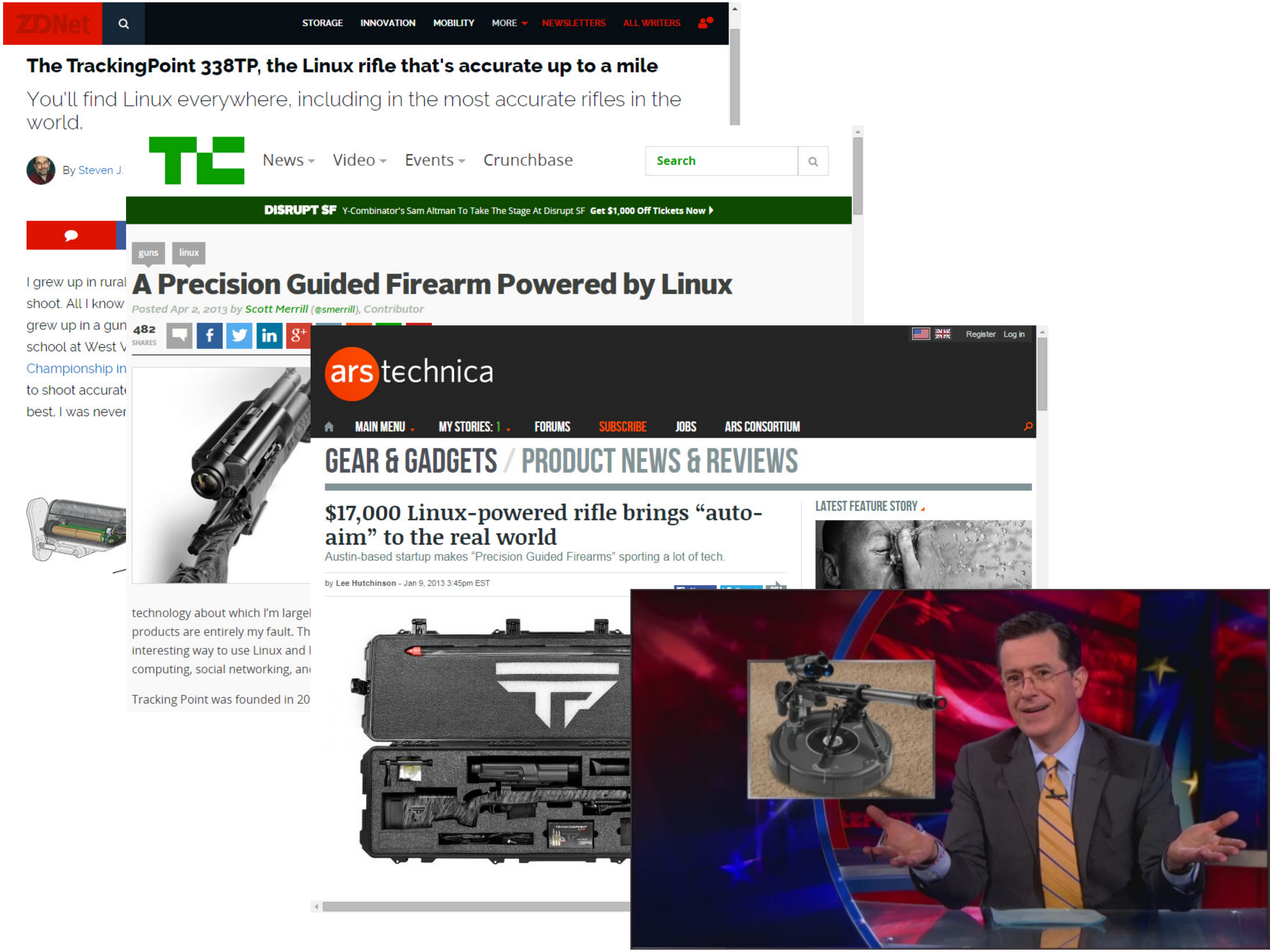
When IoT Attacks:

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.

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

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

A Precision Guided Firearm Powered by Linux

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

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

Tracking Point was founded in 20

GEAR & GADGETS / PRODUCT NEWS & REVIEWS

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

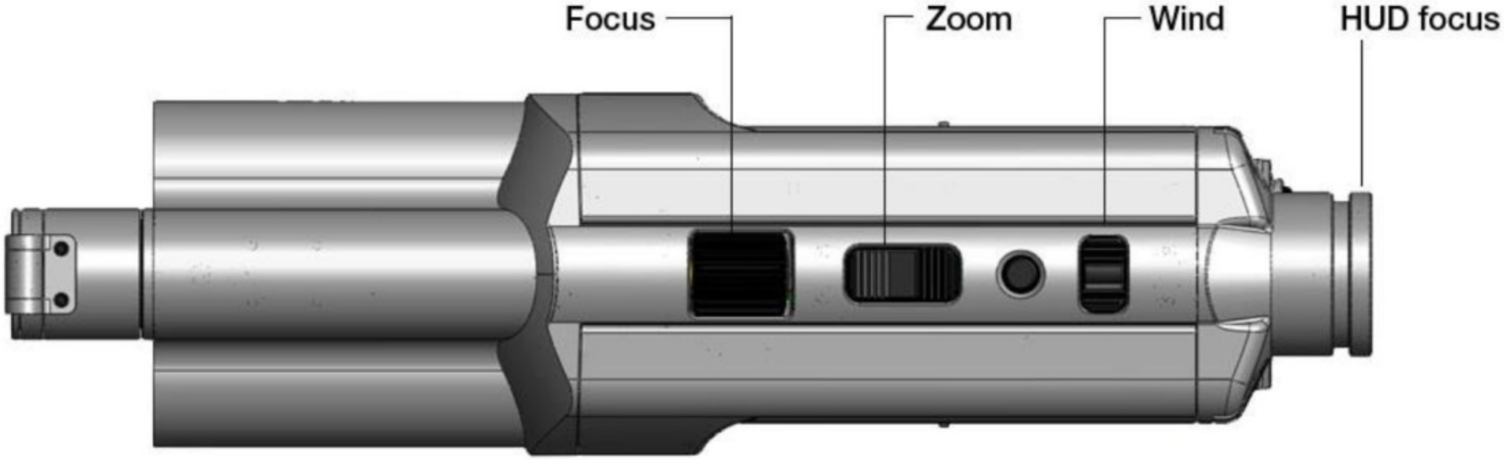
Austin-based startup makes "Precision Guided Firearms" sporting a lot of tech.

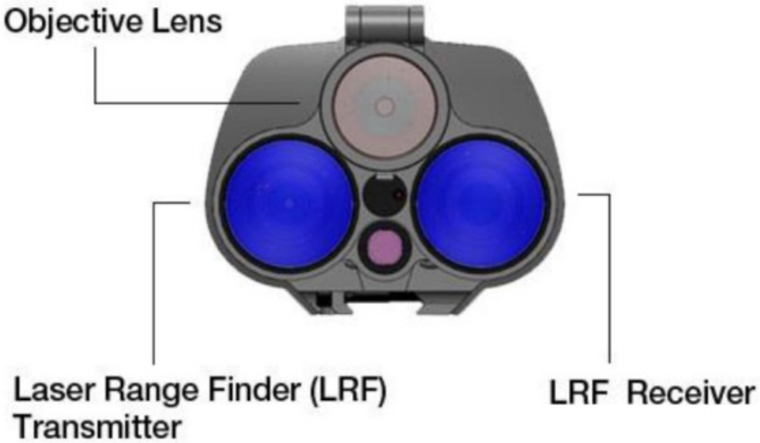
by Lee Hutchinson - Jan 9, 2013 3:45pm EST

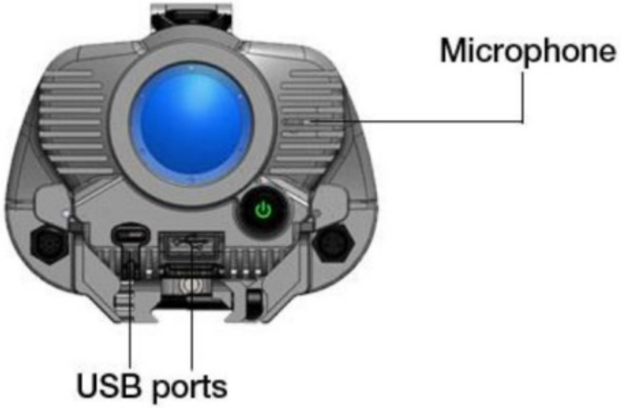
Why are we doing this?

- A gun with WiFi and fancy electronics… duh

Physical


Focus
Zoom
Wind
HUD focus


Objective Lens
Laser Range Finder (LRF)
Transmitter
LRF Receiver


Microphone
USB ports

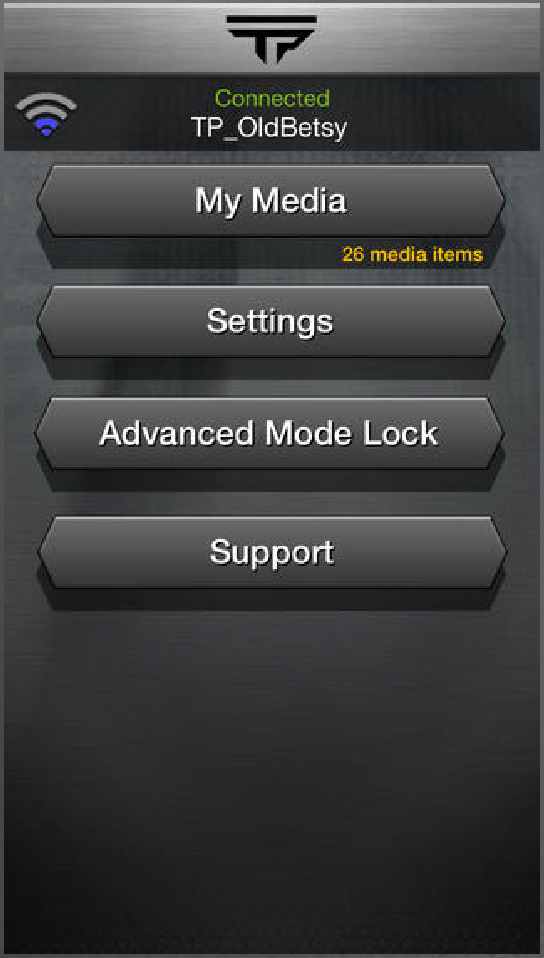
↑ ↑ ↓ ↓ ← → ← → Ⓑ Ⓐ START

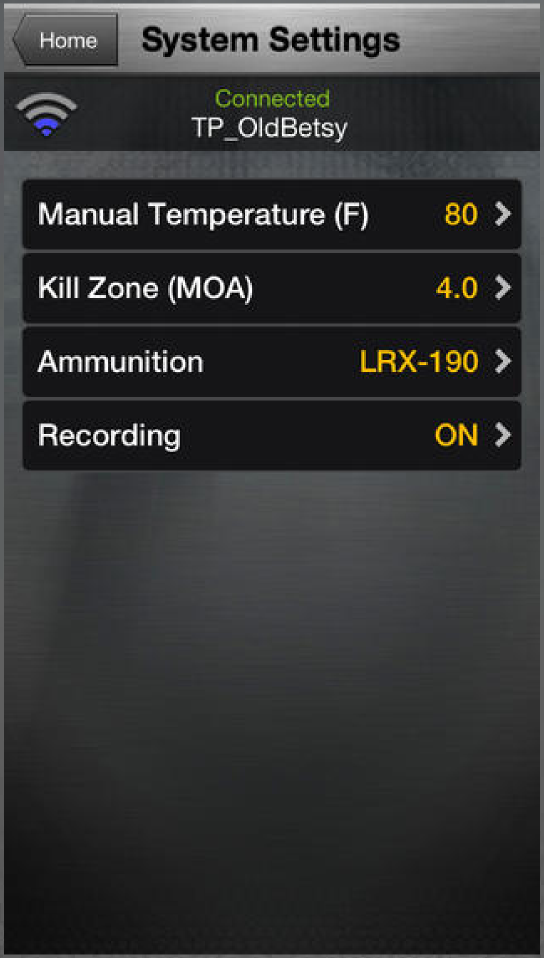
WIFI SERVER

```
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



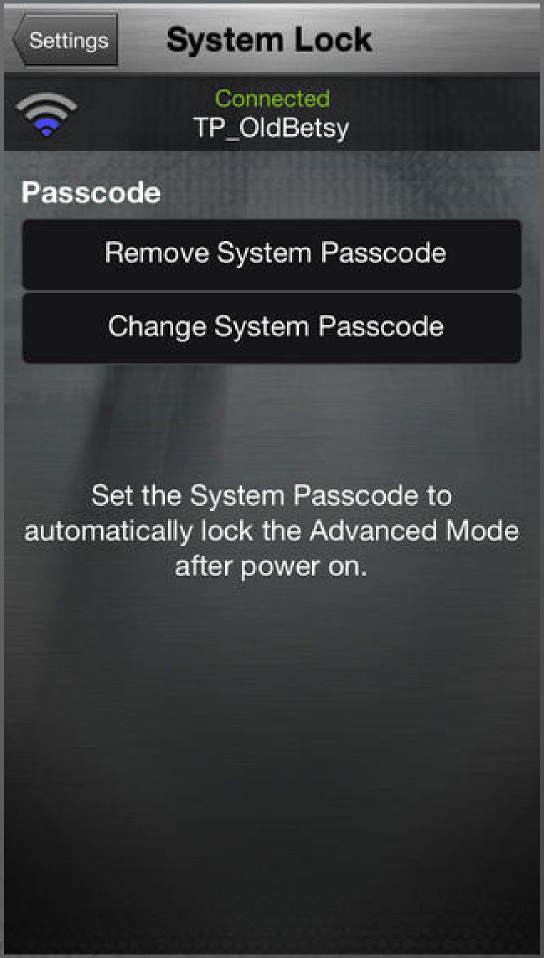


Manual Temperature (F) 80

Kill Zone (MOA) 4.0

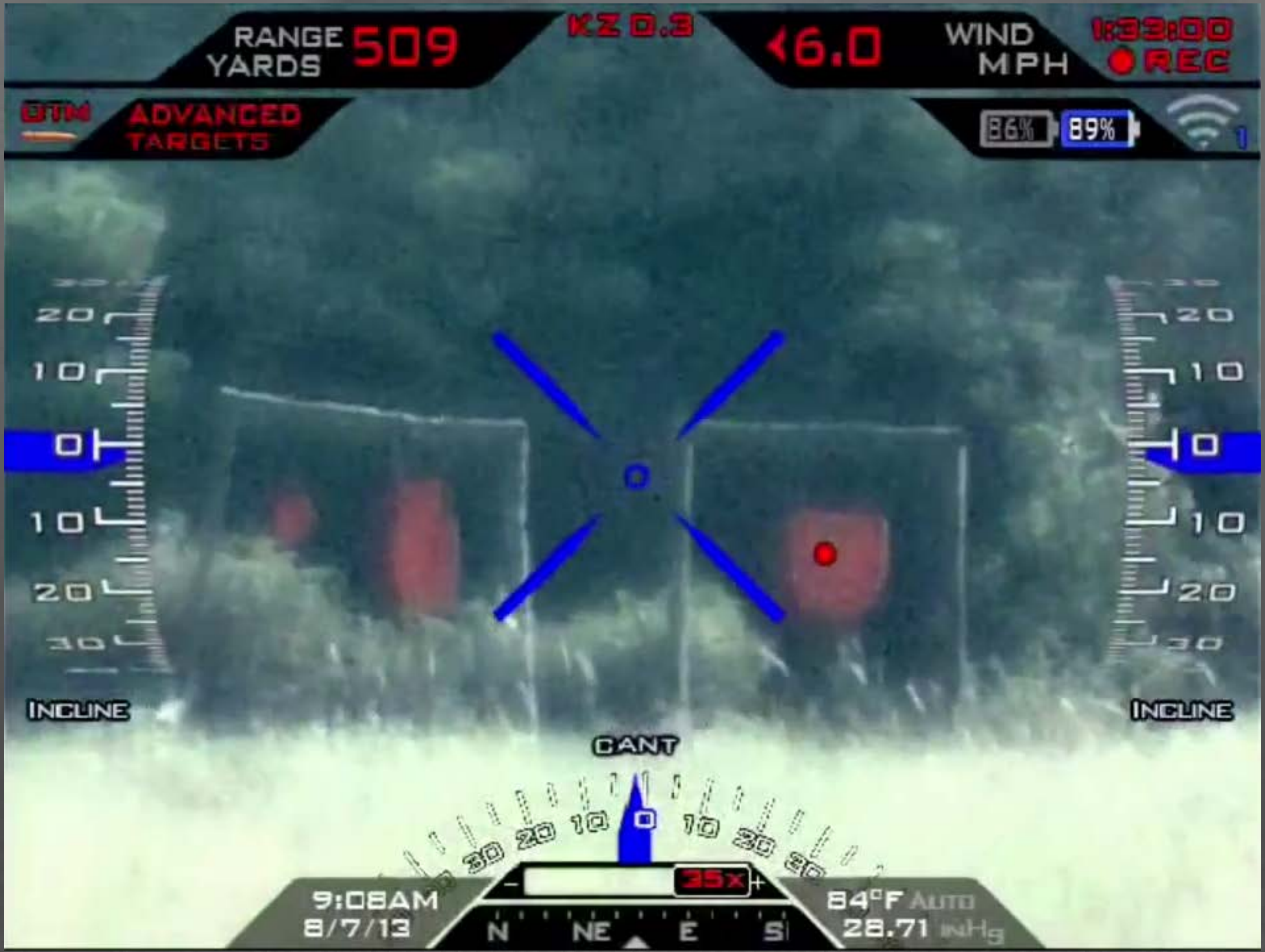
Ammunition LRX-190

Recording ON

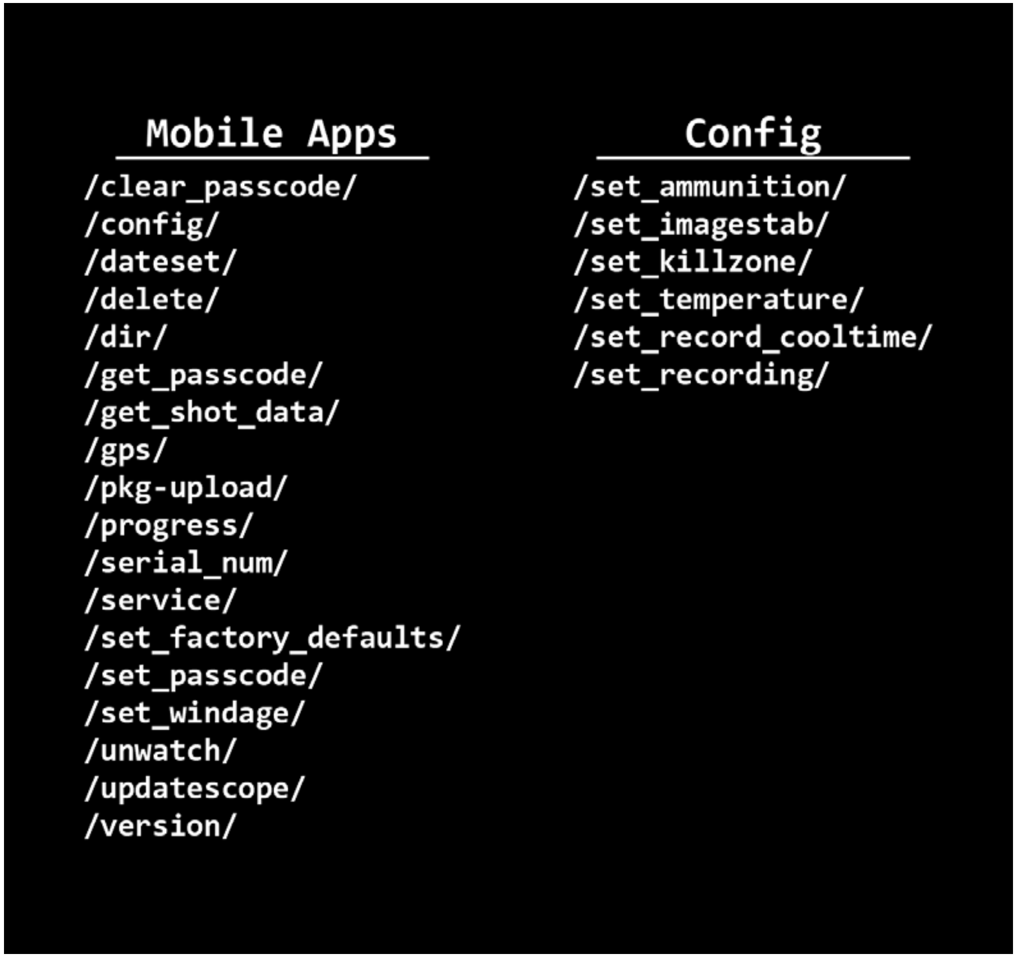


Set the System Passcode to automatically lock the Advanced Mode after power on.

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/

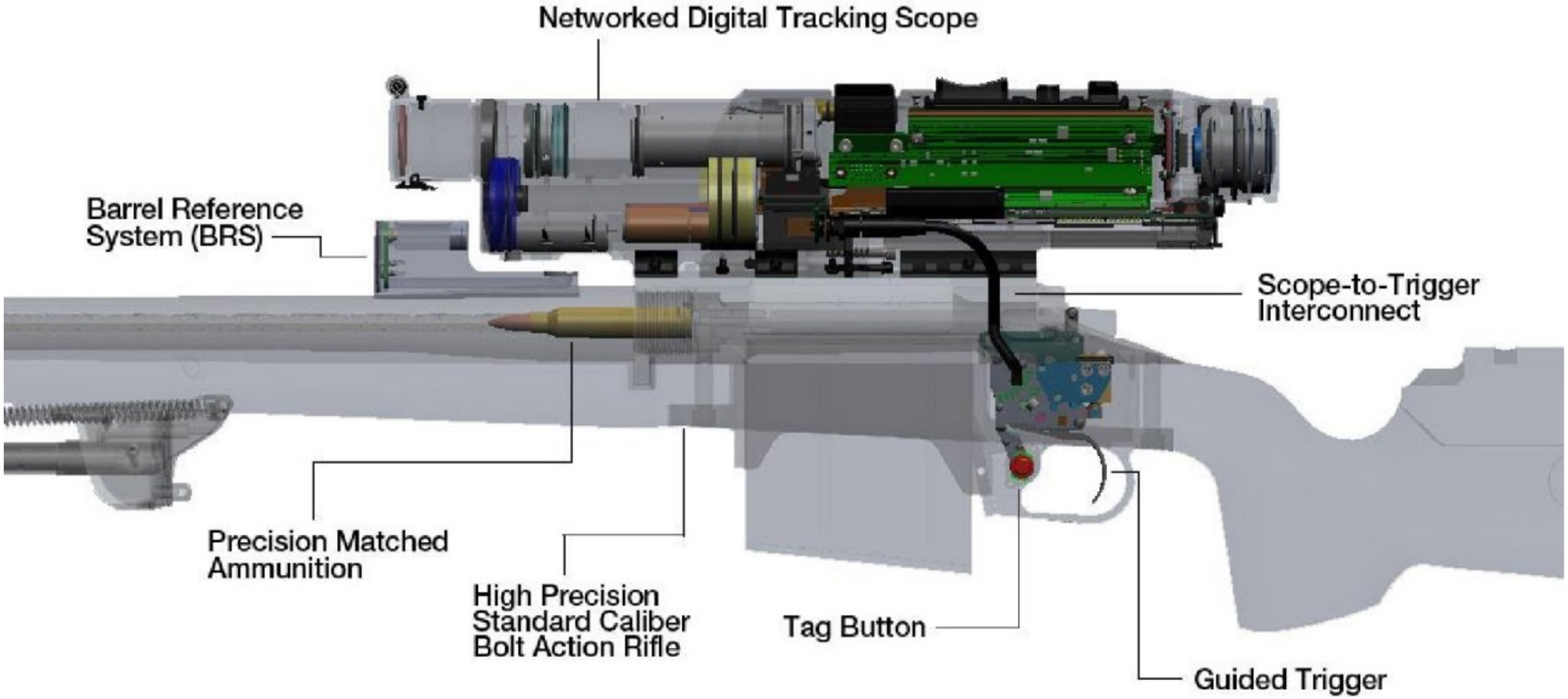
Config

/set_ammunition/
/set_imagestab/
/set_killzone/
/set_temperature/
/set_record_cooltime/
/set_recording/

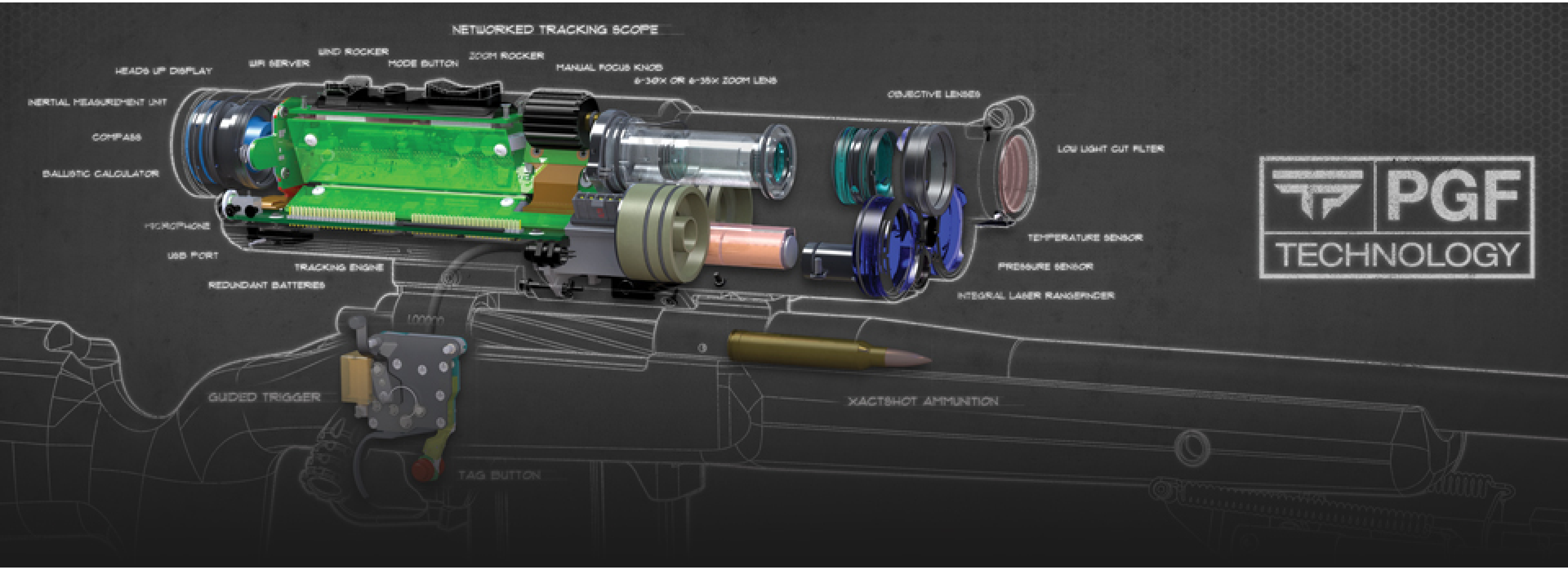
Initial Findings

- 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

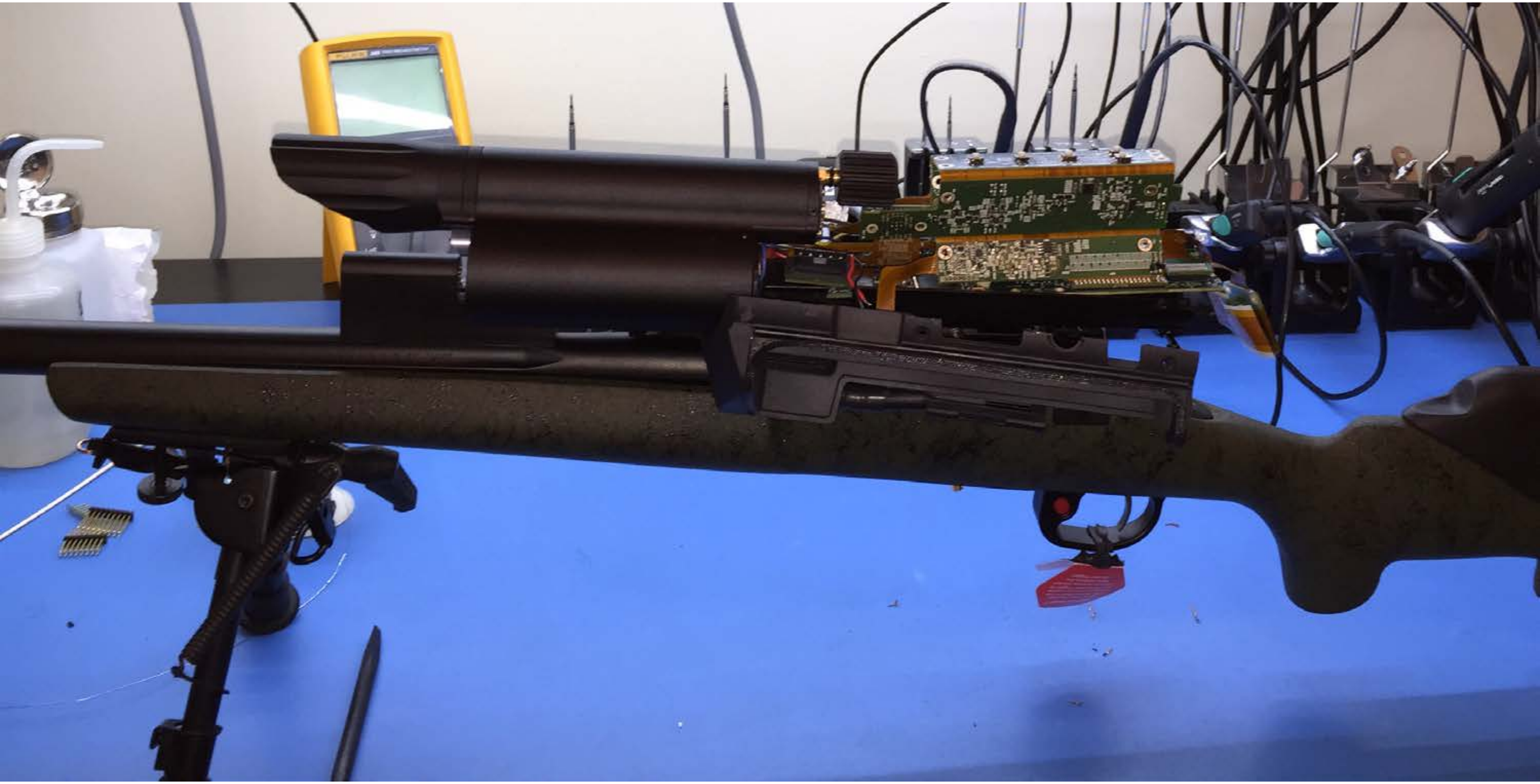
Courtesy of TrackingPoint’s Website


Networked Digital Tracking Scope
Barrel Reference System (BRS)
Scope-to-Trigger Interconnect
Precision Matched Ammunition
High Precision Standard Caliber Bolt Action Rifle
Tag Button
Guided Trigger

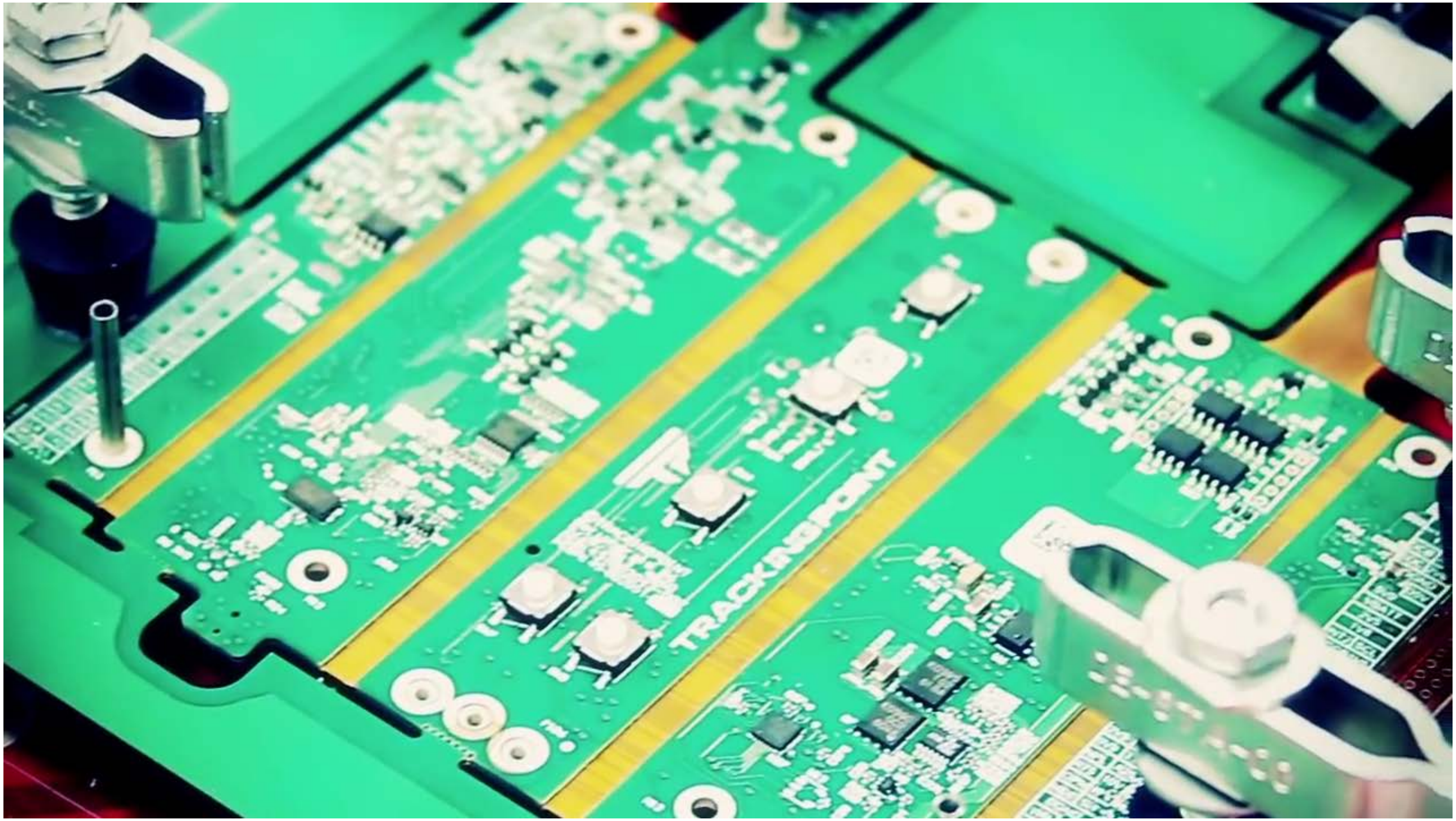
Courtesy of TrackingPoint's Website



Tearing it open

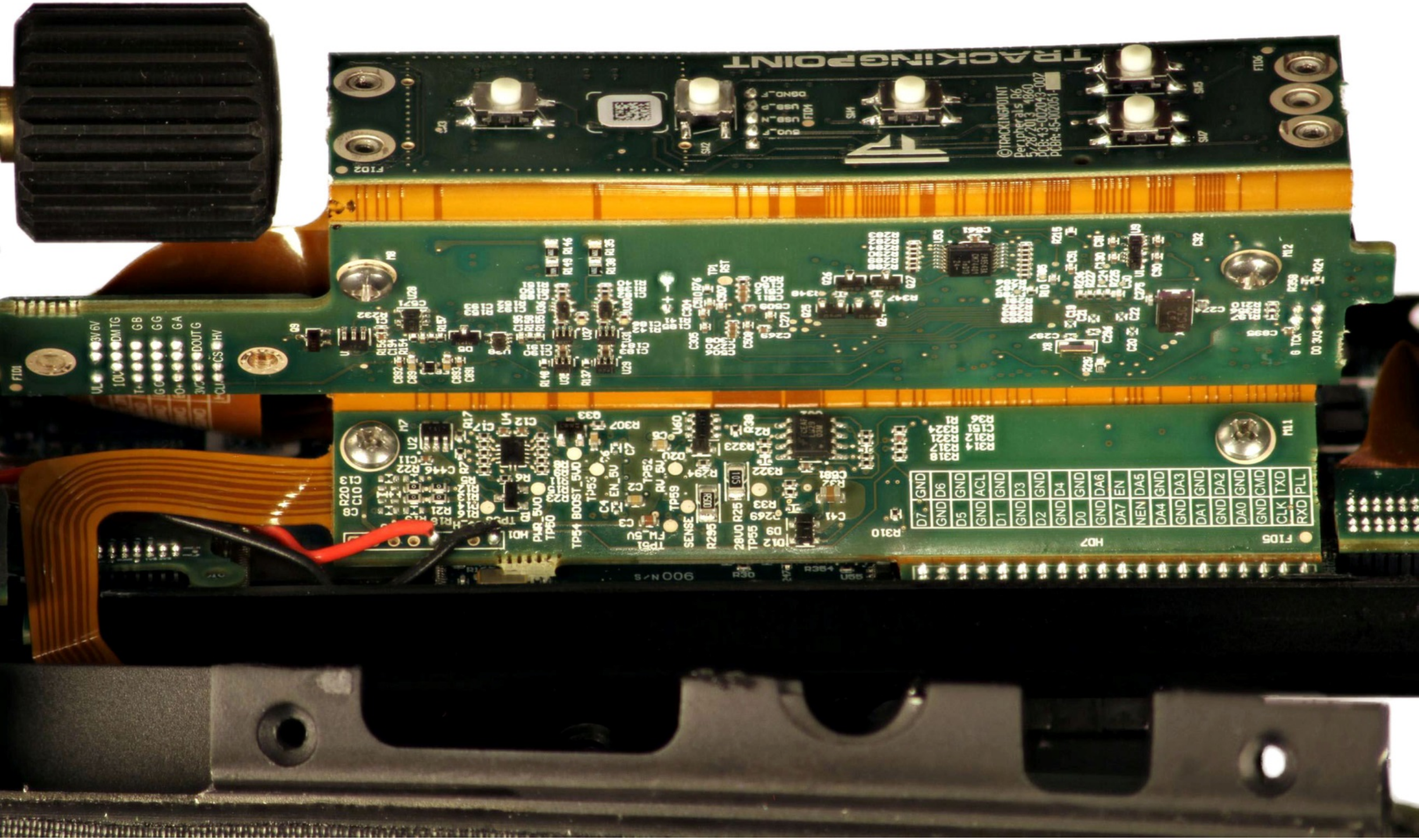


Courtesy of TrackingPoint’s YouTube



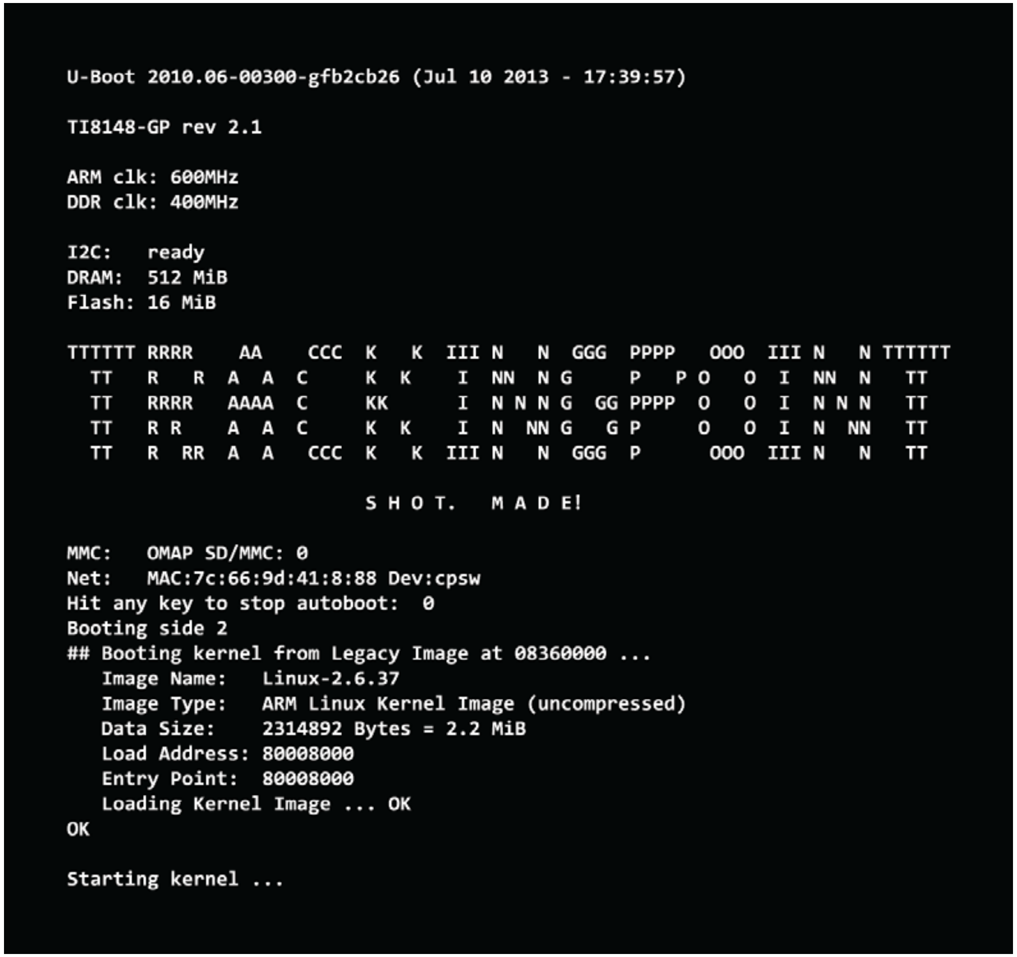
TRACKINGPOINT

Close Up


TRACKINGPOINT
©TRACKINGPOINT
Peripherals R6
5/28/2013 4860
PCB: 43-000204-007
PCBA: 45-000205-
SW2
SW4
SW5
SW7
FID2
FID4
FID5
FID6
HD7
D7 GND D5 GND D1 GND D2 GND D0 GND DA7 NEN DA4 GND DA1 GND DA0 GND CLK RXD
GND D6 GND ACL GND D3 GND D4 GND DA6 EN DA5 GND DA3 GND DA2 GND CMD TXD PLL

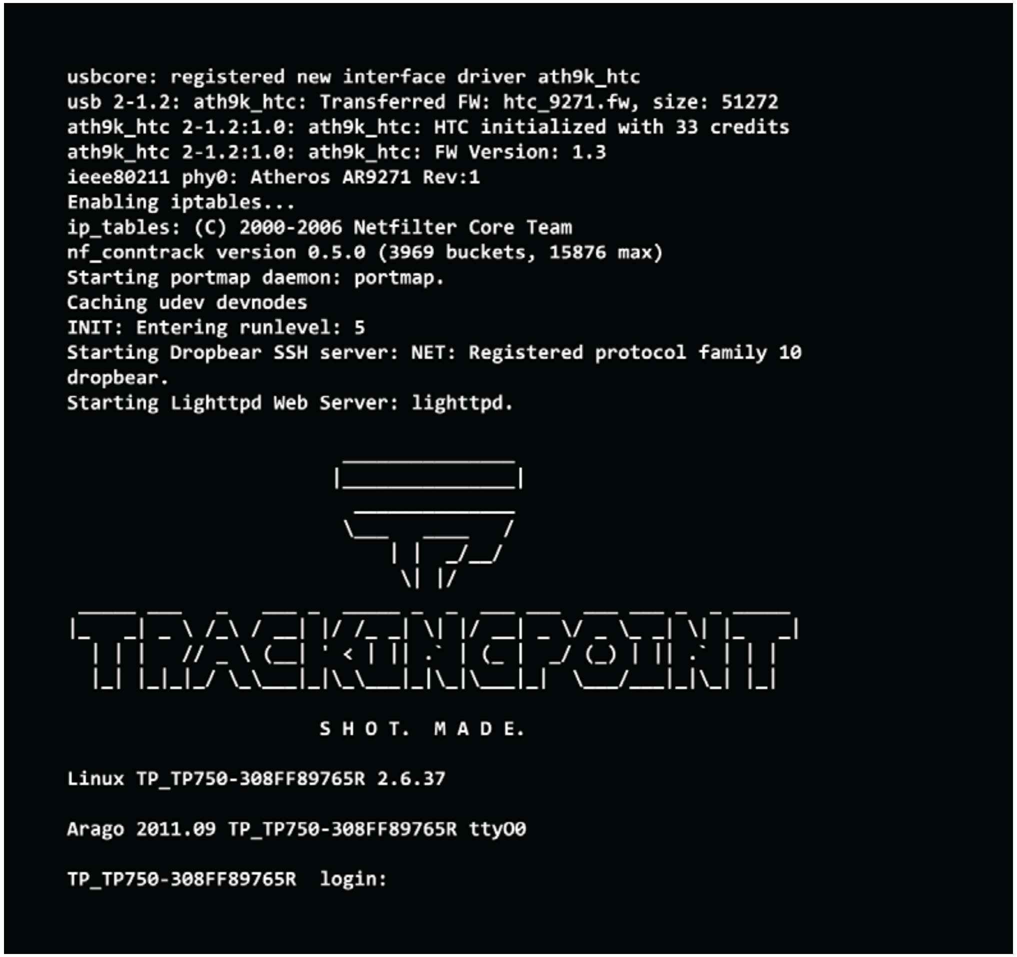
UART

Woot!



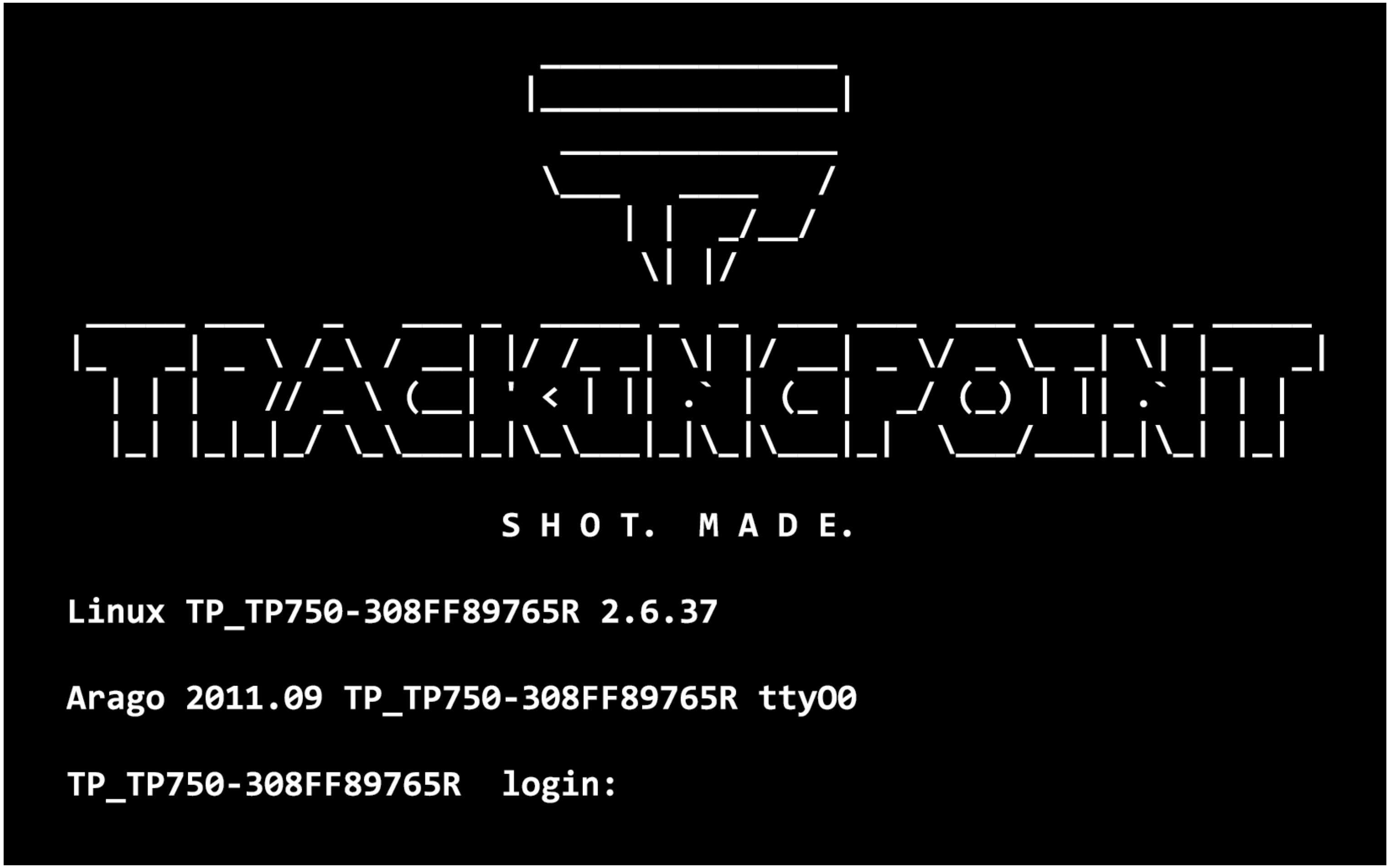
```
U-Boot 2010.06-00300-gfb2cb26 (Jul 10 2013 - 17:39:57)

TI8148-GP rev 2.1

ARM clk: 600MHz
DDR clk: 400MHz

I2C:   ready
DRAM:  512 MiB
Flash: 16 MiB

TTTTTT RRRR    AA    CCC  K   K   III N   N  GGG  PPPP   OOO   III N   N TTTTTT
  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 N N G  GG PPPP  O   O   I  N N N   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.

                        _______________
                       |_______________|
                         ______________
                        \___   ____   /
                            | |  _/__/
                             \| |/
 _____ ___   _   ___ _  _____ _  _  ___ ___  ___ ___ _  _ _____
|_   _| _ \ /_\ / __| |/ /_ _| \| |/ __| _ \/ _ \_ _| \| |_   _|
  | | |   // _ \ (__| ' < | || .` | (_ |  _/ (_) | || .` | | |
  |_| |_|_|_/ \_\___|_|\_\___|_|\_|\___|_|  \___/___|_|\_| |_|

                      S H O T.  M A D E.

Linux TP_TP750-308FF89765R 2.6.37

Arago 2011.09 TP_TP750-308FF89765R ttyO0

TP_TP750-308FF89765R  login:
```

…well played

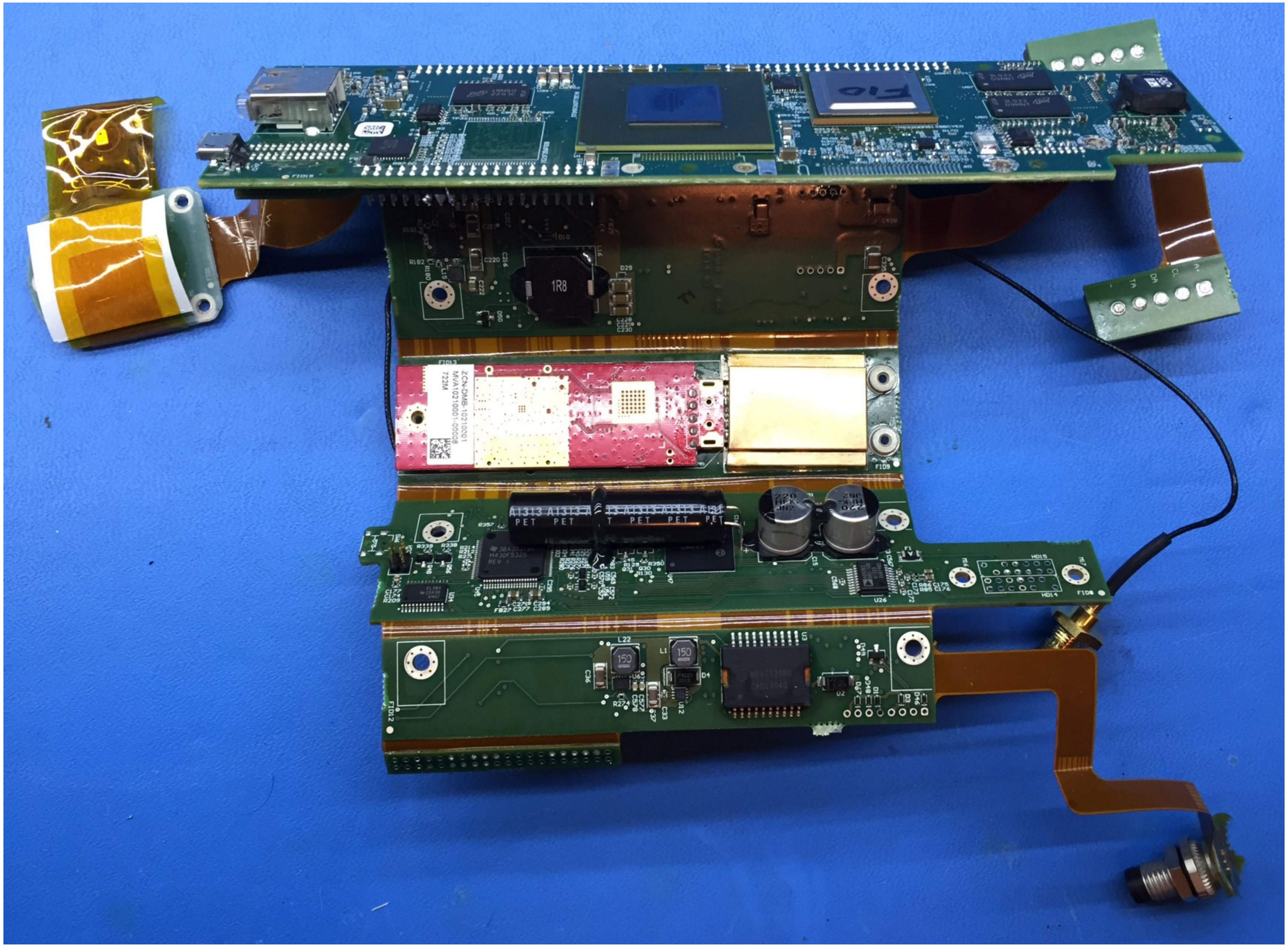


```
                  _________________
                 |_________________|
                   _______________
                  \____   _____  /
                       | |  _/__/
                        \| |/
 _____ ___    _   ___ _  _____ _  _  ___ ___  ___ ___ _  _ _____
|_   _| _ \  /_\ / __| |/ /_ _| \| |/ __| _ \/ _ \_ _| \| |_   _|
  | | |   / / _ \ (__| ' < | || .` | (_ |  _/ (_) | || .` | | |
  |_| |_|_\/_/ \_\___|_|\_\___|_|\_|\___|_|  \___/___|_|\_| |_|

                    S H O T.  M A D E.

Linux TP_TP750-308FF89765R 2.6.37

Arago 2011.09 TP_TP750-308FF89765R ttyO0

TP_TP750-308FF89765R  login:
```

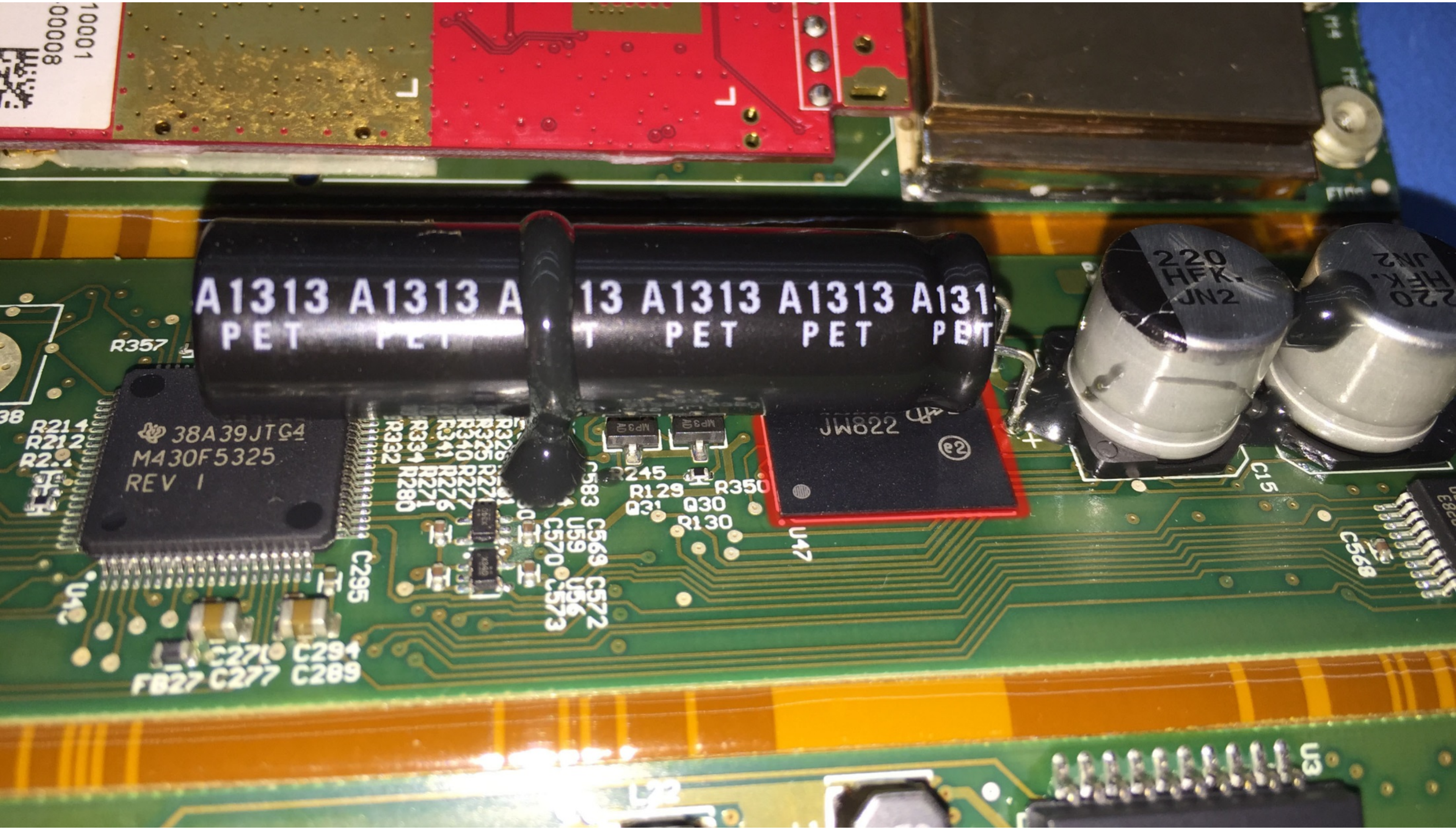
TrackingPoint wins!

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

Let’s get destructive!

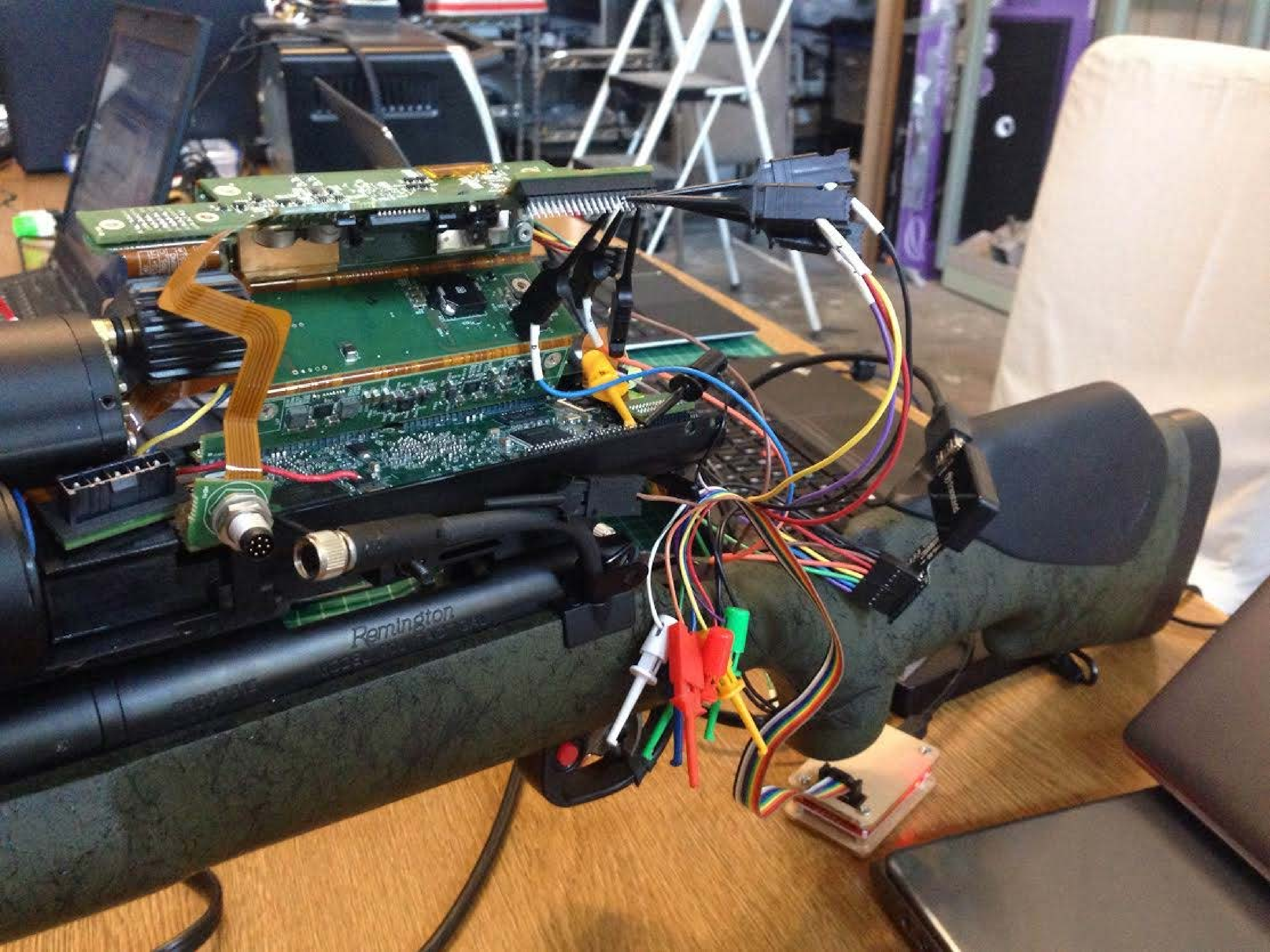


The Real Filesystem

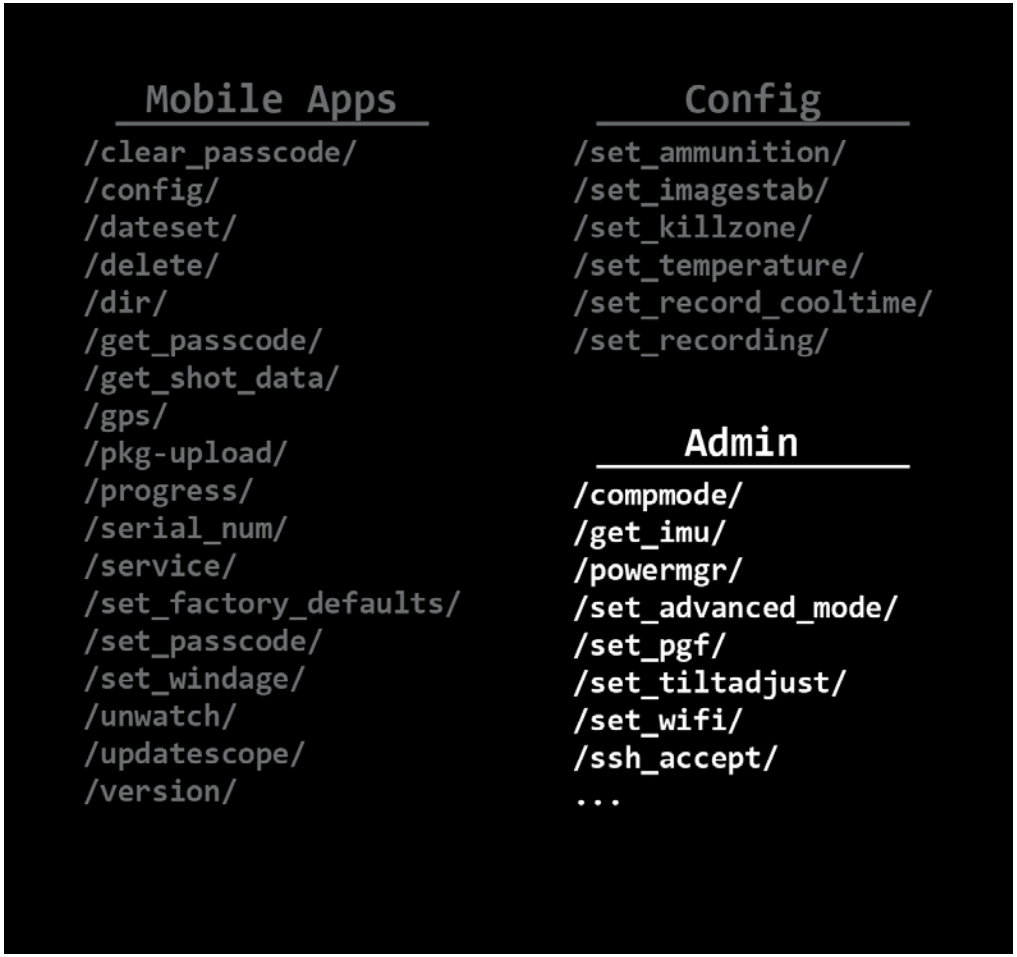


Had only we known!

AS2G0433A0
DATA


Remington

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