

Sabbatical Report

Jean Mayo

Department of Computer Science

This report describes the activities and results of my sabbatical leave during the 2006 Fall semester. The purpose of the sabbatical was to expand my expertise in distributed computing to incorporate security and privacy considerations, ultimately leading to preliminary results sufficient to justify a proposal for external funding. The work resulted in an operating system implementation for translucent redirection of file system access requests and submission of a paper, based on results developed previously with N. Bansod, A. Malgi, and B. Choi, titled "MuON: Epidemic based Mutual Anonymity" to the IEEE Transactions on Parallel and Distributed Systems. The implementation has laid the groundwork for a proposal on a firewall model for filesystem security.

Redirecting my research efforts toward system security required extensive reading, and this occupied a large portion of the sabbatical leave time. This reading led to the implementation described below. Additionally, a second, related topic and associated implementation are being researched and evaluated by one of my doctoral students.

Traditional UNIX file system access controls are not adequate to meet emerging system security demands. A primary problem is that system administrators need to restrict access for a particular process P to only those files P must access to perform its function. The UNIX group mechanism allows access to be restricted to group members. Traditionally, many system daemons ran in the *root* group, and comprised a set of *trusted* processes. Hence, processes were not restricted to only those files to which access was required, but to the set of files required by *any* trusted process. Compromise of *any* of these system daemons then allows access to any file in this set. If a group is formed for each of these daemons, it is either unwieldy or impossible to define the required group structure.

The approach identified during the sabbatical is to apply a firewall access model to the file system. Firewalls are common for providing network security and system administrators are familiar with their use. Further, firewall theory has received significant attention from the research community. This theory facilitates correct and straightforward development of firewall policies. We believe that applying this model and theory to file system access will provide an intuitive mechanism for administrators to control file system access and that much of the network firewall theory can be applied to file systems with relatively small modification.

My first step in pursuing this idea was to implement essentially transparent redirection of file system access requests. The Linux kernel was modified to allow a system administrator to load a set of redirection rules which allow requests for one file to be redirected to another file based on a number of attributes. These attributes include the traditional userid and group, but also include time of day and the binary from which the requesting process was created. The code infrastructure and model allow virtually any identifiable attribute to be used to filter requests. This provides a powerful and fine-grained access control mechanism. This initial work is being prepared for publication. Upon successful publication of initial work, we will seek funding for developing the full filesystem firewall.

A secondary goal of the sabbatical was to gain expertise to offer our students a kernel programming seminar during the summer. This goal was met. I plan to offer the seminar in a future summer. Summer 2007 will be spent preparing publications and a proposal based on the file system work.