Hacettepe University

Department of Computer Science and Engineering

BIL342 Programming Laboratory

Experiment I

Subject	**:**	Socket Programming with Linux
Advisors	**:**	Prof. Dr. Ali SAATÇİ
		R.A. Kerem ERZURUMLU
Submission Date	**:**	01/07/2002
Design Report Deadline	**:**	04/07/2002
Deadline	**:**	10/07/2002
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 distrubutions which uses MD5 passwords`- store encrypted passwords in `/etc/passwd` or `/etc/shadow` file. Unix systems use a oneway encrytion method to make passwords undecryptable. The `crypt`[1] function does encrytion. This function takes two argumants. The first one is the text to be encrypted. The second is the key –called `salt`- which is a two character string to encrypt the text with.

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

Passwords can be 8 characters at most. The rest of the characters are meaningless for .

PROBLEM DESCRIPTION

It is normally impossible to find out someone's password without using `Brute-Force` techniques. Even with a machine with dual CPU, a simple brute-force attack on a single password takes weeks. In this experiment, you will write a distributed password cracking tool. You are asked to write a server program which will distrubute plain password possibilities which is divided in to reasonable sections (for an example 1000 passwords for client) to its connected clients in order to find out concurrently a valid password in an acceptable amount of time. A client should try all possibilities in the range assigned by the server for the encrypted password. If a client finds out the password, other clients will stop processing. If client "crack" the password in given range, it will demand a new section for cracking.

[1] See manual page for details

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

USER INTERFACE

Your server program will take the 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 theads client will run will constitute the arguments of the clients.

NOTES

1. Soft copy of this paper can be found in ftp://ftp.cs.hacettepe.edu.tr/pub/dersler/bil342/2002-summer/
2. You are asked to give your `Makefile` with your program. Your `Makefile` should include "`server`", "`client`", "`clean`" and "`distclean`" programs.
3. Describe your communication flow-chart and designed protocol between server and clients in detail.
4. You are asked to follow announcements made to "bil342 discussion list". If you are not subscribed yet, please subscribe to it by sending an e-mail to:

   `majordomo@cs.hacettepe.edu.tr`

   with a message body of

   "`subscribe bil342`".
5. Your report and program must be submitted at the same time.
6. Your report must include your source codes.
7. Submission with e-mail is not accepted.
8. Late submissons will not be accepted.
9. Office hours will be held only on morning's. You can also send e-mails to kerem@linux.org.tr for your additional questions.

Good Luck