

Future Anonymity Networks

- ◆ Tor overview
- ◆ Anonymity and Usability
- ◆ Questions I want solved
- ◆ Other references

Tor overview

- ◆ Anonymizing network for TCP: web browsing, instant messaging, etc. Also provides “hidden services” -- you'll hear about those tomorrow.
- ◆ 250 servers around the world. 50.000 users?
- ◆ Funded by EFF and United States Navy.
- ◆ Picked as the anonymizing layer for the EU PRIME project.
- ◆ Listed by PC World Magazine in the top 100 products of 2005.

Tor and usability

- ◆ “Tor is just as fast as my normal net connection”
- ◆ Works great when it works.
Fails poorly.
- ◆ EFF Tor GUI Contest
- ◆ Two phases: sketches and actual code.

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 Tor's variable delay change things?
- ◆ What about a little bit of padding, e.g. long-range dummies?

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?

Helper nodes and reality

- ◆ What's the right way to do helper nodes in the presence of churn?

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?

Anonymity bibliography

- ◆ <http://freehaven.net/anonbib/>

PET 2006

- ◆ Workshop on Privacy Enhancing Technologies
- ◆ <http://petworkshop.org/>
- ◆ Cambridge, England, late June 2006.