

# Repurposing Gadgets

Daniel Maslowski

**spring();**  
break;

# Agenda



Introduction



Gadgets and Ideas



Tools and Utilities



Tinkering

```
spring();  
break;
```

# Introduction

```
spring();  
break;
```

# Hello, I am Daniel :-)



## Work and education



IT security and computer science



software engineer



infrastructure and web



apps, UIs, ecommerce

## Open Source contributions



hardware and firmware



operating systems



software distributions



reverse engineering

**spring();**  
break;

## Gadgets and Ideas

**spring();**  
break;

# Wireless Storages

... are just networked devices with storage



## old ideas

- 👤 MCU running a small application, sometimes RTOS
- 👤 SoC, Arm or MIPS, running Linux
- 👤 built-in SD card reader

## new ideas

- 👤 access point for devices in your NoT (Network of Things)
- 👤 MQTT broker for controlling things, e.g., via SUSI AI

**spring();**  
**break;**

# Network Video Recorders (NVRs)



## old ideas

- 👤 essentially storage with more connectors
  - ▶ USB, HDMI, ethernet
  - ▶ built-in network switch
  - ▶ analog video input
- 👤 SoC, mostly Arm, running Linux

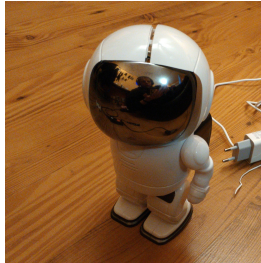
## new ideas

- 👤 little general purpose computer with web browser
- 👤 home theatre / movie player

**spring();**  
break;

# IP cameras

Essentially, these are just camera sensors attached to some SoC that is running Linux, with Wi-Fi and/or ethernet modules and often SD card readers.



They typically feature two motors to rotate and tilt, sometimes a speaker and a microphone for two-way audio communication.

OpenIPC project - <https://openipc.org/>

**spring();**  
**break;**

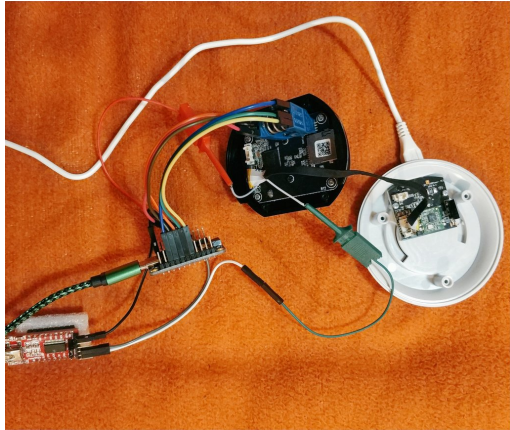


## Tools and Utilities

**spring();**  
break;

# Hardware

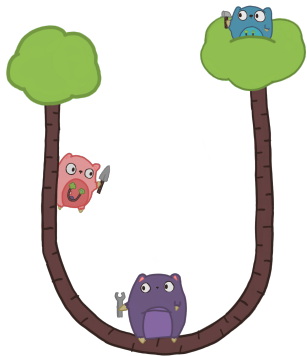
- 👤 network cables and switch
- 👤 wireless access point
- 👤 SPI flash programmer
- 👤 USB serial converter
- 👤 dupont wires and probes
- 👤 soldering equipment
- 👤 screwdrivers







`spring();`  
`break;`

# u-root

A universal root filesystem



<https://u-root.org/>

-  many small tools
-  all open, meant for studying and understanding
-  easily portable
-  written in Go



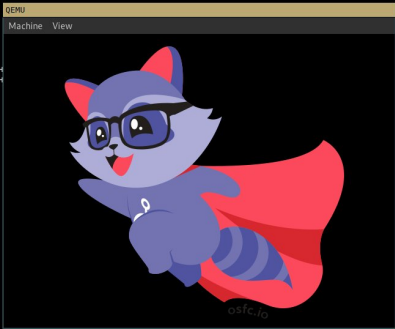
**spring();**  
break;

# u-root Graphics

```
1 2 3 4 7 [Live - Mitschnitt] EdenHeimer @ Parookavi 207G 1 day 5.6.15 orangewrt 101% 01:29 2020-06-11
tmux: /home/dan/go/src/github.com/u-root/u-root
2.609348 cfg80211: Loading compiled-in X.509 certificates for regulatory database
2.609348 cfg80211: Loading compiled-in X.509 certificates for regulatory database
2.614659 cfg80211: Loaded X.509 cert 'sforshee: 00b28ddf47aef9cea7'
2.614659 cfg80211: Loaded X.509 cert 'sforshee: 00b28ddf47aef9cea7'
2.618696 platform regulatory: Direct firmware load for regulatory.db
2.618696 platform regulatory: Direct firmware load for regulatory.db
2.626740 cfg80211: failed to load regulatory.db
2.626740 cfg80211: failed to load regulatory.db
4.128016 floppy0: no floppy controllers found
4.128016 floppy0: no floppy controllers found
4.132123 scsi 2:0:0:0: CD-ROM QEMU QEMU DVD-ROM 2.54
4.132123 scsi 2:0:0:0: CD-ROM QEMU QEMU DVD-ROM 2.54
4.156113 sr 2:0:0:0: [sr0] scsi3-mmc drive: 4x/4x cd/rw xa/form2 tray
4.156113 sr 2:0:0:0: [sr0] scsi3-mmc drive: 4x/4x cd/rw xa/form2 tray
4.161769 cdrom: Uniform CD-ROM driver Revision: 3.20
4.161769 cdrom: Uniform CD-ROM driver Revision: 3.20
4.166065 sr 2:0:0:0: Attached scsi generic sg0 type 5
4.166065 sr 2:0:0:0: Attached scsi generic sg0 type 5
4.171155 Freeing unused kernel image (initmem) memory: 1636K
4.171155 Freeing unused kernel image (initmem) memory: 1636K
4.178898 Write protecting the kernel read-only data: 32768k
4.178898 Write protecting the kernel read-only data: 32768k
4.184760 Freeing unused kernel image (text/rodata gap) memory: 2040K
4.184760 Freeing unused kernel image (text/rodata gap) memory: 2040K
4.188583 Freeing unused kernel image (rodata/data gap) memory: 200K
4.188583 Freeing unused kernel image (rodata/data gap) memory: 200K
4.192784 Run /init as init process
4.192784 Run /init as init process
2020/06/10 23:29:09 Welcome to u-root!

u-root

[ 4.214060] cgroup: Unknown subsys name 'net_cls'
[ 4.214060] cgroup: Unknown subsys name 'net_cls'
[ 4.217236] cgroup: Unknown subsys name 'hugetlb'
[ 4.217236] cgroup: Unknown subsys name 'hugetlb'
Framebuffer resolution: 640 480 640 3
- />
0 sh dan ???@webboot 0 fish 2 sh * :-| orangepad 101%
```



spring();  
break;

# centre



DHCP server



TFTP server



simple binary, written in Go



easy to run on your laptop

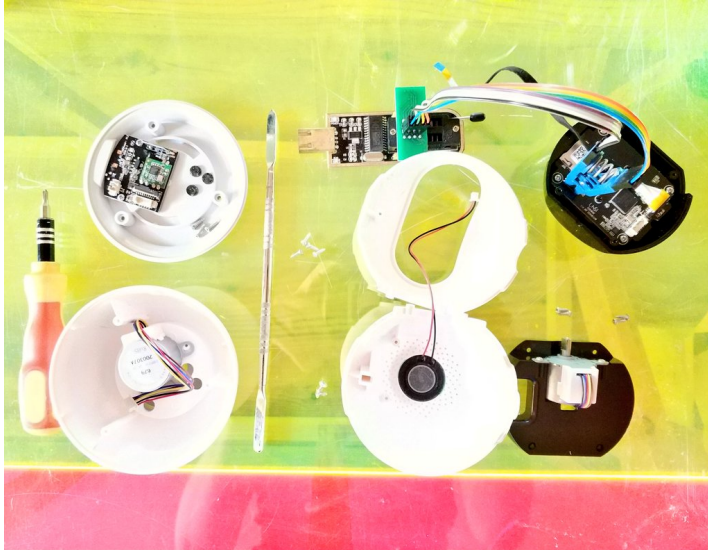
<https://github.com/Harvey-OS/go/tree/main/cmd/centre>

**spring();**  
break;

Tinkering

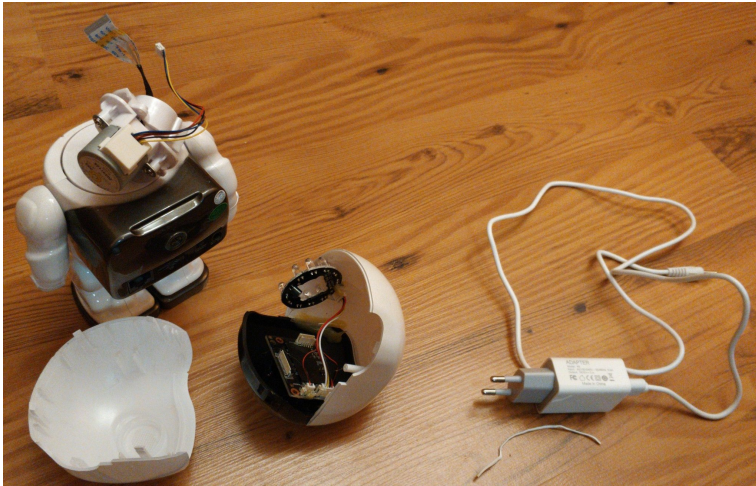
**spring();**  
break;

# IP Camera Teardown



```
spring();  
break;
```

# Astronaut Teardown



```
spring();  
break;
```

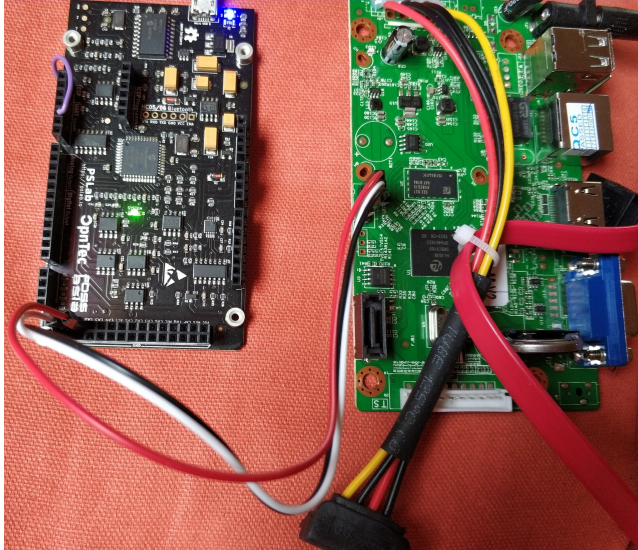


## NVRs from inside



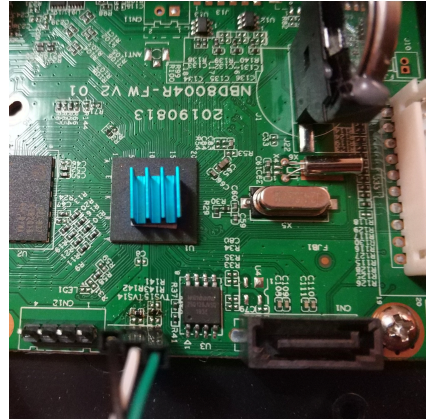
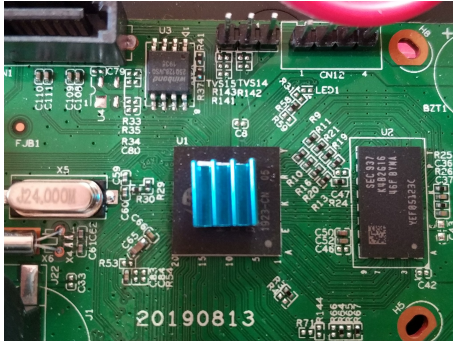
```
spring();  
break;
```

# PSLab as a Logic Analyzer



```
spring();  
break;
```

# Adding Missing Components



```
spring();  
break;
```

# Serial and U-Boot

```
0 Storage Device(s) found
i:0, No usb storage device found!
Press CTRL-C to abort autoboot in 0 seconds16384 KiB hi_fmc at 0:0 is now
current device
CFG BOOT ADDR:0x0 argc 2 argv[0] logoload
### h264dvr.jpg UbootLogoload complete:bytes oadaddr0x84000000 loaded to
0x8dc00000
### h264dvr.jpg UbootLogoload complete: 32878 bytes loaded to 0x8dc00000
jpeg decoding ...
<<addr=0x8dc00000, size=0xb85f9, vobuf=0x8dd00000>>
PicType: 3 ,Output Addr, Y: 8dd00000,UV: 8dd7b800
<<imgwidth=800, imgheight=600, linebytes=832>>
decode success!!!!
decode jpeg success.
decode jpeg!
stMaxRect.u32Width:800, stMaxRect.u32Height:600.
srcAddr 0x82000000, dstAddr 0x81000000
find_squashfs_file: name bin, start_block 0, offset 2653, type 1
find_squashfs_file: name boot, start_block 0, offset 2757, type 1
read_inode: name boot, sb 0, of 2757, type 1
find_squashfs_file: name zImage.img, start_block 0, offset 2685, type 2
read_inode: name zImage.img, sb 0, of 2685, type 2
### FS load complete: 2454195 bytes loaded to 0x81000000
## Booting kernel from Legacy Image at 81000000 ...
Image Name: Linux-4.9.37
Image Type: ARM Linux Kernel Image (uncompressed)
Data Size: 2454131 Bytes = 2.3 MiB
Load Address: 80008000
Entry Point: 80008000
Loading Kernel Image ... OK
OK
Starting kernel ...
```

spring();  
break;

# U-Boot Shell

```
System startup.....
System startup

U-Boot 2010.06-svn1338 (Oct 11 2019 - 13:43:25)

Check Flash Memory Controller v100 ... Found
SPI Nor(cs 0) ID: 0xef 0x40 0x18
eFlashType: 3.
Flash Name: XM_W25Q128FV, W25Q128JV{0xEF4018}, 0x1000000.
@hifmc spi_nor_probe(), XmspiNor ProtMgr probe(): OK.
@XmspiNor_enableQuadMode(), Disable Quad Failed, SRx: [2, 0x3F].
@XmspiNor_enable4ByteAddrMode(), isn't support 4-byte mode.
Block:64KB Chip:16MB Name:"XM_W25Q128FV,W25Q128JV"
CONFIG CLOSE SPI_8PIN_4IO = y.
read->iftype[0: STD, 1: DUAL, 2: DIO, 3: QUAD, 4: QIO]: 1.
Current level[0], lock_level_max:7.
unlock all.
SRx val: {[1, 0x2], [1, 0x3F], [1, 0xE0], [0, 0x0]}.
SPI Nor total size: 16MB
In: serial
Out: serial
Err: serial
USB: scanning bus for devices... 1 USB Device(s) found
0 Storage Device(s) found
USB: scanning bus for devices... 1 USB Device(s) found
0 Storage Device(s) found
i:0, No usb storage device found!
Press CTRL-C to abort autoboot in 2 secondshisilicon # <INTERRUPT>
hisilicon # <INTERRUPT>
hisilicon # wheee :)|
```

```
CTRL-A Z for help | 115200 8N1 | NOR | Minicom 2.7.1 | VT102 | Online 0:0 | ttyUSB0
```

spring();  
break;

# U-Boot TFTP

```
hisilicon # sf read 0x82000000 0x0 0x1000000
hisilicon # tftp 0x82000000 firmware.bin 0x1000000
Hisilicon ETH net controller
MAC: 00-0B-3F-00-00-01
eth0 : phy status change : LINK=DOWN : DUPLEX=FULL : SPEED=100M
eth0 : phy status change : LINK=UP : DUPLEX=FULL : SPEED=100M
TFTP to server 192.168.1.12; our IP address is 192.168.1.10
Upload Filename 'firmware.bin'.
Upload from address: 0x82000000, 16.000 MB to be send ...
Uploading: # [ Connected ]
##### [ 2.888 MB]
##### [ 5.752 MB]
##### [ 8.616 MB]
```

**spring();**  
**break;**

# U-Boot Kernel Commandline

```
anyka$setenv bootargs 'console=ttySAK0,115200n8 root=/dev/mtdblock4 rootfstype=squashfs
init=/sbin/init mem=64M memsize=64M single'

anyka$printenv
        backuppage=ffffffff
baudrate=115200
boot_normal=readcfg; run read kernel; bootm ${loadaddr}
bootargs=console=ttySAK0,115200n8 root=/dev/mtdblock4 rootfstype=squashfs
init=/sbin/init mem=64M memsize=64M single
...
Environment size: 979/4088 bytes

anyka$saveenv

Saving Environment to SPI Flash...
Env save done OK

anyka$reset
        resetting ...
heartbeat = 1
...
Starting kernel ...

Uncompressing Linux... done, booting the kernel.
Anyka Linux Kernel Version: 2.5.02
Booting Linux on physical CPU 0
Linux version 3.4.35 (ma@ma-PC) (gcc version 4.8.5 (anyka (gcc-4.8.5 + binutils-2.24 +
ulcibc-0.9.33.2)(20170223)) ) #19 Fri Oct 18 11:21:47 CST 2019
CPU: ARM926EJ-S [41069265] revision 5 (ARMv5TEJ), cr=00053177
...
Freeing init memory: 100K
-/bin/sh: id: not found
welcome to file system
[root@(none) ~]$ ls
bin dev etc ext init lib mnt mvs proc sbin sys tmp usr var
[root@(none) ~]$
```

spring();  
break;

# No init, just insmod

```
[root@none] ~]$ insmod /ext/modules/rtl8188fu.ko
RTL871X: module init start
RTL871X: rtl8188fu v4.3.23.1 16377.20151216
RTL871X: build time: May 31 2018 17:23:04
usbcore: registered new interface driver rtl8188fu
RTL871X: module init ret=0
[root@none] ~]$ insmod /mvs/modules/otg-hs.ko
usb-host usb-host: Anyka usb host controller
usb-host usb-host: new USB bus registered, assigned bus number 1
usb-host usb-host: irq 18, io mem 0x20200000
usb usb1: New USB device found, idVendor=1d6b, idProduct=0002
usb usb1: New USB device strings: Mfr=3, Product=2, SerialNumber=1
usb usb1: Product: Anyka usb host controller
usb usb1: Manufacturer: Linux 3.4.35 usb-host
usb usb1: SerialNumber: Anyka usb host controller
hub 1-0:1.0: USB hub found
hub 1-0:1.0: 1 port detected
usb otg-hs controller driver initialized
usb 1-1: new high-speed USB device number 2 using usb-host
usb 1-1: New USB device found, idVendor=0bda, idProduct=f179
usb 1-1: New USB device strings: Mfr=1, Product=2, SerialNumber=3
usb 1-1: Product: 802.11n
usb 1-1: Manufacturer: Realtek
usb 1-1: SerialNumber: 00e04c000001
RTL871X: hal_com config channel plan chplan:0x20
RTL871X: rtw_ndev_init(wlan0) if1 mac_addr=7c:a7:b0:55:5a:f8
[root@none] ~]$ ifconfig -a
lo        Link encap:Local Loopback
          LOOPBACK MTU:16436 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

wlan0     Link encap:Ethernet HWaddr 7C:A7:B0:55:5A:F8
          BROADCAST MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
```

spring();  
break;



# u-root on a Wireless Storage

```
root@airdisk:~# chroot mipsle/ /bin/sh
/# ls -l
Exception: exec: "ls": executable file not found in $PATH
[ttty], line 1: ls -l
/# paths=[/bbin $@paths]
/# ls -l
drwxr-xr-x 1001 1001 0 Sep 15 20:26 bbin
drwxr-xr-x 1001 1001 0 Sep 15 20:18 bin
drwxr-xr-x 1001 1001 0 Apr 22 18:02 dev
drwxr-xr-x 1001 1001 0 Sep 15 20:18 etc
Lrwxrwxrwx root 0 9 Sep 15 20:18 init -> bbin/init
drwxr-xr-x 1001 1001 0 Apr 22 18:02 lib64
drwx----- root 0 0 Sep 15 19:50 root
drwxr-xr-x 1001 1001 0 Apr 22 18:02 tcz
drwxrwxrwx 1001 1001 0 Apr 22 18:02 tmp
drwxr-xr-x 1001 1001 0 Apr 22 18:02 ubin
drwxr-xr-x 1001 1001 0 Apr 22 18:02 usr
drwxr-xr-x 1001 1001 0 Apr 22 18:02 var
/# cat /etc/resolv.conf
nameserver 8.8.8.8
/# uname -a
Linux airdisk 3.10.14+ #2 Tue Sep 15 20:03:49 CST 2015 mips (none)
/#
```

root@airdisk

spring();  
break;

u-root on an NVR



```
spring();  
break;
```

Thanks! Questions?

**spring();**  
break;

Extras

```
spring();  
break;
```

# Fun

astronaut protocol

SanDisk Media Drive disco

```
spring();  
break;
```