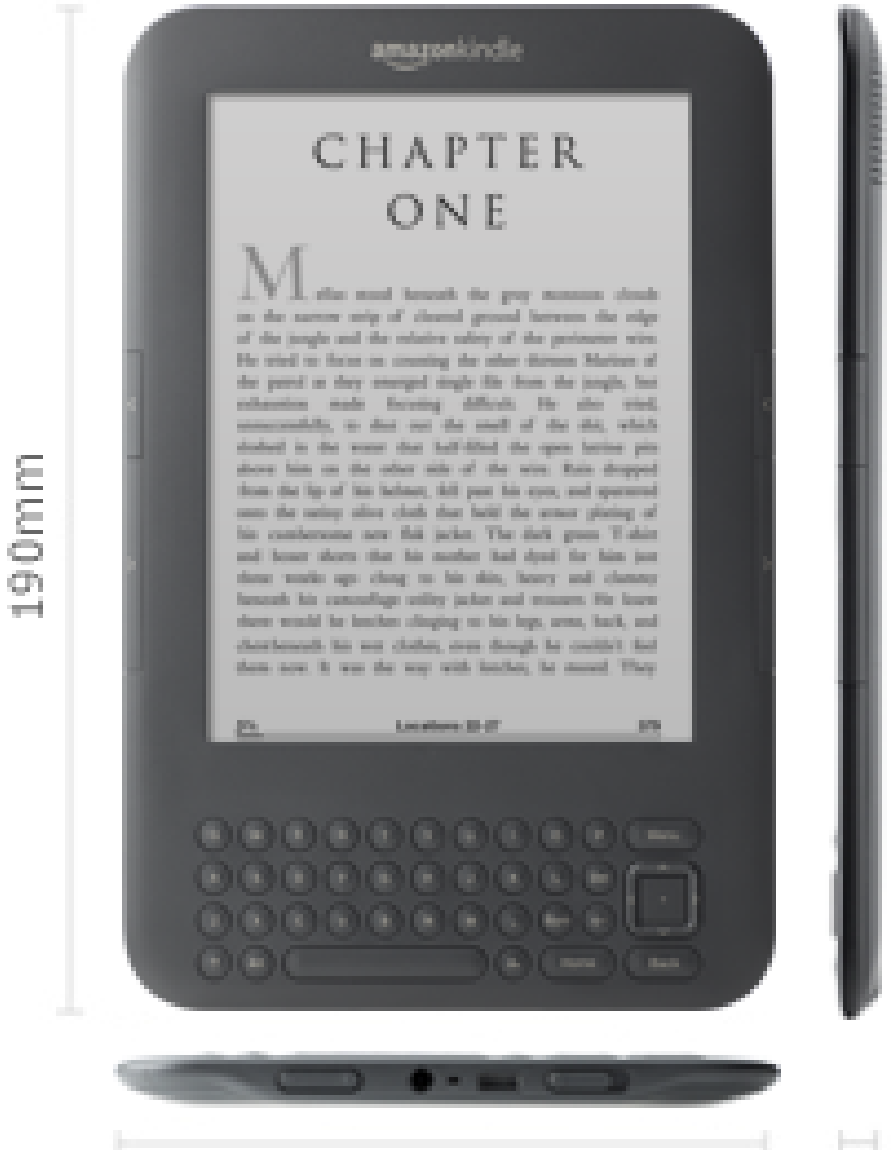
Brmlab
hackerspace Prague
Lightning talks

April 2012

Table of Contents

Table of Contents

Amazon Kindle



- CPU: ARMv6
- Hardware : Amazon MX35 Luigi Board
- BogoMIPS : 255.59
- Features : swp half thumb fastmult vfp edsp java
- Hardware : Amazon MX35 Luigi Board
- RAM : 256MB

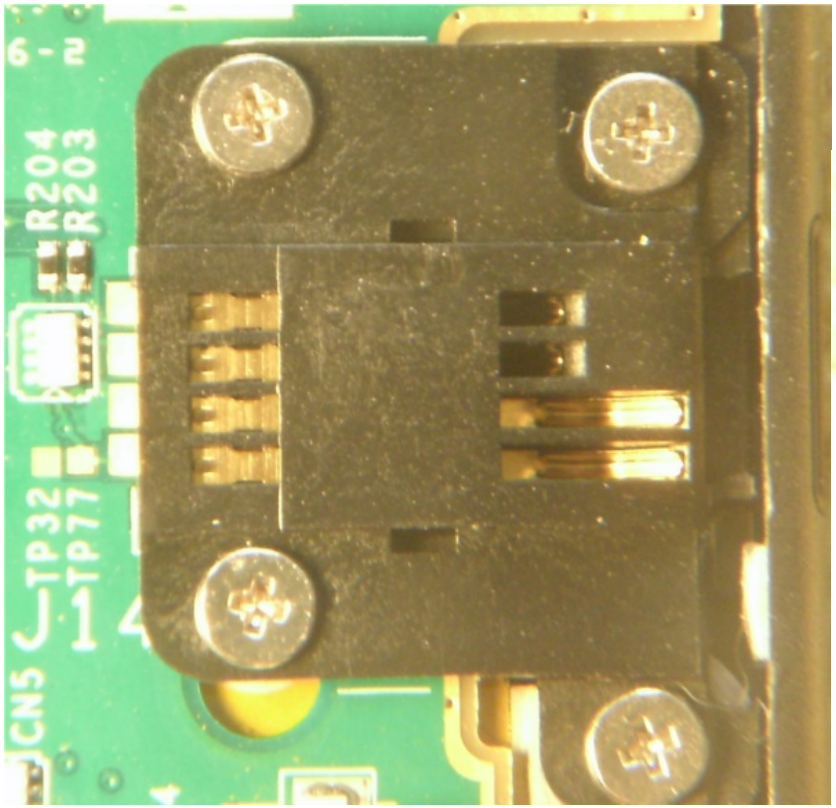
brmlab hackerspace prague

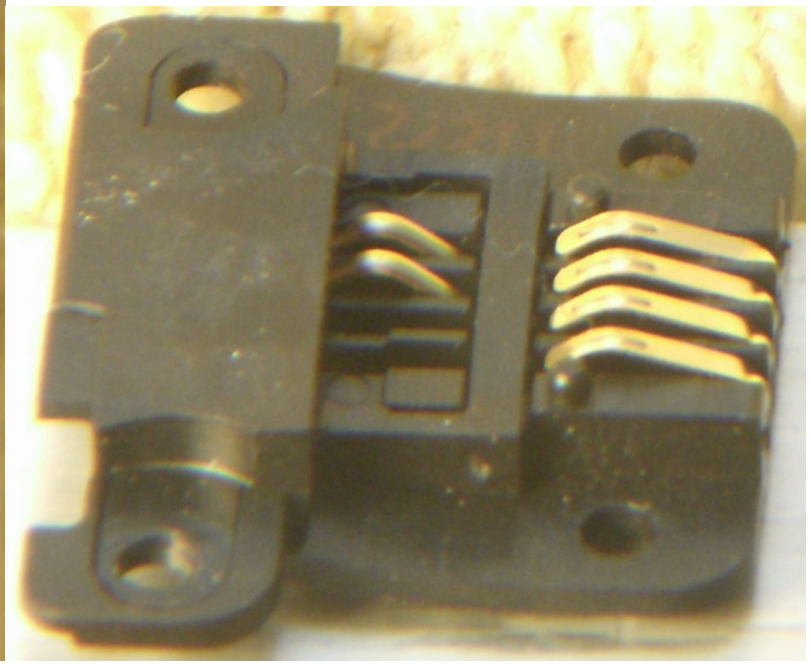
Hmm?

Hardware


WiFi
Codec &
Speaker Driver
SIM Card
3G Modem
Speaker
Battery
Speaker
amazonkindle
Model No.:S11GTSF01A
Rating:3.7V 1750mAh
6.47Wh Lithium Polymer
MADE IN CHINA BY LICO
© 2010 BlogKindle.com

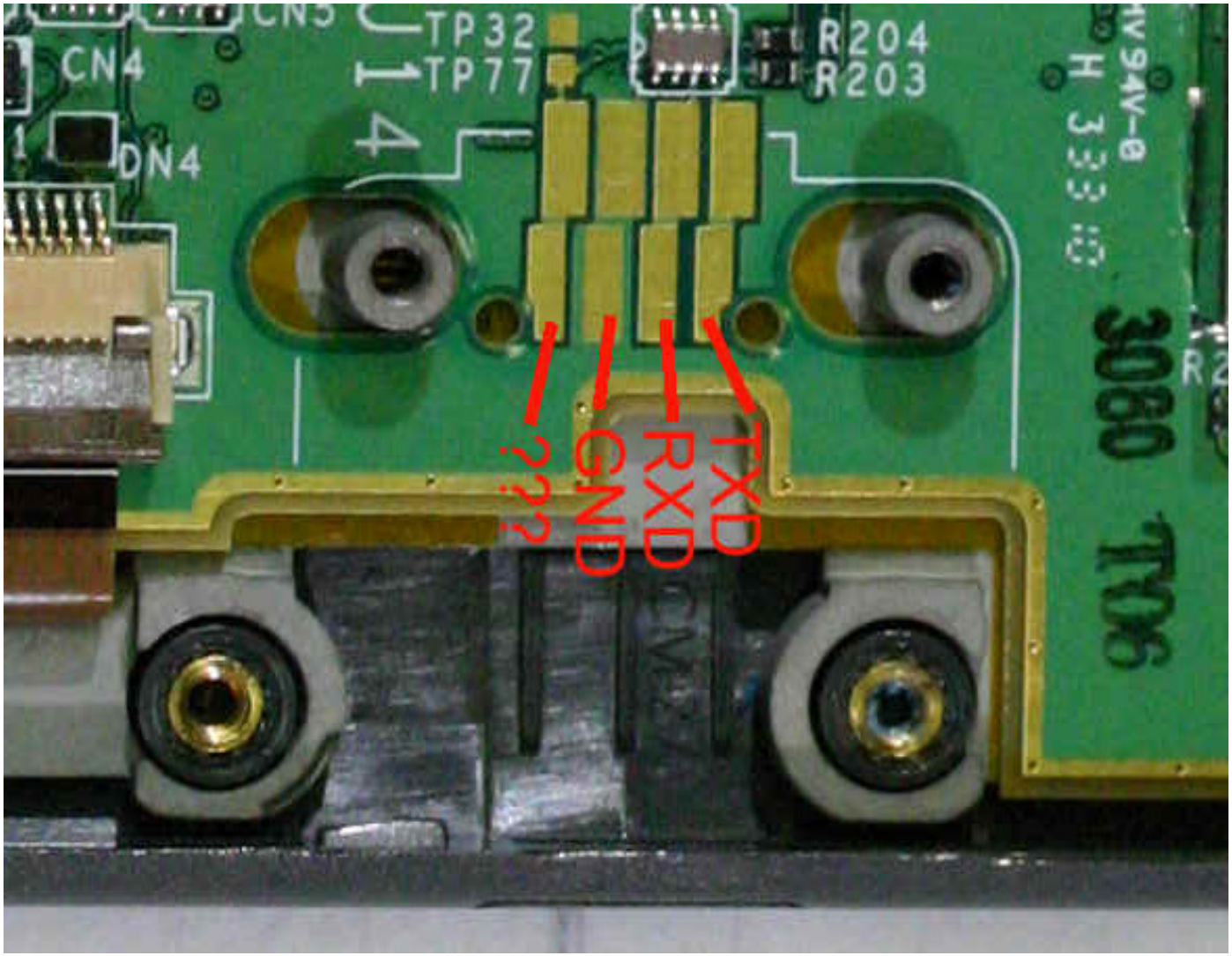
Connector, female



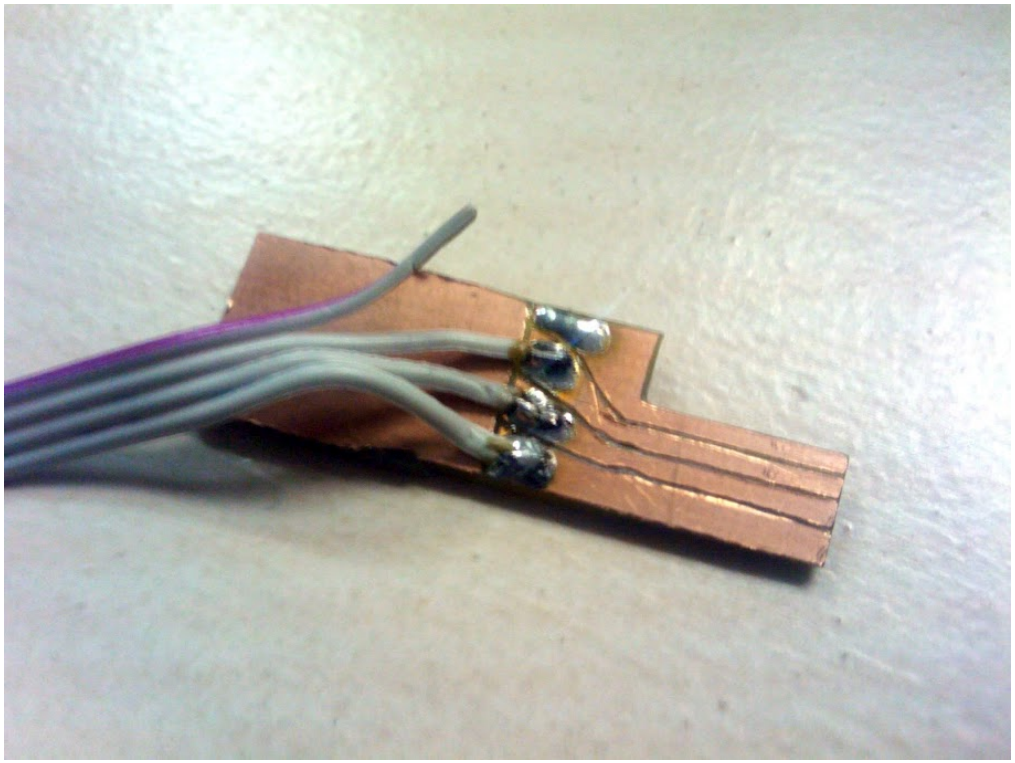


business :)

female pinout

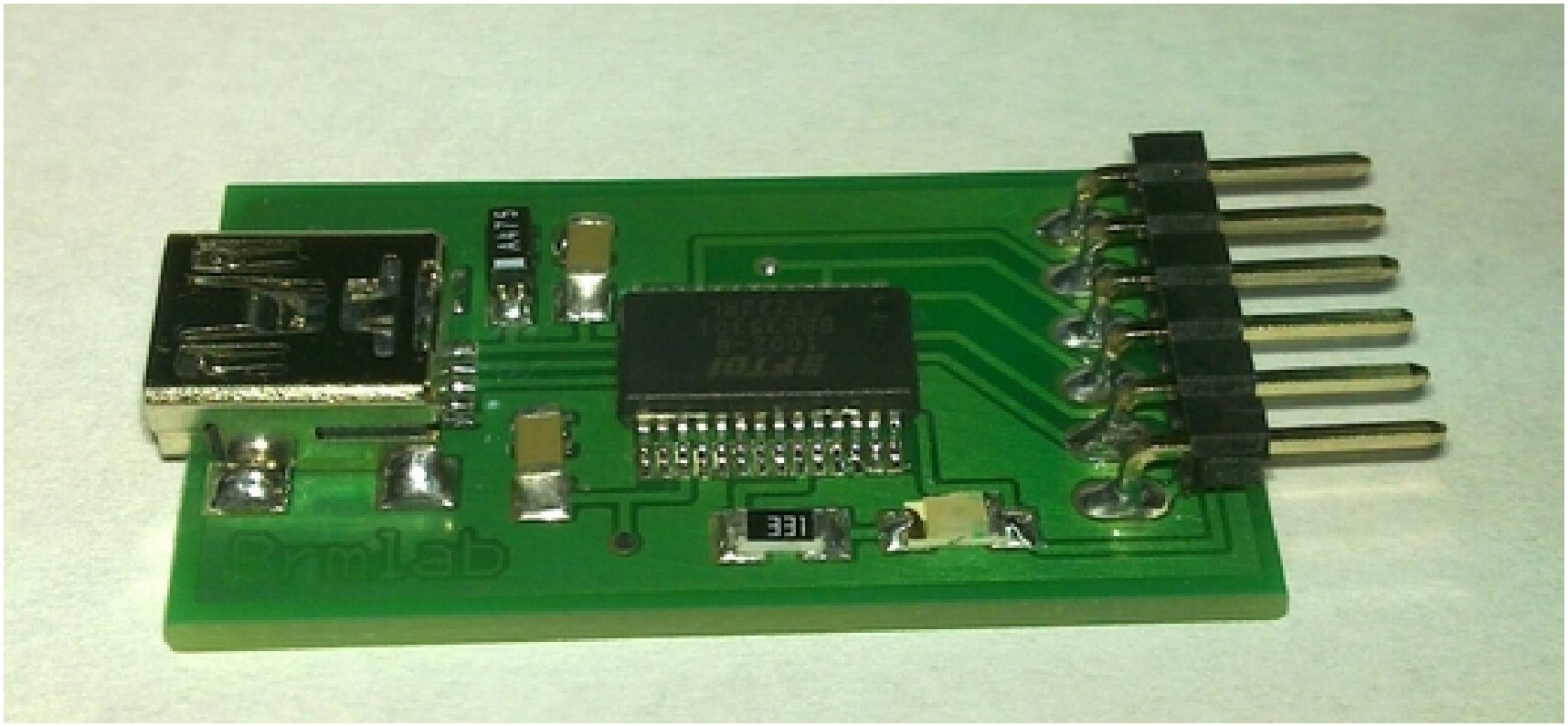


Connector, male



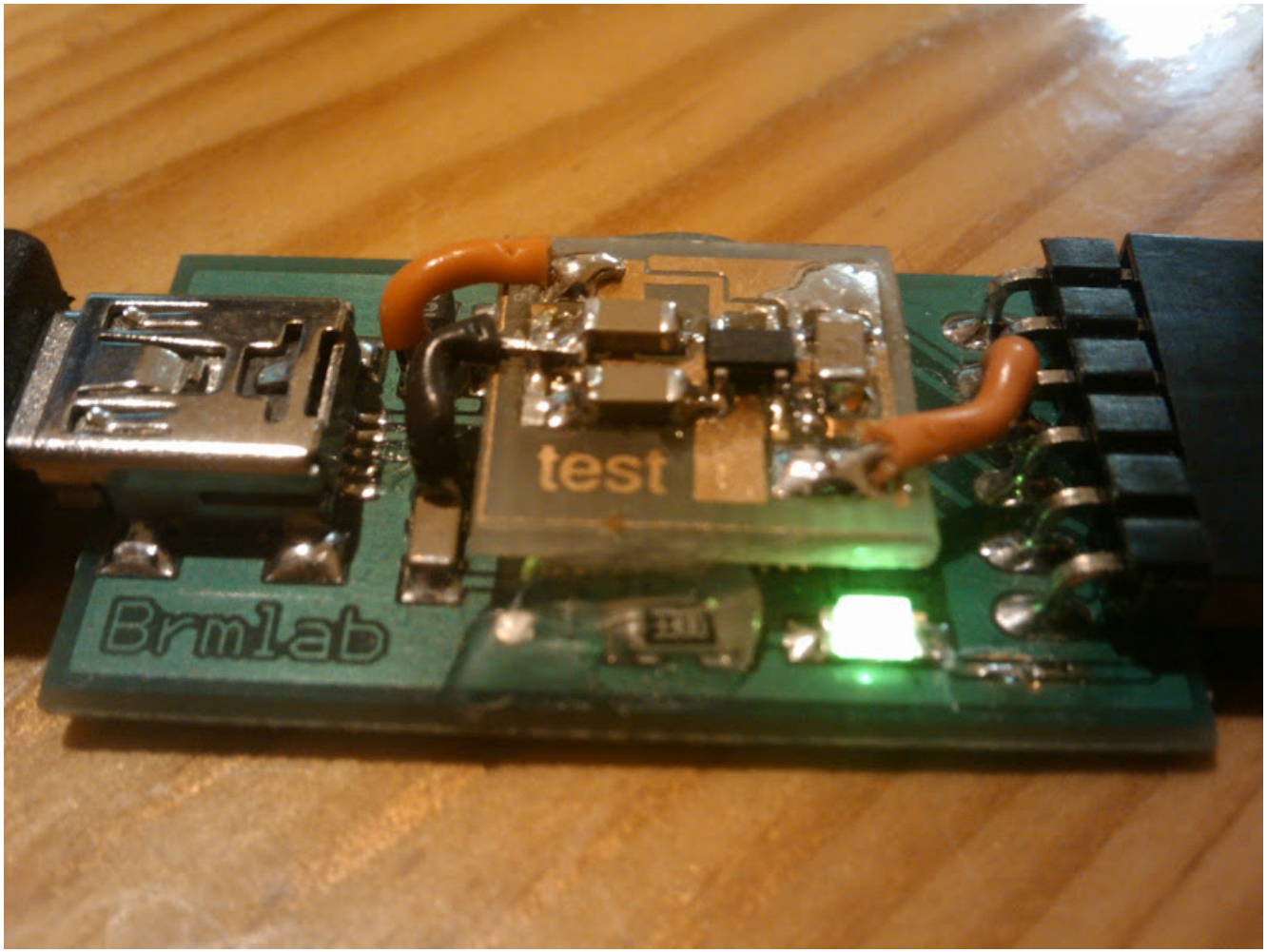
USB to male connector (FTDI)

from Brmduino project (http://brmlab.cz/project/brmduino)

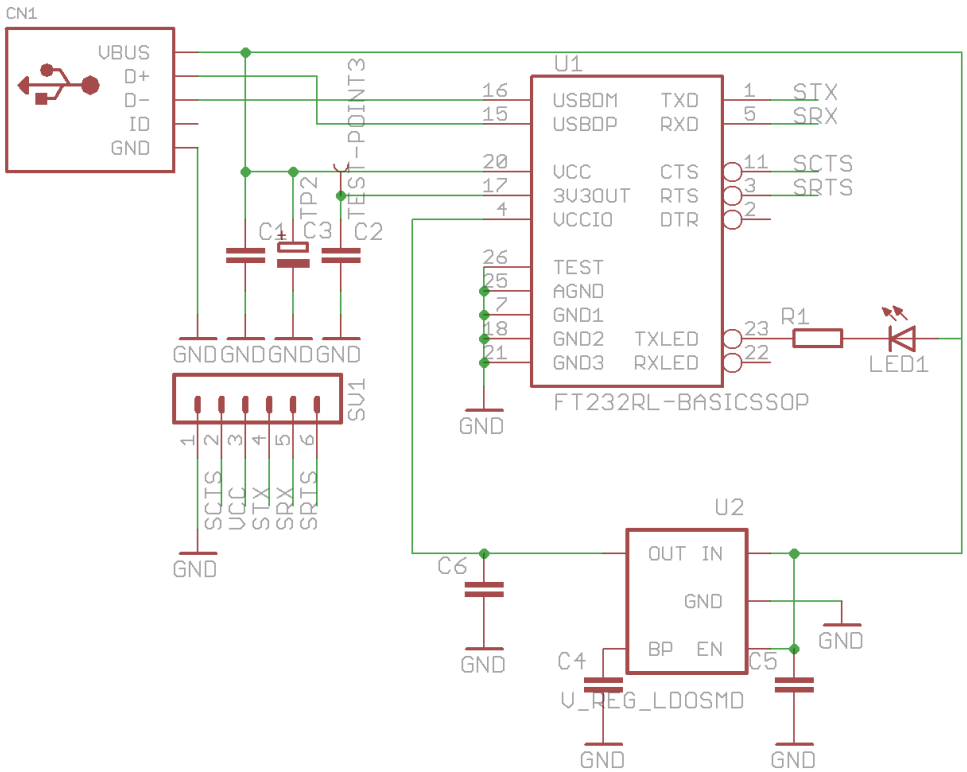


brmlab hackerspace prague

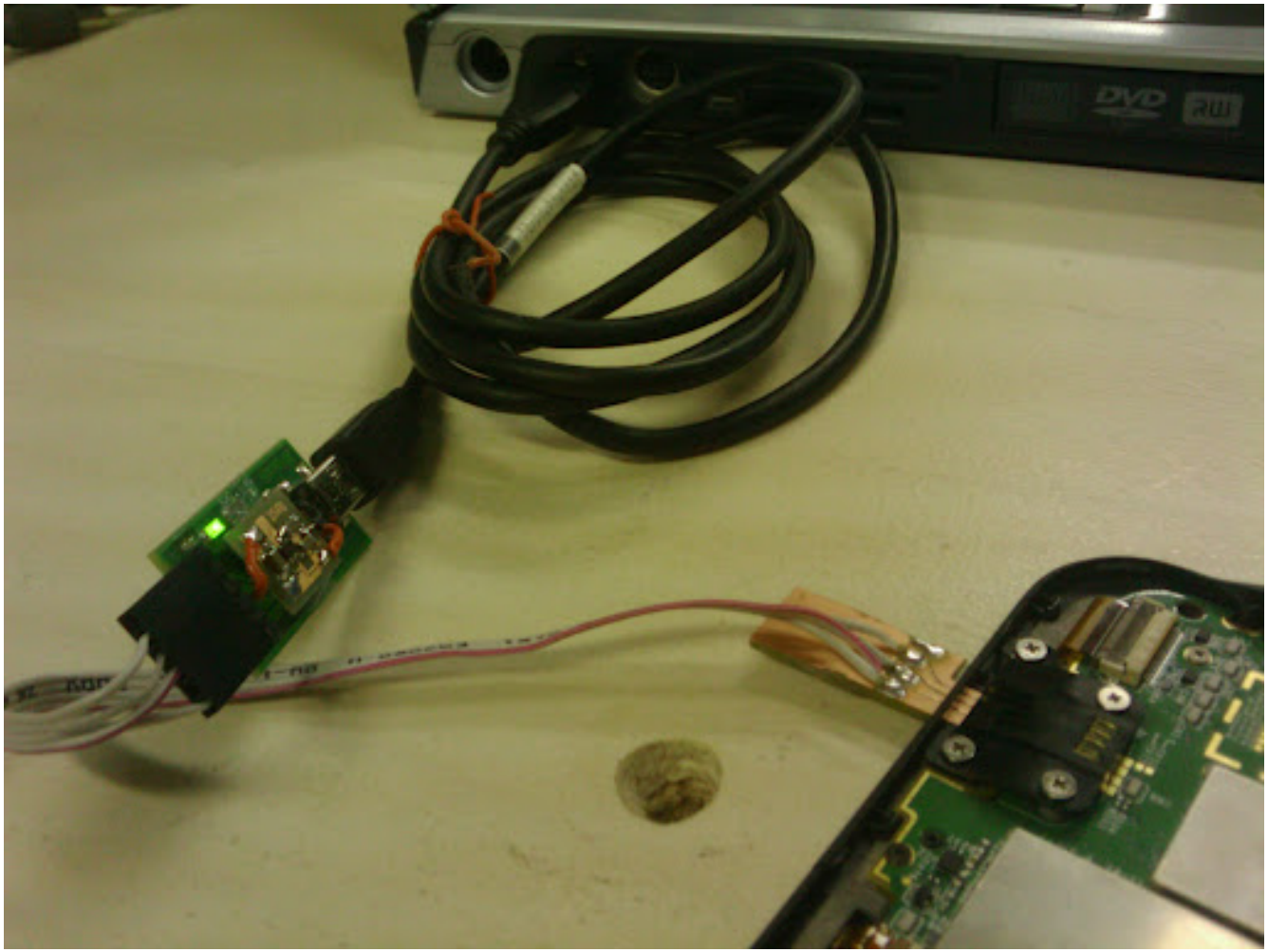
Brmduino FTDI, modified for 1.8V



Brmduino FTDI, modified for 1.8V (schema)

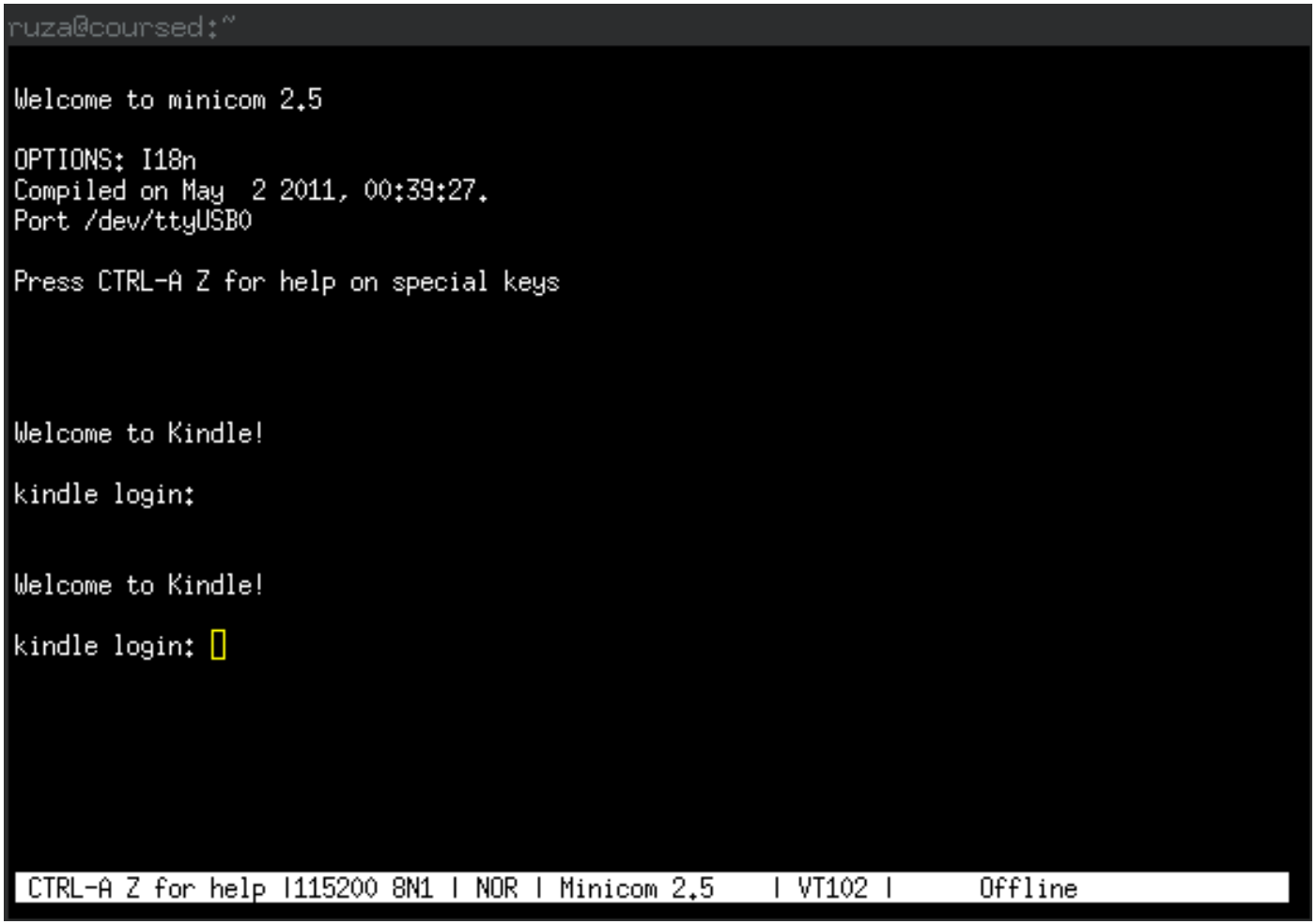


whole FTDI cable connected



- notebook/PC
- USB2 female, type A
- USB2 mini, type B
- FTDI on 1.8V
- four-wire cable
- custom male ”bastl”connector
- Kindle

minicom, ttyUSB0, 115200 8N1



note: got no tty? reboot by sliding power switch for 20sec

brmlab hackerspace prague

Table of Contents

brute force over serial

```
#!/usr/bin/expect -f

spawn socat -,icanon=0,echo=0 /dev/ttyUSB0,raw,echo=0,b115200
expect "Welcome to Kindle!"
send "\n"
send "\n"

for {set count 0} {$count < 4095} {incr count +1} {
   set counthex [format %03x $count]
   expect {
        "kindle login:"     { send "root\n" }
         "Password: "       { send "fiona$counthex\n" }
        "root@kindle root" { interact ;break }
   }
}
```

brute force over serial

```
#!/usr/bin/expect -f

spawn socat -,icanon=0,echo=0 /dev/ttyUSB0,raw,echo=0,b115200
expect "Welcome to Kindle!"
send "\n"
send "\n"

for {set count 0} {$count < 4095} {incr count +1} {
   set counthex [format %03x $count]
   expect {
        "kindle login:"     { send "root\n" }
         "Password: "       { send "fiona$counthex\n" }
        "root@kindle root" { interact ;break }
   }
}
```

brute force over serial (USELESS)

```
#!/usr/bin/expect -f

spawn socat -,icanon=0,echo=0 /dev/ttyUSB0,raw,echo=0,b115200
expect "Welcome to Kindle!"
send "\n"
send "\n"

for {set count 0} {$count < 4095} {incr count +1} {
   set counthex [format %03x $count]
   expect {
        "kindle login:"     { send "root\n" }
         "Password: "       { send "fiona$counthex\n" }
        "root@kindle root" { interact ;break }
   }
}
```

Let's try some common accounts and passwords

```
kindle login:
```

Let's try some common accounts and passwords

```
kindle login: default
```

Let's try some common accounts and passwords

```
kindle login: default
warning: cannot change to home directory
###############################################
#  N O T I C E  *  N O T I C E  *  N O T I C E  #
###############################################
Rootfs is mounted read-only. Invoke mntroot rw to
switch back to a writable rootfs.
###############################################
[default@kindle /]$
[default@kindle /]$ id
uid=1000(default) gid=1000(default)
[default@kindle /]$ uname -a
Linux kindle 2.6.26-rt-lab126 #5 Sat Apr 16 20:16:18 PDT 2011 armv6l unkn
```

cat /etc/passwd

```
root:x:0:0:root:/tmp/root:/bin/sh
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:100:sync:/bin:/bin/sync
operator:x:37:37:Operator:/var:/bin/sh
sshd:x:103:99:Operator:/var:/bin/sh
messagebus:x:92:92:messagebus:/bin/false
nobody:x:99:99:nobody:/tmp:/bin/sh
default:x:1000:1000:Default non-root
user:/dev/null:/bin/sh
framework:x:1001:150:Framework User:/tmp/framework:/bin/sh
```

file permissions

```
[default@kindle /]$ ls -l /etc/passwd /etc/shadow*
-rw-r--r--    1 root root    429 Apr 17  2011 /etc/passwd
-rw-r--r--    1 root root    350 Jul 31  2010 /etc/shadow
-rw-r--r--    1 root root    371 Apr 17  2011 /etc/shadow-
```

file permissions FAAAIL!

```
[default@kindle /]$ ls -l /etc/passwd /etc/shadow*
-rw-r--r--    1 root root    429 Apr 17  2011 /etc/passwd
-rw-r--r-- !! 1 root root    350 Jul 31  2010 /etc/shadow
-rw-r--r--    1 root root    371 Apr 17  2011 /etc/shadow-
```

cat /etc/shadow

```
default::10933:0:99999:7:::
```

cat /etc/shadow

```
root:5BueRoz.tCaOc:10933:0:99999:7:::   (DES !!)
daemon:*:10933:0:99999:7:::
bin:*:10933:0:99999:7:::
sys:*:10933:0:99999:7:::
sync:*:10933:0:99999:7:::
operator:*:10933:0:99999:7:::
sshd:*:10933:0:99999:7:::
messagebus:*:10933:0:99999:7:::
nobody:*:10933:0:99999:7:::
default::10933:0:99999:7:::
framework:$1$Cewr2/zS$SnxBS8yTMZeIgf/Tk//Xo/:14033:0:99999:7
```

cat /etc/shadow

```
default::10933:0:99999:7:::
framework:$1$Cewr2/zS$SnxBS8yTMZeIgf/Tk//Xo/:14033:0:9
```

framework password

```
$ time john kindle-shadow --format=md5
```

framework password

```
$ time john kindle-shadow --format=md5
Loaded 1 password hash (FreeBSD MD5 [32/32])
mario                (framework)
guesses: 1  time: 0:00:00:01 100% (2)  c/s: 3090  trying: mario

real    0m1.199s
user    0m0.720s
sys     0m0.016s
```

login as framework

```
kindle login: framework
Password: mario
##########################################
#  N O T I C E  *  N O T I C E  *  N O T I C E  #
##########################################
Rootfs is mounted read-only. Invoke mntroot rw to
switch back to a writable rootfs.
##########################################
[framework@kindle framework]$ id
uid=1001(framework) gid=150(javausers)
```

What we have and know at this time

- credentials of passwordless account

What we have and know at this time

- credentials of passwordless account
- credentials of user ”framework”

What we have and know at this time

- credentials of passwordless account
- credentials of user ”framework”
- hash of root password

What we have and know at this time

- credentials of passwordless account
- credentials of user ”framework”
- hash of root password
- root password id DES encrypted. That means **not more than 8 characters long!**

What we have and know at this time

- credentials of passwordless account
- credentials of user ”framework”
- hash of root password
- root password id DES encrypted. That means **not more than 8 characters long!**
- codename of this e-reader version was ”fiona”

let's crack root pass

```
for i in $(seq 0 4095); do printf 'fiona%03x\n' $i; done |\
time john -stdin kindle-shadow
```

let's crack root pass

```
for i in $(seq 0 4095); do printf 'fiona%03x\n' $i; done |\
time john -stdin kindle-shadow

Loaded 1 password hash (Traditional DES [128/128 BS SSE2])
fiona123          (root)
guesses: 1 time: 0:00:00:00  c/s:7680  trying: fiona100 - fiona17f

real    0m0.207s
user    0m0.076s
sys     0m0.016s
```

root password is generated

```
Welcome to Kindle!

kindle login:
```

root password is generated

```
Welcome to Kindle!

kindle login: PASSWORD?
```

root password is generated

```
Welcome to Kindle!

kindle login:
```

fiona

root password is generated

```
Welcome to Kindle!

kindle login:

fiona +
```

root password is generated

```
Welcome to Kindle!

kindle login:
```

fiona + md5( )

root password is generated

```
Welcome to Kindle!

kindle login:
```

fiona + md5($serial_num**)**

root password is generated

```
Welcome to Kindle!

kindle login:

fiona + md5($serial_num)[8-10]
```

this also works..

```
$ grep Serial /proc/cpuinfo|cut -b12-27|md5sum|cut -b8-10
```

Table of Contents

/var/local/java/prefs/DevicePassword.pw

DevicePassword-disabled.pw

```
0000 0000: AC ED 00 05 73 72 00 36  63 6F 6D 2E 61 6D 61 7A  ....sr.6 com.amaz
0000 0010: 6F 6E 2E 65 62 6F 6F 6B  2E 66 72 61 6D 65 77 6F  on.ebook .framewo
0000 0020: 72 6B 2E 69 6D 70 6C 2E  73 65 63 75 72 69 74 79  rk.impl. security
0000 0030: 2E 50 61 73 73 77 6F 72  64 53 74 61 74 65 B3 47  .Passwor dState.G
0000 0040: 6D 3D EC 77 58 E7 02 00  04 49 00 08 61 74 74 65  m=.wX... .I..atte
0000 0050: 6D 70 74 73 5A 00 07 65  6E 61 62 6C 65 64 4C 00  mptsZ..e nabledL.
0000 0060: 04 68 69 6E 74 74 00 12  4C 6A 61 76 61 2F 6C 61  .hintt.. Ljava/la
0000 0070: 6E 67 2F 53 74 72 69 6E  67 3B 4C 00 0C 70 61 73  ng/Strin g;L..pas
0000 0080: 73 77 6F 72 64 48 61 73  68 71 00 7E 00 01 78 70  swordHas hq.~..xp
0000 0090: 00 00 00 00 00 70 70                             .....pp
0000 00A0:
0000 00B0:
0000 00C0:
0000 00D0:
```

DevicePassword.pw

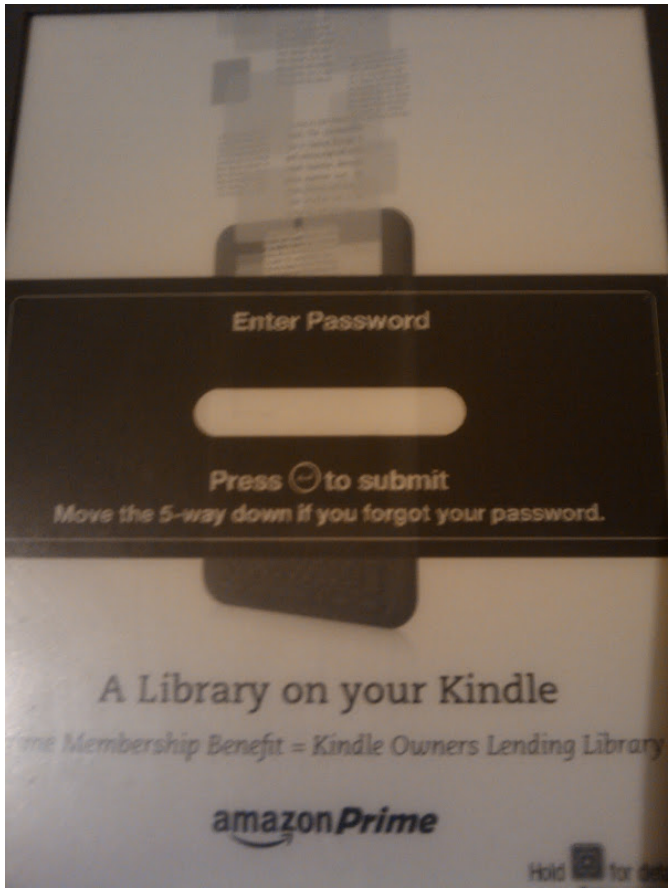
```
0000 0000: AC ED 00 05 73 72 00 36  63 6F 6D 2E 61 6D 61 7A  ....sr.6 com.amaz
0000 0010: 6F 6E 2E 65 62 6F 6F 6B  2E 66 72 61 6D 65 77 6F  on.ebook .framewo
0000 0020: 72 6B 2E 69 6D 70 6C 2E  73 65 63 75 72 69 74 79  rk.impl. security
0000 0030: 2E 50 61 73 73 77 6F 72  64 53 74 61 74 65 B3 47  .Passwor dState.G
0000 0040: 6D 3D EC 77 58 E7 02 00  04 49 00 08 61 74 74 65  m=.wX... .I..atte
0000 0050: 6D 70 74 73 5A 00 07 65  6E 61 62 6C 65 64 4C 00  mptsZ..e nabledL.
0000 0060: 04 68 69 6E 74 74 00 12  4C 6A 61 76 61 2F 6C 61  .hintt.. Ljava/la
0000 0070: 6E 67 2F 53 74 72 69 6E  67 3B 4C 00 0C 70 61 73  ng/Strin g;L..pas
0000 0080: 73 77 6F 72 64 48 61 73  68 71 00 7E 00 01 78 70  swordHas hq.~..xp
0000 0090: 00 00 00 00 01 74 00 03  77 65 70 74 00 1D 0E C3  .....t.. wept....
0000 00A0: B6 5C 72 16 07 C2 A0 2D  50 C3 9F C3 A7 C2 A8 C0  .\r....- P.......
0000 00B0: 80 C3 BA C3 BB 6B 40 13  C3 A2 7F                 .....k@. ...
0000 00C0:
0000 00D0:
```

Arrow keys move F find RET next difference ESC quit T move top
C ASCII/EBCDIC E edit file G goto position Q quit B move bottom

https://code.google.com/p/jdeserialize/

```
ruza@ingnue:~$ java -jar jdeserialize-1.1.jar DevicePassword-aaa.pw
read: com.amazon.ebook.framework.impl.security.PasswordState _h0x7e0002 = r_0x7e000

//// BEGIN class declarations (excluding array classes)
class com.amazon.ebook.framework.impl.security.PasswordState implements
 java.io.Serializable {
    int attempts;
    boolean enabled;
    java.lang.String hint;
    java.lang.String passwordHash; }

//// BEGIN instance dump
[instance 0x7e0002: 0x7e0000/com.amazon.ebook.framework.impl.security.PasswordState
  field data:
    0x7e0000/com.amazon.ebook.framework.impl.security.PasswordState:
        passwordHash: r0x7e0004: [String 0x7e0004: "ä³ÀVïE°yÌÀOû¨ã>"]
        hint: r0x7e0003: [String 0x7e0003: "a"]
        attempts: 0
        enabled: true
```

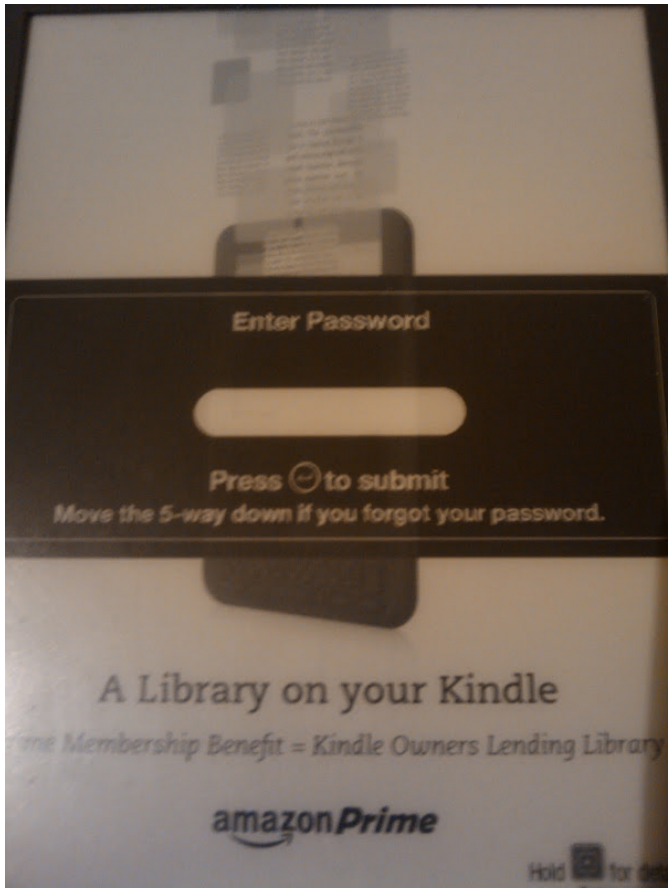
com.amazon.ebook.framework.impl.resources.PasswordReso



brmlab hackerspace prague

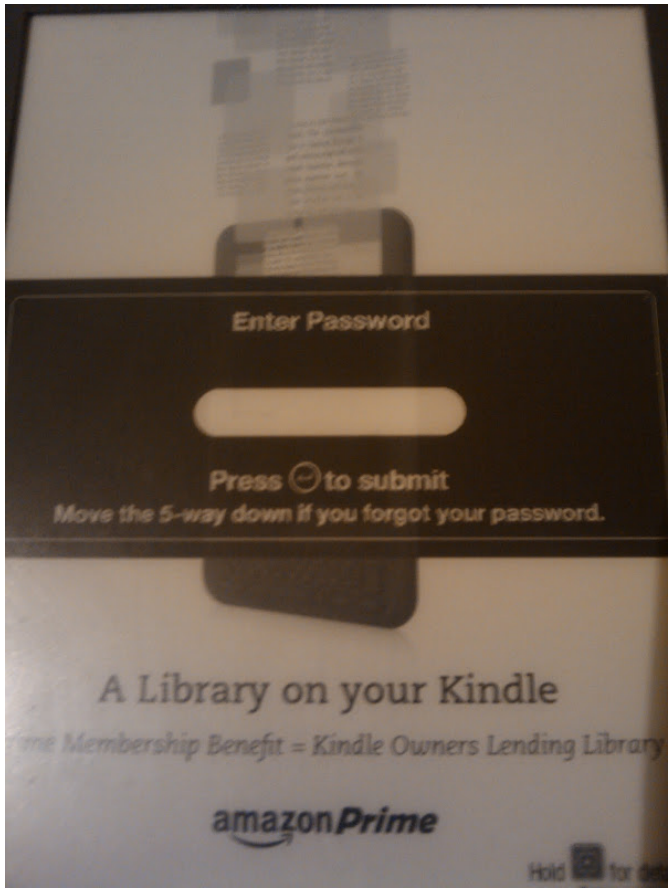
com.amazon.ebook.framework.impl.resources.PasswordReso

- ”password.reset.to.factory.defaults”
  ”resetmykindle”



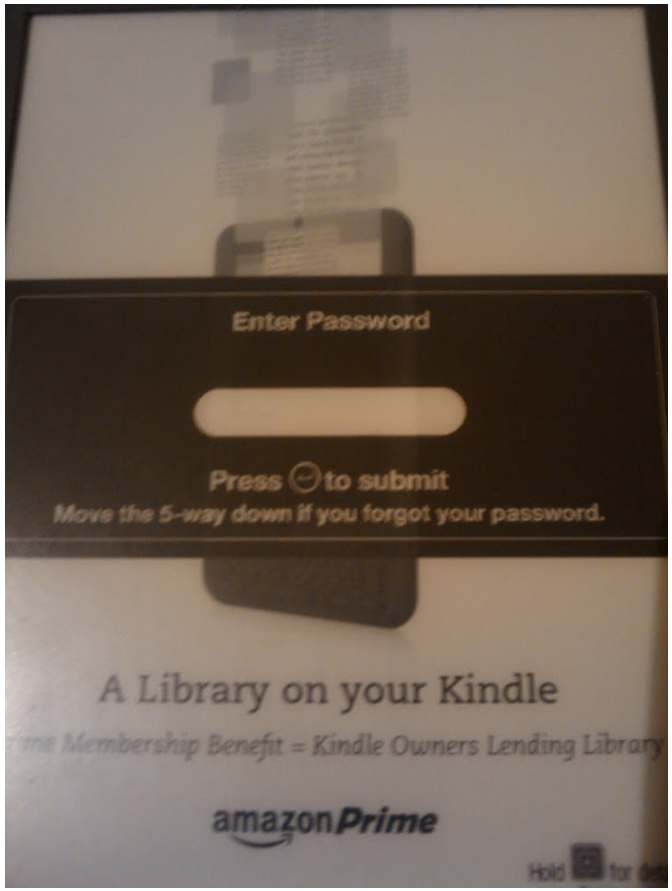
com.amazon.ebook.framework.impl.resources.PasswordReso

- ”password.reset.to.factory.defaults”
  ”resetmykindle”
- ”device.bricked.message”
  ”This device has been remotely disabled.”



com.amazon.ebook.framework.impl.resources.PasswordReso

- ”password.reset.to.factory.defaults” ”resetmykindle”
- ”device.bricked.message” ”This device has been remotely disabled.”
- Java code obfuscated by ”Allatori Obfuscator v2.8”



Allatori obfuscator vs JAva Decompiler

```
private String b(String a)
{
    byte a[];
    MessageDigest a;
    if(a == null || a.length() == 0)
        return null;
    String a = b.d().getDeviceSerialID();
    a = a + a;
    a = null;
    try
    {
        a = a.getBytes("UTF-8");
....
_L3:
    a;
    JVM INSTR icmpge 52;
       goto _L1 _L2
_L1:
    a.append((char)(a[a] & 0xff));
    ++a;
```

Allatori obfuscator vs JAva Decompiler

```
private String b(String a)
{
    byte a[];
    MessageDigest a;
    if(a == null || a.length() == 0)
        return null;
    String a = b.d().getDeviceSerialID();
    a = a + a;
     a = null;
    try
    {
        a = a.getBytes("UTF-8");
....
_L3:
    a;
    JVM INSTR icmpge 52;
       goto _L1 _L2
_L1:
    a.append((char)(a[a] & 0xff));
    ++a;
```

Allatori obfuscator vs JAva Decompiler

```
private String b(String a)
{
    byte a[];
    MessageDigest a;
    if(a == null || a.length() == 0)
        return null;
    String a = b.d().getDeviceSerialID();
    a = a + a;
    a = null;
    try
    {
        a = a.getBytes("UTF-8");
....
_L3:
     a;
     JVM INSTR icmpge 52;
        goto _L1 _L2
_L1:
    a.append((char)(a[a] & 0xff));
    ++a;
```

updates

- OTA
- update*.bin on MMC/SD

offset	size	value
0	4	signature (OTA: "FC02", manual: "FB01")
4	4	fromVersion (minimal version to update)
8	4	toVersion (maximal version to update)
0C	2	deviceCode (3rd and 4th number of the serial)
0E	1	updateOptional (seems unused)
0F	1	
10	32	scrambled md5 hash string of the tgz
20000	?	scrambled tgz with update files

Jailbreak

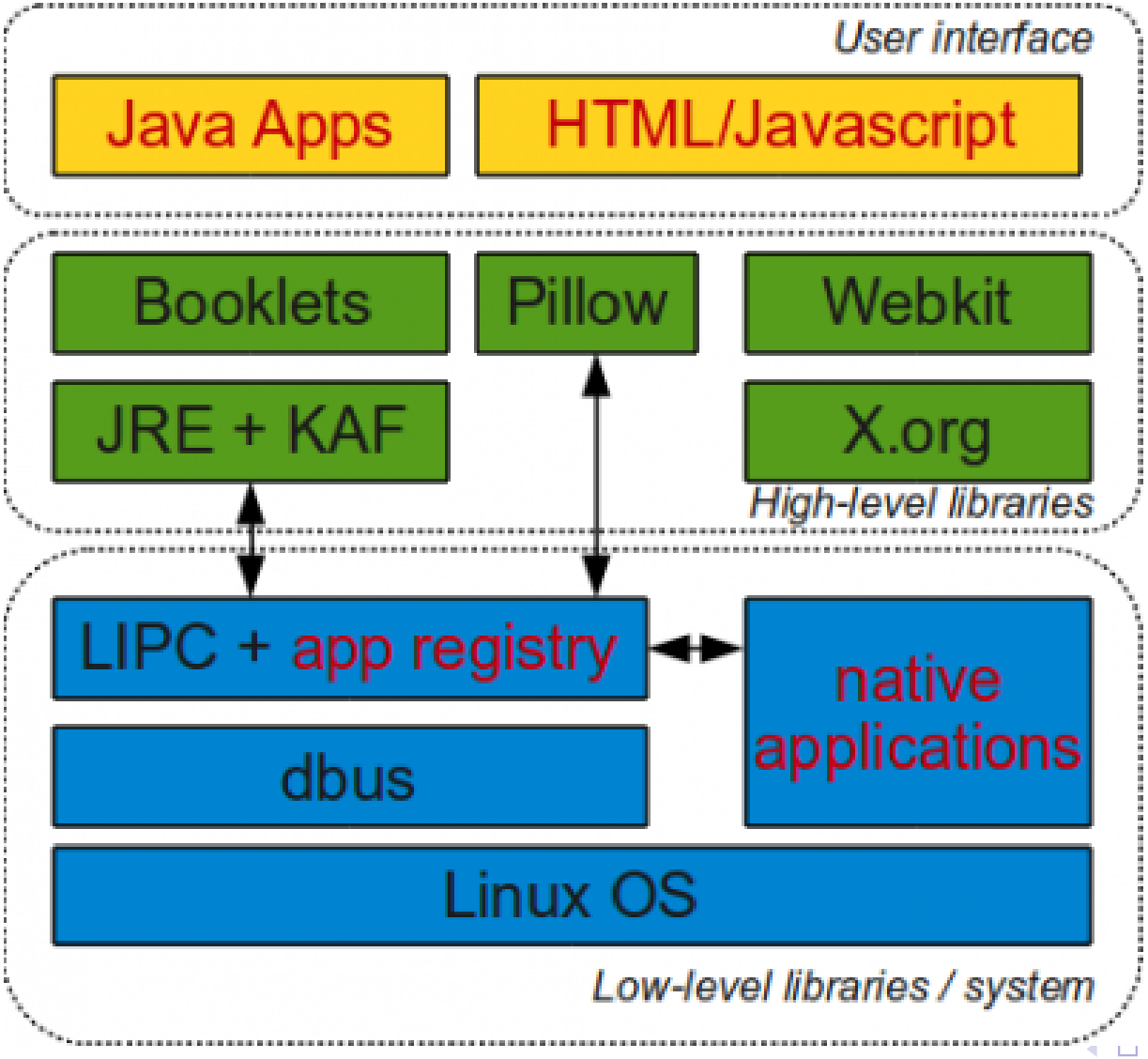
In fact, it only installs an additional "developer" key on the device, allowing for the installation of additional packages via the Kindle's own update mechanism.

Source code, semi-open system

http://goo.gl/6MDdo

alsa-lib alsa-utils atk base-files base-passwd busybox cairo
DirectFB dosfstools e2fsprogs e2fsprogs enchant fuse gdb
glib glibc gnutls gst-plugins-base gst-plugins-good gstreame
gtk+ ifupdown iptables libgcrypt libgpg-error libltdl libol
libproxy libsoup libvolume-id linux-2.6.26-lab126 lrzsz
module-init-tools mtd-utils pango picocom powertop procps
syslog-ng sysvinit taglib uboot-1.3.0-rc3/ udev util-linux
webkit wireless_tools

Big picture aka architecture

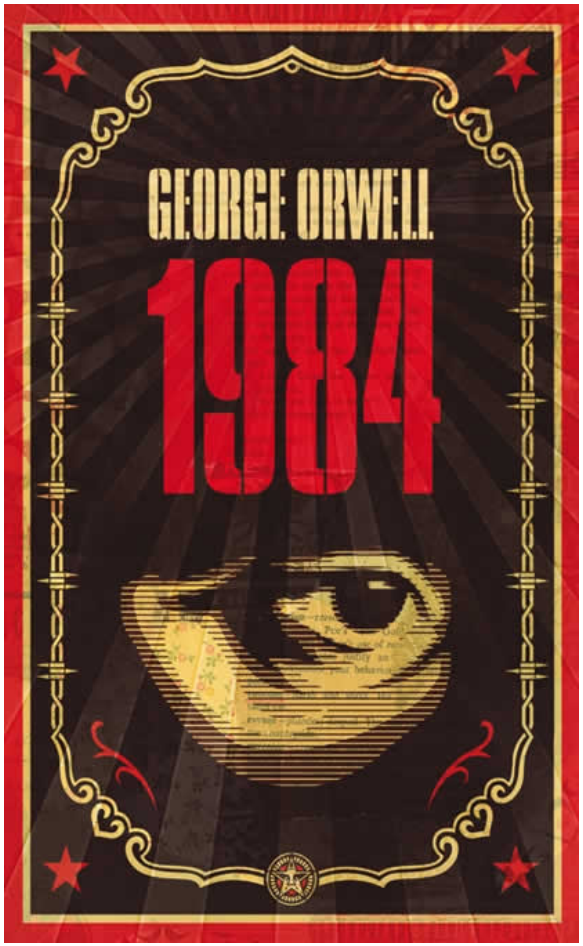


Serial cable vs USB networking

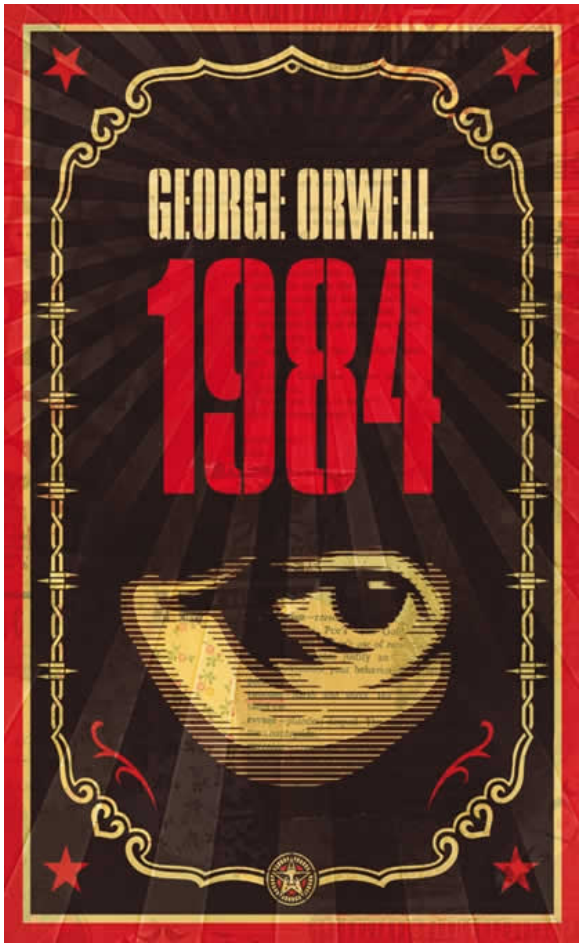
```
U-Boot 1.3.0-rc3-lab126 (Apr 16 2011 - 20:15:23)
Hit any key to stop autoboot:  0
## Booting image at 87f40400 ...
   Image Name:   Linux-2.6.26-rt-lab126
   Image Type:   ARM Linux Kernel Image (uncompressed)
   Data Size:    2168740 Bytes =  2.1 MB
   Load Address: 80008000
   Entry Point:  80008000
   Verifying Checksum ... OK
   Loading Kernel Image ... OK

Starting kernel ...
2.6.26-rt-lab126 #5 Sat Apr 16 20:16:18 PDT 2011 armv6l
Press [ENTER] for recovery menu...
```

Kindle 1984 incident (July 2009)

Kindle 1984 incident (July 2009)

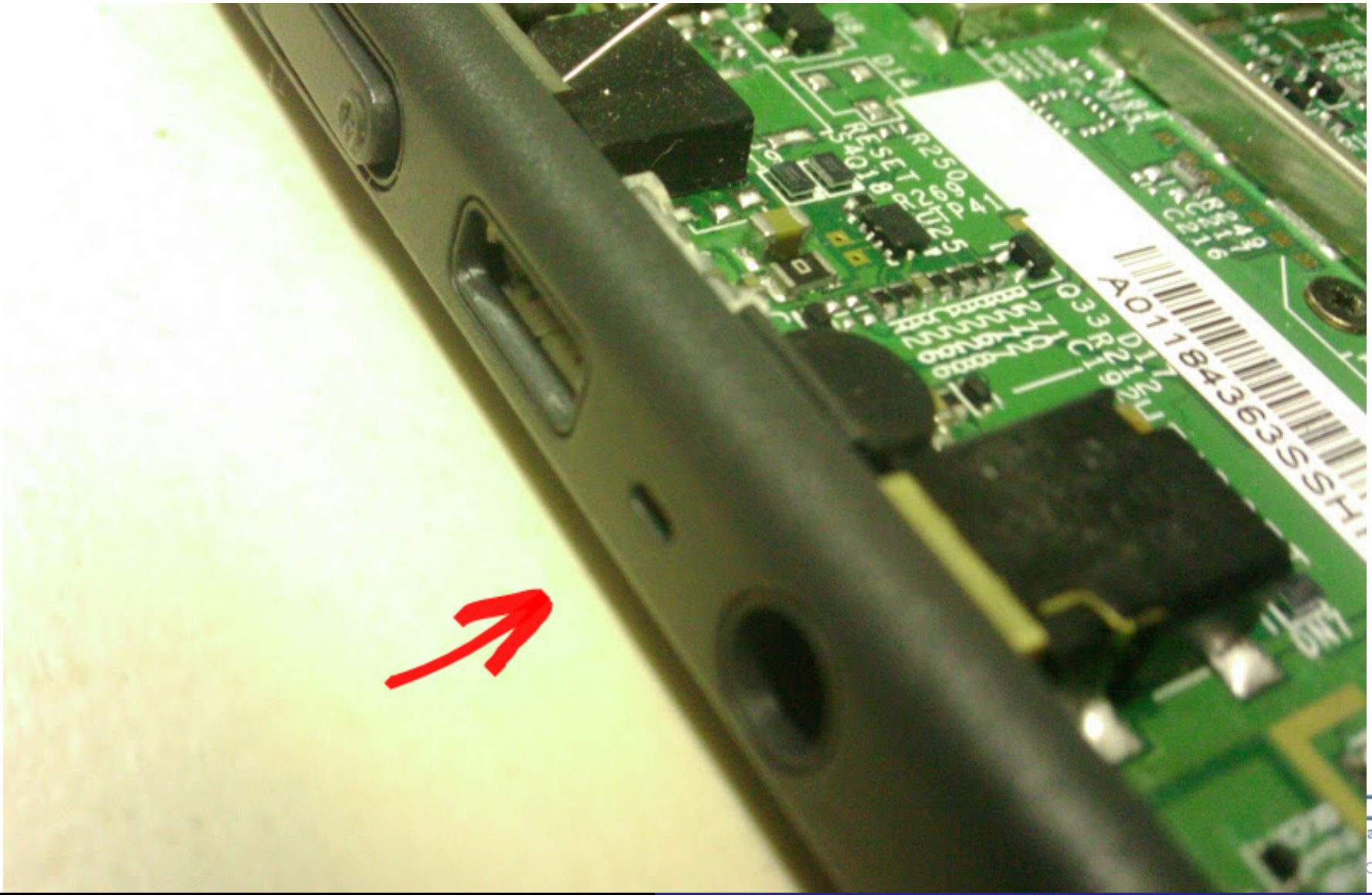


Kindle 1984 incident (July 2009)



brmlab
hackerspace prague

Internal microphone



Internal microphone!

```
[root@kindle asound]# arecord -l
**** List of CAPTURE Hardware Devices ****
card 0: mx35luigi [mx35luigi], device 0:
  WM8960 HiFi WM8960-I2S-0 []
  Subdevices: 1/1
  Subdevice #0: subdevice #0
```

Internal microphone!

```
[root@kindle asound]# arecord -l
**** List of CAPTURE Hardware Devices ****
card 0: mx35luigi [mx35luigi], device 0:
  WM8960 HiFi WM8960-I2S-0 []
  Subdevices: 1/1
  Subdevice #0: subdevice #0

[root@kindle asound]# arecord -d 10 -c 1 -r 16000 -f S16_LE /tmp/test-mi
Recording WAVE '/tmp/test-mic.wav' : Signed 16 bit Little Endian,
  Rate 16000 Hz, Mono
```

Internal microphone!

```
[root@kindle asound]# arecord -l
**** List of CAPTURE Hardware Devices ****
card 0: mx35luigi [mx35luigi], device 0:
  WM8960 HiFi WM8960-I2S-0 []
  Subdevices: 1/1
  Subdevice #0: subdevice #0

[root@kindle asound]# arecord -d 10 -c 1 -r 16000 -f S16_LE /tmp/test-mic
Recording WAVE '/tmp/test-mic.wav' : Signed 16 bit Little Endian,
  Rate 16000 Hz, Mono

[root@kindle asound]# aplay /tmp/test-mic.wav
Playing WAVE '/tmp/test-mic.wav' : Signed 16 bit Little Endian,
  Rate 16000 Hz, Mono
Aborted by signal Interrupt...
```

brmlab hackerspace prague