An Evaluation of Cooperative Decisions in Peer-to-Peer Systems - Mathematics vs. Testbed Studies

André König, Ralf Steinmetz
Multimedia Communications Lab (KOM)
Technische Universität Darmstadt
{andre.koenig, ralf.steinmetz}@kom.tu-darmstadt.de

Matthias Hollick
Departamento de Ingeniería Telemática
Universidad Carlos III de Madrid
matthias.hollick@uc3m.es

Abstract

Security-relevant decisions such as authentication and access control are commonly performed by central trusted instances based on predefined security policies. In peer-to-peer (p2p) systems, particularly in those established spontaneously e.g. to support emergency response operations, the availability of these building blocks for security can not be assumed. Yet, an appropriate security level can be achieved by performing decisions cooperatively with a set of authorized users being involved directly. We introduce techniques and interaction schemes facilitating cooperative user-based decisions in p2p systems. We further validate a stochastic model describing the decision process developed in previous work by testbed studies.

1. Cooperative User-based Decisions

The outcome of security-relevant decisions can be represented by cryptographically signed certificates. In a p2p system without central trusted instances, signing certificates can be delegated to authorized peers. Yet, to prevent possibly compromised peers from signing certificates arbitrarily, no single peer should be able to produce signatures. This can be achieved e.g. by means of threshold cryptography.

When authorized users (peers) are involved directly in the decision process due to lacking security policies, a core challenge concerns the number of users that should be queried. Assuming users that are not able to provide a decision in a moderate amount of time, sending redundant queries is reasonable. The feasibility within real world applications requires limiting the number of queried users, though. The querying process can be categorized into coordinated and uncoordinated approaches. In coordinated approaches, a dedicated peer keeps track on the status of authorized users and, thus, is able to direct queries appropriately. In uncoordinated approaches, no knowledge on the status of users is available. Therefore, the querying has to be performed statistically, by a random selection of peers.

2. Testbed Results

To validate the model developed in previous work, we implemented the cooperative decision process based on a Pastry p2p overlay. First results from experiments in the PlanetLab testbed compared to the predictions of the model are shown in Figure 1. We kept the number of users queried constant an varied the threshold, i.e., the number of users that have to cooperate in order to produce signatures. We determined the probability of a successful cooperative signature process, i.e., the probability for the cooperation of a sufficient number of authorized users with respect to the threshold. The result shows that the model predictions match the experimental results qualitatively. The offset can be explained by the packet loss that is not considered by the model but is observed during the testbed studies.

In our talk we present further results from both the PlanetLab and the G-Lab testbed. PlanetLab and G-Lab differ strongly with respect to their topology, the hardware deployed, and the connectivity of the nodes. From comparing results from the test-beds and the model we expect comprehensive insights regarding the feasibility of cooperative decisions in p2p systems and regarding the effect of different testbed topologies.

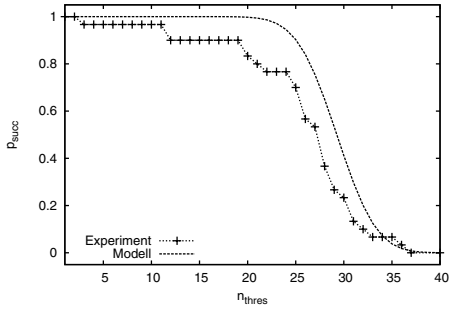

Figure 1. Comparison of model predictions and PlanetLab results