



Turtle – Safe and Private Data Sharing

Turtle is a new tool for facilitating free speech by combining encryption with peer-to-peer (P2P) technology. Turtle users can exchange information deemed “controversial” or “risky” (for example whistleblowers exposing government or corporate abuse) without being exposed to legal or economic pressure from parties that may want to censor or suppress this information.

The basic idea behind Turtle is to build a P2P overlay on top of pre-existing trust relationships among Turtle users. Each user acts as node in the overlay by running a copy of the Turtle client software. Unlike existing P2P networks, Turtle does not allow arbitrary nodes to connect and exchange information. Instead, each user establishes secure and authenticated channels with a limited number of other nodes controlled by people he or she trusts (friends). In the Turtle overlay, both queries and results move hop by hop; the net result is that information is only exchanged between people that trust each other and is always encrypted. Consequently, a snooper or adversary has no way to determine who is requesting/providing information, and what that information is. Given this design, a Turtle network offers a number of useful security properties, such as confined damage in case of node compromise, and resilience against denial of service attacks.

<http://www.turtle4privacy.org>

In order to join the Turtle network, you need to install the Turtle client software, which is distributed on the Turtle CD-ROM. Alternatively, you can download the Turtle client software from the Turtle Project Web site:

<http://www.turtle4privacy.org>

At the moment, the Turtle client has been ported on Linux. Detailed instructions on how to install and configure Turtel can be found in the Turtle user's manual, available on the Turtle CD-ROM, as well as on the project Web site.

<http://www.turtle4privacy.org>

