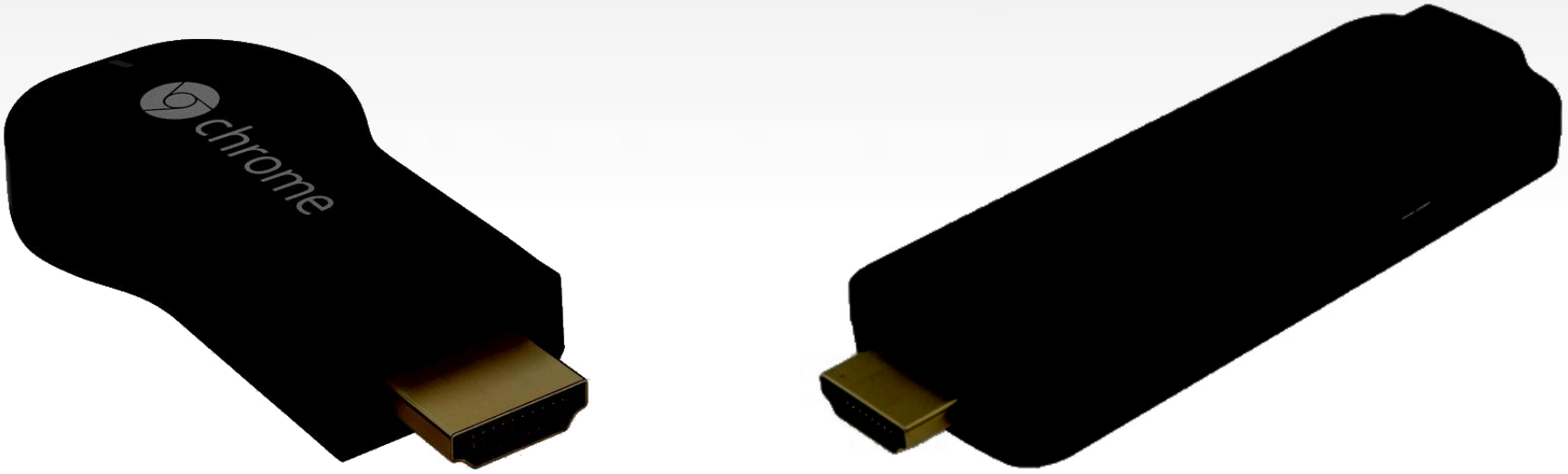
Forensics on Chromecast and Miracast

Cedric Van Bockhaven*
Peter van Bolhuis

*It's a Belgian thing

Introduction



Chromecast

Google

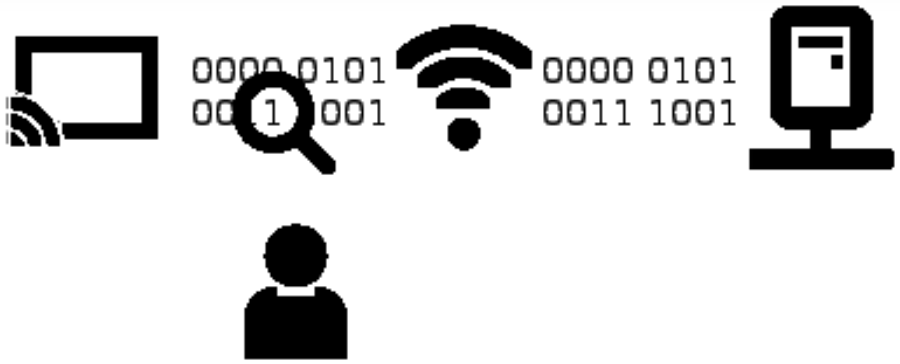
Enables *casting* to TV

2GB flash chip

Encrypted *with per device key*

Chromecast

- Updates on first connect
- Downloaded the update manually



Chromecast

```
C3CPT@CCF /tmp $ binwalk -y filesystem system.img

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
--------------------------------------------
0             0x0             Squashfs filesystem, little endian, version 4.0, compression:gzip, size:
98169632 bytes,  1738 inodes, blocksize: 131072 bytes, created: Wed Feb 26 11:37:17 2014
```

Crash reports over HTTP?

```
C3CPT@CCF /tmp/squasfs-root $ find . -type f -exec strings -f {} \; | grep "http://.."
./bin/net_mgr: http://dl.google.com/googletv-eureka/dogfood-channel/eureka-b1_ota_9284.zip
./bin/crash_uploader: http://clients2.google.com/cr/staging_report
./bin/crash_uploader: http://clients2.google.com/cr/report
```

Chromecast

Let's scan with nmap:

- sV
- Pn

Results:

- 8008
- 8009
- **Crash**

Chromecast

Report is sent to Google in a gzipped file:

```
============================================================
== dumpstate: 2014-05-11 13:40:45
== Why: crash_manager-request
============================================================

Build: OPENMASTER.16664
Build fingerprint: 'google/anchovy/anchovy:1.6/OPENMASTER/16664:user/test-keys'
Bootloader: 664352e
Kernel: Linux version 3.8.13 (mosaic-role@eurekabuild6.mtv.corp.google.com) (gcc
(gtv 20120928-afe6864) ) #3 PREEMPT Mon Mar 31 21:54:56 PDT 2014
Command line: (unknown)

------ UPTIME (uptime) ------
up time: 00:38:29, idle time: 00:32:03
[uptime: 0.0s elapsed]

------ MEMORY INFO (/proc/meminfo) ------
MemTotal:         305652 kB
MemFree:           45704 kB
Buffers:           33916 kB
Cached:            76628 kB
SwapCached:            0 kB
Active:           151540 kB
Inactive:          78304 kB
Active(anon):     129784 kB
```

Chromecast

```
--------- beginning of /dev/log/main
05-11 13:38:35.461  1697  1697 I eureka_shell: HTMLMediaElement::currentTime - see
05-11 13:38:35.461  1697  1697 I eureka_shell: HTMLMediaElement::play()
05-11 13:38:35.461  1697  1697 I eureka_shell: HTMLMediaElement::playInternal
05-11 13:38:35.461  1697  1697 I eureka_shell: HTMLMediaElement::currentTime - see
05-11 13:38:35.461  1697  1697 I eureka_shell: HTMLMediaElement::invalidateCachedT
05-11 13:38:35.461  1697  1697 I eureka_shell: HTMLMediaElement::currentTime - see
05-11 13:38:35.461  1697  1697 I eureka_shell: HTMLMediaElement::updatePlayState -
```

Logs contain information about:

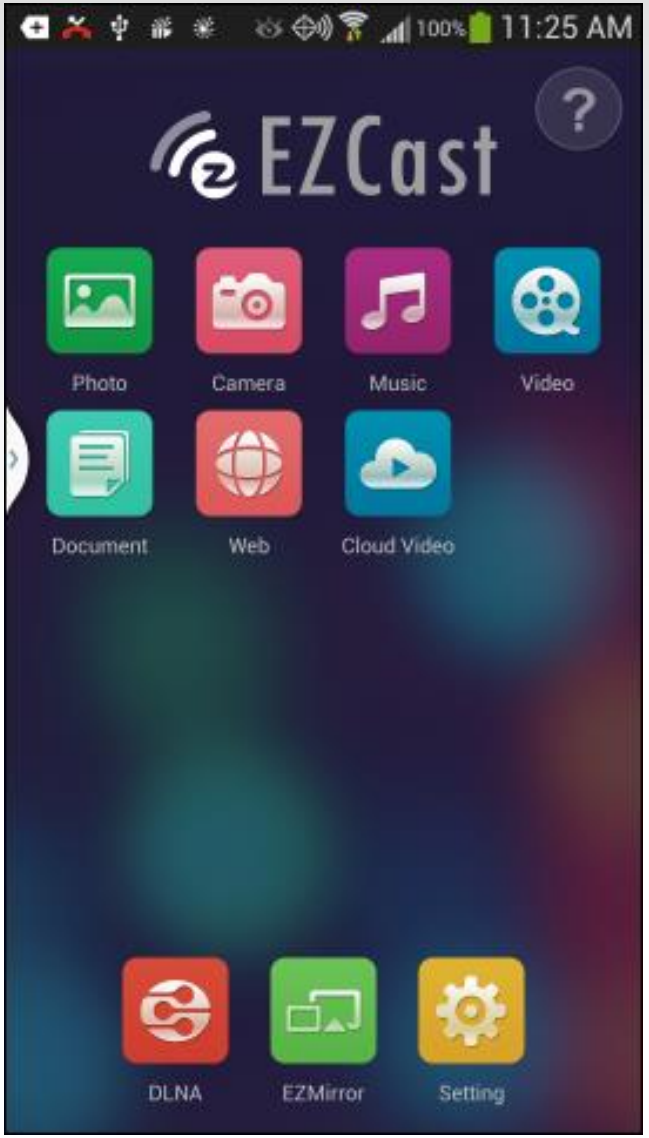
- Running processes, CPU info, Memory info
- Kernel-log, Boot-log, **Main-log**
- Date/time of starting/stopping videos
- Memory mapping of processes

Miracast

Measy A2W Miracast
128MB RAM, 1GB NAND
Enables *casting* to TV

A2W Miracast

- Developed by Actions-Micro
- EZCast firmware on all their Miracast devices
- Controlled by computer or Android/iOS app



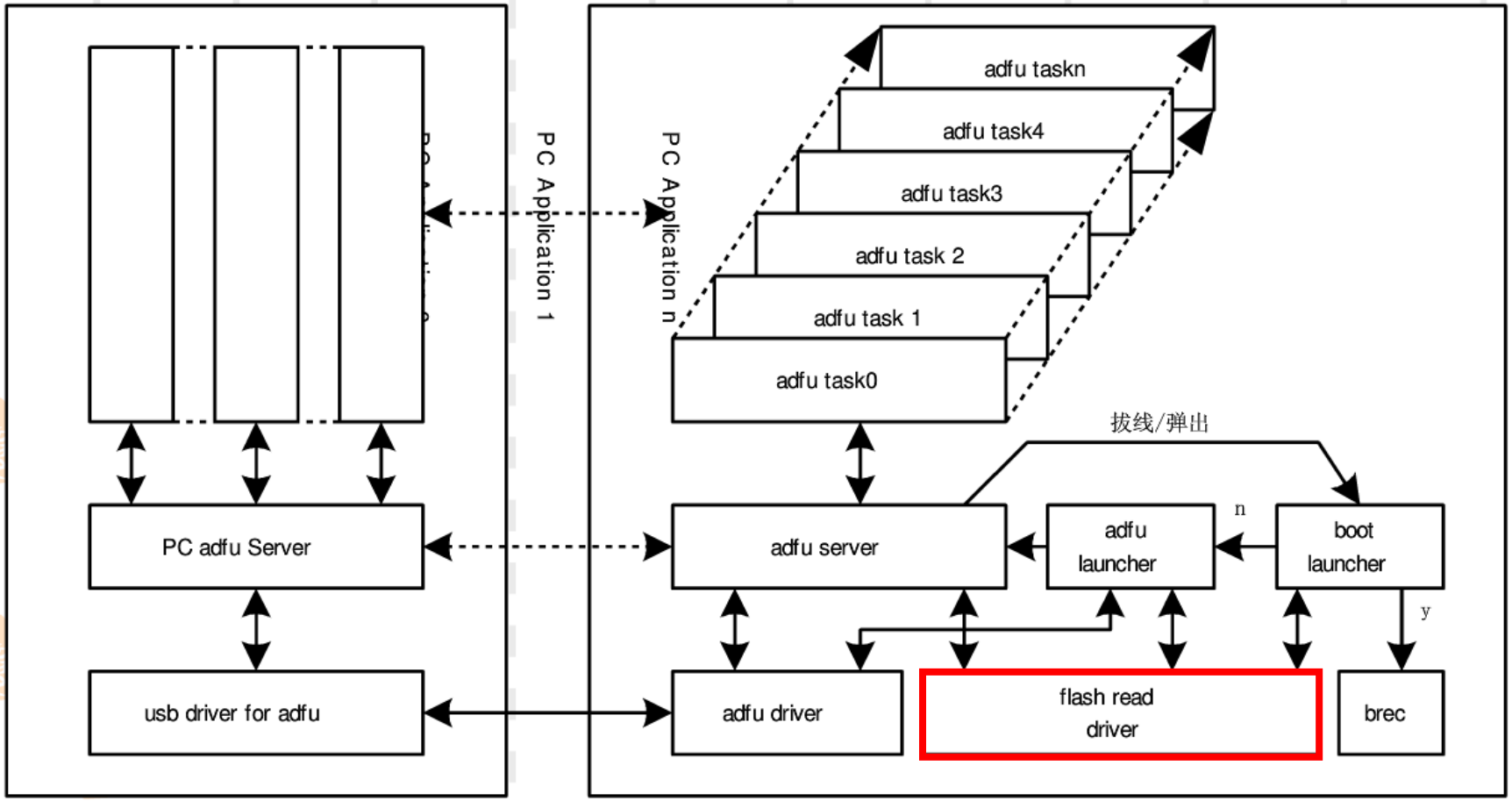
A2W Miracast
Software

- Runs EZCast firmware
  - BusyBox/1.15.1 (udhcpc exploit)
  - thttpd/2.25b (directory traversal)
- Badly designed CGI binaries
  - String formatting vulnerabilities
  - Arbitrary file writing in /tmp
  - Unfinished
- ... But nothing that could be exploited ☹

A2W Miracast
ADFU

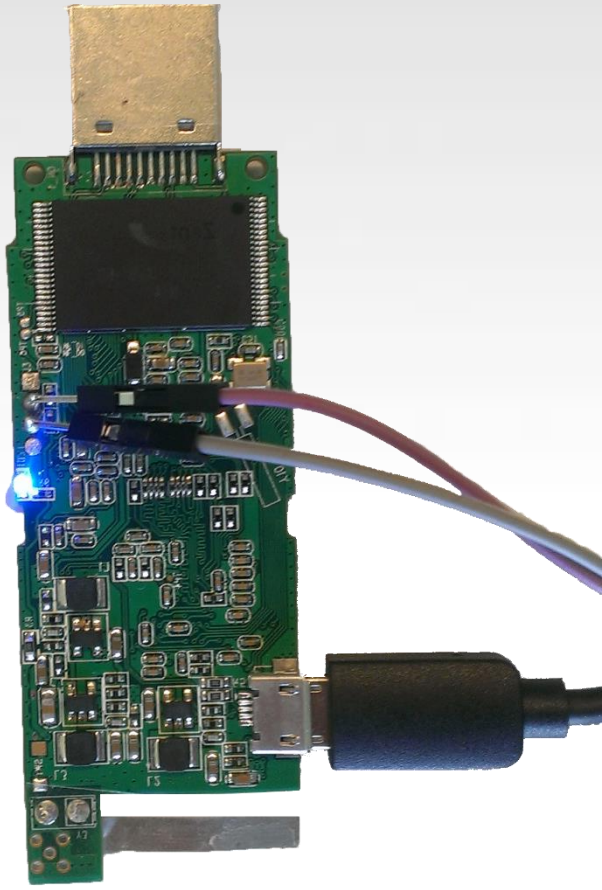
- Similar hardware has test pins to access ADFU mode
  - Actions Device Firmware Update
  - We can now write our own firmware
  - Kind of useless for forensics
  - USB protocol is proprietary

ADFU
actions device firmware update



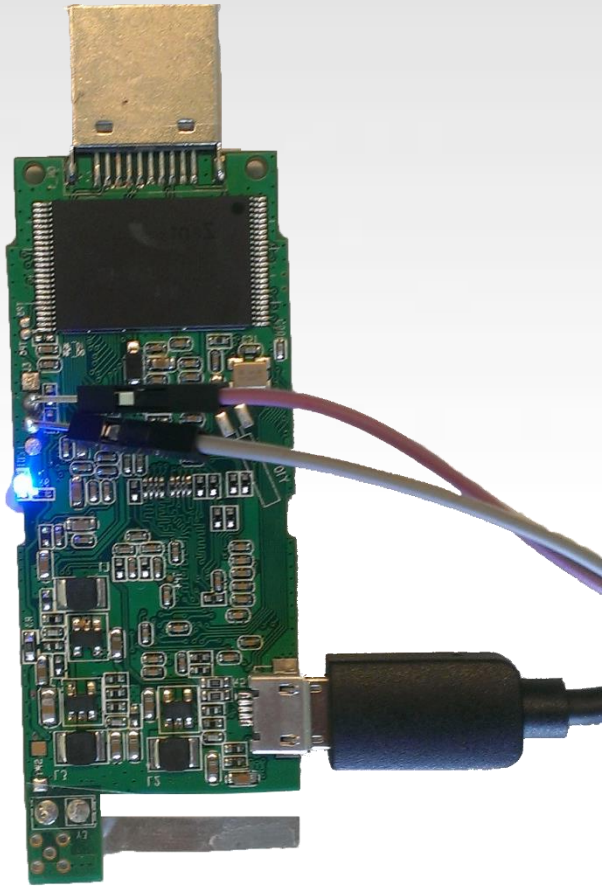
A2W Miracast
Debug interface

- BusPirate scanning of interfaces
  - Found garbage!
  - UART baudrate 115200
  - root shell
- Flash
  - dmesg output (startup times)
  - Nothing else is saved except the wifi password



A2W Miracast
Memory

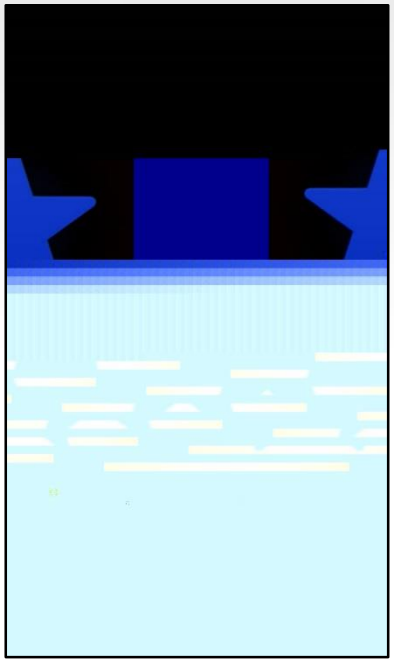
- Memory dumping over wireless
  - dd if=/dev/mem | netcat host 5353
- Found:
  - Carved images (probably useless)



A2W Miracast
Carving

Original

Carved

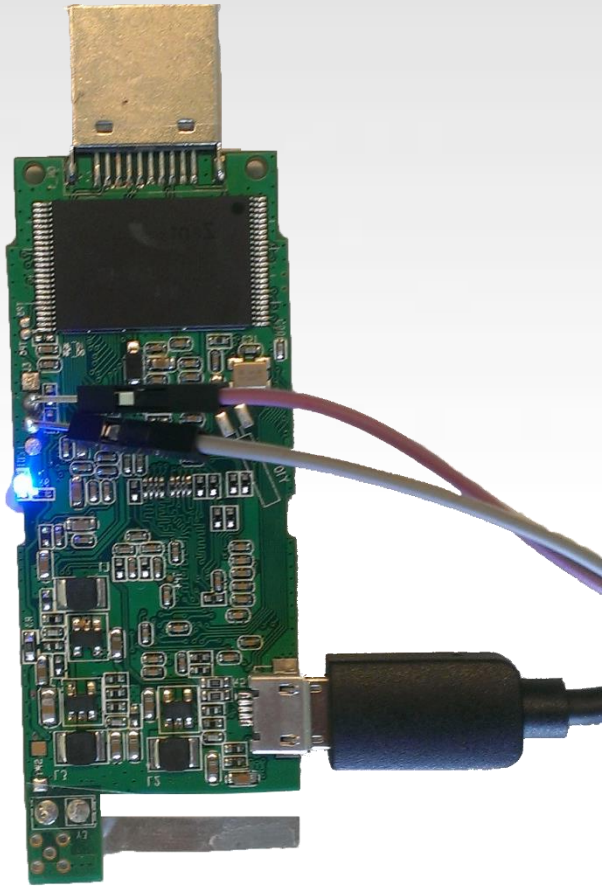


Phone view

HDMI view

A2W Miracast
Memory

- Memory dumping over wireless
  - dd if=/dev/mem | netcat host 5353
- Found:
  - Carved images (probably useless)
  - Browsed links (long time in memory)
  - YouTube videos (long time in memory)
  - MAC addresses (probably useless)
- Note:
  - Transfering of memory overwrites memory



Conclusion

- Chromecast
  - Crash dumps over HTTP tell us when the device was used
  - If NAND accessible in the future, links could be extracted of played videos

- Miracast
  - NAND extractable, but nothing of interest except wifi password
  - For a limited time, images, links, MAC addresses can be carved from the memory