DEVELOPING AN AUTHORIZATION TOOL

FOR LINUX-NTFS MOUNTER

A Mini-Thesis

Presented to

The Faculty of the Computer Science Division

Ateneo de Davao University

In Partial Fulfillment

of the Requirements for the Degree

Bachelor of Science major in Computer Science

by

Stan Mallonga Baylon Jr

John Paul Cua Chen

Ronald Edgar Viduya Rojas

March 2002

TABLE OF CONTENTS

CHAPTER IV

ABSTRACT

Current Linux to NTFS mounters discards all permission rights made from the NT operating system, the security mechanism of the file system is bypassed. This research focuses on developing a secure mounting utility by using Linux 7.1 Operating System in mounting to Windows NT 4.1. This authorization tool is beneficial to OS users especially to LINUX-NT users for it provides access authentication to files. The steps taken are systematical installations, analysis of data gathered, implementation of the tool proposed and covering remote access for the tool developed.

Many mounters found these days are still without authentication, network areas are the most vulnerable targets for file interventions. The tool developed by the proponents provides NTFS security and permission; security parity bits are basis for the tool produced for viewing permissions. The tool uses Linux account authorization which makes it a bit limited. The proponents recommend that writing in NT partitions be developed and better group permissions be developed.

CHAPTER I

INTRODUCTION

1.1 Background of the Study

To provide an efficient, convenient and secure authorization to the disk, operating systems impose file systems to allow the data stored on disk to be retrieved by using group membership. Those group memberships are granted permissions to access different resources like files and directories and things alike. By using group memberships, users can centrally manage the access permissions or the access rights that users can attain. This task involves the definition of a file and its attributes, operations allowed on a certain file, and the directory structure for organizing the files. Algorithms and data structures must be created to map the logical file system onto the physical secondary-storage device.

Just as a file must be opened before it is used, a file system must be mounted before it can be available for processing on the system. The mount procedure is straightforward. The operating system is given the name of the device and the location within the file structure at which to attach the file system, the attachment location is called the mount point.

Currently there are numerous operating systems available to users. Most of the operating systems have set its own file system in which has its own pros and cons. Choosing of the file system to use on a computer relies heavily on the operating system to be used to run the said machine. For example, the Windows NT 4.0 uses New Technology File System (NTFS) while Linux supports Extended File System (EXT2).

1.2 Statement of the Problem

Since the current mounter discards all permission rights made from the NT operating system, the security mechanism of the file system is bypassed.

The main problem to be tackled on this research is in developing a secure mounting utility for Linux.

Specifically the proponents of this research would like to address:

- How does Windows NT 4.0 implement its security architecture?
- How does Linux implement the security of its files?
- How can we implement the proposed security system for the Windows NT partition?

1.3 Objectives of the Study

The general objective of this study is to provide NTFS support for Linux. Currently, Linux has read-only support for NTFS without regarding access permissions.

Specifically, the objectives of this study are:

- To provide NTFS support for authentication/authorization
- To be able to access files while maintaining security
- To provide secured access to the NTFS partition from a remote terminal

1.4 Scope and Limitation of the Study

The study will be limited to a mountable Linux kernel for NTFS authentication only. Other operations are beyond the scope of this study.

The study will also be limited to Windows NT version 4.0. NTFS 5.0 has just been released and the file system is used in new operating systems of Microsoft such as Windows 2000 and Windows XP. The said version offers an embedded encrypting technology on the file system as part of its security mechanism. The inclusion of a support for NTFS 5.0 may increase the complexity of the study and may not fit the allocated time frame.

Linux is an open sourced operating system and a lot of companies like Red Hat and Mandrake offer their own improved version. The proponents would like to limit this study to the Red Hat's Linux 7.1 for now, since the software is easily available.

1.5 Significance of the Study

One of the important characteristic of the New Technology File System (NTFS) is the capability to provide secure access to files. Unfortunately, the current Linux NTFS driver, which provides the ability to mount an NTFS partition, bypasses these security measures by ignoring the permission rights made in Windows NT.

The study could also be used as a migration utility for system administrators shifting from a Window's Network from a Linux based one. The system administrator need not reformat all their NTFS partitions into Ext2. Instead, the system administrators could just mount the partition and apply the access permission needed.

The proposed authorization tool to be developed would be of beneficial to OS users especially to LINUX-NT users for it can keep provides access authentication to files.