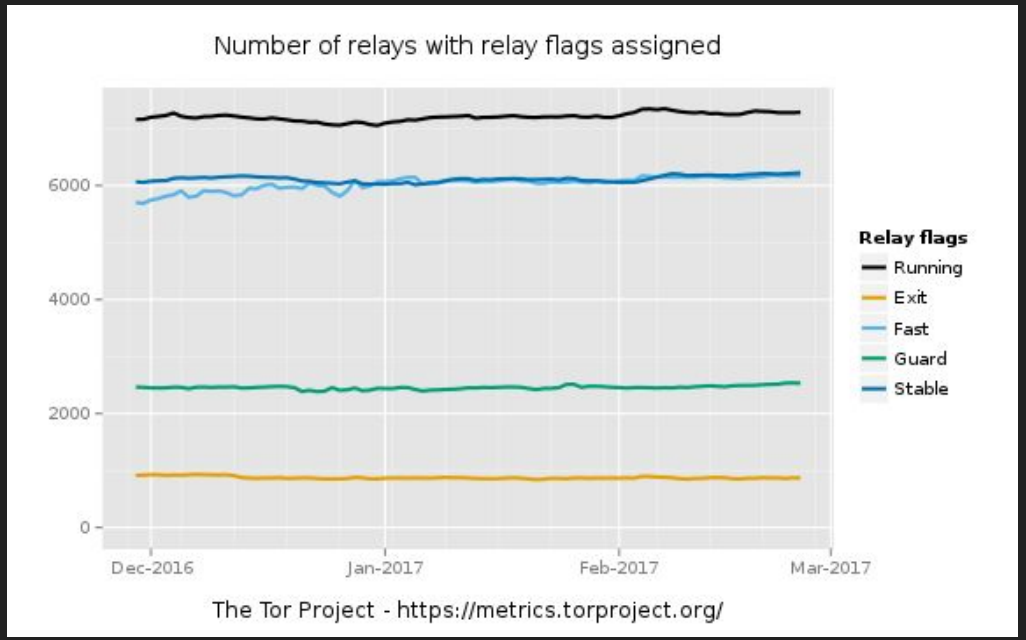
Background

Tor relies on network diversity for many of its anonymity features

Example: If there were only 5 relays on the network, your path is very predictable

The consensus document (eventually) contains all of the ports available on the tor network



Premise

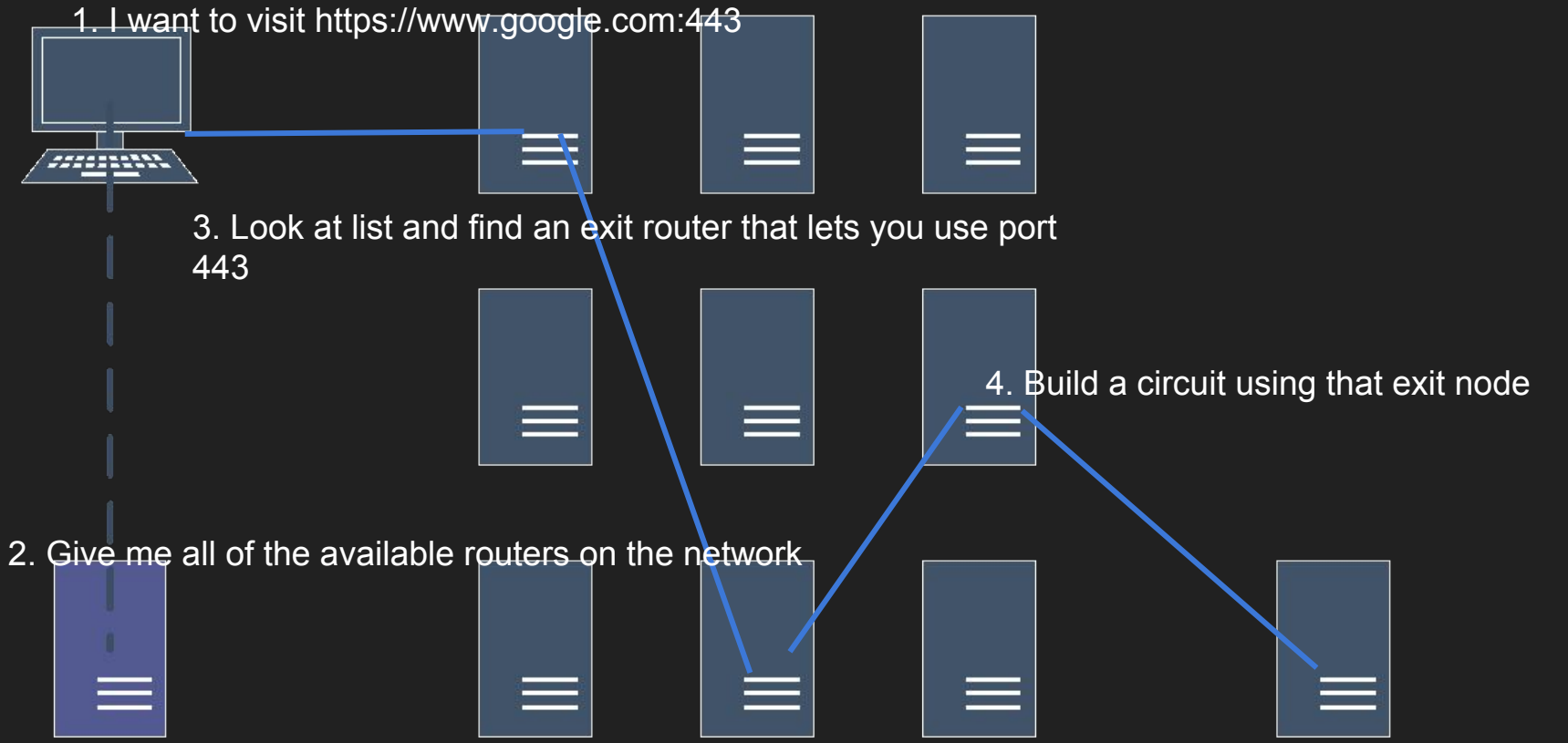
Anonymity is determined by diversity

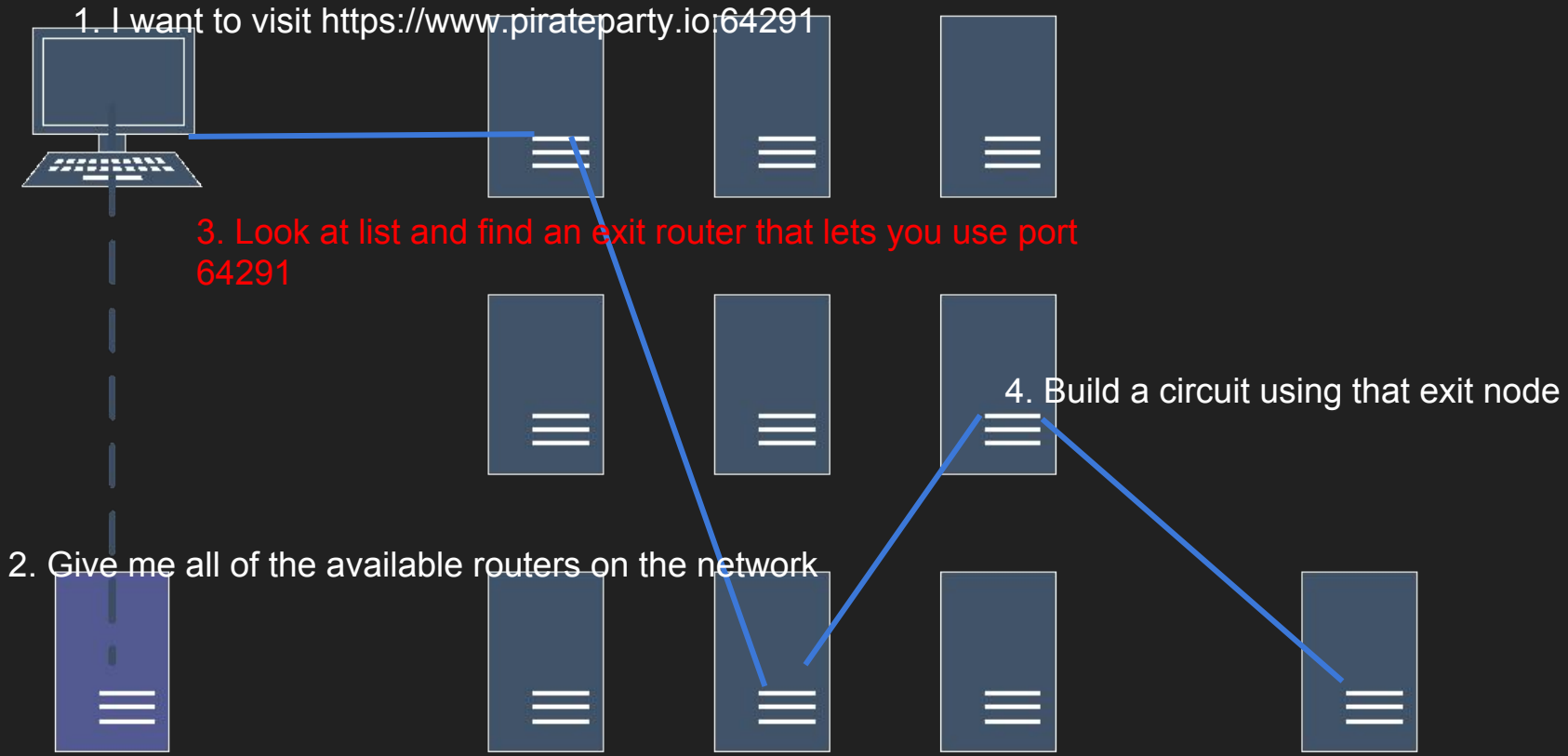
People run “Reduced Exit Policies”

- 80, 443, 9999, 8080, etc

On ports that are not in the reduced exit policies list, you have much less anonymity

Questions: How much less and is it exploitable?


1. I want to visit https://www.google.com:443
3. Look at list and find an exit router that lets you use port 443
4. Build a circuit using that exit node
2. Give me all of the available routers on the network


1. I want to visit https://www.pirateparty.io:64291
3. Look at list and find an exit router that lets you use port 64291
4. Build a circuit using that exit node
2. Give me all of the available routers on the network

Data crunching

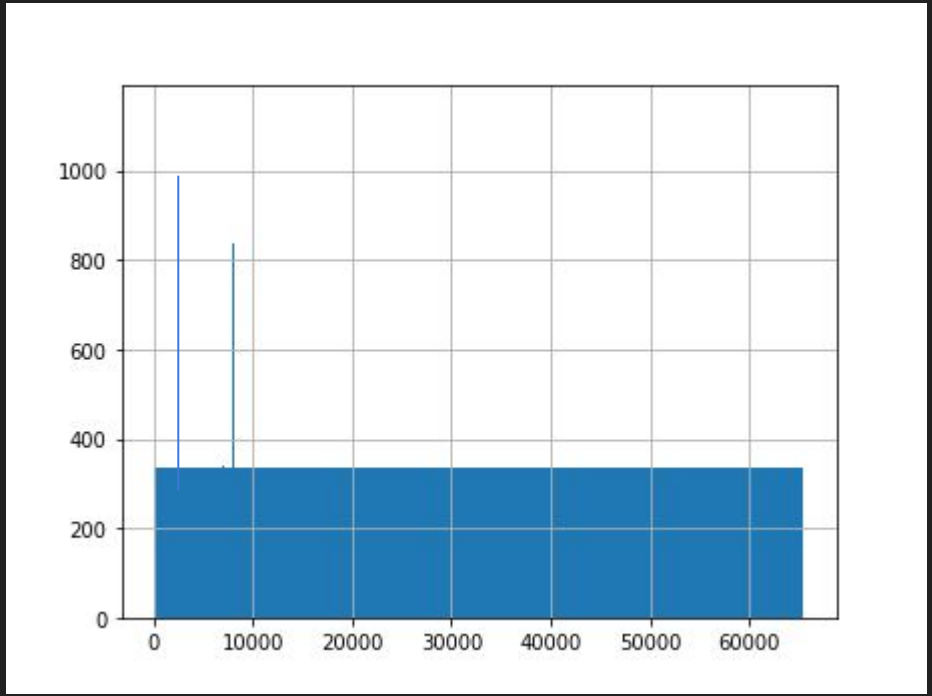
Download the consensus document

Extract the exit policies of each node

Enumerate the open ports that are available

- accept *:* vs accept 80:81

Plot the results (terribly)



How many...

Total Network Servers: 7000

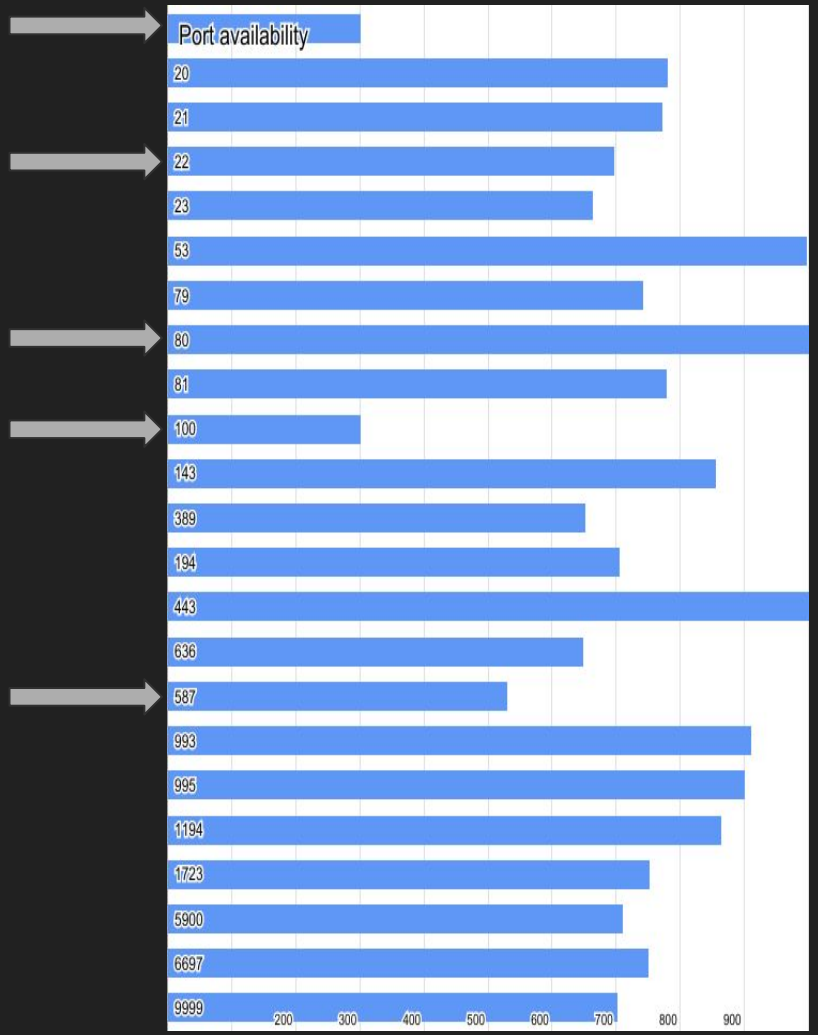
Total available exit nodes: 1143

Total available exit nodes HTTP: 1067

Total available exit nodes SSH: 700

Total available exit nodes SMTPS: 531

Total available exit nodes TCP/65281: 303



Bill’s Management Slide: TL:DL

1. There are ~300 exit nodes on the network allowing all ports
2. GCHQ believes that need to run ~3500 (sibil) nodes to effectively compromise the network.
3. Malicious websites could force you to make a circuit to a service on an obscure port which would reduce your potential anonymity down to 33%
4. If GCHQ can induce you into visiting a service hosted on an obscure port, they reduce their level of effort to exploit you by 15%
5. If the level of anonymity provided is correlated to the diversity of the network, the level of anonymity provided is correlated to the obscurity of the port