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.

I grew up in rural WV to shoot. All I knew was to shoot accurately. I was never the best, I was never the best.

A Precision Guided Firearm Powered by Linux

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

482

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

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

Tracking Point was founded in 2010.
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
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%)
TrackingPoint App

Connected
TP_OldBetsy

My Media
26 media items

Settings

Advanced Mode Lock

Support

Connected
TP_OldBetsy

System Settings

Manual Temperature (F) 80
Kill Zone (MOA) 4.0
Ammunition LRX-190
Recording ON

Connected
TP_OldBetsy

System Lock

Passcode
Remove System Passcode
Change System Passcode

Set the System Passcode to automatically lock the Advanced Mode after power on.
ShotView App
## Public API

<table>
<thead>
<tr>
<th>Mobile Apps</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>/clear_passcode/</td>
<td>/set_ammunition/</td>
</tr>
<tr>
<td>/config/</td>
<td>/set_imagestab/</td>
</tr>
<tr>
<td>/dataset/</td>
<td>/set_killzone/</td>
</tr>
<tr>
<td>/delete/</td>
<td>/set_temperature/</td>
</tr>
<tr>
<td>/dir/</td>
<td>/set_record_cooltime/</td>
</tr>
<tr>
<td>/get_passcode/</td>
<td>/set_recording/</td>
</tr>
<tr>
<td>/get_shot_data/</td>
<td></td>
</tr>
<tr>
<td>/gps/</td>
<td></td>
</tr>
<tr>
<td>/pkg-upload/</td>
<td></td>
</tr>
<tr>
<td>/progress/</td>
<td></td>
</tr>
<tr>
<td>/serial_num/</td>
<td></td>
</tr>
<tr>
<td>/service/</td>
<td></td>
</tr>
<tr>
<td>/set_factory_defaults/</td>
<td></td>
</tr>
<tr>
<td>/set_passcode/</td>
<td></td>
</tr>
<tr>
<td>/set_windage/</td>
<td></td>
</tr>
<tr>
<td>/unwatch/</td>
<td></td>
</tr>
<tr>
<td>/updatescope/</td>
<td></td>
</tr>
<tr>
<td>/version/</td>
<td></td>
</tr>
</tbody>
</table>
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
Tearing it open
Courtesy of TrackingPoint’s YouTube
Woot!

```
U-Boot 2010.06-00300-gfb2cb26 (Jul 10 2013 - 17:39:57)
TIB148-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 TTTTT
TT R R A A C K K I N N N G G P P O O I N N N T T
TT RRRR AAAA C K K I N N N G G G P P O O I N N N T T
TT R R A A C K K I N N N G G G P P O O I N N N T T
TT R RR A A CCC K K III N N GGG P OOO III N N T T

SHOT. MADE!

MMC: OMAP SD/MMC: 0
Hit any key to stop autoboot: 0
Booting side 2
## Booting kernel from Legacy Image at 00360000 ...
  Image Name: Linux-2.6.37
  Image Type: ARM Linux Kernel Image (uncompressed)
  Data Size: 2314892 Bytes = 2.2 MiB
  Load Address: 80000000
  Entry Point: 80008000
  Loading Kernel Image ... OK
OK
Starting kernel ...
```
Well played TrackingPoint...

usbc core: 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
SHOT MADE.

Linux TP_TP750-308FF89765R 2.6.37
Arago 2011.09 TP_TP750-308FF89765R tty00
TP_TP750-308FF89765R login:
...well played
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

<table>
<thead>
<tr>
<th>Mobile Apps</th>
<th>Config</th>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>/clear_passcode/</td>
<td>/set_ammunition/</td>
<td>/compmode/</td>
</tr>
<tr>
<td>/config/</td>
<td>/set_imagestab/</td>
<td>/get_imu/</td>
</tr>
<tr>
<td>/dataset/</td>
<td>/set_killzone/</td>
<td>/powermgr/</td>
</tr>
<tr>
<td>/delete/</td>
<td>/set_temperature/</td>
<td>/set_advanced_mode/</td>
</tr>
<tr>
<td>/dir/</td>
<td>/set_record_cooltime/</td>
<td>/set_pgf/</td>
</tr>
<tr>
<td>/get_passcode/</td>
<td>/set_recording/</td>
<td>/set_tiltadjust/</td>
</tr>
<tr>
<td>/get_shot_data/</td>
<td></td>
<td>/set_wifi/</td>
</tr>
<tr>
<td>/gps/</td>
<td></td>
<td>/ssh_accept/</td>
</tr>
<tr>
<td>/pkg-upload/</td>
<td></td>
<td>...</td>
</tr>
<tr>
<td>/progress/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/serial_num/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/service/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/set_factory_defaults/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/set_passcode/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/set_windage/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/unwatch/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/updatescope/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/version/</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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