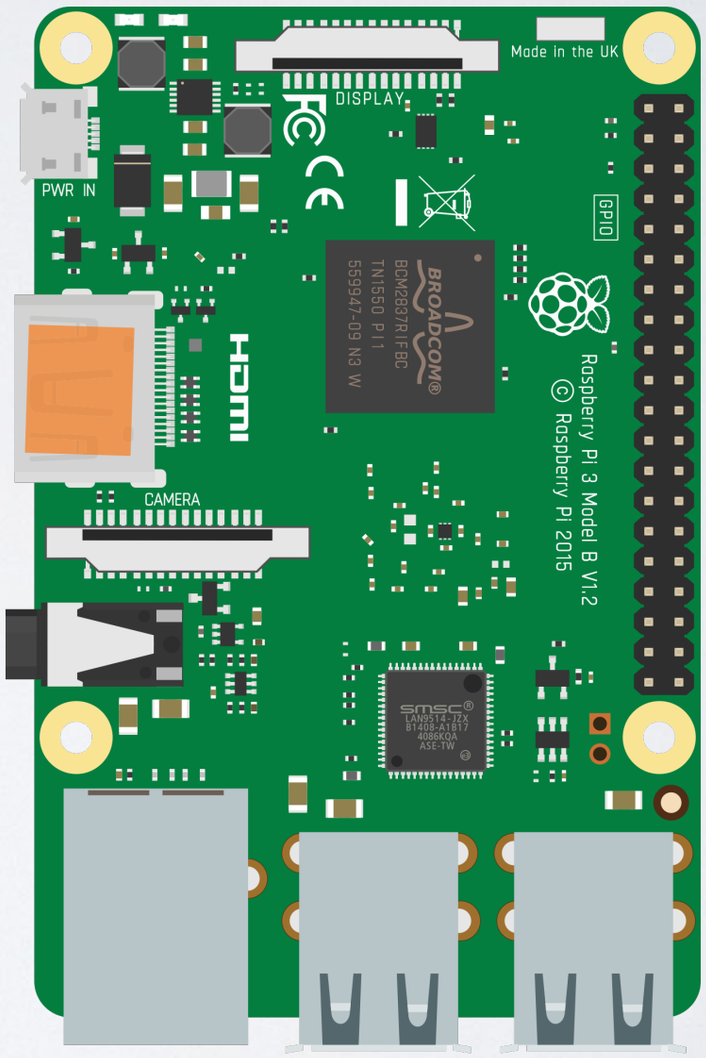
TLS, VPN & TOR… OH MY!

Who knew $35 would stretch this far?

WHY?

- (TLS) Secure network traffic to/from Pi Hole
- (VPN) Surf safe & secure from anywhere
- (Tor) Explore the unknown side streets of the Internet
- Increased security posture



SECURING PI-HOLE WITH TLS

- Pi-hole ships without a TLS cert
    - This allows quick and error-less blocking of ads that are displayed over a TLS connection
- Blindly enabling TLS on your Pi-hole? You're gonna have a bad time
    - Slows down general web surfing
    - Browser errors (mismatched certificate)
    - OS popups on sites containing blocked content on macOS/iOS

SECURING PI-HOLE WITH TLS

- Doing this is contingent on the Pi-hole having a FQDN (and a valid TLS certificate)
- Relatively easy if deployed on a publicly routable network segment
- More difficult on a home network, but not impossible!

SECURING PI-HOLE WITH TLS

- Public deployment guides
  - https://discourse.pi-hole.net/t/enabling-https-for-your-pi-hole-web-interface/5771
  - https://scotthelme.co.uk/securing-dns-across-all-of-my-devices-with-pihole-dns-over-https-1-1-1-1/

PI-HOLE TLS FOR HOME NETWORKS

1. Create an /etc/hosts entry for the Pi-hole

2. Generate a self-signed TLS cert & CA cert

3. (Optional) Add CA cert to home network devices

4. Modify lighttpd configuration & enjoy!

ADDING /ETC/HOSTS ENTRIES

```
$ ping -c 1 example.com
 PING example.com (93.184.216.119) 56(84) bytes of data.
```

```
$ sudo vi /etc/hosts
```

```
# IP Domain ShortHost
192.168.0.193 example.com example
```

```
$ ping -c 1 example.com
PING example.com (192.168.0.193) 56(84) bytes of data.
```

GENERATE TLS CERT

```
umc-251083:~ sysaaron$ openssl req -newkey rsa:2048 -new -nodes
 -x509 -days 3650 -keyout privkey.pem -out cert.pem
```

```
umc-251083:~ sysaaron$ sudo cat /path/to/privkey.pem \
> /path/to/cert.pem | \
> sudo tee /path/to/combined.pem
```

```
umc-251083:~ sysaaron$ sudo chown www-data -R /path/to/cert/
```

GENERATE CA CERT

```
umc-251083:~ sysaaron$ openssl genrsa -des3 -out privateCA.key 2048
```

```
umc-251083:~ sysaaron$ openssl req -x509 -new -nodes -key privateCA.key
-sha256 -days 3650 -out privateCA.pem
```

EDIT LIGHTTPD CONFIG

```
umc-251083:~ sysaaron$ sudo nano /etc/lighttpd/external.conf
```

```
$HTTP["host"] == "pihole.example.com" {
  # Ensure the Pi-hole Block Page knows that this is not a blocked domain
  setenv.add-environment = ("fqdn" => "true")

  # Enable the SSL engine with a LE cert, only for this specific host
  $SERVER["socket"] == ":443" {
    ssl.engine = "enable"
    ssl.pemfile = "/etc/letsencrypt/live/pihole.example.com/combined.pem"
    ssl.ca-file =  "/etc/letsencrypt/live/pihole.example.com/fullchain.pem"
    ssl.honor-cipher-order = "enable"
    ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH"
    ssl.use-sslv2 = "disable"
    ssl.use-sslv3 = "disable"
  }

  # Redirect HTTP to HTTPS
  $HTTP["scheme"] == "http" {
    $HTTP["host"] =~ ".*" {
      url.redirect = (".*" => "https://%0$0")
    }
  }
}
```

ADDING AN OPENVPN NODE

- https://www.sitepoint.com/setting-up-a-home-vpn-using-your-raspberry-pi/

ADDING A TOR NODE

- https://www.instructables.com/id/Raspberry-Pi-Tor-relay/

GET AT US, YO!

Arden: @that_guy_ego, meyerar@iastate.edu, github.com/that_guy_ego, & secdsm.org
Aaron: @sysaaron, aaron@scantl.in, github.com/coffeebro & seckc.slack.com