

Overview

In order to prevent data and identity theft in the event of computer theft, a cryptographic file system will be implemented on a standard PC running the Linux operating system. Upon boot-up, the decryption passphrase will be obtained from a microcontroller-based hardware module located in a separate room of the home or office, and connected via a serial RS-232 connection. As long as the connection to the hardware module remains intact, no user input is required to decrypt the hard drive during boot. This will allow for normal remote connections and remote reboots. If the computer is disconnected from the hardware module, the microcontroller will immediately erase its stored passphrase. Upon a subsequent boot, the user will be prompted to re-enter the decryption passphrase, which will decrypt the hard drive and restore it in the microcontroller.

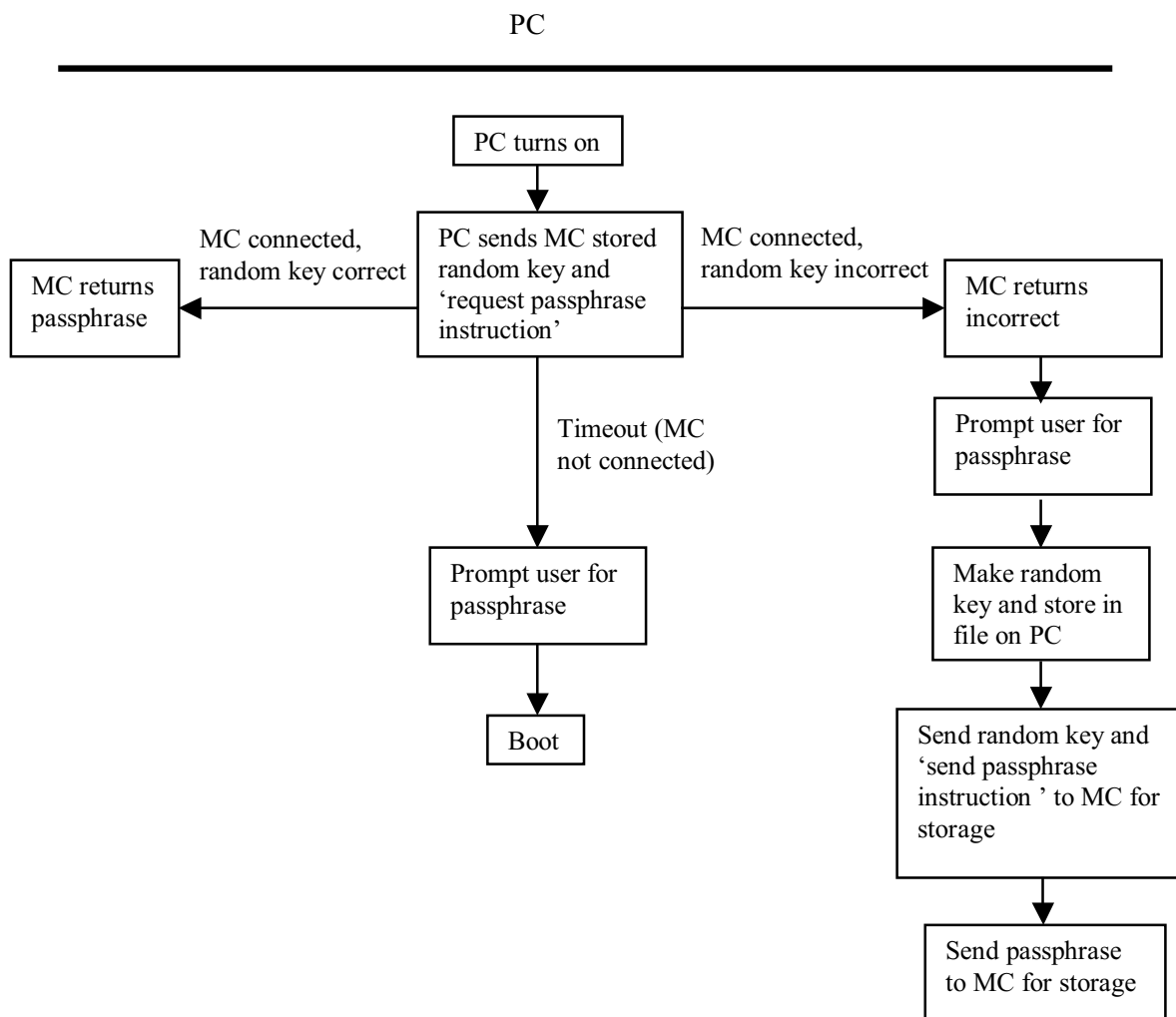
See the project proposal for more information.

Status of Main Project Tasks

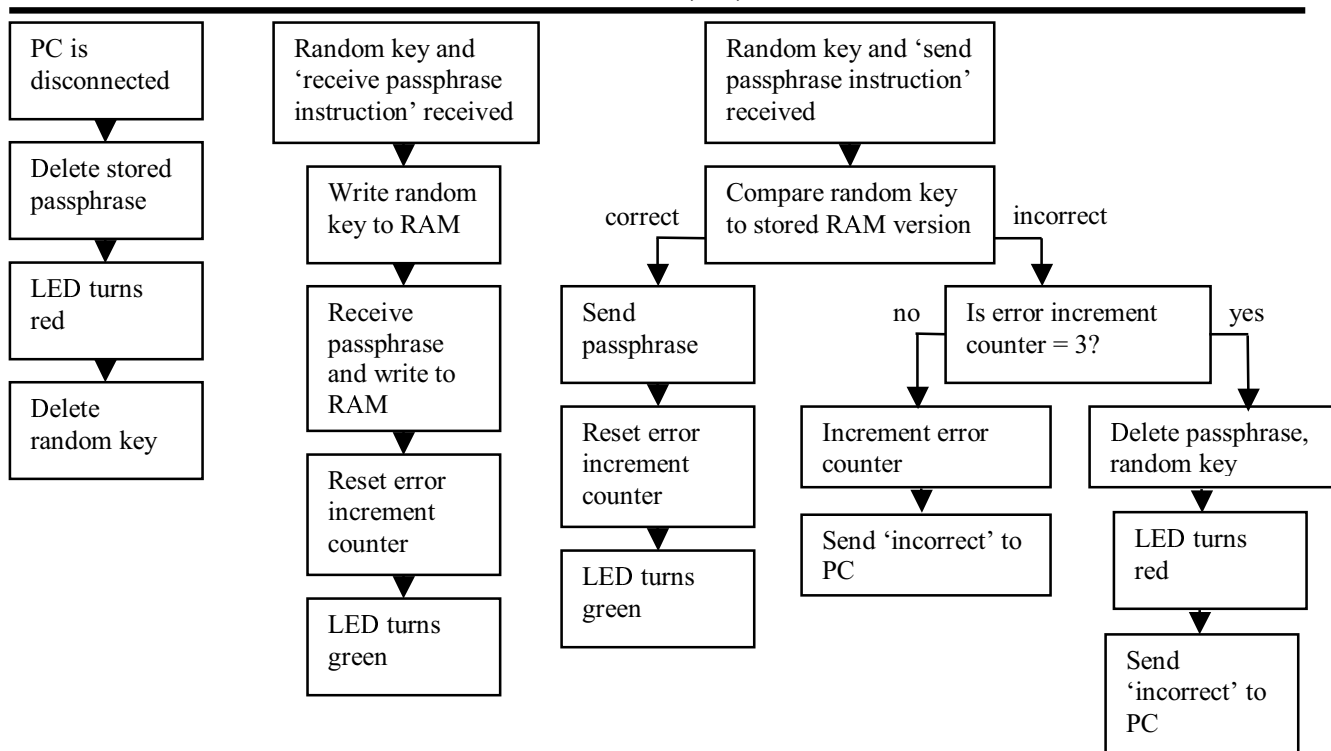
1. Design communication logic for PC and microcontroller communication.

The communication logic has been fully defined for both the PC and the microcontroller (MC) and is represented in the following flow charts. More detail will be provided in the final report.

Status: Completed



Microcontroller (MC)



2. Research appropriate microcontrollers, circuitry; purchase parts

The hardware design has been finalized. It consists of two indicator LEDs, an RS-232 transceiver (Maxim MAX218), a microcontroller (Texas Instruments MSP430F2011), and supporting circuitry. The circuit is powered by two AA batteries and will be designed to enter sleep-mode after a preset time in order to save power, enabling the batteries to power the system for longer time periods. The LEDs will indicate the system state, lighting green when the PC is connected and the microcontroller contains the passphrase, or red if the PC is disconnected and/or the microcontroller does not contain the passphrase. All necessary components were purchased during the week of Oct 9/06.

Status: Completed

3. Review cryptographic file systems and select system for implementation

Research into various cryptographic file systems was performed. A comparison of the various options will be included in the final report. LUKS (Linux Unified Key Setup) was selected due to its flexibility and compatibility between various Linux distributions. The test system will be implemented on Debian GNU/Linux 4.0 (etch).

Status: Completed

4. Learn about RS-232 communication in Linux; implement communication system on the PC

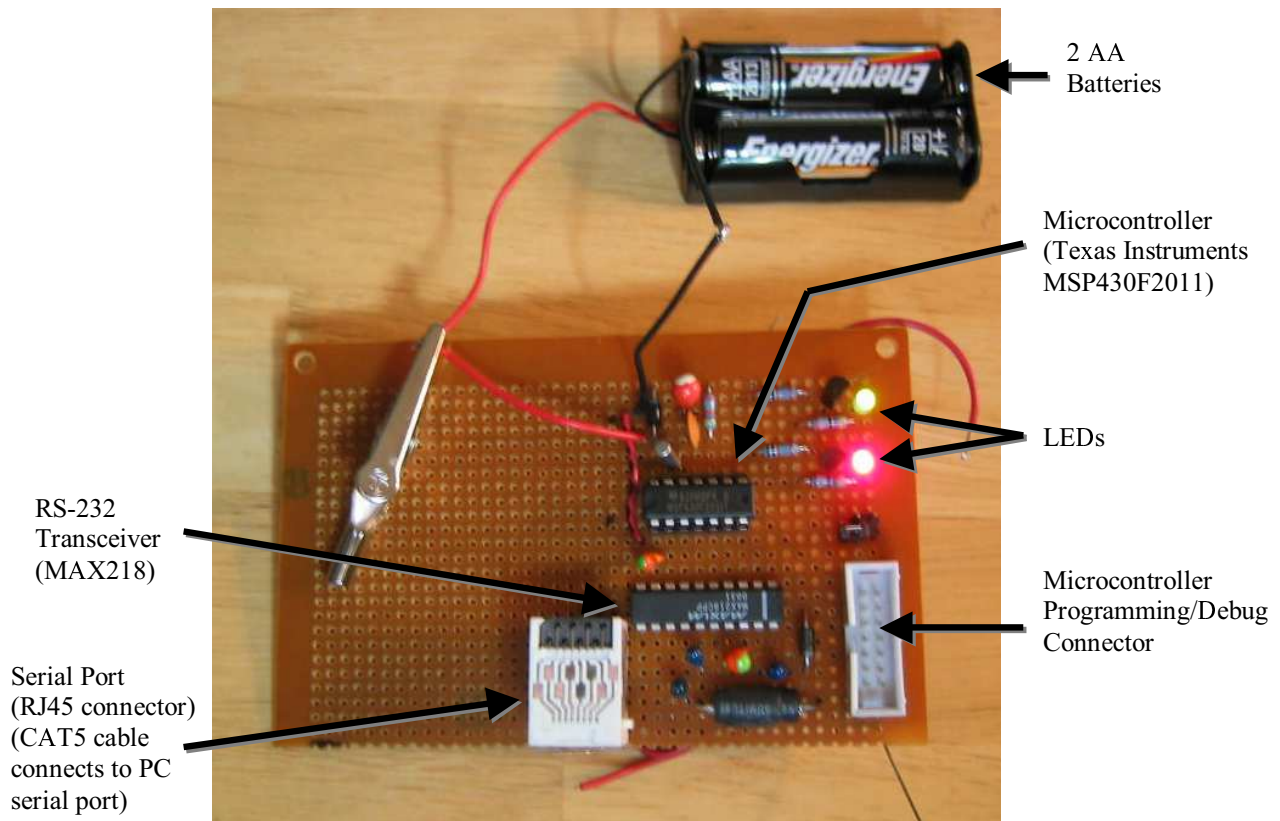
The RS-232 communication protocol has been reviewed and a simple program to setup the serial port on the PC has been implemented. This program will be tested after the microcontroller's RS-232 communication has been completed.

Status: In progress

5. Implement and test microcontroller circuitry on prototype board

The microcontroller circuitry has been fully implemented on the prototype board. The LED circuitry is operational, and the microcontroller can be programmed and debugged with programming interface. RS-232 circuitry is implemented but not yet tested. See picture below.

Status: In progress



6. Microcontroller programming

The development environment to program the microcontroller has been setup. The microcontroller's user's guide and manual have been reviewed. Initial work has begun on programming the microcontroller to utilize the RS-232 interface for transmitting and receiving bits via the serial port. It has only been partially implemented in the microcontroller development software simulation environment and has not yet been tested in the circuit. A microcontroller program has been developed and implemented to turn the LEDs on and off. The RS-232 communication protocol will be tested using a serial port communication program in Linux (gtkterm).

Status: In progress

7. Design boot-up script and user interface

This task involves developing the software to implement the communication logic described in the above flow chart for the PC. It has not yet been implemented.

Status: Pending

Problems Encountered

The main problem encountered was finding a technique to verify that the serial cable was attached to the PC when the PC was powered off. Though research into PC serial port hardware and experimentation with a multimeter, it was observed that the PC passively pulls several pins to ground regardless of the PC powered state. A weaker pull-up resistor in the microcontroller circuit will bring the signal to logic high whenever the PC is disconnected, allowing the microcontroller to detect this and immediately erase the stored passphrase.