Research questions for Tor

- **Part one: research questions, current and soon.**
- Part two: research questions we need help on.

Decentralizing the directory

- Server descriptors are self-signed, so get them anywhere.
- Each dirserver distributes a “network status” with its belief about who's in the network, location, timestamp of their latest descriptor, etc.
- Threshold belief.
- Partitioning attacks!

Incentives to relay

- 1) Incentives to relay traffic
- 2) Incentives to do it well
- 3) Incentives to allow exits.
- Naïve tit-for-tat probably not so smart. But maybe something like it?

“Run two servers and wait”

- Over time, Alice will choose your nodes as entry and exit.
- Helper nodes.
- What's the right way to do helper nodes in the presence of churn?

Hidden service safety

- Against an adversary who runs a tor node, how long do hidden service locations stay safe?
- Helper nodes are one answer. Authentication/authorization is another answer.

Location diversity

- When many nodes are at a single ISP, and many paths are observable by a single ISP, what **local** algorithms can Alice use to improve (maximize?) her safety?

Tor GUI competition

- Two phase competition: first sketches, then implementation.
- Judges: Patrick Ball, Simson Garfinkel, Bruce Schneier, Adam Shostack, Edward Tufte, Ka-Ping Yee
- User studies from CMU?

University interest in Tor

- Exit nodes at Harvard, CMU, Georgia Tech, RPI, Drexel, U Texas Arlington, Rose-Hulman, Michigan Tech, U Puerto Rico, ICM (Poland), Politecnico di Milano (Italy), CTI Patras (Greece), University of Thessaloniki (Greece), ...
- Middleman nodes at Berkeley, MIT, MU Ohio, Virginia Tech, TU Dresden, RWTH Aachen, Cambridge University, Mirovni Institut (Slovenia), Universiteit Maastricht (NL), Uni Bremen (Germany), ...
- Previous nodes at Brown, Rice, UMass Amherst, U Toronto, United Nations
- Planetlab?

Research questions for Tor

- Part one: research questions, current and soon
- **Part two: research questions we need help on.**

Non-clique topology

- Right now we assume all nodes can reach all other nodes. We're fine as long as that's mostly true.
- What about Internet splits?
- What about nodes in China – or entire Tor networks in China?
- One answer is Geoff Goodell's “Blossom” project at Harvard.

Mid-latency

- How much latency do you need to add to start seeing end-to-end defense?

Does it mix?

- Does low-latency traffic provide cover (“mix”) with mid/high-latency traffic?

Website fingerprinting

- Do these attacks work against Tor?
- Does cell size change things?
- Does variable delay change things?
- What about a little bit of padding, e.g. long-range dummies?

Fragmenting streams

- Should we fragment streams across multiple paths?

Congestion attacks

- Can you “measure” Alice by ICMP pings even if she doesn't relay traffic for you?
- (Cf Murdoch/Danezis Oakland05 paper)

Incentives to relay

- Is it always unsafe to use your server for your anonymous traffic?

Pseudonyms/profiles

- Logging into your gmail account and then posting to Indymedia is bad.
- But a new circuit for every request is also bad.
- What's the right compromise/strategy?

Puzzles to manage load?

- If each server demands that Alice solves a puzzle, can we make the puzzle proportional to load?
- Alice's delay reveals which node she's solving a puzzle for?

Transporting UDP and IP

- Need IP-level packet normalization library.
- Application-level streams still need scrubbing (e.g. privoxy).
- DNS requests to your local nameserver still leak information.
- DTLS exists now, but we still need a new Tor protocol that handles tagging attacks, drops, resends, etc.
- Exit policies for arbitrary IP packets mean building a secure IDS.
- The Tor-internal name spaces (.onion, .exit) must be redesigned.

Government-level firewalls

- Step one: need a set of exit nodes on the "free" side.
- Step two: need a set of entry nodes on the "free" side.
- Step three: need a way to give out IP addresses to the good guys without letting the bad guys enumerate them.
- Step four: need a steg approach that makes an observer not realize you're speaking Tor.