Tor

Benjamin Toll
benjamintoll.com
benjam72@yahoo.com

What is Tor?

- An onion router
- A network that defends against traffic analysis
  - Routes traffic from sender to open Internet
  - Traffic can stay internal, i.e., Tor onion services, aka “The Dark Web”
- Run by volunteers
- There are many application protocol specific tools that use the Tor network to communicate with remote hosts, i.e., “Torified”
  - Tor browser
  - OTR
  - SOCKS5
  - tor-resolve (DNS)

Why do we need Tor?

- Provides anonymity and privacy
- Best strategy currently available*
- Free and open source
- First Amendment protection

* VPNs are arguably safer, but read the fine print if using a public service (and then do more research)!!!

Who uses Tor?

- “Regular” people
  - Citizens in repressive regimes
  - Anyone who values privacy
  - Programmers and sysadmins
  - Mom and Dad
- Journalists
- Activists
- Whistleblowers and dissidents
- Governments
- Law enforcement
- Bad actors

Elephants (in the Room)

- But there are bad actors!
  - They also use public proxies, VPNs, GPG, etc.
- It’s the Dark Web!
  - Marketing term that MSM loves….scary!
  - Many legitimate sites, such as ProPublica, DuckDuckGo and Facebook, also run onion servers
- Let’s put in back doors for the “good guys”!
  - Bad actors will find and leverage back doors
- Tor is safe!
  - Unless you’re being targeted by a nation state and/or an entity with deep pockets
  - If NSA wants in, they’re in
  - Safety is directly proportional to the number of Tor users!
- Tor isn’t safe!
  - Yes, the NSA runs many exit nodes, but that’s only half the battle
  - Traffic analysis needs a concerted effort
  - The more Tor users, the safer (needle in a haystack)

Let’s dig in!

How does Tor work?

- Builds a circuit of three relays (guard, middle and exit relays) between sender and the Internet
- Each node only knows about the relay before and after
  - The guard or entry node is the only relay that knows the true IP address of the sender
  - The exit node is the only node that knows the true destination
- Layers of encryption (*onion* routing) are generated on sender before leaving host machine
  - Public key cryptography
  - Payload is at the center of the “onion” surrounded by layers of encryption
  - Each relay unwraps a layer of encryption
  - Exit node unlocks final encryption layer, is able to read true tcp headers and sends to destination over open Internet

How do I know Tor is working?

- There are any number of sites that will show you the IP address that the open Internet “sees”:
  - Verify IP address of exit node with IP Chicken (https://www.ipchicken.com/)
- Verify IP address of exit node in server logs:
  - `sudo tail -f /var/log/nginx/access.log`
- Sniff traffic network traffic:
  - Localhost
    - `sudo tcpdump -nX host <ip.of.guard.node> and port 443`
  - Remote
    - `sudo tcpdump -nX host <ip.of.exit.node> and port 80`
- If using Tor browser, visit https://check.torproject.org/.

Tor traffic can be blocked

- The IP addresses of all Tor exit nodes are published, so it’s trivial to blacklist those IPs
- Censors can perform deep packet inspection between the sender and the guard relay
- Because of the latter, Tor has developed pluggable transports so traffic between the sender and the first hop (guard relay) can’t be identified as Tor network traffic

What not to do when using Tor

- Fill out any web forms with personal information
- Download files, i.e., pdf and Word docs whose loader programs could then leak the true IP address
- Torrent
- Visit sites that only a small number of people could know about, i.e. staging servers or “deep web” IP addresses*

Other privacy tools

- torsocks
- tor-resolve
- GNU Privacy Guard (GPG)
- Signal
- OTR
- DuckDuckGo search engine (NOT Google!!!)

FIN

Benjamin Toll
benjamintoll.com
benjam72@yahoo.com