Contact Information

Publications@ipcg.com

ipCapital Group, Inc.
400 Cornerstone Drive, Suite 325
Williston, VT 05495
United States of America
(802) 872-3200 x214

Title of the Invention

File Lock System

Description of the Invention

Rather than rely on 3rd party software to provide data security, the Operating System contains a Security Subsystem that manages access to any Locked File in the system. Locked Files contain author-defined access permissions for a specific set of usernames and passwords. On accessing a Locked File, the Operating System enters a Secure Mode, which prevents data from being digitally copied or broadcasted over a public output device.

Problem/Opportunity

Currently, security measures for ensuring the safety of digitally stored sensitive information can only be provided through the use of encryption software. However, once a user obtains the file and successfully decrypts its contents, there are no safeguards against what the user can do with the information contained within; it could be copied, broadcasted over the internet, or even played publicly over speakers, any of which compromise the security of the data. Current systems also fail to provide a means to encrypt only the sensitive portions of documents, such as an audio file attached to a text document.

Detailed Description of the Invention

A system is needed where, rather than having encryption handled by individual programs, all file security measures are handled within the Operating System of the User Machine. In this system, the files themselves are locked and contain all user access privileges. In this way, an author can provide different users of a given file with different levels of access privileges, while having the file still accessible by any of these pre-determined users on any machine. It would also need to prevent the distribution of sensitive information. For this, the locking mechanism ensures the security of data, despite the potential existence of multiple copies of the Locked File; only those with certain privileges would be able to access the data. To prevent compromising the security of data over a public output device, such as speakers, a projector, or even a printer, the

Operating System can use the access privileges defined for a user to modify access to such output devices.

The structure of the system is provided in Figure 1:

1.1 User Machine – a processing device, running an operating system, with a user interface, internet connection, and internal storage

1.2 OS – The Operating System (i.e. Linux) running on the user machine, responsible for handling the user interface and all hardware or software operations on the User Machine

1.3 Security Subsystem – A module of the Operating System, which contains a File Registry, Encryption Program, Monitor Program, and a set of System Calls. The Security Subsystem is responsible for managing access to Locked Files

1.4 File Registry – component of the Security Subsystem, keeps track of all Locked Files and their locations in Local Storage, and their access permissions for each individual user/password combination

1.5 System Calls – A set of function calls provided by the Security Subsystem to allow 3rd Party Software Applications to interface with Locked Files

1.6 Encryption Program – Program responsible for encrypting or decrypting parts of Locked Files.

1.7 Monitor Program – Program responsible for "watching" the local file system. Prevents sensitive information from being copied from Locked Files, and identifies Locked Files downloaded/imported from External Sources

1.8 Local Storage – Where all data on the User Machine is stored, composed of a Hard Disk Drive, Magnetic Storage, Solid State Drive, or other Storage Device.

1.9 External File Source – Any potential external source of data, such as an Internet Directory, Flash Drive, Removable Hard Drive, etc that may be accessed from the User Machine

Once the user has provided the username and password for the Locked File, files located on a user's machine can be directly accessed on their machine. When the Locked File is opened, the Monitor Program switches the OS into secure mode. While operating in secure mode, the Monitor Program monitors the file system and prevents any information from being saved to storage or memory, except the already opened Locked File. At the same time, secure mode prevents any use of public output devices, such as sound cards, removable storage devices, or additional displays such as projectors. If the user attempts to save data while the Locked File is open, the Monitor Program will signal the OS to flag the user with a dialog box, explaining that the file can not be saved at this time, and to close all Locked Files before trying again. When the Locked File is closed, the security subsystem locks and encrypts the Locked File once again to prevent any unwanted access, before switching the OS out of secure mode. Once out of secure mode, the system is once again able to save and copy files. Since the Locked Files are secure, copying them or moving them between storage systems or devices does not compromise security; any actual access to the Locked File must still be done through the Operating System.

Unlike locally created Locked Files, externally created Locked Files can not be directly accessed, but rather must first be moved or copied to the local file system. When a Locked File is added to the file system – either copied from an external storage device (such as a hard drive or flash drive) or is downloaded from the Internet - the Monitor Program can recognize it as a Locked File by checking a data switch at the start of the file (e.g. if it is turned "on", the file is locked). If the file is a Locked File, it then adds the access information contained in the Locked File to the File Registry. To access the sensitive information contained in the Locked File, the user must first provide a valid username and password. The Security Subsystem in the OS uses this information, and checks it against the File Registry and the information in the Locked File itself to confirm the user's access privileges. By checking user credentials against both security records, it prevents a situation where a Locked File may have been tampered with. If the user has sufficient privileges, the Security Subsystem switches the OS into secure mode, and proceeds to operate in the same way as above.

Figure 2 illustrates the operation of the Security Subsystem:

2.1 The user requests the Operating System to access to a Locked File.

2.2 The Monitor Program notices an attempt to access a Locked File, and checks to see if the Locked File is stored locally. If the Locked File is stored on the User Machine, The system proceeds directly to step 2.5

2.3 If the Locked File is not stored on the User Machine (e.g. externally created files, files located on removable storage) the Operating System copies the Locked File to local storage.

2.4 The Monitor Program recognizes a Locked File has been added to the local File System, and proceeds to add it to the File Registry.

2.5 The Security Subsystem prompts the user for their access information for the Locked File using a dialog box.

2.6 The Security Subsystem checks the access information against the Locked File.

2.7 If the user's access information is incorrect, proceed to step 2.8, otherwise proceed to step 2.9

2.8 The Locked File is not opened, and the user is notified of invalid access information through a dialog box.

2.9 If the user's access information is valid, then the Security Subsystem switches the Operating System into secure mode, preventing any file access outside of the Locked File. The Operating System also prevents any access to external output devices, such as sound or video cards.

2.10 The Locked File is accessed by the Security Subsystem using the physical memory address provided in the File Registry. The Unlocked File can now be opened in the appropriate program, with read and write privileges based on the User's access information.

2.11 When the Unlocked File is closed, the Security Subsystem re-locks the file, encrypts it, and returns the Operating System to normal mode.

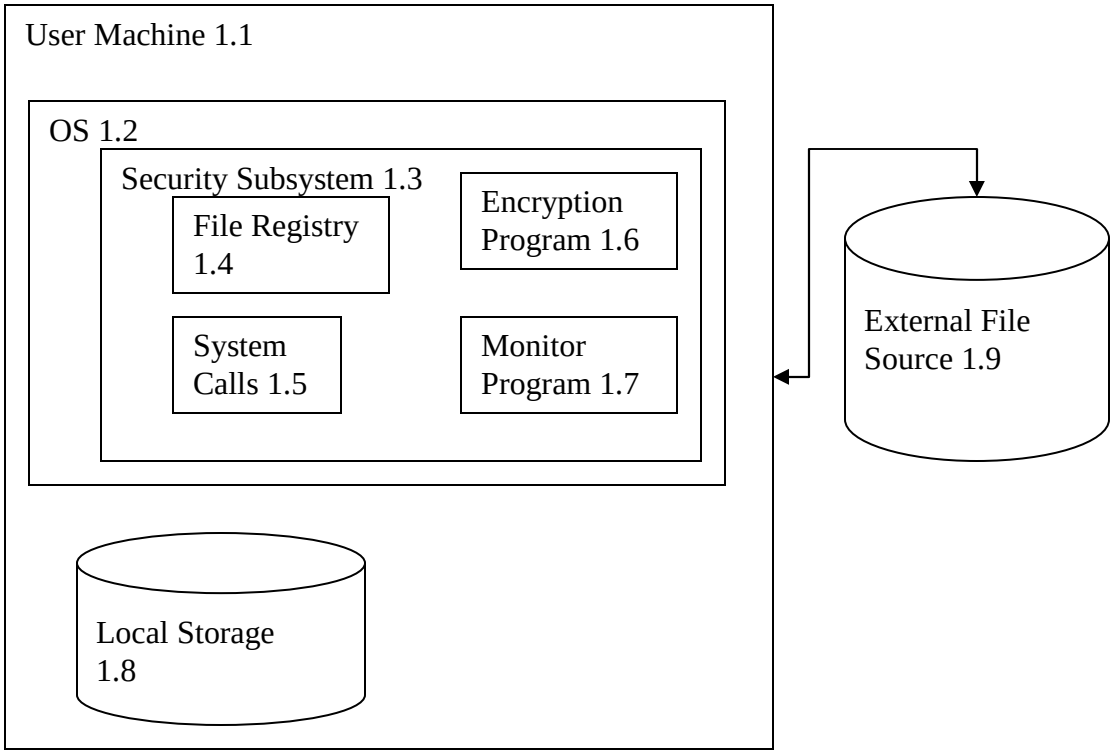

Figure 1: Structural Diagram of the File Lock System

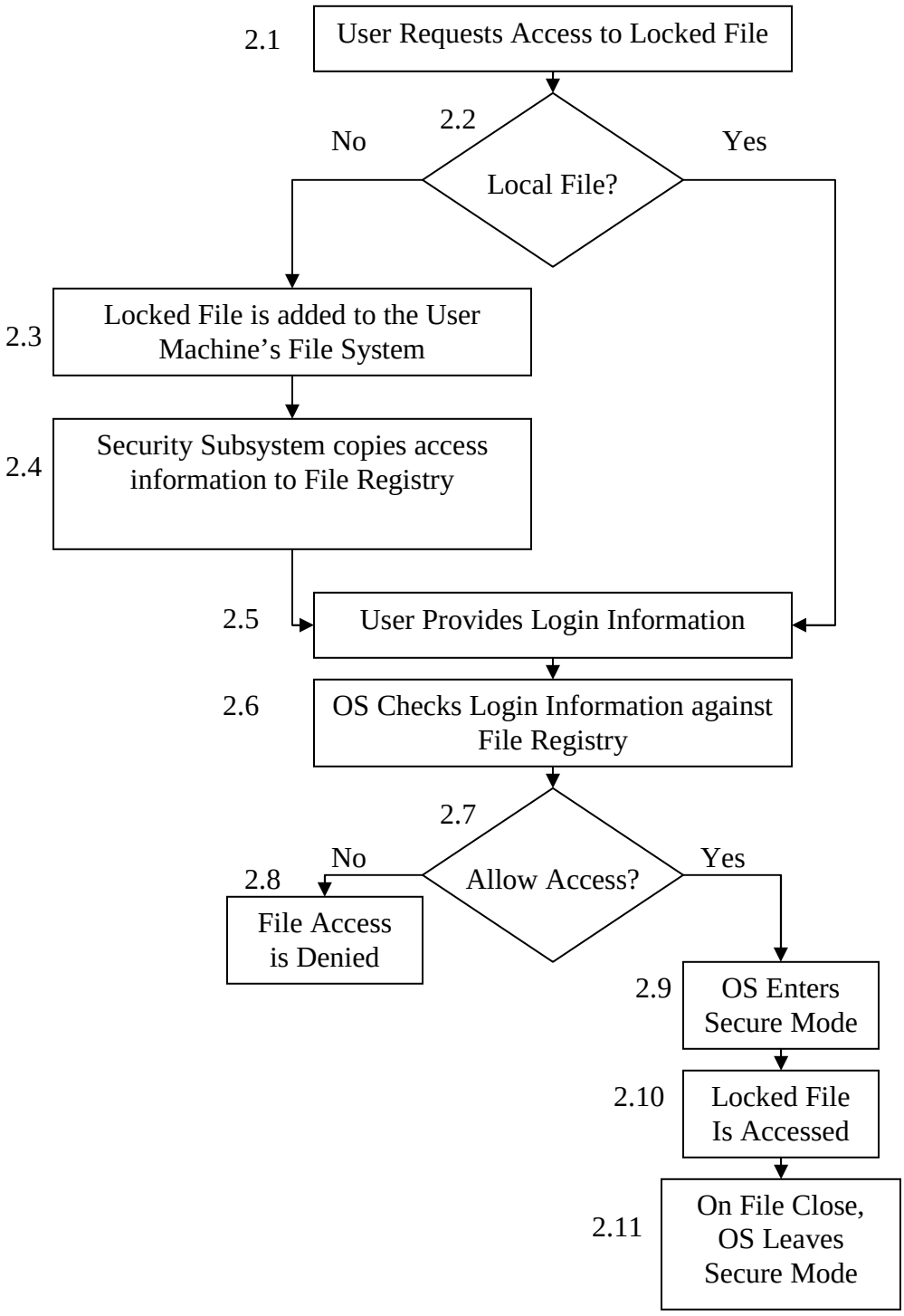

Figure 2: Flowchart showing File Lock System Operation