Providing Trust and Reputation in Peer-to-Peer Networks

Tanja Ažderska[1,2]

[1] Laboratory for Open Systems and Networks, Jožef Stefan Institut, Ljubljana, Slovenia
[2] Jožef Stefan International Postgraduate School (ICT3, 1st year)

atanja@e5.ijs.si

The Internet has already set its users free of any kind of building infrastructure. It has evolved beyond e-mail, content, and e-commerce, becoming a true platform that combines the qualities of service of enterprise computing with the ability to share resources across the web. Moreover, Internet is becoming more and more distributed, and so are the expectations for its aligning protocols. According to Ipoque Internet Study for 2008/09, P2P generates most of the Internet traffic in all regions (even up to 70% in Eastern Europe), with predictions that it will account for more than 90% by 2013. This huge amount of P2P usage is due to its open, anonymous and self-organizing nature. P2P computing has incredibly wide range of usage: from simple every-day communication (Skype), content sharing (BitTorrent), and e-commerce (eBay), to great research projects that require the processing power of numerous interconnected computers (SETI@Home). The whole area of distributed computing is a hot bed of significant development that has been generating amazing advances [3] [4].

Nevertheless, P2P systems are not just about distributing information. Their open nature has attracted vast amount of users and dragged even greater attention to attackers who use impressive amount of resources trying to subvert these systems. There is now a strategic shift by the attackers that mainly target personal computers with high Internet connectivity that can be useful for the miscreants. The complexity of distributed networks brings equally complex issues for defending them against attacks [1] [2]. Future systems are not likely to ease that job, as new threats will emerge due to the billions of components comprising them. In this new "world of emerging technological opportunities", reputation is one of the few tools that can still provide trust: trust among the users of distributed services, and even the trust necessary to maintain reliability and accountability of these services [3].

Our contribution is attributed through BarterCast, a fully distributed reputation mechanism that is part of the NextShare software developed in the P2P-Next project [4]. We have mapped BarterCast's design onto the Taxonomy of Trust proposed by the Stanford Peer Research group and obtained important conclusions mainly related to the design and partially to the purpose of the mechanism [3]. While BarterCast is more reputation oriented (choosing appropriate collaborator based on her past behavior and performance, incentivizing collaborative behavior etc.), there are security issues that have not been tackled yet in the present design. Some of them are identity and trust management, threat modeling, information integrity check and information time convergence. Our research not only considers the social aspect of a reputation system design, but also strives to base users' collaboration on strong security mechanisms. Fostered reputable and trustworthy collaboration would lead any Internet based application closer to its"Future Internet" ideal.

References:

[1] Meulpolder, M. and Pouwelse, J. A. and Epema, D. H. J. and Sips, H. J., BarterCast: A Practical Approach to Prevent Lazy Freeriding in P2P Networks, Proc. of the 6th International Workshop on Hot Topics in Peer-to-Peer Systems (Hot-P2P'09) in conjunction with IPDPS 2009, May, 2009, 1-8,

[2] J. A. Pouwelse and P. Garbacki and D.H.J. Epema and H. J. Sips, The BitTorrent P2P File-Sharing System: Measurements and Analysis, , 2005,

[3] Marti, Sergio and Garcia-Molina, Hector, Taxonomy of trust: Categorizing P2P reputation systems, Management in Peer-to-Peer Systems, Computer Networks, 50, 4, March, 2006, 50, 472--484, http://dx.doi.org/10.1016/j.comnet.2005.07.011;

[4] http://www.p2p-next.org/, the P2P-Next project page.