



# When IoT Attacks:

## Hacking A Linux-Powered Rifle

# Who are we?

- Runa A. Sandvik
- Michael Auger

## The TrackingPoint 338TP, the Linux rifle that's accurate up to a mile

You'll find Linux everywhere, including in the most accurate rifles in the world.



By Steven J.



News Video Events Crunchbase

Search

DISRUPT SF Y-Combinator's Sam Altman To Take The Stage At Disrupt SF Get \$1,000 Off Tickets Now

guns

linux

I grew up in rural  
shoot. All I know  
grew up in a gun  
school at West V  
Championship in  
to shoot accurate  
best. I was never

## A Precision Guided Firearm Powered by Linux

Posted Apr 2, 2013 by Scott Merrill (@smerrill), Contributor

482  
SHARES



ars technica

MAIN MENU MY STORIES: 1 FORUMS SUBSCRIBE JOBS ARS CONSORTIUM

### GEAR & GADGETS / PRODUCT NEWS & REVIEWS

## \$17,000 Linux-powered rifle brings "auto-aim" to the real world

Austin-based startup makes "Precision Guided Firearms" sporting a lot of tech.

by Lee Hutchinson - Jan 9, 2013 3:45pm EST

LATEST FEATURE STORY



technology about which I'm large  
products are entirely my fault. Th  
interesting way to use Linux and I  
computing, social networking, an

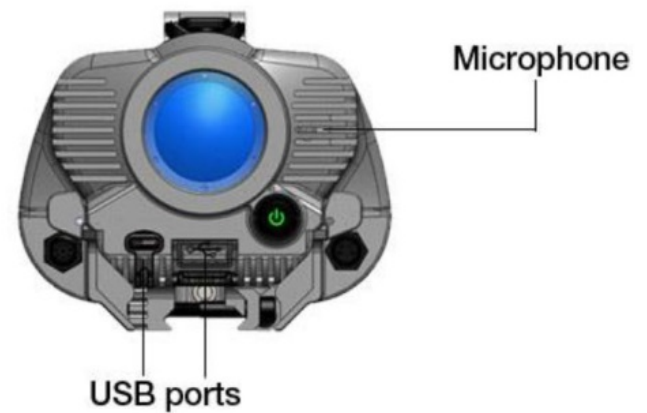
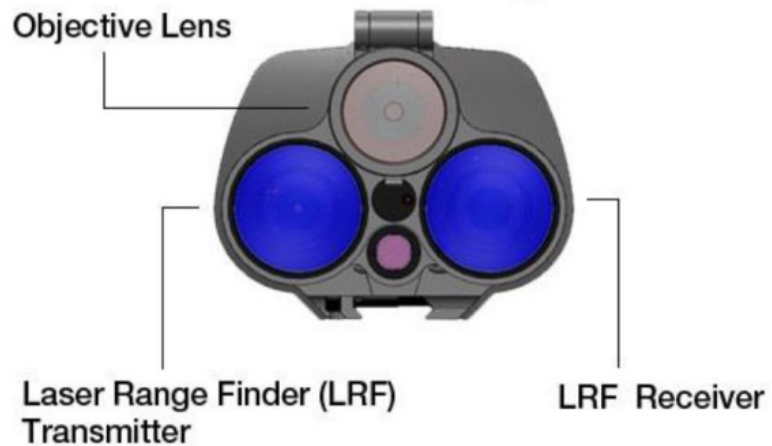
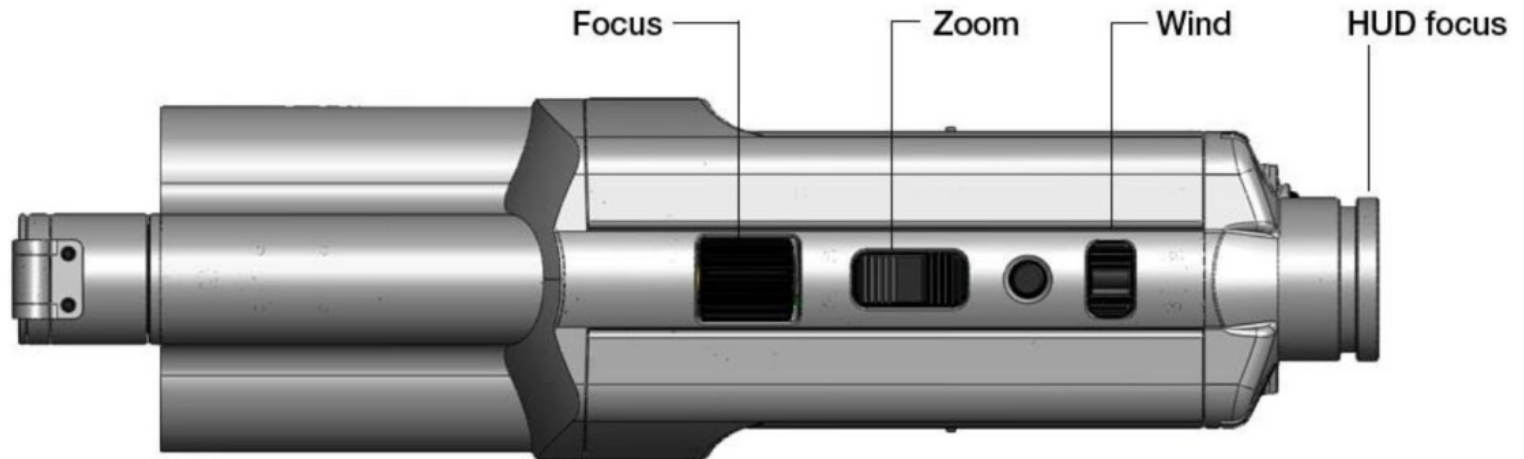
Tracking Point was founded in 20



# Why are we doing this?

- A gun with WiFi and fancy electronics... duh

# Physical







Nmap scan report for 192.168.1.1

Host is up (0.0049s latency).

Not shown: 65533 filtered ports

| PORT | STATE | SERVICE | VERSION |
|------|-------|---------|---------|
|------|-------|---------|---------|

|        |      |      |          |
|--------|------|------|----------|
| 80/tcp | open | http | lighttpd |
|--------|------|------|----------|

|\_http-methods: OPTIONS GET HEAD POST

|\_http-title: Site doesn't have a title (text/html).

|         |      |      |                 |
|---------|------|------|-----------------|
| 554/tcp | open | rtsp | GStreamer rtspd |
|---------|------|------|-----------------|

|\_rtsp-methods: ERROR: Script execution failed (use -d to debug)

Warning: OSScan results may be unreliable because we could not find at least...

Device type: storage-misc|general purpose|specialized|WAP|media device|phone

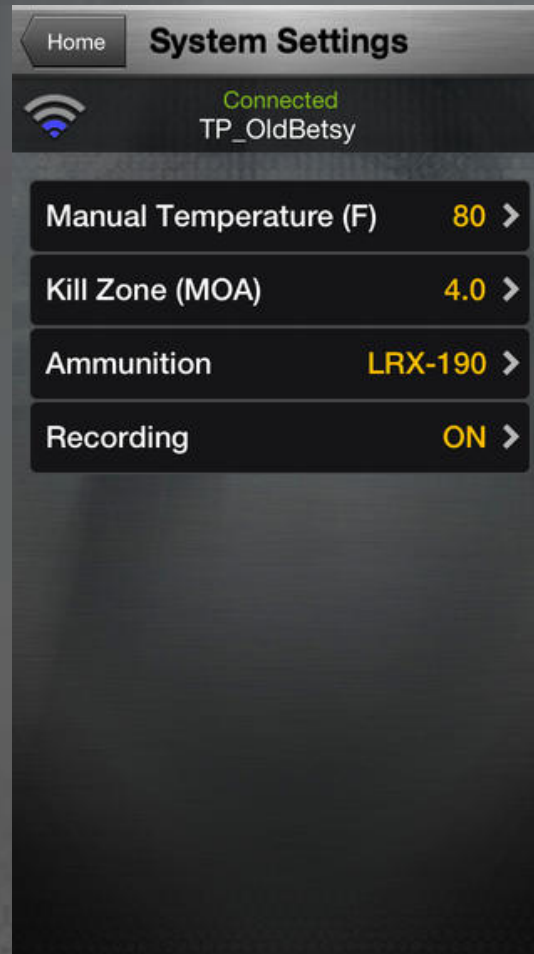
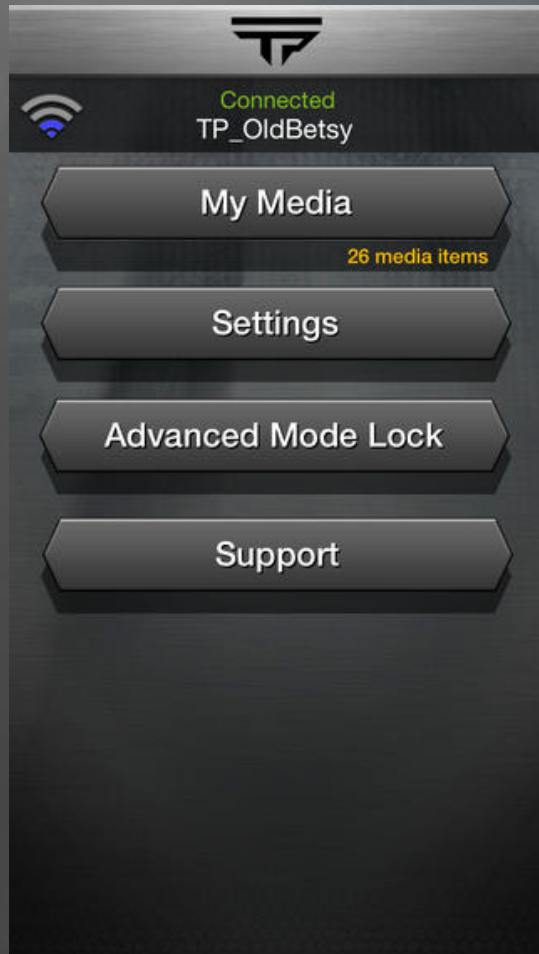
Running (JUST GUESSING): HP embedded (97%), Linux 2.6.X|3.X (95%)...

Aggressive OS guesses: HP P2000 G3 NAS device (97%), Linux 2.6.36 - 2.6.37 (95%)

# Mobile Apps



# TrackingPoint App



# ShotView App



# Public API

## Mobile Apps

/clear\_passcode/  
/config/  
/dateset/  
/delete/  
/dir/  
/get\_passcode/  
/get\_shot\_data/  
/gps/  
/pkg-upload/  
/progress/  
/serial\_num/  
/service/  
/set\_factory\_defaults/  
/set\_passcode/  
/set\_windage/  
/unwatch/  
/updatescope/  
/version/

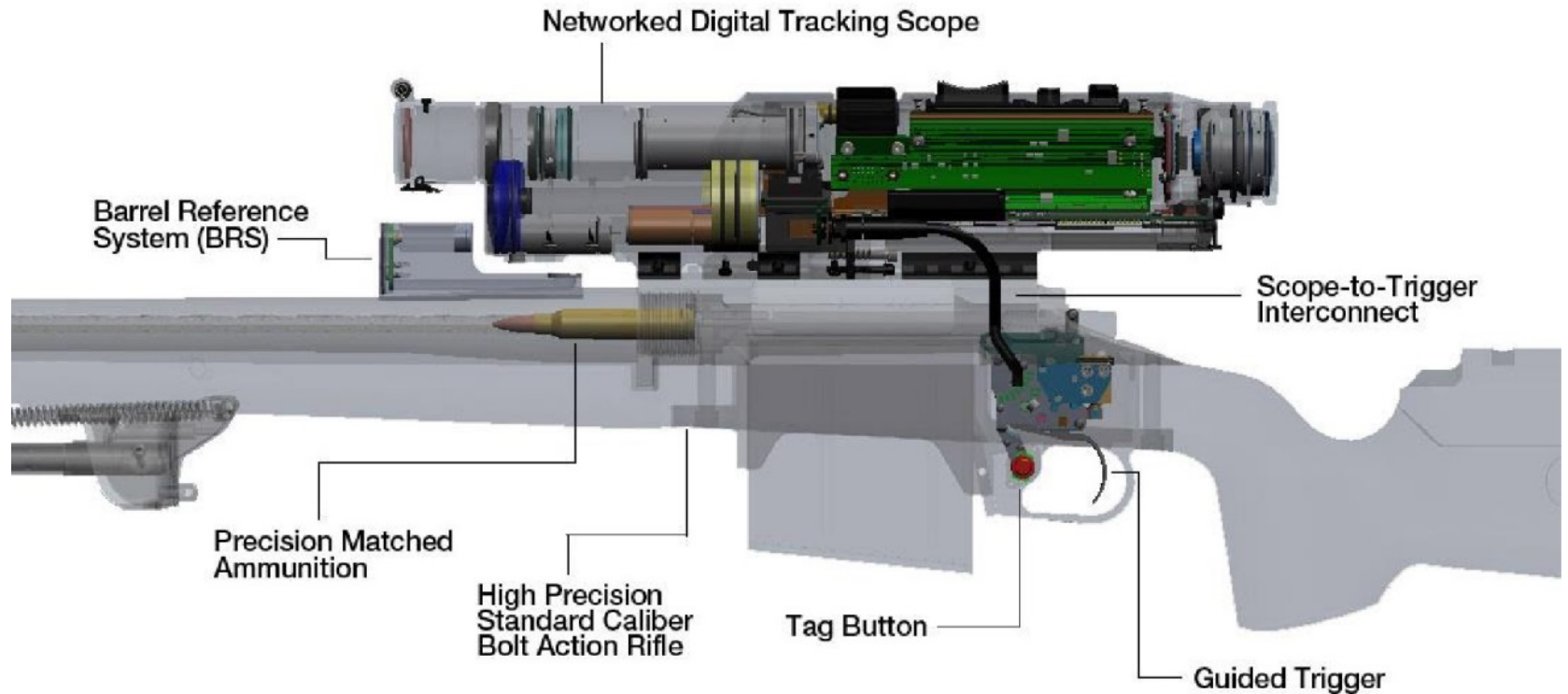
## Config

/set\_ammunition/  
/set\_imagestab/  
/set\_killzone/  
/set\_temperature/  
/set\_record\_cooltime/  
/set\_recording/

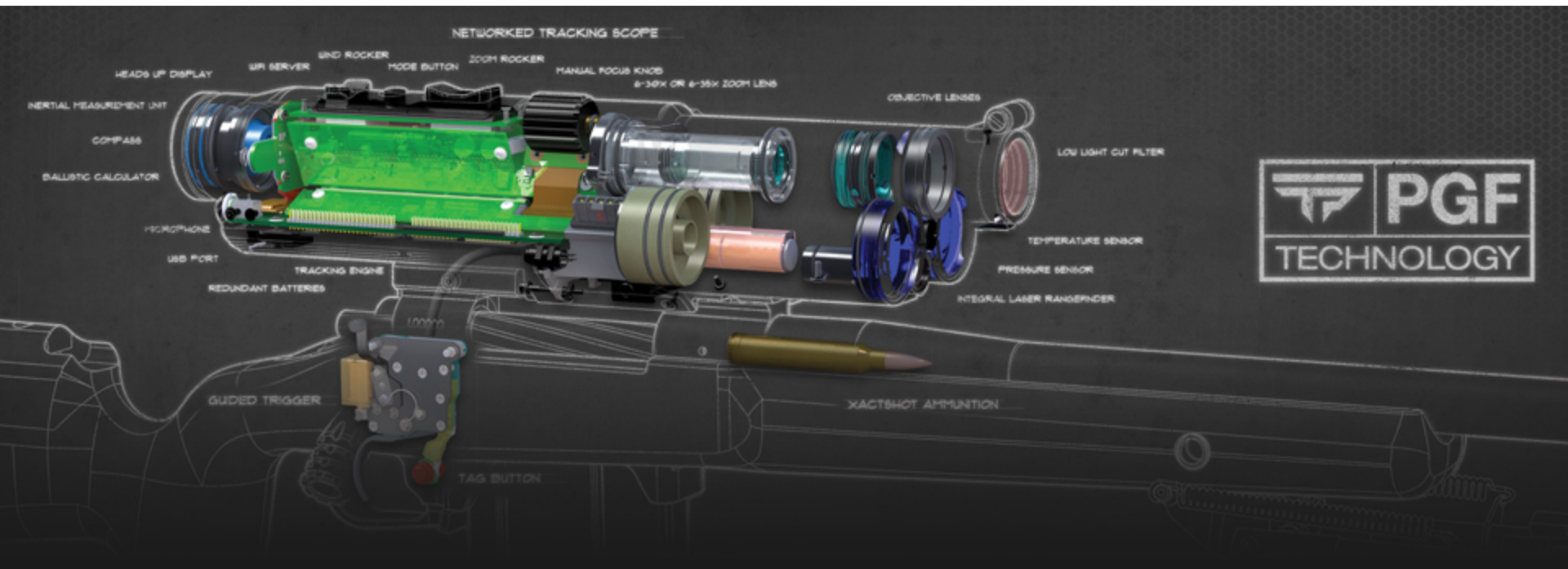
# Initial Findings

- SSID contains the serial number, can't be changed
- WPA2 key can't be changed
- VLC or anything can stream the scope view
- Advanced mode lock is only a 4 digit pin and can be brute forced
- API is un-authenticated
- API settings can be modified regardless of advanced mode lock

# Courtesy of TrackingPoint's Website



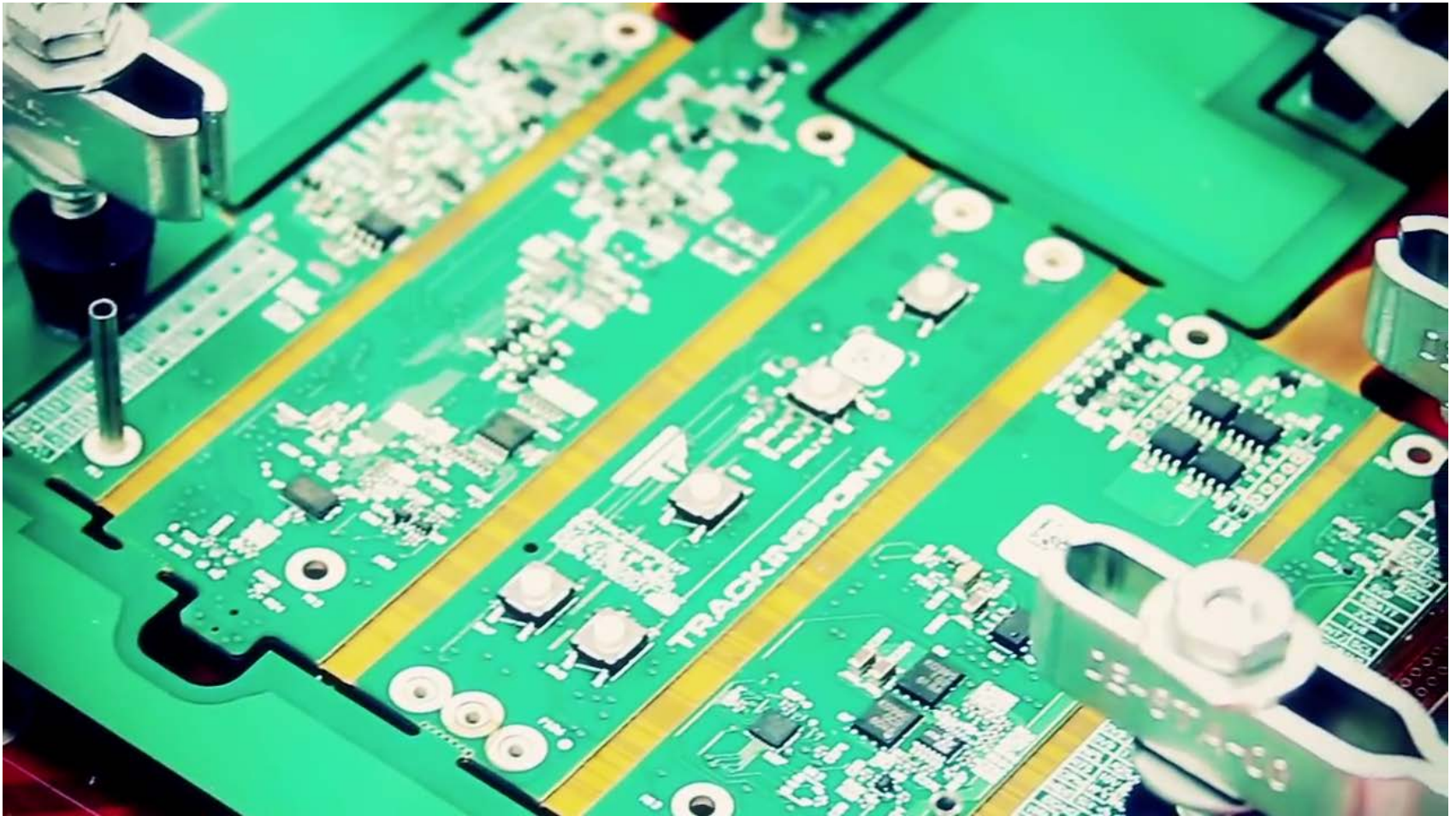
# Courtesy of TrackingPoint's Website



# Tearing it open

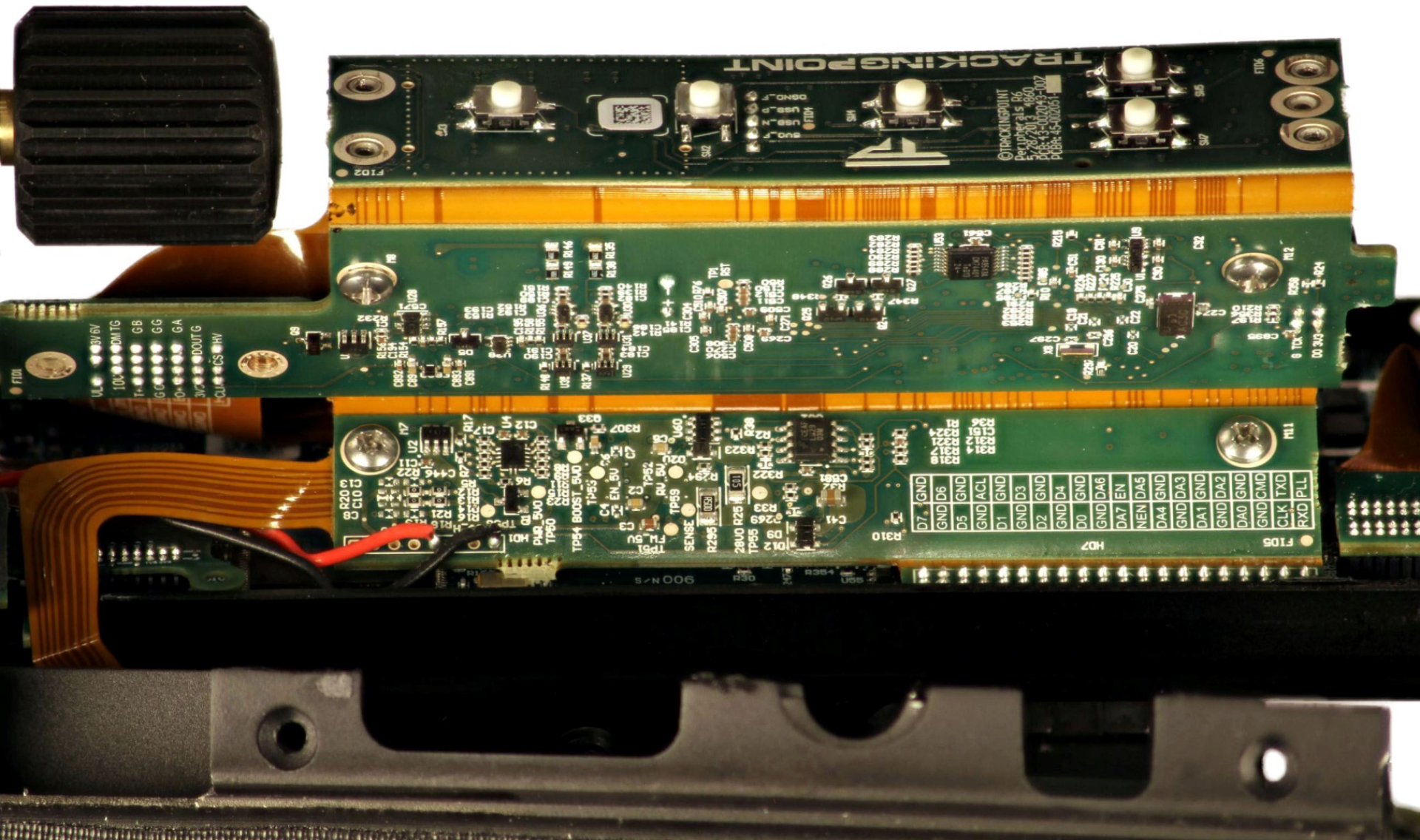


Courtesy of TrackingPoint's YouTube

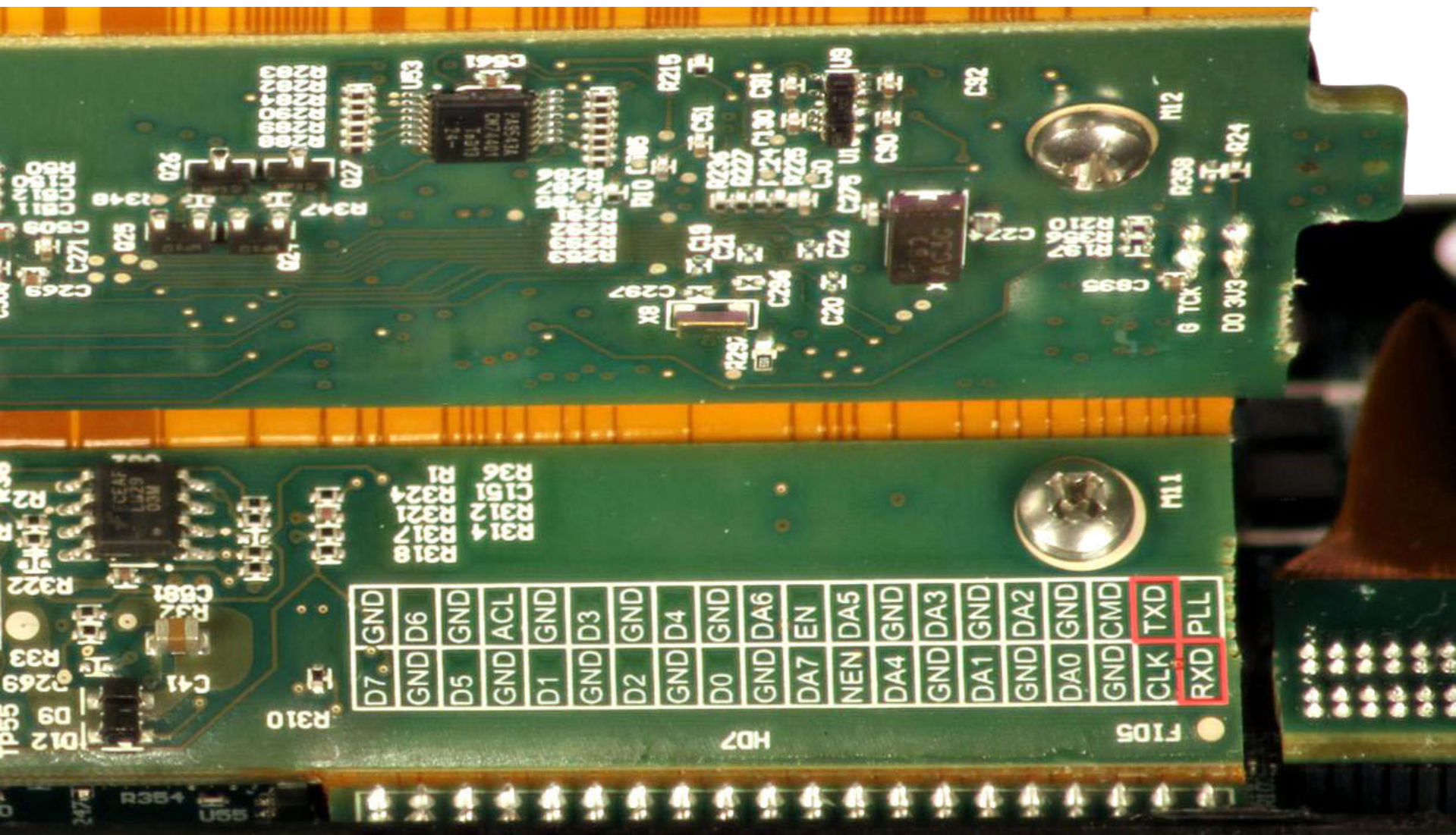




# Close Up



# UART



# Woot!

U-Boot 2010.06-00300-gfb2cb26 (Jul 10 2013 - 17:39:57)

TI8148-GP rev 2.1

ARM clk: 600MHz

DDR clk: 400MHz

I2C: ready

DRAM: 512 MiB

Flash: 16 MiB

```
TTTTT RRRR AA CCC K K III N N GGG PPPP OOO III N N TTTTT
TT R R A A C K K I NN N G P P O O I NN N TT
TT RRRR AAAA C KK I N NN G GG PPPP O O I N NN TT
TT R R A A C K K I N NN G G P O O I N NN TT
TT R RR A A CCC K K III N N GGG P OOO III N N TT
```

S H O T. M A D E!

MMC: OMAP SD/MMC: 0

Net: MAC:7c:66:9d:41:8:88 Dev:cpsw

Hit any key to stop autoboot: 0

Booting side 2

## Booting kernel from Legacy Image at 08360000 ...

Image Name: Linux-2.6.37

Image Type: ARM Linux Kernel Image (uncompressed)

Data Size: 2314892 Bytes = 2.2 MiB

Load Address: 80008000

Entry Point: 80008000

Loading Kernel Image ... OK

OK

Starting kernel ...

# Well played TrackingPoint...

```
usbcore: registered new interface driver ath9k_htc
usb 2-1.2: ath9k_htc: Transferred FW: htc_9271.fw, size: 51272
ath9k_htc 2-1.2:1.0: ath9k_htc: HTC initialized with 33 credits
ath9k_htc 2-1.2:1.0: ath9k_htc: FW Version: 1.3
ieee80211 phy0: Atheros AR9271 Rev:1
Enabling iptables...
ip_tables: (C) 2000-2006 Netfilter Core Team
nf_conntrack version 0.5.0 (3969 buckets, 15876 max)
Starting portmap daemon: portmap.
Caching udev devnodes
INIT: Entering runlevel: 5
Starting Dropbear SSH server: NET: Registered protocol family 10
dropbear.
Starting Lighttpd Web Server: lighttpd.
```



TRACKINGPOINT

S H O T . M A D E .

Linux TP\_TP750-308FF89765R 2.6.37

Arago 2011.09 TP\_TP750-308FF89765R tty00

TP\_TP750-308FF89765R login:

# ...well played



TETRIS

SHOT. MADE.

Linux TP\_TP750-308FF89765R 2.6.37

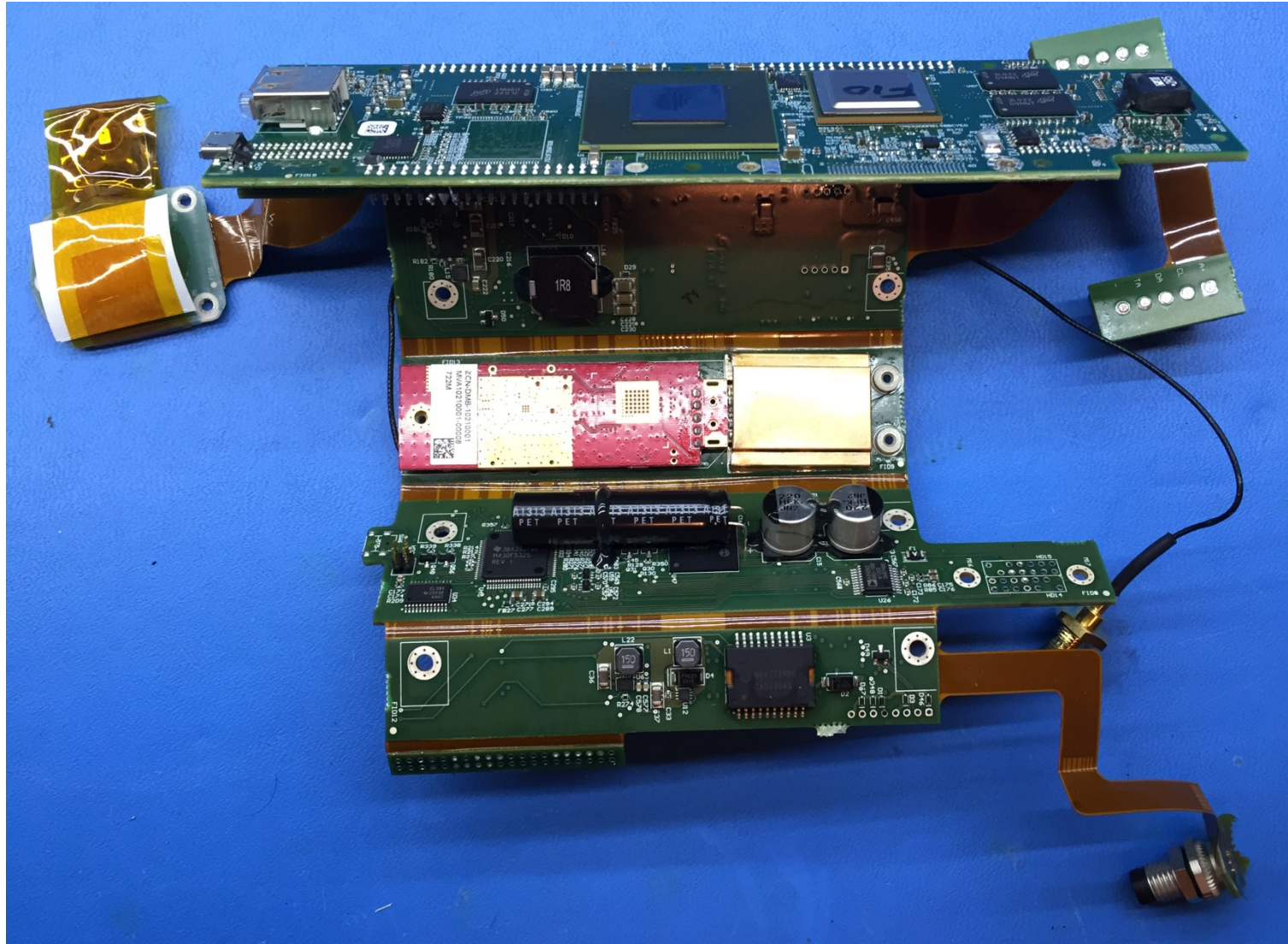
Arago 2011.09 TP\_TP750-308FF89765R tty00

TP\_TP750-308FF89765R login:

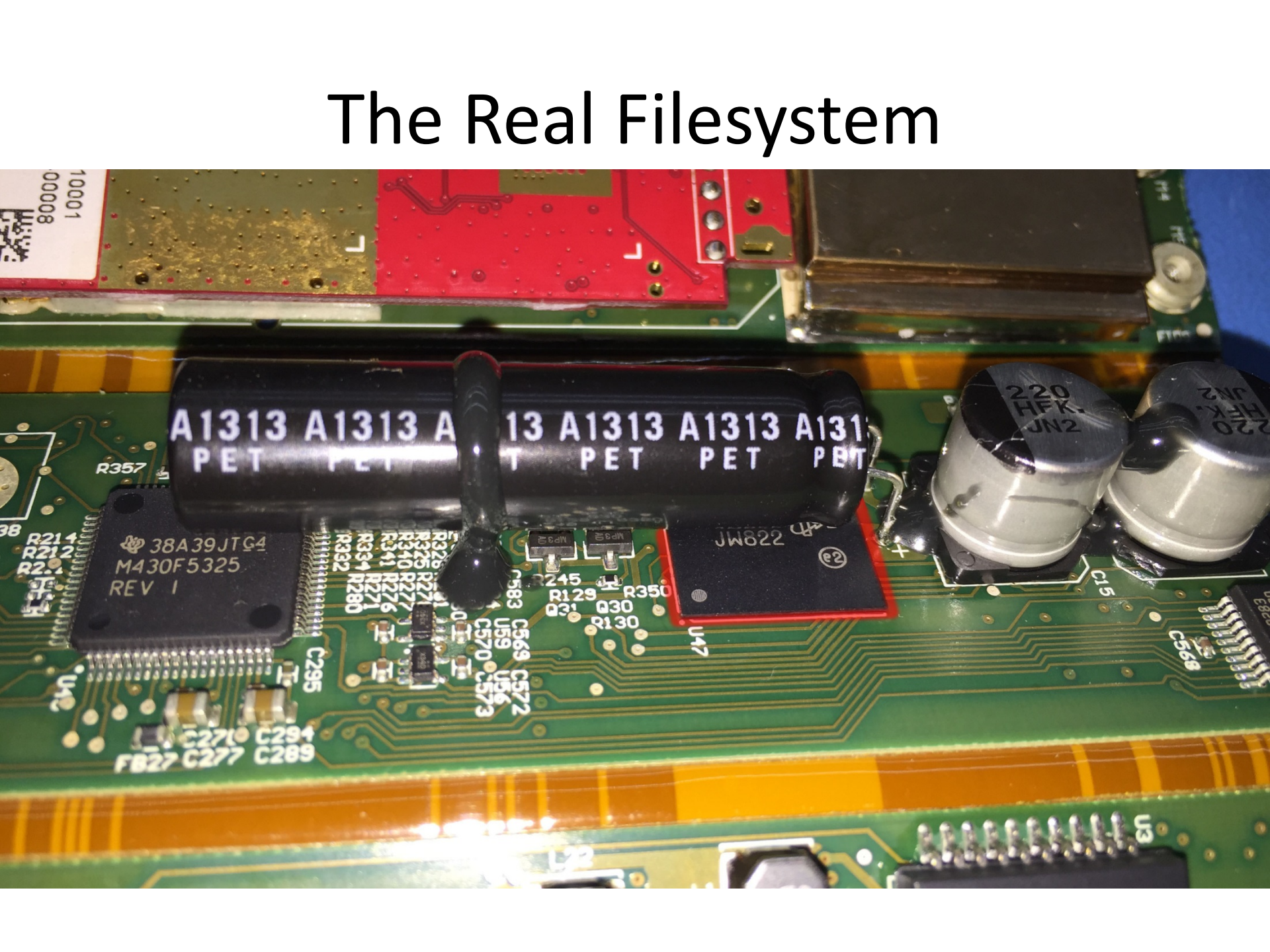
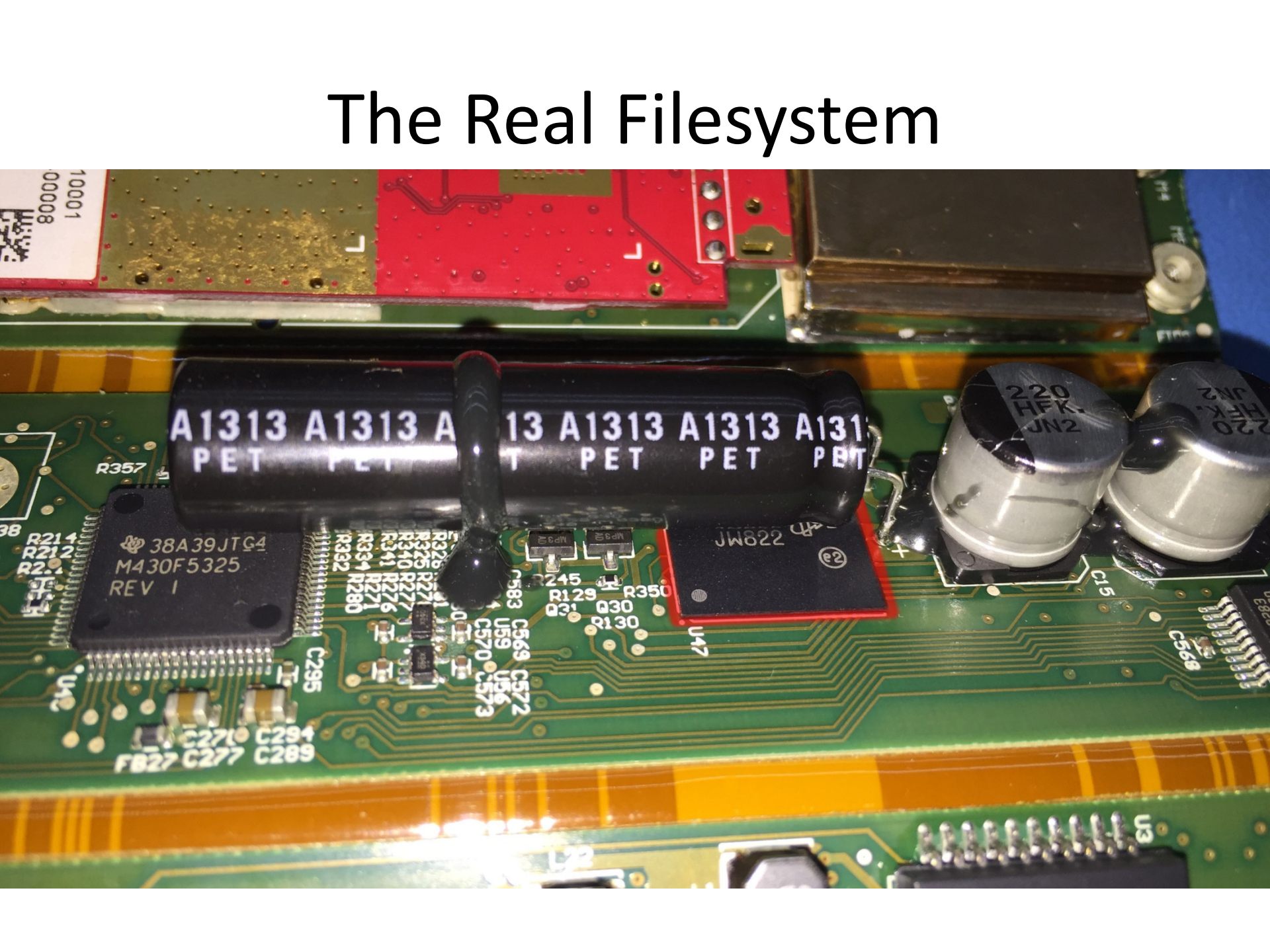
# TrackingPoint wins!

- Validating API input
- GPG signed and encrypted updates
- Password Protected Console

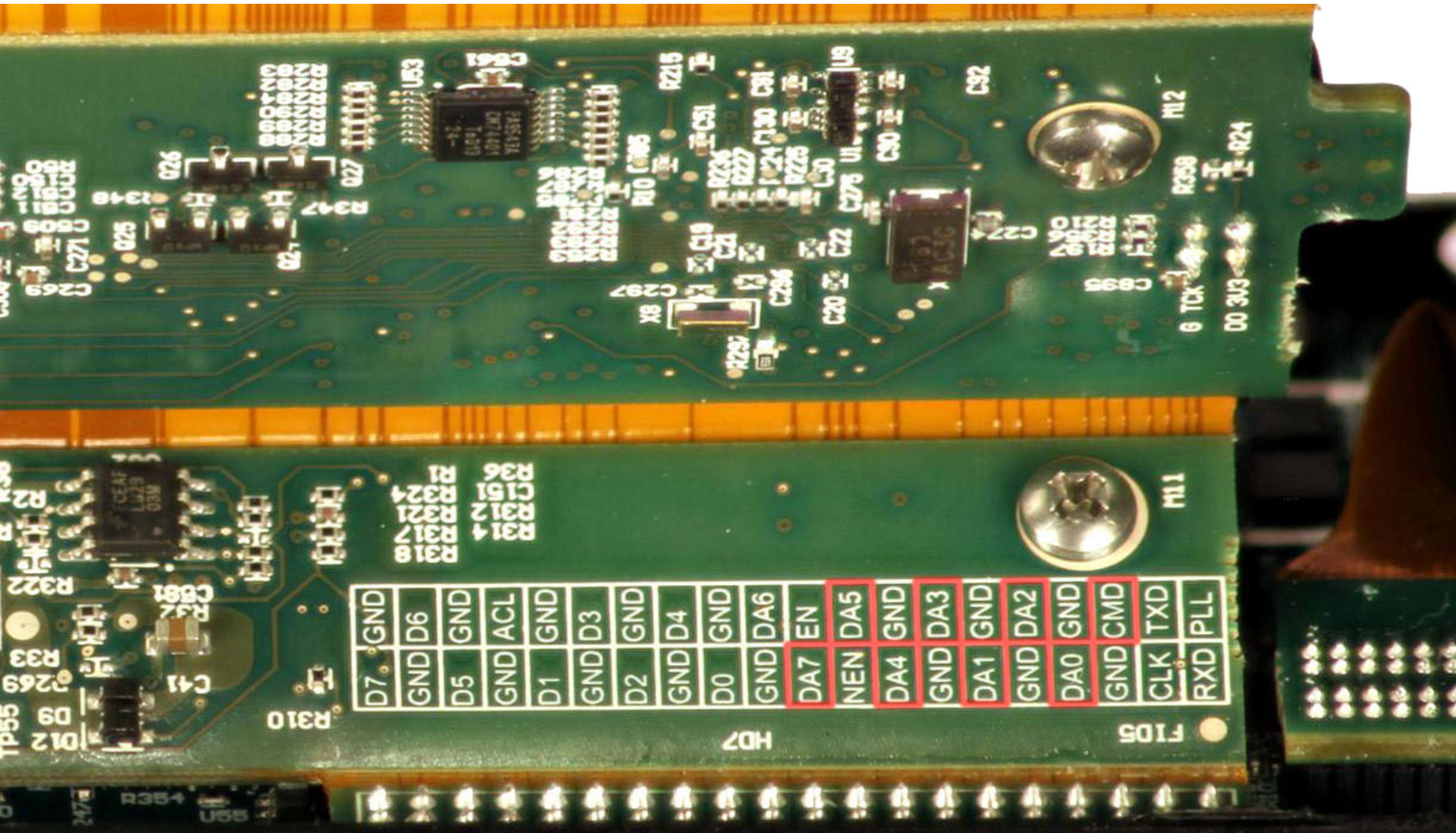
# Let's get destructive!



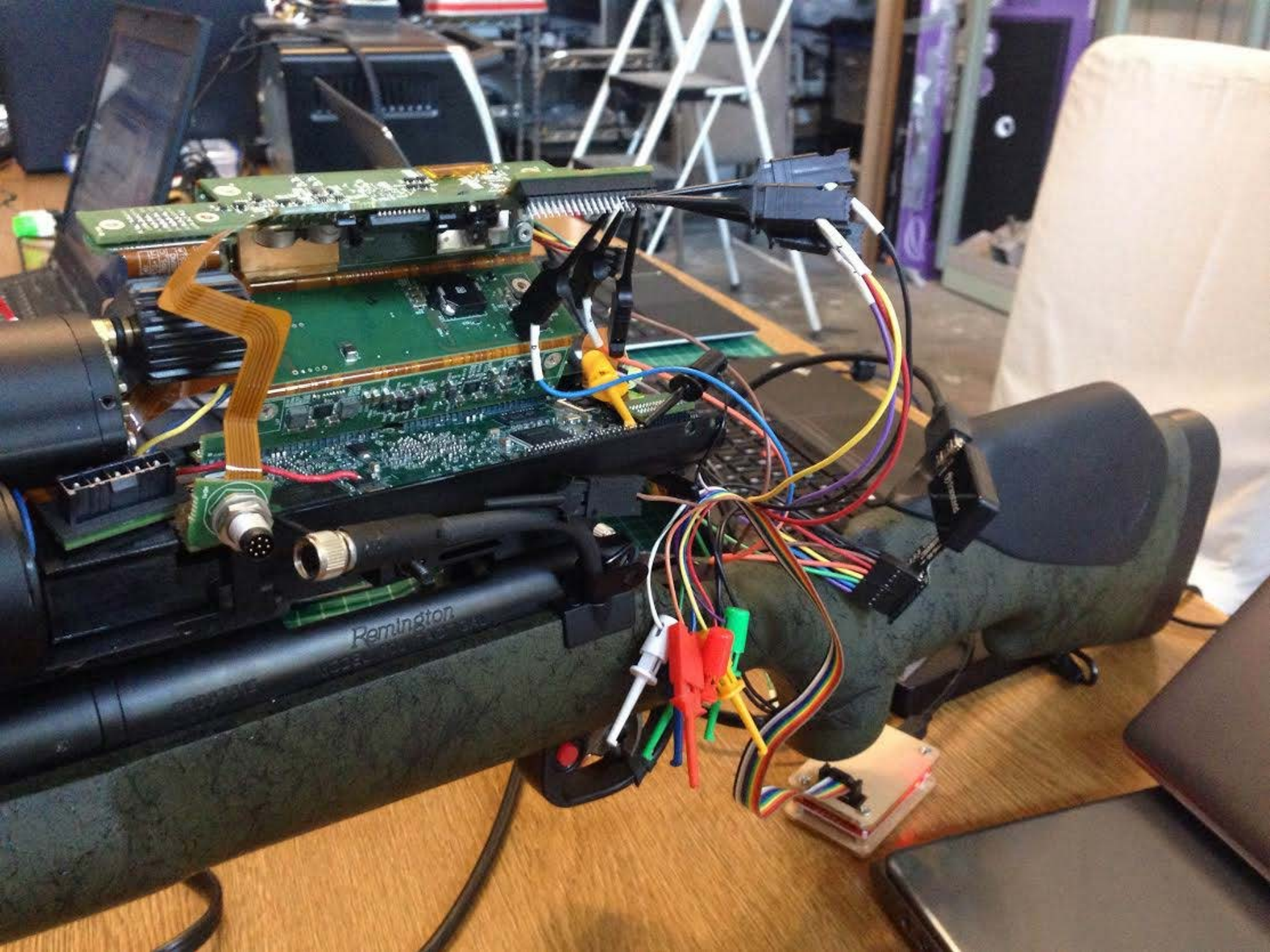
# The Real Filesystem



# Had only we known!









# Admin API

## Mobile Apps

/clear\_passcode/  
/config/  
/dateset/  
/delete/  
/dir/  
/get\_passcode/  
/get\_shot\_data/  
/gps/  
/pkg-upload/  
/progress/  
/serial\_num/  
/service/  
/set\_factory\_defaults/  
/set\_passcode/  
/set\_windage/  
/unwatch/  
/updatescope/  
/version/

## Config

/set\_ammunition/  
/set\_imagestab/  
/set\_killzone/  
/set\_temperature/  
/set\_record\_cooltime/  
/set\_recording/

## Admin

/compmode/  
/get\_imu/  
/powermgr/  
/set\_advanced\_mode/  
/set\_pgf/  
/set\_tiltadjust/  
/set\_wifi/  
/ssh\_accept/  
...

# Demo: Got root?

Demo: You missed!

# Findings

- Admin API is un-authenticated
- Un-authenticated access to core system functions
- Any GPG key in trust DB can encrypt and sign updates

# Takeaways

- Small attack surface and a lot was done right:
  - USB ports are disabled during boot
  - Media is deleted from scope once downloaded
  - WPA2 is in use, even if the key cannot be changed
  - API settings are validated on the backend
  - Password protected console and single user mode
  - GPG signed and encrypted software updates

# Thanks!

- Travis Goodspeed
- Babak Javadi -- The CORE Group
- Mickey Shkatov -- Intel Advanced Threat Research
- Joe FitzPatrick
- Jesse
- Kenny
- ^H -- Portland's Hackerspace