Hacking Embedded Devices

Sören Heisrath

October 16, 2008

Handys

Beispiele:

- Trolltech Greenphone
- Neo Freerunner
- Diverse Handys von Motorola, Samsung, Grundig, ...

Netzwerkstuff

- Accesspoints
- Print,Media, Wollmilch-Server
- Router
- (DSL)-Modems
- Telefonanlagen

Sonstiges

- PDAs

Sonstiges

- PDAs
- Navis

Sonstiges

- PDAs
- Navis
- Kassensysteme

Sonstiges

- PDAs
- Navis
- Kassensysteme
- ...

Firmwareformate

Kraut und Rüben:

- Simples (tar-)Archiv

Firmwareformate

Kraut und Rüben:

- Simples (tar-)Archiv
- Irgendwie komprimiertes Archiv

Firmwareformate

Kraut und Rüben:

- Simples (tar-)Archiv
- Irgendwie komprimiertes Archiv
- Herstellereigenes Binärformat

Firmwareformate

Kraut und Rüben:

- Simples (tar-)Archiv
- Irgendwie komprimiertes Archiv
- Herstellereigenes Binärformat
- "diff"-Archiv

Handwerkzeuge

- `file`, `strings` & co

Handwerkzeuge

- `file`, `strings` & co
- Forensik-Tools

Handwerkzeuge

- `file`, `strings` & co
- Forensik-Tools
- Hexeditor

Meta-Informationen

```
file firmware.bin
 firmware.bin:  data
```

Strings

```
strings firmware.bin
2.4.21 (marvin@compilebitch) ...
```

Strings

```
strings firmware.bin
2.4.21 (marvin@compilebitch) ...
```

OMG Liiiinuks!!

Forensik-Tools

```
foremost firmware.bin
ls output
```

Forensik-Tools

```
foremost firmware.bin
ls output
audit.txt zip
```

Werkzeuge

- tcpdump

Werkzeuge

- tcpdump
- nmap

Passiv lauschen

```
tcpdump -i eth0 -v -n
```

Aktiver Scan

```
nmap -O -p 1- 1.2.3.4
```

Gebräuchliche Adressen

- 192.168.0.1
- 192.168.1.1
- 192.168.178.254 (AVM)
- 150.150.150.[2,4] (Zyxel)

Was ist zu erwarten?

- (T)FTP Server
- Webinterface
- Shell

Patient schweigt?

- Reset-Taster gedrückt halten

Patient schweigt?

- Reset-Taster gedrückt halten
- Anderen Port probieren

Patient schweigt?

- Reset-Taster gedrückt halten
- Anderen Port probieren
- Anpingen (`nmap -n -sP 192.168.1.0/24`)

Verdachtsmomente

nifty picture of shiny device.

Anschlussbelegung

- GND
- RX
- TX
- (VCC)

Lauschen

Lauschen wir doch mal...

Hardware bauen

Hardware bauen

- MAX 232 (5V) || MAX 3232 (3.3V) || Transistoren

Hardware bauen

- MAX 232 (5V) || MAX 3232 (3.3V) || Transistoren
- Ein paar Kondensatoren

Hardware bauen

- MAX 232 (5V) || MAX 3232 (3.3V) || Transistoren
- Ein paar Kondensatoren
- Sub-D Stecker & Kabel

Hardware bauen

- MAX 232 (5V) || MAX 3232 (3.3V) || Transistoren
- Ein paar Kondensatoren
- Sub-D Stecker & Kabel
- Ggf. Spannungsversorgung

Wissenswertes

Wissenswertes

- Architektur (mips, armX)

Wissenswertes

- Architektur (mips, armX)
- libc Version

Wissenswertes

- Architektur (mips, armX)
- libc Version
- ggf. busybox Version

Häufig verwendete Software

Häufig verwendete Software

- busybox (basissystem)

Häufig verwendete Software

- busybox (basissystem)
- dropbear (ssh server)

Häufig verwendete Software

- busybox (basissystem)
- dropbear (ssh server)
- uClibc oder dietlibc

Problemstellungen

Problemstellungen

- Signaturen, Checksummen & Verschlüsselung

Problemstellungen

- Signaturen, Checksummen & Verschlüsselung
- Inkrementelle Updates

Problemstellungen

- Signaturen, Checksummen & Verschlüsselung
- Inkrementelle Updates
- Sonstige Meta-Informationen

Umsehen

- telnet- oder ssh server installieren oder aktivieren
- serielle nutzen

Proprietäre Software

Proprietäre Software

- Services

Proprietäre Software

- Services
- Kernel Module

Proprietäre Software

- Services
- Kernel Module
- Policies

OpenSource & Hardwarehersteller...

OpenSource & Hardwarehersteller...

- Variante 1: "Wir geben nix frei"

OpenSource & Hardwarehersteller...

- Variante 1: "Wir geben nix frei"
- Variante 2: "Wir werfen alle Archive zusammen"

OpenSource & Hardwarehersteller...

- Variante 1: "Wir geben nix frei"
- Variante 2: "Wir werfen alle Archive zusammen"
- Variante 3: "Wir geben 'ne Toolchain mit"

OpenSource & Hardwarehersteller...

- Variante 1: "Wir geben nix frei"
- Variante 2: "Wir werfen alle Archive zusammen"
- Variante 3: "Wir geben 'ne Toolchain mit"
- Variante 4: "Wir machen's gleich richtig"

Die Welt verbessern...

Die Welt verbessern...

- Neue Features hinzufügen

Die Welt verbessern...

- Neue Features hinzufügen
- GPL violations anzeigen

Die Welt verbessern...

- Neue Features hinzufügen
- GPL violations anzeigen
- Es besser machen

Mods

Mods

- SD-Card

Mods

- SD-Card
- Microcontroller an die Serielle

Mods

- SD-Card
- Microcontroller an die Serielle
- Hardware-Features aktivieren (USB, Mini-PCI)

Mods

- SD-Card
- Microcontroller an die Serielle
- Hardware-Features aktivieren (USB, Mini-PCI)
- ...