US005633934A

United States Patent [19]

Hember

[11] Patent Number: 5,633,934

[45] Date of Patent: May 27, 1997

[54] **LOCAL AREA NEWORK ENCRYPTION DECRYPTION SYSTEM**

[76] Inventor: **John T. Hember**, 412 Pickford Drive, Kanata, Ontario, Canada

[21] Appl. No.: **670,438**

[22] Filed: **Jun. 26, 1996**

Related U.S. Application Data

[63] Continuation of Ser. No. 164,961, Dec. 9, 1993, abandoned.

[51] **Int. Cl.**[6] **H04L 9/00**

[52] **U.S. Cl.** **380/50**

[58] **Field of Search** 380/3, 4, 25, 50

[56] **References Cited**

U.S. PATENT DOCUMENTS

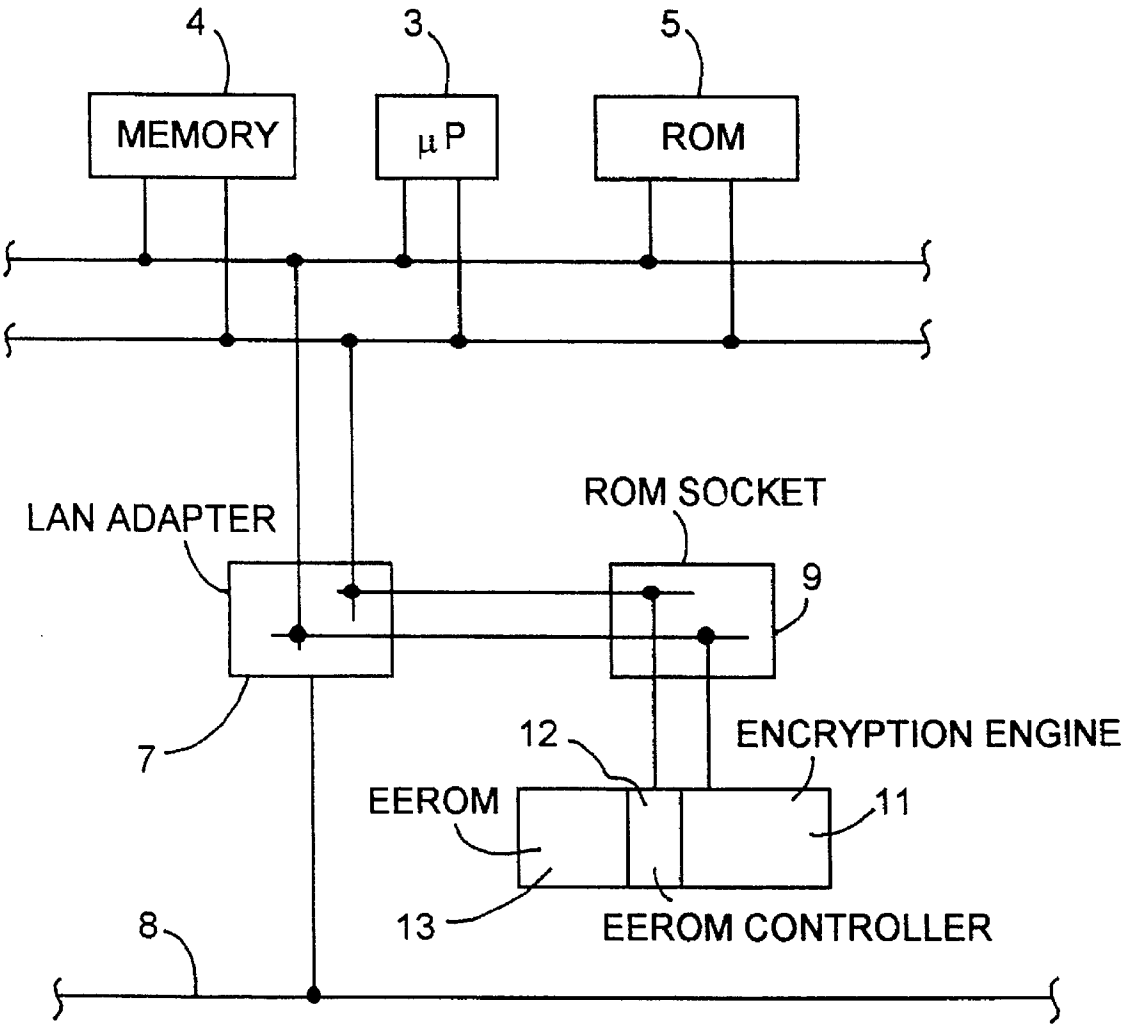
4,937,861	6/1990	Cummins	380/50
5,007,082	4/1991	Cummins	380/25
5,249,232	9/1993	Erbes et al.	380/50
5,444,850	8/1995	Chang	380/3

Primary Examiner—Salvatore Cangialosi
Attorney, Agent, or Firm—Pascal & Associates

[57] **ABSTRACT**

The present invention relates to a data encryption and/or decryption system comprised of apparatus for storing encryption and/or decryption keys, an encryption and or decryption processor for receiving data signals, for receiving the key or keys from the storing apparatus, and for encrypting or decrypting the data signals in accordance with the key or keys, an output data bus for receiving the encrypted or decrypted signals from the processor, apparatus for plugging the system into a read-only memory (ROM) socket of a computer for access to a source of the data signals and to the output data bus, whereby the data signals are received, and encrypted data signals are passed through the ROM socket.

9 Claims, 2 Drawing Sheets



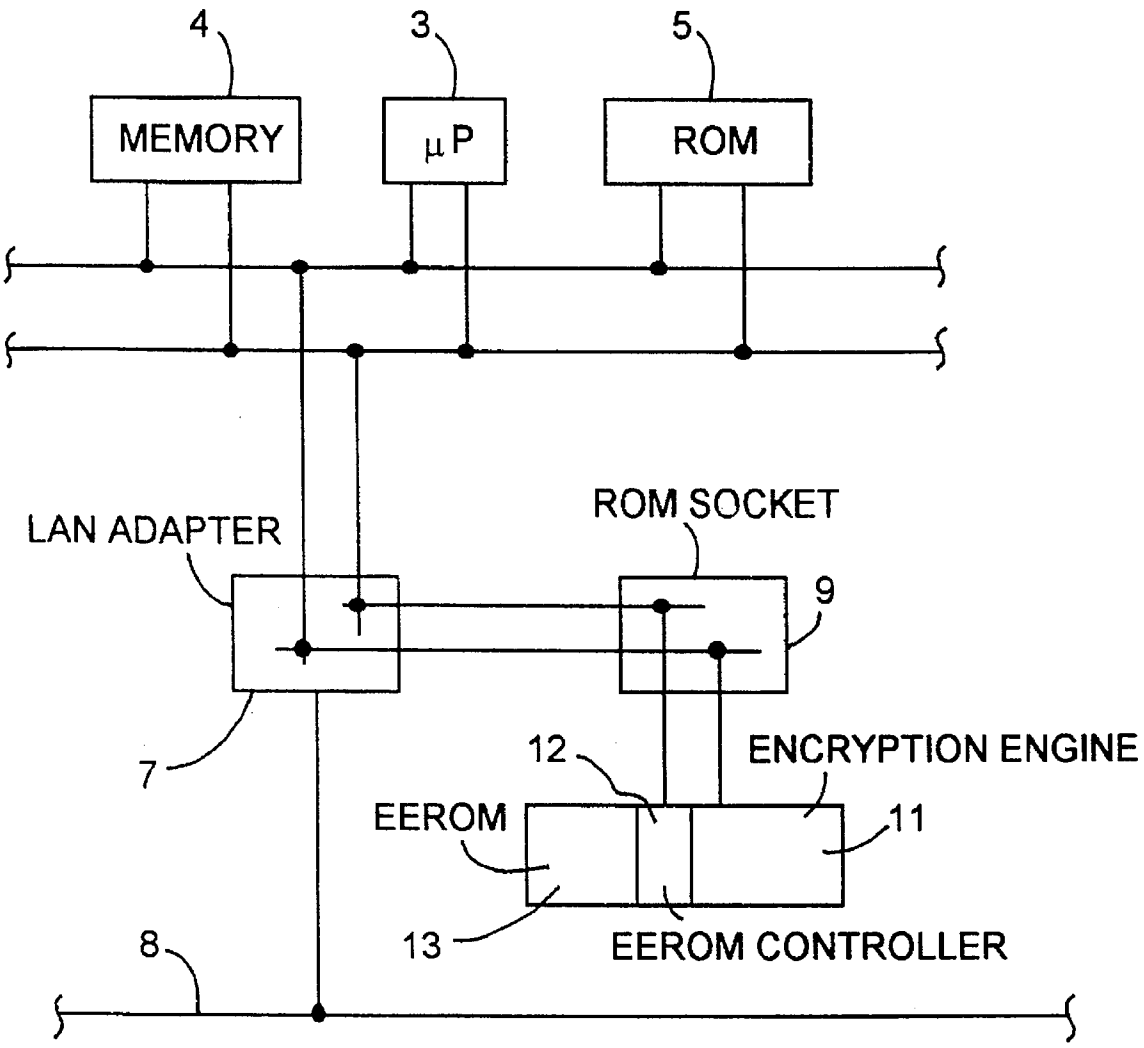


Fig. 1

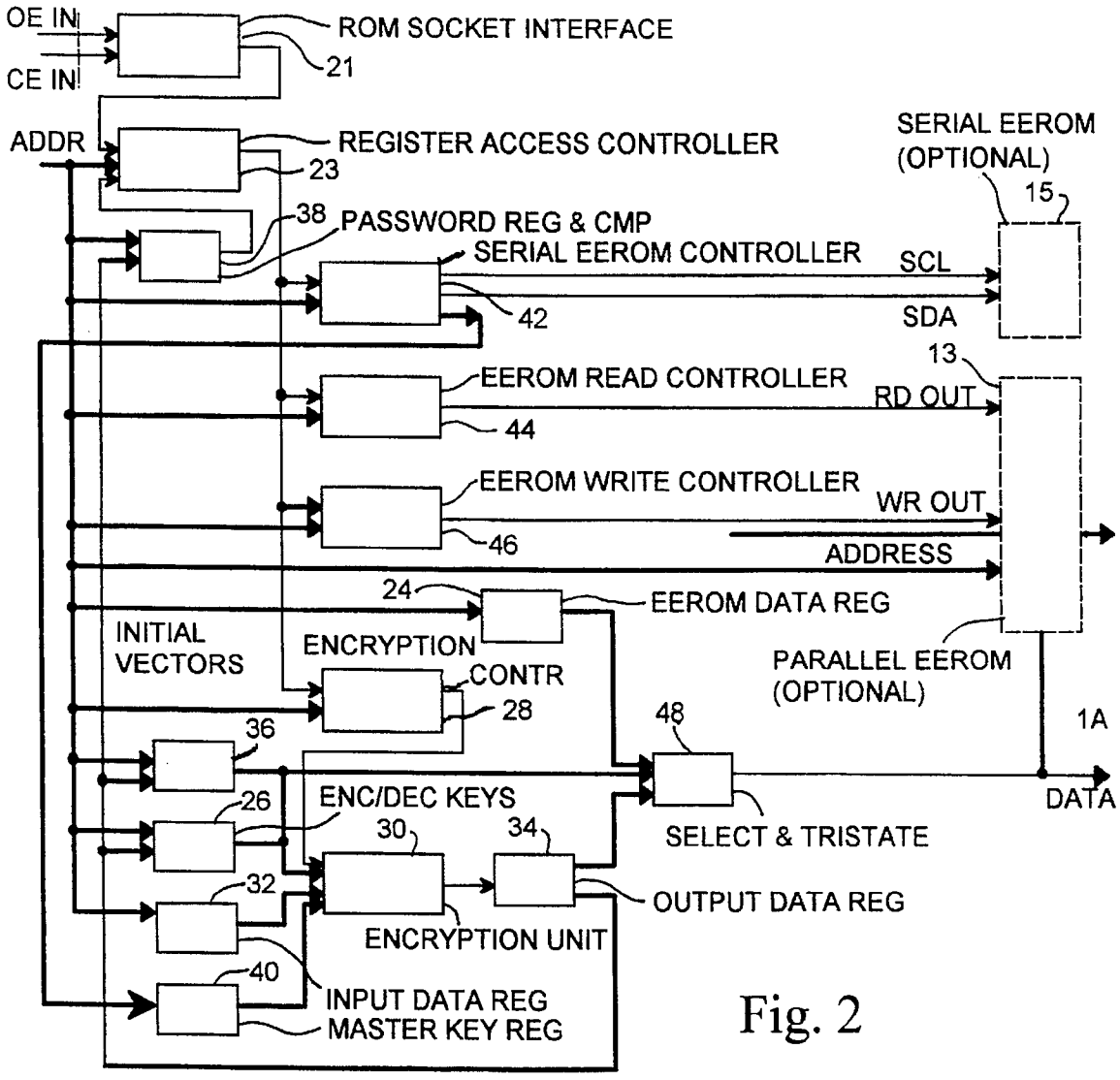


Fig. 2

LOCAL AREA NEWORK ENCRYPTION DECRYPTION SYSTEM

This is a continuation of application Ser. No. 08/164,961 filed Dec. 9, 1993 now abandoned.

FIELD OF THE INVENTION

The invention relates to a system for encrypting and decrypting data traffic to be passed along a Local Area Network (LAN) using a standard Personal Computer (PC) LAN adapter.

BACKGROUND TO THE INVENTION

Local Area Networks are used to connect computers in such a way that they can communicate with each other at very high speeds, e.g. of the order of 10 Mbps. In larger user organizations these computers are connected to backbone networks so that different department LANs can communicate and finally the backbone network may have a bridge to a Wide Area Network (WAN) in order to communicate to the outside world. As computers become more powerful LAN's and WANs allow organizations to distribute the power and still maintain connectivity.

Many user organizations have a need to keep certain types of data secure. This may range from a small company which has a responsibility to protect its employee's confidential data, to companies working on defense related contracts, to the government security and diplomatic services. More and more of this data is being placed on computers.

Data encryption devices secure sensitive information while it is electronically transmitted, stored, or otherwise processed. Encryption systems which include both hardware devices and software programs employ a mathematical algorithm to scramble plain text, rendering it unintelligible until it is unscrambled through the use of a special digital key. The security of the system is a direct function of the possession of the key.

Many hardware-based encryptors are simple microprocessor-based systems that electronically encode data at the sending end and decode data at a receiving end. Several effective software programs run as applications programs on a user's computer system.

Hardware encryption devices provide certain advantages over application software. For example, the installation of encryption hardware has a minimal effect on the user's existing computer system. Also, an encryption process employing hardware is virtually immune to unauthorized, undetected alteration. Software, on the other hand, is susceptible to programmer modification.

There are two categories of means for providing data security on LANs connected to personal computers: the first category is comprised of software-only programs which are inexpensive but which have been found to be somewhat ineffective, and the second category of hardware/software combinations that offer adequate security but are expensive due to the addition of a circuit board.

SUMMARY OF THE INVENTION

To connect to a LAN, a computer such as a personal computer has a LAN adapter subsystem connected to (plugged into) its main address and data buses which are accessible by the main processor of the computer. In order to provide means for a computer without disk drive storage to boot up (be controlled by a bootstrap program in order to retrieve its operating system from the LAN and become operational), LAN adapters are typically provided with a read-only memory (ROM) socket into which the bootstrap ROM may be plugged. The ROM socket is typically connected to a LAN adapter, and has its pin signals accessible to the main system processor. Communication paths to the ROM socket are typically non-standard, and are arranged with only reading a ROM in mind. Consequently, interface circuits to the ROM, and the conductive paths to the ROM have been made specialized for reading, and not writing data.

It has been found that the bootstrap ROM socket on the LAN is virtually never used, personal computer users preferring to bootstrap their computers using bootstrap ROMS in their own computers to retrieve the operating system from resident disk drives. The present invention utilizes the empty ROM socket on LAN adapters (such as those connectable to IBM PC compatible computers) and can provide line rate, standard data encryption and secure, non-volatile key storage. A hybrid module embodying the present invention is a pin-for-pin multi-chip hybrid module replacement for a conventional ROM. Yet the present invention provides for both writing and reading, in order to encrypt data, store keys, and read the keys, and thus allowing the hybrid module to offer the advantages of the hardware solution at the price of the software-only solution.

The present invention security module referred to herein as LanDES (local area network data encryption security) can provide line rate standard data encryption to all personal computer LANs without degradation of performance and in a manner which is completely transparent to the user. The user need not buy an expensive board to retrofit a computer. The module in volume could be produced at such a low cost that it could be shipped with LAN adapters as a low cost option. The user can protect its LAN traffic for tens of dollars instead of hundreds of dollars per client.

As noted above, the LanDES module plugs into the empty ROM socket on typically an IBM PC, PS/2 compatible LAN adapters and provides line rate, standard data encryption and secure, non-volatile key storage. The LanDES module is a pin-for-pin multi-chip hybrid module replacement for a conventional ROM. Unlike a conventional ROM, the LanDES module allows data to be written to the device. A commercial LanDES module may provide encryption at a sustained 32 Mbit/sec throughput, and it may provide from 128 bytes to 8 Kbytes of secure, non-volatile storage depending on the memory device selection.

In order to present easy access to key information and further enhance the security of the system, the keys may be super encrypted with an unique master key. This master key is stored in serial EEROM in each LanDES module.

In order to be fully compatible with the major LAN operating systems and transparent to the network, a main computer device driver of conventional form accesses the present invention, as will be described in more detail below. The device driver will embody typical data security applications and may include key management, line encryption, audit trailing, message and user authentication, access control, user groups and password aging.

In accordance with an embodiment of the present invention, a data encryption and/or decryption system is comprised of apparatus for storing encryption and decryption keys, an encryption and/or decryption processor for receiving data signals, for receiving the key or keys from the storing means, and for encrypting or decrypting the data signals in accordance with the key or keys, an output data bus for receiving the encrypted or decrypted signals from the

data encryption processor, apparatus for plugging the system into a read-only memory (ROM) socket of a computer for access to a source of the data signals and to the output data bus, whereby the data signals are received, and encrypted data signals are passed through the ROM socket.

In accordance with another embodiment, the source of data signals is a ROM socket address bus accessible by the computer microprocessor and the encrypted data signals are applied to the data bus, the output data bus being accessible to a computer microprocessor.

In accordance with another embodiment, the system includes a local area network (LAN) adapter system for connection to the computer which contains the ROM socket, the ROM socket being a socket, designated for a boot ROM for the computer, in the LAN adapter system for booting the computer from the boot ROM of the LAN adapter.

In accordance with another embodiment, the system includes an electrically erasable read only memory (EEROM) for storing a master key, and apparatus for securely loading or modifying the master key in EEROM and for reading the master key from EEROM into the encryption engine.

BRIEF INTRODUCTION TO THE DRAWINGS

A better understanding of the invention will be obtained by reading the description of the invention below, with reference to the following drawings, in which:

FIG. **1** is a general block diagram of the invention, and

FIG. **2** is a more detailed block diagram of the invention.

DETAILED DESCRIPTION OF THE INVENTION

FIG. **1** illustrates a portion of personal computer, comprised of a data bus **1**, an address bus **2**, a microprocessor **3** which is connected to the buses, a random access memory (RAM) **4**, connected to the buses, and a bootstrap ROM **5** also connected to the buses, both memories being accessible to the microprocessor via the buses. The remaining parts of the computer are not shown, in order not to clutter the drawing with elements that are not essential to an explanation of the present invention.

In order to connect the computer to a LAN, a LAN adapter **7**, typically formed of a circuit on a printed circuit board, is connected (plugged into) the buses, for access by the computer microprocessor, and is also connectable to a LAN **8**. The LAN adapter has a ROM socket **9** mounted on it, into which another bootstrap ROM is expected to be plugged in. As noted above, this is virtually never used, for the reason that the computer can be booted up by using a bootstrap program stored in ROM **5**. Thus while the buses **1** and **2** are accessible by the LAN adapter, extensions of those buses to ROM socket **9** are typically passed through an internal non-standard interface which has the expectation only of being able to read from, and not write to, a ROM plugged into ROM socket **9**.

In accordance with the present invention, a data security device **10** (LanDES) which is a pin-for-pin hybrid replacement for a conventional ROM device is plugged into ROM socket **9**. However unlike a conventional ROM the LanDES allows for the device to be written to. The device **10** has an integrated data encryption engine **11** and a secure EEROM read/write access controller **12**. The data encryption engine **11** and the EEROM controller **12** are independent and may be used independently, an EEROM **13** optionally may accompany the controller on the LanDES hybrid. Since the EEROM may be used independently, it can contain a bootstrap program which can be used to allow the computer to boot up from the LAN.

The data encryption engine can support the Cipher-Block-Chaining (CBC) and other modes of encryption such as EBC and CFB modes of data encryption.

The EEROM controller **12** allows reading of the EEROM during normal operation. When a protection window is open and a password has been matched or when password protection is disabled, the EEROM **12** controller allows the modification of the EEROM's contents, read-protection of selectable portions of the EEROM and modification of the password. The EEROM may be used for computer bootcode and/or secure key storage.

In operation, the invention can be used in any of three modes.

In the first mode, data is passed under control of microprocessor **3** to the LAN adapter, which applies the data to the data security device **10** via ROM socket **9**, which applies the EEROM data to data bus **1**, also via ROM socket **9**.

In second mode, the data to be applied to the LAN is prefixed with a predetermined sequence. The encryption controller, having stored an encryption code in a manner as will be described below, detects the sequence on the address bus **2**, and instead of passing the data out to the data bus, applies the stored encryption keys to the data using an encryption algorithm, resulting in encryption of the data. The encrypted data is output on the data bus **1** for application to the LAN**8** by the LAN adapter **7**.

In a third mode, the data to be applied to the LAN is prefixed with a different predetermined sequence. The encryption controller **11**, detecting this different predetermined sequence, enables storage of subsequent data in the EEROM. The subsequent data can be for example a master key which is used for encryption of data received on the address bus. That key can then be used to encrypt subsequent data received on the address bus that is prefixed with another predetermined sequence.

The third mode of operation is the most secure, since the key or keys stored in the EEROM can only be changed by persons who know the aforenoted different predetermined sequence. The second mode of operation may be less secure, since the predetermined sequence used may be obtained from the driving program used by the microprocessor **3**, and thus can be changed at will by the user.

Either of the second and third modes may be used to encrypt data automatically for all data that arrives on the address bus, only if that data that is prefixed by a special prefix that places the encryption controller into an encryption mode.

FIG. **2** is more detailed block diagram of the invention.

A ROM interface circuit **21** samples the read enable (CE) and output enable (OE) strobe signals generated by processor **3** and carried of buses **1** and **2**, to determine if a single valid ROM read access command has occurred. The ROM interface interprets multiple and false strobe edges and strobe to address/data setup and hold violations to produce a single access strobe of fixed duration, which is applied to register access controller **23**. Address bus **2**A, which is derived from address bus **2**, is connected via ROM socket **9** to register address controller **23**. Register access controller **23** may be a microprocessor.

Register access controller **23** preferably has two distinct modes of operation, which may be termed as window-closed mode and window-open mode. The "window" is a write

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.