Panel Discussion — Mix Cascades Versus Peer-to-Peer: Is One Concept Superior?

Claudia Díaz[1,**], George Danezis[2,*], Christian Grothoff[3,*], Andreas Pfitzmann[4,*], and Paul Syverson[5,*]

[1] Katholieke Universiteit Leuven, Belgium
Claudia.Diaz@esat.kuleuven.ac.be
[2] George Danezis, University of Cambridge, UK
George.Danezis@cl.cam.ac.uk
[3] Purdue University, USA
[4] Technische Universität Dresden, GER
pfitza@inf.tu-dresden.de
[5] Naval Research Lab, USA
syverson@itd.nrl.navy.mil

David Chaum's initial work on Mixes led to a vast number of proposals how to provide anonymous communication on the Internet. They all have in common, that a multiple of Mixes are used to establish a certain amount of anonymity. The most salient difference between those approaches is the way, how the Mixes are connected and organised.

Two idealised concepts set the range on a continuum of possible designs. On the one end, we have Mix cascades: dedicated servers joining traffic from a large set of users and uniformly redirecting it on a predefined route. The other end is defined by Peer-to-Peer (P2P) systems: widely distributed and equal client applications unpredictably routing their traffic over all possible routes. As these design options have implications on the achievable anonymity and performance, this panel discussion aims to elaborate the advantages and disadvantages of either concept.

As this major design decision has implications on several aspects, the panel is supposed to discuss the issue from multiple points of views: anonymity, deployment, availability, as well as performance.

The discussion is likely to focus rather on the appropriateness of attack models, than on details of analyses of certain implementations. This is intended, because we believe that the choice of attack models is an expression of the researcher's view of the world.

** Moderator.
* Panelists.

D. Martin and A. Serjantov (Eds.): PET 2004, LNCS 3424, p. 242, 2005.