**Tor Weaknesses**

**Tor is high profile**

**The Tor browser isn’t sufficiently isolated**

We know nation states use the Quantum System, FoxAcid and EgotisticalGiraffe to actively compromise browsers

US agencies also had success in 2013

Harden browser, make attack surface a small as possible

* Browser exploitation is one of the biggest attack vectors for deanonymisation
* Must be hardened

Never install on main OS

* Must use isolation and compartmentalisation

**Lack of Browser Non-Persistence**

After closing all tabs, Tor invokes a purging of browser data

* **But only non-persistence can protect against the next unknown tracking threat**

Can be achieved through Live OS, VM snapshots, whole disk encryption, Portable apps

**Browser Fingerprint**

* Tor has a unique fingerprint which will show the observer that you are using the Tor browser
* You will look like all other Tor browser users though

Traffic confirmation (e2e correlation) with sybil attacks and DDoS attacks

* Low latency anonymising service
  + Susceptible to traffic confirmation correlation attacks

This happens when an attacker observes the traffic on both ends of the circuit, so guard node and exit node and compares traffic timing, volume or other characteristics to conclude the two relays are on the same circuit

* If the guard knows the ip of the user and the exit knows the resource or destination that the user is accessing, then together these can be used to deanonymise

**Website Traffic Fingerprinting**

Passive eavesdropping attack that looks at the size and timings of encrypted traffic streams

Even though data is encrypted, the adversary can still guess what websites are being visited because all webpages have specific traffic patterns

* Can only be guessed if the pattern for that website is already known

**Exit relay sniffing**

The data that comes out of the exit node is not private if not encrypted

* Can be injected with things like zombie supercookies, code and sniffed
* E2e encryption is the answer to this, TLS, PGP etc.

**Traffic analysis attacks**

Can be done by a passive observer if they can see enough relays

**MITM/MOTS**

An attacker between the exit and the destination can intercept requests and respond to them before the destination, fooling you into thinking you’re communicating with the dst

**Ports are blocked**

Sometimes ports you need to use are blocked by some relays (e.g., to get through a firewall) so you’ll have to use a different circuit which may be slower

**Directory Authorities**

If the Das ever become compromised, the Tor network is also fully compromised

**Protocol leaking**

Like DNS leaking

Do not use BitTorrent’s as they can leak on Tor

**Tor blocked for some websites**

**No UDP support – does provide DNS port**

**Speed and Latency**

**The guardian**

**Attacking tor: how the nsa targets users onoline anonymity**