P. Thiemann, M. Neubauer

Sommersemester 2005

Internetprogrammierung

http://proglang.informatik.uni-freiburg.de/teaching/inetprog/2005

Übungsblatt 2

Submission deadline: Monday, 2.5.2005

Exercise 1: The lecture has briefly introduced the Unix command line tool `nslookup`, which can query the DNS for information. Using this tool, perform an iterative DNS query manually to obtain the IP address of `www.darwinawards.cjb.net`. Start from the information about the root domain obtained from your local DNS server and follow the hierarchical structure by successively querying for the next authoritative nameserver (and its address) and then pointing `nslookup` to that server for the next query.

Exercise 2: The web site `http://www.med.uni-jena.de/wzi/internet2000/sld021.htm` contains the list of commands understood by the Unix `ftp` command line tool. Using this tool, connect to `ftp.informatik.uni-freiburg.de`, search for the directory of the AI group, and list the contents of this directory. (Be careful, all you do is logged.)

Exercise 3: Get together with at least two partners in this course and create a secure chat system using SSL connections.

- First, everyone has to produce a personal key, export it, and have the public certificates stored in the truststores of all partners.

- Implement a simple client and a server which connect via a SSL connection. The client accepts lines from the terminal and sends them to the server. The server displays each line as it is received with a suitable prefix (*e.g.*, **Client:. . .**). Vice versa, the operator of the server can type lines to the client which the client displays in the same way.

- The client displays the certificate of the server so that it is possible to verify its identity.