

Read It Twice!

A mass-storage-based TOCTTOU attack

Collin Mulliner and Benjamin Michéle

Security in Telecommunications
Technische Universität Berlin and Telekom Innovation Laboratories
Germany
{collin,ben}@sec.t-labs.tu-berlin.de

August 7, 2012



What is this talk about?

- Compromising CE devices via emulated USB mass-storage



What is this talk about?

- Compromising CE devices via emulated USB mass-storage



Our contribution

- Mass-storage-based *time-of-check-to-time-of-use* (TOCTTOU) attack: *Read It Twice* (RIT)
 - Mass-storage device that changes its content between check and execute/install phase of a connected host
 - Circumvention of block and file system caches
- Black box analysis of file accesses to mass-storage devices
 - Method and tool
 - Maps block accesses to file accesses at run time
- POC against a Samsung TV, using our RIT analysis and attack tool
 - Used in this talk to demonstrate the general attack and tool

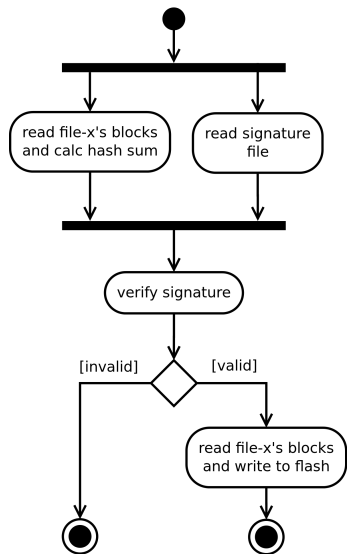
Our contribution

- Mass-storage-based *time-of-check-to-time-of-use* (TOCTTOU) attack: *Read It Twice* (RIT)
 - Mass-storage device that changes its content between check and execute/install phase of a connected host
 - Circumvention of block and file system caches
- Black box analysis of file accesses to mass-storage devices
 - Method and tool
 - Maps block accesses to file accesses at run time
- POC against a Samsung TV, using our RIT analysis and attack tool
 - Used in this talk to demonstrate the general attack and tool

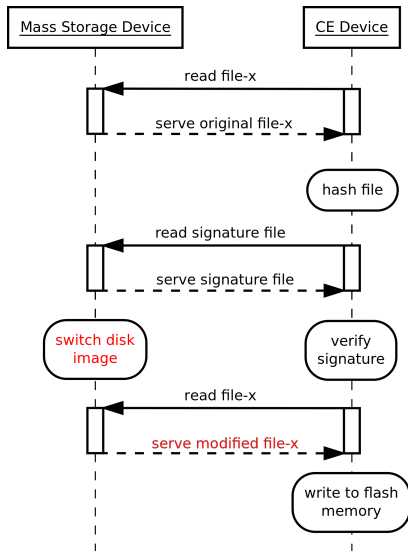
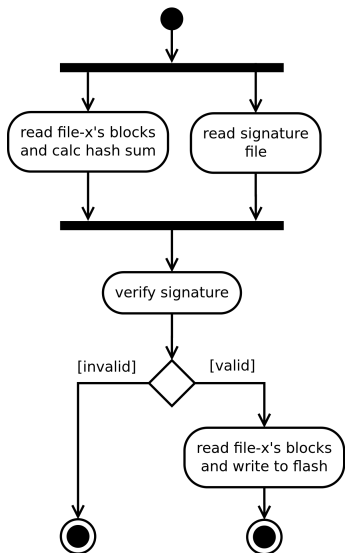
Our contribution

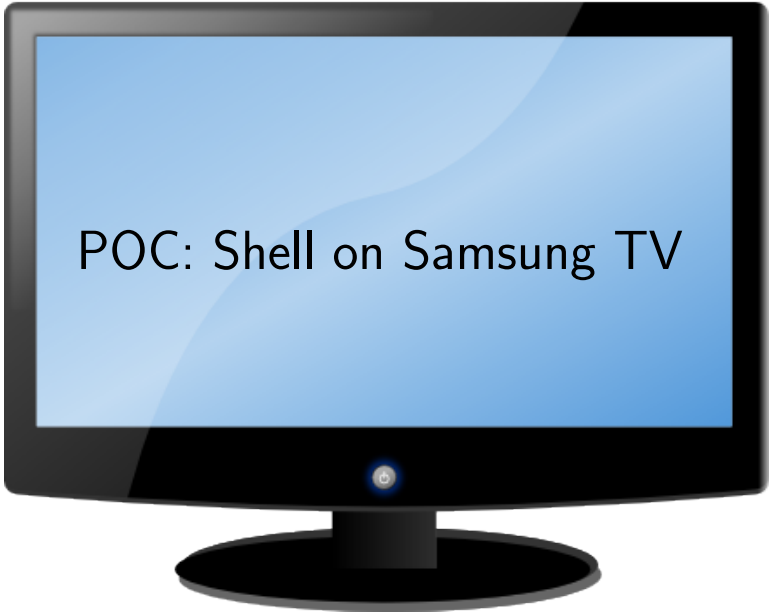
- Mass-storage-based *time-of-check-to-time-of-use* (TOCTTOU) attack: *Read It Twice* (RIT)
 - Mass-storage device that changes its content between check and execute/install phase of a connected host
 - Circumvention of block and file system caches
- Black box analysis of file accesses to mass-storage devices
 - Method and tool
 - Maps block accesses to file accesses at run time
- POC against a Samsung TV, using our RIT analysis and attack tool
 - Used in this talk to demonstrate the general attack and tool

Software installation: Program flow



Software installation: Program flow and attack





POC: Shell on Samsung TV

Modern TV features

- USB interface for mass-storage
 - Watch movies
 - Install apps
 - Upgrade firmware
- CI+ card slot for pay TV
- Network and Internet connection
- Integrated camera and microphone



Modern TV features

- USB interface for mass-storage
 - Watch movies
 - **Install apps**
 - Upgrade firmware
- CI+ card slot for pay TV
- Network and Internet connection
- Integrated camera and microphone



Conflict of interest

User

- Enable missing features
- Fix bugs
- Customize product
- Record pay TV

Conflict of interest

User

- Enable missing features
- Fix bugs
- Customize product
- Record pay TV

Vendor

- Protect intellectual property
- Avoid warranty issues
- Adhere to the specifications
- Protect multimedia content

Conflict of interest

User

- Enable missing features
- Fix bugs
- Customize product
- Record pay TV

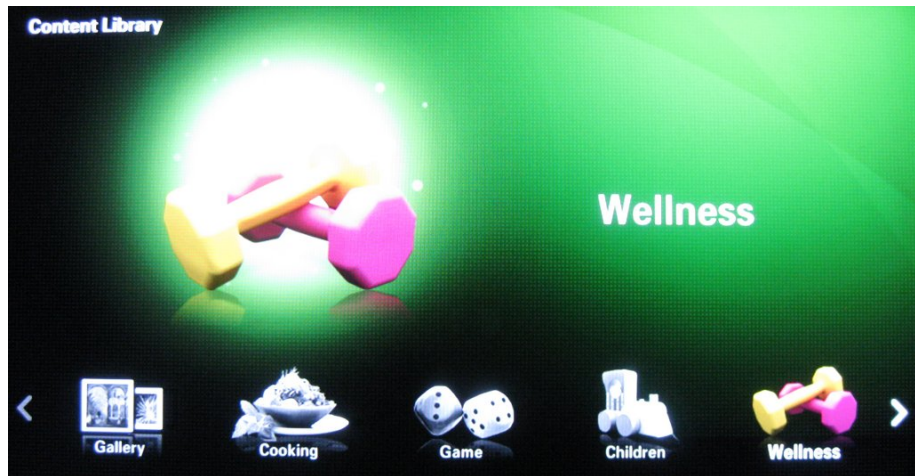
Vendor

- Protect intellectual property
- Avoid warranty issues
- Adhere to the specifications
- Protect multimedia content

Locked-down devices

User access disabled by vendor ...

Samsung LExxB650: Content library / app launcher



Samsung LExxB650: Two types of apps

clmeta.dat

- XML file
- Contains app category
- Evaluated at install time
- Evaluated at load time

Unprivileged apps

- Category **Wellness**, ...
- Macromedia Flash-based
- No signature required

Privileged apps

- Category **Game**
- Shared objects
- Native code
- Run as root
- Require valid signature for installation, but not at run time

Samsung LExxB650: Two types of apps

clmeta.dat

- XML file
- Contains app category
- Evaluated at install time
- Evaluated at load time

Unprivileged apps

- Category **Wellness**, ...
- Macromedia Flash-based
- No signature required

Privileged apps

- Category **Game**
- Shared objects
- Native code
- Run as root
- Require valid signature for installation, but not at run time

Samsung LExxB650: Two types of apps

clmeta.dat

- XML file
- Contains app category
- Evaluated at install time
- Evaluated at load time

Unprivileged apps

- Category **Wellness**, ...
- Macromedia Flash-based
- No signature required

Privileged apps

- Category **Game**
- Shared objects
- Native code
- Run as root
- Require valid signature for installation, but not at run time

Samsung LExxB650: Two types of apps

clmeta.dat

- XML file
- Contains app category
- **Evaluated at install time**
- **Evaluated at load time**

Unprivileged apps

- Category **Wellness**, ...
- Macromedia Flash-based
- No signature required

Privileged apps

- Category **Game**
- Shared objects
- Native code
- Run as root
- Require valid signature for installation, but not at run time

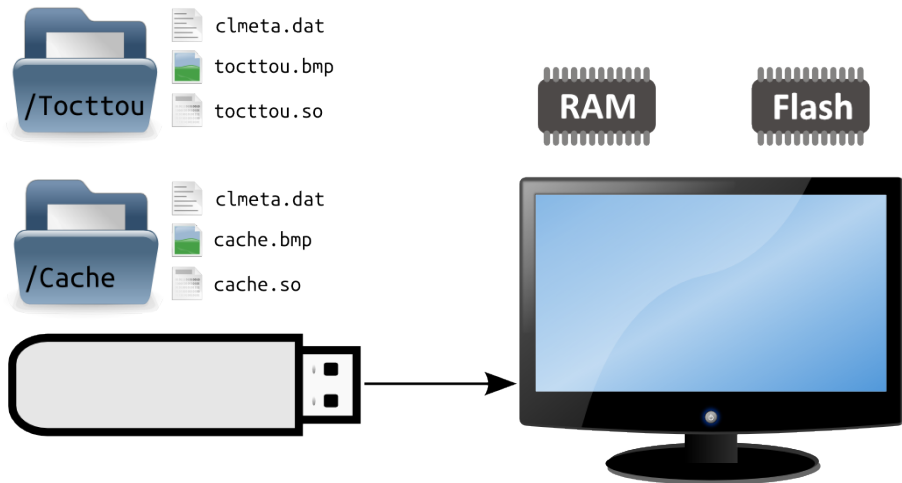
clmeta.dat: Unprivileged app

```
<?xml version="1.0" encoding="utf-8"?>
<contentlibrary>
<contentpack id="tocttou">
<category>Wellness</category>
<title language_id="English">tocttou</title>
<startpoint language_id="English">
tocttou.so</startpoint>
<thumbnailpath>tocttou.bmp</thumbnailpath>
<totalsize>1</totalsize>
</contentpack>
</contentlibrary>
```

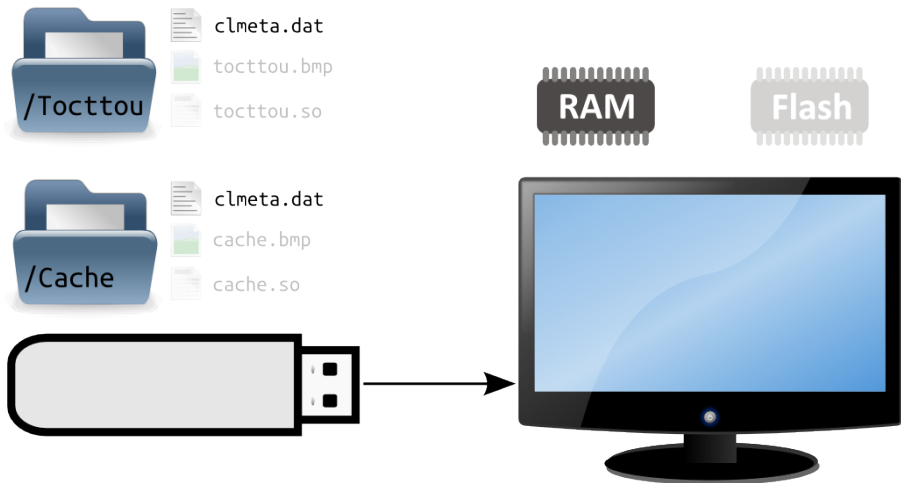
clmeta.dat: Privileged app

```
<?xml version="1.0" encoding="utf-8"?>
<contentlibrary>
<contentpack id="tocttou">
<category>Game</category>
<title language_id="English">tocttou</title>
<startpoint language_id="English">
tocttou.so</startpoint>
<thumbnailpath>tocttou.bmp</thumbnailpath>
<totalsize>1</totalsize>
</contentpack>
</contentlibrary>
```

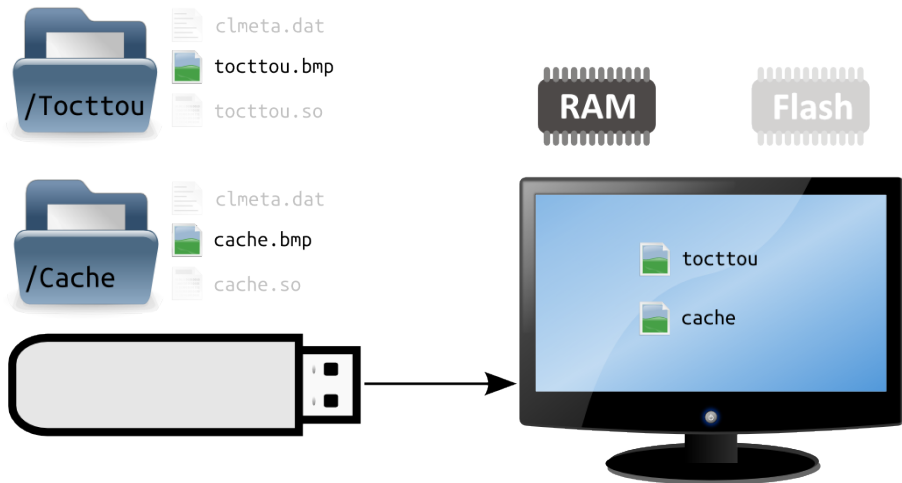
App install: Two apps on USB mass-storage



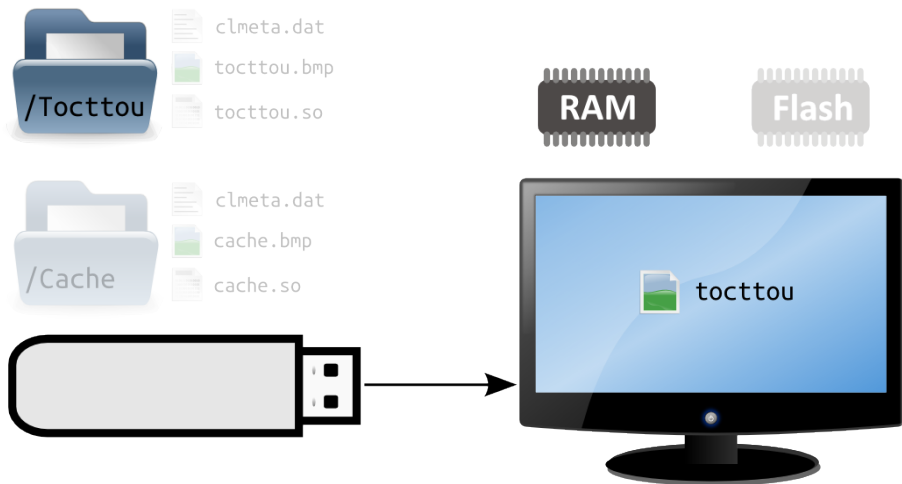
App install: TV checks all folders for apps



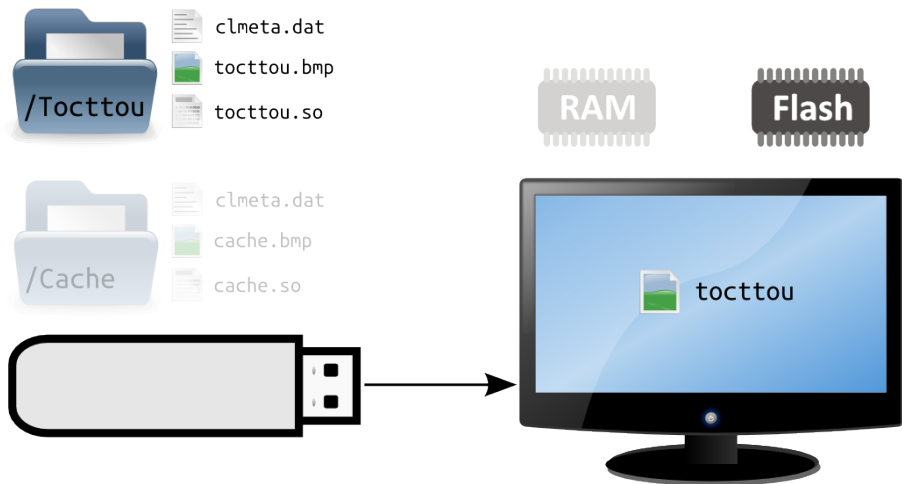
App install: TV offers unprivileged apps



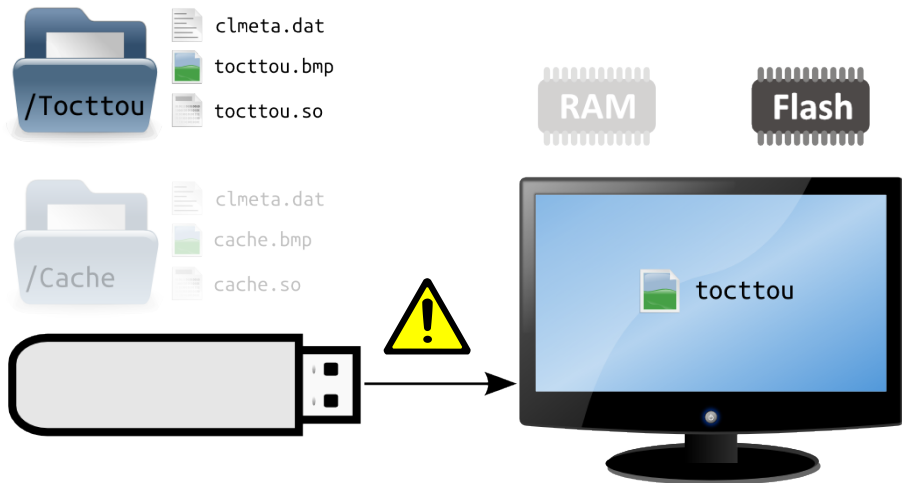
App install: User chooses app



App install: TV copies app folder to internal flash memory



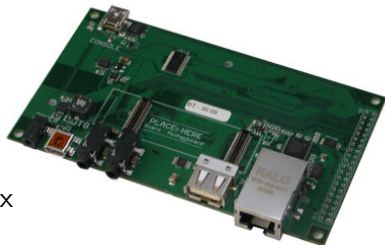
App install: TV copies app folder to internal flash memory



Requirements for TOCTTOU attack

- USB mass-storage device
 - Able to change content while connected
 - Client or OTG USB interface to connect to host
- Content change triggered by file accesses

Implementation



- Gumstix developer board running Linux
 - USB OTG port
- Linux USB stack offers mass-storage emulation via Gadget API
 - `linux/drivers/usb/gadget/file_storage.c` → `g_file_storage.ko`
- Modifications
 - Block and file system access tracking for FAT16/32
 - Switch file system based on file access counters

Tool output: Unprivileged app installation

```
11:18:56 TOCTTOU      (DIR)
11:18:56 CLMETA.DAT      (471b) [/TOCTTOU]
11:18:56 CLMETA.DAT      -> read completed!
11:18:56 CACHE          (DIR)
11:18:57 CLMETA.DAT      (450b) [/CACHE]
11:18:57 CLMETA.DAT      -> read completed!
```

→ Directories are scanned for clmeta.dat files

```
11:19:29 CACHE.BMP       (843758b) [/CACHE]
11:19:29 CACHE.BMP       -> read completed!
11:19:29 TOCTTOU.BMP     (490734b) [/TOCTTOU]
11:19:29 TOCTTOU.BMP     -> read completed!
```

→ Apps are displayed with their icon

```
11:19:52 TOCTTOU.SO      (4608b) [/TOCTTOU]
11:19:52 TOCTTOU.SO      -> read completed!
```

→ Tocttou app folder copied to internal memory

Tool output: Unprivileged app installation

```
11:18:56 TOCTTOU      (DIR)
11:18:56 CLMETA.DAT      (471b) [/TOCTTOU]
11:18:56 CLMETA.DAT      -> read completed!
11:18:56 CACHE          (DIR)
11:18:57 CLMETA.DAT      (450b) [/CACHE]
11:18:57 CLMETA.DAT      -> read completed!
```

→ Directories are scanned for clmeta.dat files

```
11:19:29 CACHE.BMP       (843758b) [/CACHE]
11:19:29 CACHE.BMP       -> read completed!
11:19:29 TOCTTOU.BMP     (490734b) [/TOCTTOU]
11:19:29 TOCTTOU.BMP     -> read completed!
```

→ Apps are displayed with their icon

```
11:19:52 TOCTTOU.SO      (4608b) [/TOCTTOU]
11:19:52 TOCTTOU.SO      -> read completed!
```

→ Tocttou app folder copied to internal memory

TOCTTOU attack would fail

/TOCTTOU/clmeta.dat read only once from emulated storage!

Problem

TV's OS caches all block accesses to mass-storage in unused RAM

Block cache

Problem

TV's OS caches all block accesses to mass-storage in unused RAM

Replace `clmeta.dat` in block cache

Force TV to read large file between checking and copying of `clmeta.dat`

Candidate files

```
11:18:56 TOCTTOU      (DIR)
11:18:56 CLMETA.DAT      (471b) [/TOCTTOU]
11:18:56 CLMETA.DAT      -> read completed! [1/2]
11:18:56 CACHE          (DIR)
11:18:57 CLMETA.DAT      (450b) [/CACHE]
11:18:57 CLMETA.DAT      -> read completed! [2/2] [S!]
11:19:29 CACHE.BMP      (843758b) [/CACHE]
11:19:29 CACHE.BMP      -> read completed!
11:19:29 TOCTTOU.BMP     (490734b) [/TOCTTOU]
11:19:29 TOCTTOU.BMP     -> read completed!
11:19:52 TOCTTOU.SO      (4608b) [/TOCTTOU]
11:19:52 TOCTTOU.SO      -> read completed!
```

Candidate files

```
11:18:56 TOCTTOU      (DIR)
11:18:56 CLMETA.DAT  (471b) [/TOCTTOU]
11:18:56 CLMETA.DAT  -> read completed! [1/2]
11:18:56 CACHE      (DIR)
11:18:57 CLMETA.DAT  (450b) [/CACHE]
11:18:57 CLMETA.DAT  -> read completed! [2/2] [S!]
11:19:29 CACHE.BMP   (843758b) [/CACHE]
11:19:29 CACHE.BMP   -> read completed!
11:19:29 TOCTTOU.BMP (490734b) [/TOCTTOU]
11:19:29 TOCTTOU.BMP -> read completed!
11:19:52 TOCTTOU.SO  (4608b) [/TOCTTOU]
11:19:52 TOCTTOU.SO  -> read completed!
```

Output of successful attack

```
TOCTTOU      (DIR)
CLMETA.DAT   (471b) [/TOCTTOU]
CLMETA.DAT   -> read completed! [1/2]
CACHE        (DIR)
CLMETA.DAT   (272630223b) [/CACHE]
CLMETA.DAT   -> read completed! [2/2] [file system switched!]
CACHE.BMP    (843758b) [/CACHE]
CACHE.BMP    -> read completed!
TOCTTOU      (DIR)
TOCTTOU      (DIR)
TOCTTOU.BMP  (490734b) [/TOCTTOU]
TOCTTOU.BMP  -> read completed!
TOCTTOU.SO   (4608b) [/TOCTTOU]
TOCTTOU.SO   -> read completed!
CLMETA.DAT   (471b) [/TOCTTOU]
CLMETA.DAT   -> read completed! [3/2]
```

TV's Wellness apps after successful attack

Relaxing sound
SamyGO RSA-Di...

Toctou



Execution of own native code on TV

- Present unprivileged app to TV
- Elevate privileges between check and install
- Execute app with full privileges, i.e., root user
- Start telnet daemon
- Disable firmware upgrade signature check
→ Modify firmware

- Copy to internal trusted memory before check and install/execute
 - Low-cost embedded devices
 - Sufficient free memory available?

Future work

- Further CE devices
 - App install code
 - Firmware upgrade process
- Further mass-storage devices
 - SD cards
 - Hard disks

fgsect.de

{collin,ben}@sec.t-labs.tu-berlin.de