How to use a Raspberry PI as a Network Sensor

Bill Stearns


TWO-DAY TRAINING
March 10th & 11th
CONFERENCE
March 11th (afternoon) - March 13th
WAY WEST
WILD WEST
HACKIN' FEST
2020
SAN DIEGO, CA
Wildwesthackinfest.com

Link to downloads

- PDF of talk, spreadsheet of parts, scripts
  - Download now from:

https://www.activecountermeasures.com/raspberry_pi_sensor/

What We Will Cover

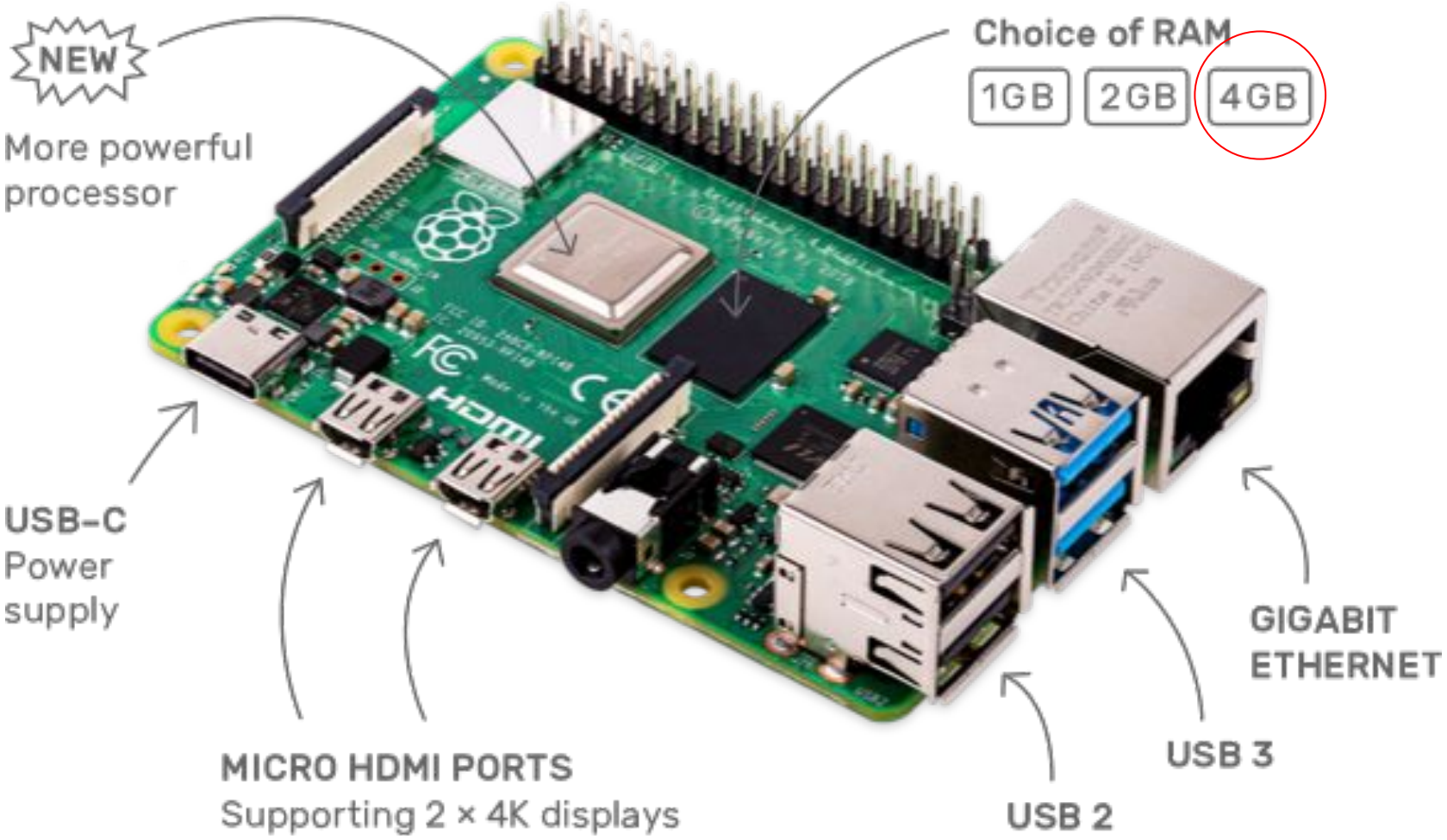
- Goals - What we want to accomplish
- Raspberry PI - Quick overview
- How to source the parts
- How to build the system
- Configuring it as network probe
- Processing the data
- Other cool stuff with you can do with a PI

Goals

- Small/cheap system
- Easy to source parts
- Capable of sniffing traffic
- Keep up with medium speed networks
  - 300 Mb to 1 Gb (common Internet links)
- Sniff traffic without an IP
- Process data as needed
- Meet sniffing needs of **red & blue teams**

What's a Raspberry Pi?

- Small PC
- Runs Linux
  - Full dual screen desktop or command line only
  - Anything in Linux on another physical system
  - All Debian clients, servers, languages, libraries
  - Other distributions available
- Full suite of packet capture/analysis tools
- This talk: Pi version 4 only


NEW
More powerful processor
Choice of RAM
1GB
2GB
4GB
USB-C
Power supply
MICRO HDMI PORTS
Supporting 2 × 4K displays
USB 2
USB 3
GIGABIT ETHERNET

Pi Hardware

- Built-in Gig Ethernet for sniffing (Pi 4)
- Wifi (802.11ac) and Bluetooth 5.0 BLE
- 1, 2, or 4 GB ram
- 2x USB 3.0, 2x USB 2.0
- Quad-core arm CPU (1.5GHz)
- 40 pin header (special uses)
- Optional - Keyboard/mouse/2x HDMI
- Case, power supply, microsd sold separately

Usable for packet capture

- Can it sniff?
  - Promiscuous drivers for 1 Gbps Ethernet port
  - CLI tools included or download more
- Can CPU keep up?
  - Depends on amount of processing
  - Reduce load w/multiple PIs or offload processing
- BPF filtering
  - Ignore uninteresting traffic to reduce load
  - Monitor for dropped packets

Too much traffic!

- Gigabit or more?
- No problem - use a beefier box
  - May want to look at Corelight systems
  - Preconfigured and tuned, ready to go.

    https://www.corelight.com/
- Disclaimer
  - Corelight is a partner
  - This is **not** a paid advertisement. No celebrity spokespeople were harmed to make this slide.

Where to source the parts

- Adafruit https://www.adafruit.com
  - Most of the parts
  - Tons of tutorials
- Canakit https://www.canakit.com/
  - All of the parts in one kit
- Amazon https://www.amazon.com/
  - Ethernet (cables, switch)
- Shopping list spreadsheet

Building the system

- Snap Pi board into case
  - Put heat sinks on 2 silver chips in upper left
  - Microsd in slot underneath
  - Attach HDMI, Keyboard and mouse
  - USB storage in USB 3 port (blue center)
  - USB Ethernet in USB 2 port (black center)
  - Power in USB-C port
  - Fan encouraged as Pi slows down if it gets too hot

Software setup

- Attach KB, mouse, and monitor
- Microsd to boot from
  - Buy with Noobs pre-installed
    - Choice of Linux distros, easy to install
  - Installs Raspbian (Debian for Rasp Pi) by default
    - Others can be auto-installed

After install

`ssh pi@raspberrypi.local.`

- Default password is "raspberry"
  - Change asap :-)
- "raspberrypi.local" auto-shared with local dns
- IP also on monitor, or:

`arp -an | grep -i 'dc.*a6.*32'`

- on your laptop

Network setup

- eth0 used for sniffing
  - No IP address
  - Promiscuous mode
- eth1 normal internet access

/etc/network/interfaces

```
auto eth0
iface eth0 inet manual
   up ifconfig 0.0.0.0 up
   up ip link set eth0 promisc on
   down ip link set eth0 promisc off
   down ip link set eth0 down
```

/etc/dhcpcd.conf

- Add the line

```
denyinterfaces eth0
```

/etc/rc.local

```
#ethtool command to reduce processing at eth0
ethtool -K eth0 gro off lro off rx off tx off gso off
mkdir -p /opt/bro/pcaps

screen -S capture -t capture -d -m bash -c "nice -n 15
tcpdump -i eth0 -G 3600 -w '/opt/bro/pcaps/'`hostname
-s`'.%Y%m%d%H%M%S.pcap' -z bzip2 '(tcp[13] & 0x17 !=
0x10) or not tcp'"

/usr/bin/zeekctl deploy
/usr/local/bin/pi_show.py >/tmp/pi_show.out 2>&1 &
exit 0
```

/etc/fstab

```
/dev/sda1 swap          swap    defaults 0 0
/dev/sda2 /opt/bro/     ext4    defaults 0 0
```

Additional steps

- Shell scripts
  - Provided in a zip file, see link at the end
  - Enable ssh
  - System patching
    - Including firmware to handle heat issue
  - Install needed tools
  - Format external drive
  - Force eth0 to have no ip address

Actually getting the packets...

- Need a span/mirror port or Ethernet tap
- If none available, use cheap managed switch
  - Netgear GS305E (managed)
  - Has span port capability (1 monitor port only)
  - GS305E 5 port: https://www.amazon.com/gp/product/B07PJ7XZ7X/
- Cost is about $33

Monitor the span port

- Ethernet cat 5E/6 cable
- Span port on switch to Eth port on PI
- Capture on eth0
- `watch ifconfig eth0`
  - should show steadily RX packet increase

Cost so far

- Pi 4 4GB kit - $100
- USB-Ethernet - $15
- 3 Ethernet cables - $7
- 500GB SSD - $80
- Fan - $9
- Optional
  - Netgear GS305E - $33
- Total price about $250

What sniffing tools to use

- Will depend on your goals
- tcpdump or tshark
  - Grab all packets
- Zeek
  - Grab useful summary data
- Suricata or Snort
  - IDS capability
- If load permits, run multiple options

For this example

- Capture full pcaps with tcpdump
  - Provides full fidelity
  - Comes pre-installed
- Zeek
  - Summary data data for security review
- RITA
  - Analyze Zeek data for C2 patterns
  - Compromise assessment

Autocapture with tcpdump

/etc/rc.local

```
mkdir -p /opt/pcaps

screen -S capture -t capture -d -m bash -c "nice -n 15 tcpdump -i eth0 -G 3600 -w
'/opt/bro/pcaps/'`hostname -s`'.%Y%m%d%H%M%S.pcap' -z bzip2 '(tcp[13] & 0x17 !=
0x10) or not tcp'"


# ls -A1 /opt/pcaps

raspberrypi.20191025150233.pcap.bz2

...
```

Installing Zeek and RITA

- RITA will install Zeek if not present
- Go to RITA Github page

https://github.com/activecm/rita

- Page down to "Install" section
- Click link to latest install script
- Right click "install.sh"
- Copy URL

RITA install script

$ wget https://github.com/activecm/<full URL you copied>

Resolving github.com (github.com)... 192.30.255.113
Connecting to github.com (github.com)|192.30.255.113|:443... connected.
HTTP request sent, awaiting response... 302 Found
…

install.sh 100%[==========>] 18.79K --.-KB/s in 0.07s

2019-12-17 12:07:35 (256 KB/s) - ‘install.sh’ saved [19239/19239]

$ chmod +x ./install.sh
$ sudo ./install.sh

RITA install script (2)

Would you like to continue running the Bro configuration script?
You might answer no if you know you have already created a working node.cfg and do not wish to replace it. Otherwise we recommend continuing with this script.
(y/n)? y

The potentially sniffable interface is: eth0
Would you like to include it as a sniff interface (y/n)? y

<node.cfg output>
Would you like to replace the existing node.cfg with the above file? y

Once complete, Zeek and RITA are ready for use!

Logs

- Bro output logs
  - /opt/bro/logs
    - `current` and `yyyy-mm-dd`
- Usable as is and with Rita

Why not use a traditional PC?

- Cost; 1/3-1/20 of PC or rackmount (~$210 with all components except KB, mouse, monitor)
  - Easier to get signoff
- Size
  - Isolated sites with little network management
  - Clandestine pentest
- Downsides: moderately powered CPU and max 4GB RAM now

To infinity...

- Additional nic(s) connected to USB
- Live display of results
  - 2x HDMI
  - 40 pin connector display (E-ink, LCD, others)
- Remote access/file transfer/remote execution via wifi or USB Ethernet
- Cluster of PIs for capture and analysis
- Network/physical monitoring

...and beyond

- Custom circuitry
- Power (POE, battery, solar)
- BLE/wifi sniffing (conflicting reports on whether built-in wifi supports monitor mode)
  - Can always add monitor-capable wifi dongle

Additional connections

- 40 Pin connector
  - Touch/non-touch screens, 2.2" - 7"
  - 2-8 line character displays
  - Sensors (temperature, humidity, accelerometer, magnetometer, air quality....)
  - GPS, speaker, audio out
- LoRa, Cellular, GPS
- Alarm: motion sensor, window sensor
- Camera connector (IR and visible light)

References

- www.raspberrypi.org (Source of Raspberry Pi image)
- https://www.adafruit.com/category/105 (Raspberry pi hardware)
- https://learn.adafruit.com/category/raspberry-pi (hundreds of project tutorials)
- https://www.adafruit.com/category/35 (hundreds of sensors)
- https://www.canakit.com/raspberry-pi/pi-4-kits (Kits with all the parts to get started)

Ref 2

- https://medium.com/@elkentaro/snooppi-a-raspberry-pi-based-wifi-packet-capture-workhorse-part-1-n-for-snooppi-1fa14ed67e01 (wifi sniffing)
- https://pimylifeup.com/raspberry-pi-network-scanner/ (wifi scanner with Kismet)
- http://fruitywifi.com/index_eng.html (Wireless network auditing tool)
- https://www.raspberrypi.org/downloads/noobs/ (Noobs OS for microsd)

Ref 3

- https://www.raspberrypi.org/documentation/installation/noobs.md (Noobs specifics)
- https://github.com/activecm/pi_show (PiOled display script/library)
- https://www.blackhillsinfosec.com/pentesting-dropbox-on-steroids/ (Cellular modem setup)
- https://shop.pimoroni.com/products/fan-shim (gpio-mounted fan)

Shopping list

- Shopping list spreadsheet
  - https://www.activecountermeasures.com/raspberry_pi_sensor/
  - Along with the zip file with scripts and the pdf of this talk
- Questions?
  - bill@activecountermeasures.com