

# Securing Data in the Event of Computer Theft

Sept 26, 2006

ECE1776 Project Proposal

Renee Warriner

## Problem:

Computer theft from homes and businesses significantly increases the risk of identity theft and release of confidential information by facilitating access to hard drive data. Thieves may only desire to sell the hardware components for profit, however hard drives can be sold on the black market for data harvesting. Hard drive contents are often protected with only a password.

## Background:

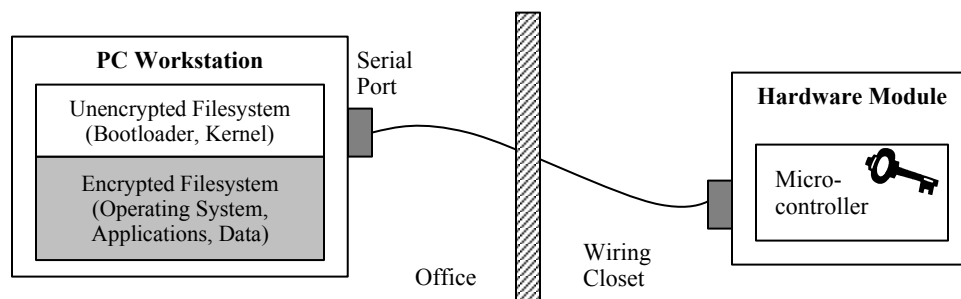
In 2006, two major incidents of computer theft have been reported by the media to have greatly increased the risk of theft to an incredible number of potential victims. In June, the insurance company, AIG, was robbed of a computer server containing personal electronic information for 930 000 clients [1]. Personal data stored on the server consisted of client names, social security numbers, and medical records. The server was only password protected. Fidelity Investments reported in March [2] that a laptop was stolen containing personal retirement portfolio information for 196 000 clients. Although Fidelity agreed to reimburse accountholders in the event of stolen funds, they advised their clients to monitor account activity and personal credit reports for the next 12 to 24 months. The US Federal Trade Commission has also reported that approximately 10 million Americans have their personal information stolen and used per year at an annual cost of \$5 billion to consumers and \$48 billion to businesses [3]. Hard drive manufacturer, Western Digital, has reported on their support webpage that hard drive theft is a lucrative target for the black market for both 'sophisticated and unsophisticated thieves' [4].

## Objectives:

1. Design a cryptographic system for protecting hard drive contents should the workstation be stolen.
2. The implemented system would allow for remote user access and remote reboot of the workstation.
3. The encrypted system will be transparent to the user. The user will not be required to enter a decryption passphrase if the computer has not been moved from its normal environment.
4. If the workstation is moved, the user must enter the passphrase to decrypt the hard drive.

## Solution:

The proposed solution involves both a hardware and software implementation, as shown in the figure below. The system will be designed to run on a Linux workstation using a cryptographic filesystem. Upon boot-up, the decryption key will be obtained from a microcontroller-based hardware module located in a separate room of the home or office (e.g. an ethernet wiring closet), 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 (e.g. SSH, VNC), as well as remote reboots when necessary. If the computer is disconnected from the hardware module, the microcontroller will immediately erase its stored key. Upon a subsequent boot, the user will be prompted to reenter the decryption passphrase, which will decrypt the hard drive and restore the key in the microcontroller. We assume the thief is primarily interested in the computer hardware and does not have the time or knowledge required to obtain the decryption key while stealing the workstation.



# Securing Data in the Event of Computer Theft

Sept 26, 2006

ECE1776 Project Proposal

Renee Warriner

## Project Milestones:

	Task	Date Complete
1	Research Linux cryptographic filesystems; test implementation on spare laptop	Sep 29
2	Research appropriate microcontrollers, circuitry; purchase parts	Sep 29
3	Learn about the Linux boot process	Oct 6
4	Learn about RS-232 communication in Linux; implement test system	Oct 20
5	Design script to prompt user for passphrase	Oct 20
6	Midterm presentation	Oct 24
7	Implement and test microcontroller circuitry on prototype board	Nov 3
8	Design script to request key from microcontroller; microcontroller programming	Nov 17
9	Final presentation	Nov 28

## Related Work:

This project proposal has several advantages over existing systems. The most basic implementation consists of using a cryptographic filesystem requiring a local user to enter the passphrase upon boot [5]. Another technique uses storage of the decryption key on a USB drive carried by the user [6]. Both of these systems make it difficult to access and reboot the workstation remotely. Also, if a USB drive was used in the proposed solution, its distance from the workstation would be limited to 5m [7]. Serial RS-232 connections however, are capable of transmitting signals 50m on Cat-5 cable. Storing the decryption key in a room far away from the workstation provides additional security. Finally, the feature of automatically erasing the decryption key on the microcontroller upon serial disconnection prevents the thief from returning to the site to obtain the decryption key.

## References:

[1] Popkin J., Sandler T., NBC Investigative Unit. *Stolen computer server sparks ID theft fears*. NBC News: June 14, 2006. <http://www.msnbc.msn.com/id/13327187/>

[2] *Stolen Fidelity computer raises privacy fears*. Associated Press: March 23 2006. <http://www.msnbc.msn.com/id/11974062/>

[3] Zeller T. *Black market in stolen credit card data thrives on internet*. The New York Times: June 21, 2005. <http://www.nytimes.com/2005/06/21/technology/21data.html?ei=5088&en=c06809aa240685f8&ex=1277006400>

[4] *Hard drive theft alert*. Western Digital Service and Support: September 24, 2006 (access date). <http://support.wdc.com/warranty/stolen.asp>

[5] Devine, C. *Encrypted root filesystem HOWTO. Rev 1.3*. The Linux Documentation Project: March 13, 2005. <http://tldp.org/HOWTO/Encrypted-Root-Filesystem-HOWTO/>

[6] Petullo M. *Encrypt your root filesystem*. Linux Journal. 129, Dec 2004. <http://www.linuxjournal.com/article/7743>

[7] *USB info: frequently asked questions*. USB Implementers Forum Inc.: September 24, 2006 (access date). <http://www.usb.org/about/faq/ans5/>