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

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

Let's Talk About … IPSec, SSL, and plain IP

Motivation

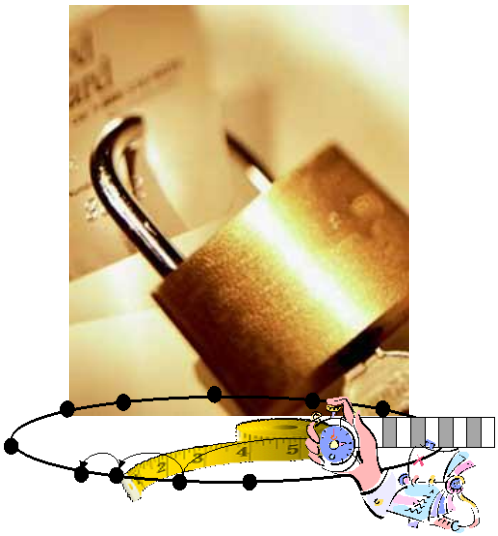
Why is the Internet not secure yet? Good question. The protocols are there, but they are rarely used. Is performance the reason or is it something else? Or approaching the question from a different angle: should performance be a reason to avoid secure protocols?

Our goal in this thesis is to acquire data by bandwidth measurements. Certainly, others have done this before. But we want to go further: we want to measure the throughput between a large number of hosts, and we want to do this over a longer period of time in order to obtain meaningful results. The protocols to be investigated are IPSec, SSL and plain IP for comparison. We will not use the common VPN setups but set up point-to-point connections. We are not interested in algorithmic delay or performance of cryptographic algorithms – we are interested in what happens on the network.
Building on the data we acquire, we hope to add facts to an ongoing discussion.

Your Task

Your task consists of the following steps.

1) Set up the tools to create IPSec and SSL point-to-point connections. You will have access to a number of rented servers plus all the hosts of our PlanetLab slice.
2) Set up the tools to do the actual measurements and store the data in a database. We will probably collect it nightly and store it here at TUM.
3) The measurements will also include determining the path that the packets take through the Internet, i.e. the Autonomous Systems.
4) Evaluate your data. Find out what the performance impact on the network layer is compared to using plain IP.

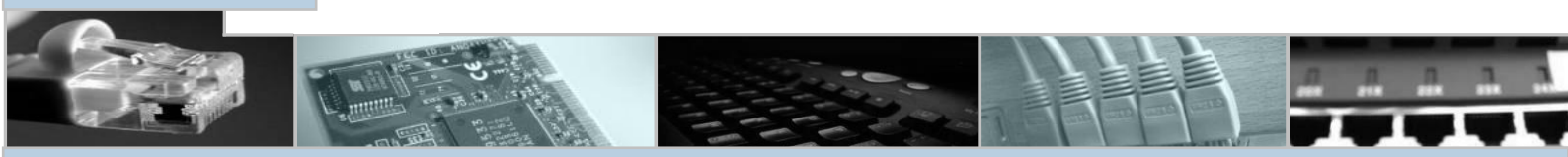


Requirements

Knowledge of network technologies is required, i.e. you should have attended relevant lectures on networks and network security. We will likely use a scripting language to create the tools – possibly Python, so you should not be afraid of getting your hands on code.

Keywords

Network Security, IPSec, SSL/TLS



Ralph Holz, Alexander Klein, Lothar Braun
{holz,klein,braun}@net.in.tum.de