CALIFORNIA STATE SCIENCE FAIR
2005 PROJECT SUMMARY

Name(s)
Ivan Sergeev

Project Number
S1219

Project Title
Encryption Algorithm Performance on an AVR Microcontroller

Abstract

Objectives/Goals
Secure data transfer is important task of the today communications. Benchmarking several reputable encryption algorithms on an embedded micro-controller was the primary goal of this project. Obtained data illustrate the implementation of the security algorithms on an embedded platform that can be used successfully by business corporations and end-users.

Methods/Materials
Atmel AVR ATMega128 micro-controller was chosen for this project due to its popularity and because it meets the hardware requirements for an encryption application. Using the SRAM interface on the chip, external memory was added to the project. In addition, I/O communication was provided by using the micro-controller built-in UART serial interface. A software driver was developed to operate a LCD attached to the micro-controller and used for debugging. Open source encryption algorithms from libtomcrypt were ported and optimized with AVR-GCC, a GCC tool-chain ported to the AVR platform. A program was developed on the personal computer to perform benchmarks and tests. All board design and assembly were done by author.

Results
Using a benchmarking program developed and compiled on the personal computer, the key and data was sent to the micro-controller. The micro-controller then confirmed the acceptance of the key, and gave the signal to begin the timing. The program kept time, and stopped when the signal of completion from the micro-controller was sent. I/O communication was done over a RS232 serial interface. Encryption and decryption tests consisted of the encryption or decryption operations in sets of rounds with the same data and key that was sent initially. The time of round execution was measured, compared and presented for each algorithm, along with the compiled program, and key and data size.

Conclusions/Discussion
This project demonstrates that it is feasible to implement security solutions on inexpensive embedded devices. Such implementation is less vulnerable compared to a software only implementation because the encryption program itself is written to a read-only memory space. The program execution speed indicates that today's encryption algorithms can be practically used in embedded devices which can be efficiently utilized by the corporations, the government or the end-users. Future work can show that these inexpensive embedded devices with implemented security can be used as a secure data exchange connections between computers.

Summary Statement
Security solutions can be more safely implemented in embedded devices versus in a pure software solution where the security software itself is vulnerable.

Help Received
Dr. Andrei Sergeev dedicated time to brainstorming the initial project idea and project review.