Hacettepe University

Department of Computer Engineering

BIL342 Programming Laboratory

Experiment V

Subject	**:**	Socket Programming on Linux
Advisors	**:**	Dr. Kayhan İMRE
		R.A. Kerem ERZURUMLU
Submission Date	**:**	17/04/2008
Design Report Deadline	**:**	23/04/2008
Deadline	**:**	06/05/2008
Programming Language	**:**	ANSI C

AIM

The aim of this experiment is to give students the ability to cope with the basic concepts of socket programming on Linux. Within this context you are asked to write two C programs: a server and a client.

BACKGROUND

Unix and all unix variants –`expect totally new Linux distributions which use MD5 passwords`- store encrypted passwords in `/etc/passwd` or `/etc/shadow` file. Unix systems use a oneway encryption method to prevent passwords being decrypted. The `crypt`[1] function does encryption. This function takes two arguments. The first one is the text to be encrypted. The second is the encryption key (called `salt`) which is a two character string.

The password entered by a user is first encrypted using the current encrypted passwords first two character as key. Then the encrypted string obtained is compared with the one stored in `/etc/passwd` or `/etc/shadow` file. If there is a match then the user is allowed to log on to the system.

Passwords can be 8 characters at most. If a password is longer than 8 characters, the characters exceeding the limit are ignored.

PROBLEM DESCRIPTION

It is normally impossible to decrypt someone's password without using `Brute-Force` techniques. Even with a machine with a dual CPU, a simple brute-force attack on a single password takes weeks. In this experiment, you are going to write a distributed password cracking tool. You are asked to write a server program which distributes a chunk of plain password possibilities (for an example 1000 passwords for client) to each of its connected clients in order to find out a valid password in parallel and in an acceptable amount of time. A client should explore all possibilities the encrypted password in the range assigned by the server. If a

[1] See manual page for details

client finds out the password, other clients will stop processing. If a client cracks the password in given range, it will demand a new section for cracking.

Hence the password possibilities are big enough, you are asked to check only 4, 5 and 6 digit passwords. You are also asked to compare the necessary amounts of time with a single, 2 and 3 client systems for 4 digit passwords.

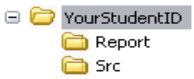
USER INTERFACE

Your server program will take an encrypted password and the server's port number as arguments. The IP address or the DNS name, the port number of the server and how many threads that client run will constitute the arguments of the clients.

NOTES

1. You are asked to follow announcements made to Courses.Bil342 newsgroup which is located at nntp://news.cs.hacettepe.edu.tr.
2. A copy of this sheet can be found at

   ftp://ftp.cs.hacettepe.edu.tr/pub/dersler/Bil3XX/Bil342/07-08/5
3. Your report and program must be submitted together.
4. You are asked to give a soft copy of your reports. Valid Soft-Copy formats are HTML and PDF.
5. You should submit your work and report with the following structure:



6. E-mail submissions are not accepted.
7. Late submissions will not be accepted.
8. Upon the submission, your experiments will be checked for common errors. Incomplete work may not be graded. Do not leave everything to the last minute.
9. Please send additional questions to Courses.Bil342 newsgroup.

Have a nice work!