CALIFORNIA STATE SCIENCE FAIR
2003 PROJECT SUMMARY

Name(s)
David G. McIntosh

Project Number
S1219

Project Title
Scalable Encryption

Abstract

Objectives/Goals
Today, people can transfer information over high-speed Internet faster than ever. Unfortunately it also means that others can steal information faster than ever. A thief can steal thousands of credit card numbers in seconds. With the large number of businesses that perform transactions on the Internet, a portable, scalable, and fast program is needed to ensure privacy.

Methods/Materials
Development Machine was:
1.5 GHZ Athlon
20 GB Hard Drive
Red Hat Linux 8.0
Program uses:
make, gcc, GMU MP, bash, md5sum, sha1sum, dd, gawk, html, apache webserver for Linux, and perl

Results
My program, based on RSA encryption, generates secure keys, and then uses the two keys to encrypt and decrypt data, keeping it private. The strength of my program lies in its portability, speed, and scalability. The program uses the GNU MP Programming Library to manipulate numbers that are hundreds of digits long. Instead of writing my own library that was optimized or one computer, I used the free GNU MP which is optimized to work on computers ranging from Pentium's to Cray supercomputers. This means my program is extremely portable, and can run on almost any UNIX-based platform. The program uses several new approaches, including a simple prime checking method. Instead of using lengthy algorithms that guarantee a number is prime, my program checks the keys at the end of the process, to verify that they work.
Thirdly, my program is scalable. It can easily be configured to generate keys of any but number larger than 256. It can easily handle secure 1024 bit encryption in less than a second. It can be used for data authentication as well as data encryption

Conclusions/Discussion
My focus was on the core algorithm, making it portable, fast and scalable.

Summary Statement
The project contains five programs which allow users to protect their privacy.

Help Received
During the summer the Rocks NPACI team helped me become acquainted with linux.