Turtle: Safe and Private Data Sharing

Bogdan C. Popescu, Bruno Crispo, Andrew S. Tanenbaum
Vrije Universiteit, Amsterdam, The Netherlands
{bpopescu, crispo, ast}@cs.vu.nl

Petr Matejka
Charles University, Prague, Czech Republic
pmatejka@ontheweb.cz

In this WiP report, we present Turtle, a peer-to-peer (P2P) architecture for safe and private sharing of sensitive information. We envision Turtle as a tool for facilitating free speech, by allowing its users to exchange information deemed "controversial" or "risky" by traditional media, without being exposed to legal and economic pressure from parties that may want to suppress this information.

The basic idea behind Turtle is to build a P2P overlay on top of pre-existent trust relationships among Turtle users. Each user acts as node in the overlay by running a copy of the Turtle client software. Different from 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 she trusts (friends). Given that the users behind connecting Turtle nodes know and trust each other, they can agree on channel encryption keys out of band; this allows for a totally de-centralized key distribution mechanism, which fits well the P2P paradigm. In the Turtle overlay, both queries and results move hop by hop; the net result is that at any moment, information is only exchanged between people that trust each other, and is always encrypted, so an adversary has no way to determine who is requesting/providing information, and what that information is about. 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 Sybil attacks [3]. At this moment we are developing the Turtle client software (an early-beta prototype is available at *http://sourceforge.net/projects/turtle-p2p/*). We are also looking at ways to realistically simulate large Turtle networks, in order to evaluate Turtle's performance against other P2P protocols such as Gnutella or BitTorrent; one idea is to model Turtle overlays based on social graphs derived from "social networking" services, such as Orkut [2], or Friendster [1].

References

[1] Friendster Web Site. http://www.friendster.com.
[2] Orkut Web Site. http://www.orkut.com.
[3] J. Douceur. The Sybil Attack. In *Proc. of the IPTPS '02 Workshop*, Mar. 2002.