

# TOR: AN ANONYMOUS INTERNET COMMUNICATION SYSTEM

Roger Dingledine  
The Free Haven Project  
arma@freehaven.net

Low-latency communication over large networks is subject to traffic analysis – cryptography alone will not hide the existence of confidential communication relationships. We have implemented and deployed a low-latency anonymous communication overlay network called Tor, based on Onion Routing.<sup>1</sup> Tor aims to resist observers and insiders by distributing each transaction over several nodes in the network. This “distributed trust” approach means the Tor network can be safely operated and used by a wide variety of mutually distrustful users, providing more sustainability and security than previous attempts at anonymizing networks. Tor works on the real-world Internet, requires little synchronization or coordination between nodes, and provides a reasonable trade-off between anonymity, usability, and efficiency.

We deployed the public Tor network in October 2003; since then it has grown to over a hundred volunteer-operated nodes and as much as 80 megabits of overage traffic per second. Tor’s research strategy has focused on deploying a network to as many users as possible; thus we have resisted designs that would compromise deployability by imposing high resource demands on node operators, and designs that would compromise usability by imposing unacceptable restrictions on which applications we support. Although this strategy has drawbacks (including a weakened threat model), it has made it possible for Tor to serve many thousands of users and attract funding from diverse sources whose goals range from security on a national scale down to individual liberties.

---

<sup>1</sup> R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. In *Proceedings of the 13<sup>th</sup> USENIX Security Symposium*, August 2004.

To connect to a remote server via Tor, the client software learns a signed list of Tor nodes from one of several central *directories servers*, and incrementally creates a private pathway or *circuit* of encrypted connections through authenticated Tor nodes on the network, negotiating a separate set of encryption keys for each hop along the circuit. The circuit is extended one node at a time, and each node along the way know only the immediately previous and following nodes in the circuit, so no individual Tor node knows the complete path that each fixed-sized data packet (or *cell*) will take. Thus, neither an eavesdropper nor a compromised node can see both the connection's source and destination. Later requests use a new circuit, to complicate long-term linkability between different actions by a single user.

Individuals use Tor to keep remote websites from tracking them and their family members, or to connect to resources such as news sites or instant messaging services that are blocked by their local Internet providers. Activist groups like the Electronic Frontier Foundation (EFF) are funding further Tor development to help maintain civil liberties on line. Corporations are investigating Tor as a safe way to conduct competitive analysis, and are considering using Tor to test new experimental projects without associating their names with these projects. A branch of the U.S. Navy uses Tor for open source intelligence gathering, and one of its teams used Tor while deployed in the Middle East recently. The Tor protocol is one of the leading choices for the anonymizing layer in the European Union's PRIME directive to help maintain privacy in Europe. the AN.ON project in Germany has integrated an independent implementation of the Tor protocol into their popular Java Anon Proxy anonymizing client. This wide variety of interests helps maintain both the stability and the security of the network.

Ongoing trends in law, policy, and technology threaten anonymity as never before, undermining our ability to speak and read freely online. These trends also undermine national security and critical infrastructure by making communication among individuals, organizations, corporations, and governments more vulnerable to analysis. Tor's security is improved as its user base grows and as more people volunteer to run servers. We have

many open research and design problems as well. For design documents, byte-level specifications, and free software packages, read more at <http://tor.eff.org/>