Technische Universität München
Lehrstuhl für Netzarchitekturen und Netzdienste
Prof. Dr. Georg Carle

Thesis (B.Sc./M.Sc.)

Spontaneous Private Networking - Governed By Security Policies

Motivation

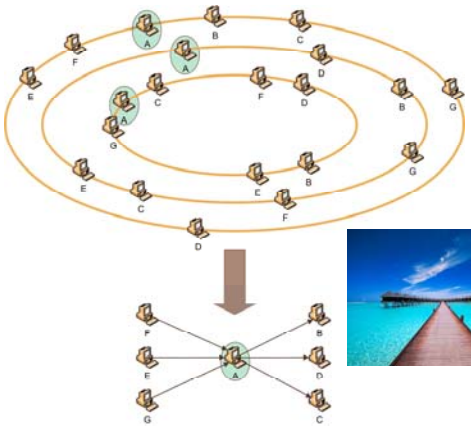
You open your video client, allow some friends from your contact list, select a few security settings, click OK and the video from your last holidays on Bora Bora is streamed towards them – safely and secure. You even note how some late-comers hop onto the stream. No need to upload it to Youtube, no need to send around cryptic links, and no concerns about privacy. All that is required is that your friends are online and in your contact list. Wouldn't it be sweet if it worked just like that?

Unfortunately, we're not there yet. The idea of spontaneous networking as described above is to allow applications of the same kind to quickly set up and operate an infrastructure for their communication. There are plenty of solutions around that can take care of the actual networking. **We have ourselves already conceived of a nice workable concept that addresses exactly that**: we use overlay networks to quickly set up a communication infrastructure. **However, we're still concerned with security**. Our **current approach is to use user-defined security policies** to determine who's allowed to participate in the network.

In this work, we explore these policies in a practical way. We are going to write a Policy Engine and combine it with the overlay software we use. The result will be a software for spontaneous, user-driven networking.

Your Task

Your task consists of the following steps.



First, you will use the **Ponder** policy framework and **OpenSSL** to write a software that can evaluate some simpler, but yet very effective policies.

Second, you will need to make some changes to the **Pastry** overlay and add cryptographic identifiers to it.

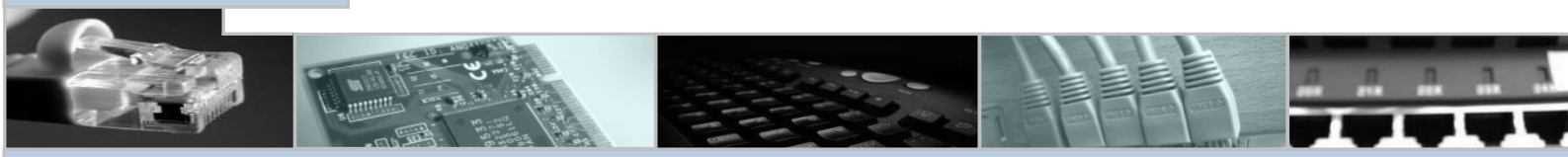
Finally, you will integrate your policy solution into **Pastry**. You show that your implementation works - either in a **testbed** or in a real deployment on **PlanetLab**. You also conduct some measurements and evaluate the security that your chosen policy offers to the users. Ideally, your software can be made available under the GPL afterwards.

Requirements

We will program in **Java**, so some programming skill and knowledge of this language is mandatory. Background in P2P networks is useful, but not a pre-requisite – we can teach you fairly quickly what you need to know. However, what we appreciate most in a candidate is **passion**: we want someone who enjoys doing his work with us. And for our part, we'll do everything we can to help you enjoy your work – promise.

Keywords

Spontaneous Networking, Network Security, P2P



Ralph Holz, Heiko Niedermayer
holz@net.in.tum.de, niedermayer@net.in.tum.de