Tor and the Censorship Arms Race: Lessons Learned

Roger Dingledine

The Tor Project, USA
`arma@freehaven.net`

Abstract. Tor is a free-software anonymizing network that helps people around the world use the Internet in safety. Tor's 2500 volunteer relays carry traffic for several hundred thousand users, including ordinary citizens who want protection from identity theft and prying corporations, corporations who want to look at a competitor's website in private, and soldiers and aid workers in the Middle East who need to contact their home servers without fear of physical harm.

Tor was originally designed as a civil liberties tool for people in the West. But if governments can block connections to the Tor network, who cares that it provides great anonymity? A few years ago we started adapting Tor to be more robust in countries like China. We streamlined its network communications to look more like ordinary SSL, and we introduced "bridge relays" that are harder for an attacker to find and block than Tor's public relays.

Through the Iranian elections in June 2009, the periodic blockings in China, the demonstrations in Tunisia and Egypt, and whatever's coming next, we're learning a lot about how circumvention tools work in reality for activists in tough situations. This talk will start with a brief overview of the Tor design and its diverse users, and then jump into the technical and social problems we're encountering, what technical approaches we've tried so far (and how they went), and what approaches I think we're going to need to try next.