12-16-99

A

Imation Corp.
PO Box 64898
St. Paul, Minnesota 55164-0898
651/704-5516

PATENT

Docket No
10179US01

Transmittal of Patent Application - Rule 1.53(b)

Assistant Commissioner for Patents
Box: Patent Application
Washington, D.C. 20231

Inventor(s): **Jeffrey A. Morgan, C. Thomas Jennings, Larold L. Olson, Luiz S. Pires, and Daniel P. Stubbs**

Title: ***COMPUTING ENVIRONMENT HAVING SECURE STORAGE DEVICE***

☒ Enclosed is the above-mentioned new patent application. It includes 5 sheets of ***Informal*** drawings.

☒ Enclosed is an executed declaration or oath.

☒ Enclosed are an application assignment to Imation Corp. and a completed Assignment Recordation Cover Sheet.

☐ Enclosed is _____.

☒ The fee for filing the application is computed as follows:

Claims As Filed					
(1) For	(2) Number Filed		(3) Number Extra	(4) Rate	(5) Basic Fee $760.
Total Claims	67	-20 =	47	x $18.	846.
Independent Claims	11	-3 =	8	x $78.	624.
Additional fee for filing one or more multiple dependent claims				$260.	0
			Total amount due →		$2230.

☒ Please charge to Deposit Account O9-0069 any fees under 37 CFR 1.16 and 1.17 which may be required to file and during the entire pendency of this application. This authorization includes the fee for any extension of time under 37 CFR 1.136(a) that may be necessary. To the extent any such extension should become necessary it is hereby requested. A duplicate for fee processing is enclosed.

☒ Enclosed is a return receipt postcard

Registration Number	Telephone Number
35,814	651/704-3604
Date 12/15/99	

Signature: Eric Levinson
Print Name: Eric D. Levinson

Certificate of Express Mailing

Pursuant to 37 CFR 1.10 I certify that this application is being deposited on the date indicated below with the United States Postal Service "Express Mail Post Office to Addressee" service addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231.

Express Mail Mailing Label No.	Signature of Person Mailing Application
EL328557004US	Printed Name of Person Mailing Application: Susan J. Daley
Date of Deposit: December 15, 1999	

Form q \e\oipcfrms\App Trans-1-53(b) Original doc Rev 12/01/97

COMPUTING ENVIRONMENT HAVING SECURE STORAGE DEVICE

Technical Field

This invention relates generally to the field of data storage devices, and more particularly to a computer that automatically operates in a full-access data storage mode when the computer senses the use of a secure storage device.

Background

There are many challenges to creating a highly secure computing environment including preventing eavesdroppers from accessing private communications, preventing vandals from tampering with information while in transit from sender to receiver, authenticating users logging into a network, verifying a network server is indeed the server it professes to be and safeguarding confidential documents from unauthorized individuals.

One of the greatest challenges, however, is preventing the authorized user from using sensitive data in an unauthorized manner. For example, with conventional security measures it is very difficult to prevent an authorized user from appropriating sensitive data by simply copying the sensitive data to a removable storage device such as floppy diskette. For these reasons, and for other reasons stated below which will become apparent to those skilled in the art upon reading and understanding the present specification, there is a need in the art for an improved mechanism for preventing the appropriation of sensitive data.

Summary

According to the invention, the above-mentioned problems are addressed by a secure computing environment in which a computer automatically operates in a secure "full-access" data storage mode when the computer detects the presence of a

secure removable storage device. If the computer senses a non-secure removable storage device then the computer automatically operates in a "restricted-access" mode.

In the secure full-access mode, storage management software uses a cryptographic key to encrypt and decrypt the data stream between the computer and the removable storage device. Depending upon the selected security level, the cryptographic key is generated by a combination of the following: (1) device-specific information derived of the removable storage device, (2) manufacturing information that has been etched onto the storage device, (3) drive-specific information, such as drive calibration parameters, retrieved from the storage drive, and (4) user-specific information such as a password or biometric information such as input received from a fingerprint scan or retina scan.

In addition, the present invention facilitates the use of a secure storage device as a secure "access card" by which the user gains access to sensitive data of the organization. More specifically, the user is permitted to access sensitive data stored on other local storage devices, or on remote computers within the organization, only when the computer is operating in full-access data storage mode.

In the restricted-access mode, however, the computer operates the storage drive as a read-only drive such that the user can read data from the removable storage device but cannot write data to the drive. Alternatively, the user can access only non-sensitive data within the organization and may be allowed to write the non-sensitive data to the removable storage device in an unencrypted format.

Brief Description of the Drawings

Figure 1 is a block diagram of a computer that automatically operates in a secure data storage mode when a secure storage device is detected;

Figure 2 is a flow chart illustrating one embodiment of a method by which a software application executing on the computer of Figure 1 determines whether to configure the computer to operate in full-access mode on restricted-access mode;

Figures 3A and 3B illustrate one embodiment in which the storage device of Figure 1 is an LS-120 SuperDisk™ diskette from Imation Corporation; and

Figure 4 illustrates a layout for storing data on a disc-shaped magnetic medium within the Imation SuperDisk.

Detailed Description

The following sections describe in detail how the present invention addresses the problems outlined above. In the following detailed description, references are made to the accompanying drawings that illustrate specific embodiments in which the invention may be practiced.

System Level Overview

Figure 1 illustrates a block diagram of a computer 100 that automatically operates in a secure data storage mode when the computer 100 senses that storage device 151 is a secure storage device. As shown in Figure 1, the computer 100 includes a processor 112 that in one embodiment belongs to the PENTIUM® family of microprocessors manufactured by the Intel Corporation of Santa Clara, California. However, it should be understood that the invention can be implemented on computers based upon other microprocessors, such as the MIPS® family of microprocessors from the Silicon Graphics Corporation, the POWERPC® family of microprocessors from both the Motorola Corporation and the IBM Corporation, the PRECISION ARCHITECTURE® family of microprocessors from the Hewlett-Packard Company, the SPARC® family of microprocessors from the Sun Microsystems Corporation, or the ALPHA® family of microprocessors from the Compaq Computer Corporation. Computer 100 represents any server, personal computer, laptop or even a battery-powered, pocket-sized, mobile computer known as a hand-held PC.

Computer 100 includes system memory 113 (including read only memory (ROM) 114 and random access memory (RAM) 115), which is connected to the

processor 112 by a system data/address bus 116. ROM 114 represents any device that is primarily read-only including electrically erasable programmable read-only memory (EEPROM), flash memory, etc. RAM 115 represents any random access memory such as Synchronous Dynamic Random Access Memory.

Within the computer 100, input/output bus 118 is connected to the data/address bus 116 via bus controller 119. In one embodiment, input/output bus 118 is implemented as a standard Peripheral Component Interconnect (PCI) bus. The bus controller 119 examines all signals from the processor 112 to route the signals to the appropriate bus. Signals between the processor 112 and the system memory 113 are merely passed through the bus controller 119. However, signals from the processor 112 intended for devices other than system memory 113 are routed onto the input/output bus 118. Video display 124 or other kind of display is connected to the input/output bus 118 via a video adapter 125.

Various storage drives are connected to the input/output bus 118 including hard disk drive 120 and one or more removable media drives 121 that are used to access one or more removable storage devices 151. Each storage device 151 represents a removable device having a storage medium for holding digital information such as a floppy diskette, a magneto-optical storage device, an optical disk, a SuperDisk™ diskette, a Zip™ disk, a Jazz™ disk, a tape cartridge, etc. Each removable media drive 121 represents a device suitable for servicing access requests for storage device 151 such as a floppy drive, a magneto-optical drive, a CD-ROM drive, a SuperDisk™ drive, a removable-cartridge drive such as a Zip™ drive, or even a tape drive.

A user enters commands and information into the computer 100 by using a keyboard 40 and/or pointing device, such as a mouse 42, which are connected to bus 118 via input/output ports 128. Other types of pointing devices (not shown in Figure 1) include track pads, track balls, joy sticks, data gloves, head trackers, and other devices suitable for positioning a cursor on the video display 124.

Software applications 136 and data are typically stored via one of the storage devices, which may include the hard disk 120 or storage devices 151, and are copied to

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.