US005734819A

United States Patent [19]

Lewis

[11] Patent Number: 5,734,819

[45] Date of Patent: Mar. 31, 1998

[54] **METHOD AND APPARATUS FOR VALIDATING SYSTEM OPERATION**

[75] Inventor: **David Otto Lewis**, Rochester, Minn.

[73] Assignee: **International Business Machines Corporation**, Armonk, N.Y.

[21] Appl. No.: **322,246**

[22] Filed: **Oct. 12, 1994**

[51] **Int. Cl.**[6] **G06F 11/00**

[52] **U.S. Cl.** **395/186**; 380/45; 364/260.81; 364/286.4

[58] **Field of Search** 395/186, 187.01, 395/188.01; 380/4, 25, 30, 45; 364/222.5, 260.81, 286.4, 286.5

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,264,782	4/1981	Konheim	395/186 X
4,424,573	1/1984	Eckert, Jr. et al.	364/900
4,442,486	4/1984	Mayer	364/200
4,454,594	6/1984	Heffron et al.	364/900
4,462,076	7/1984	Smith, III	364/200
4,634,807	1/1987	Chorley	178/22.08
4,652,990	3/1987	Pailen et al.	364/200
4,670,857	6/1987	Rackman	380/4
4,688,169	8/1987	Joshi	364/200
4,731,748	3/1988	Haneda	364/900
4,751,667	6/1988	Ross	364/900
4,866,769	9/1989	Karp	380/4
4,903,299	2/1990	Lee et al.	380/25
4,933,969	6/1990	Marshall	380/125
5,068,894	11/1991	Hoppe	380/23
5,075,805	12/1991	Peddle et al.	360/61
5,113,518	5/1992	Durst, Jr. et al.	395/550
5,182,770	1/1993	Medveczky	380/4
5,199,066	3/1993	Logan	380/4
5,276,738	1/1994	Hirsch	380/46
5,282,247	1/1994	McLean et al.	380/4
5,287,408	2/1994	Samson	380/4
5,337,357	8/1994	Chou	380/4
5,343,524	8/1994	Mu et al.	380/4
5,379,433	1/1995	Yamagishi	395/186
5,386,468	1/1995	Akiyama	380/25
5,388,212	2/1995	Grube	395/186
5,392,356	2/1995	Konno	380/23
5,402,492	3/1995	Goodman et al.	380/25
5,416,840	5/1995	Cane	380/4
5,481,672	1/1996	Okuno	395/186 X
5,483,658	1/1996	Grube	395/186 X
5,530,753	6/1996	Easter	380/4
5,546,463	8/1996	Caputo	380/25

FOREIGN PATENT DOCUMENTS

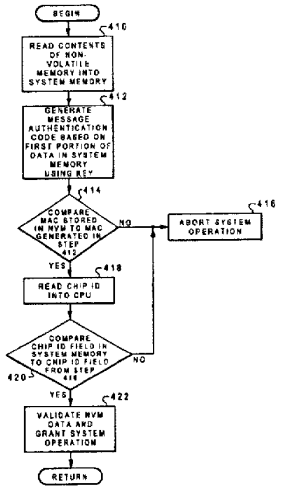
0 175 359 A2	9/1985	European Pat. Off. .
0 302 710 A3	8/1988	European Pat. Off. .
0 425 053 A1	10/1990	European Pat. Off. .
WO 93/23807	5/1993	European Pat. Off. .

Primary Examiner—Robert W. Beausoliel, Jr.
Assistant Examiner—Dieu-Minh Le
Attorney, Agent, or Firm—Andrew J. Dillon

[57] **ABSTRACT**

A method and apparatus for providing system operation validation is disclosed. The method and apparatus for validation operates within a computer system comprising a central processing unit coupled to a programmable memory, and to a system device. The programmable memory may store programs and instructions executable on the CPU and a non-volatile memory is also provided for access by the CPU. The system operation validation is provided by a chip identifier located within a device memory within the system device, which memory also serves as a chip identifier register. Selected information stored within the non-volatile memory is used, along with the chip identifier, to generate a first encryption code associated with the system device. An encryption key is used to generate a second encryption code associated with the computer system. The first and second encryption codes are matched to provide a first level system operation validation. A second chip identifier is generated, which identifier is associated with the computer system. Both chip identifiers are compared to provide a second level system operation validation.

11 Claims, 3 Drawing Sheets



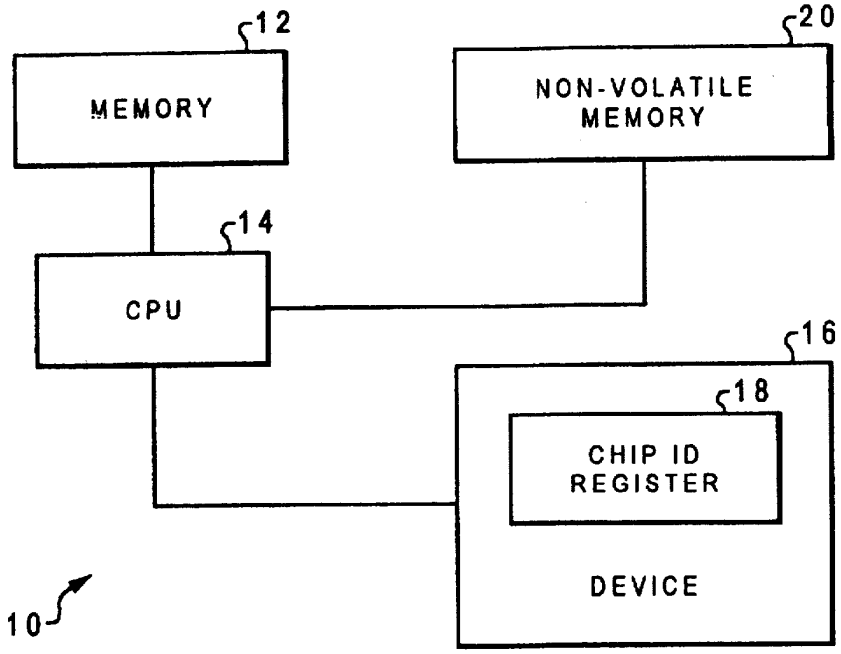


Fig. 1

120

ADDRESS IN BYTES	
0 - 7	DEVICE TYPE
8 - 15	DEVICE SERIAL NUMBER
16 - 23	CHIP ID
24 - 31	UNIQUE DEVICE DATA
32 - 39	MESSAGE AUTHENTICATION CODE
40 -	DEVICE DATA AREA

Fig. 2

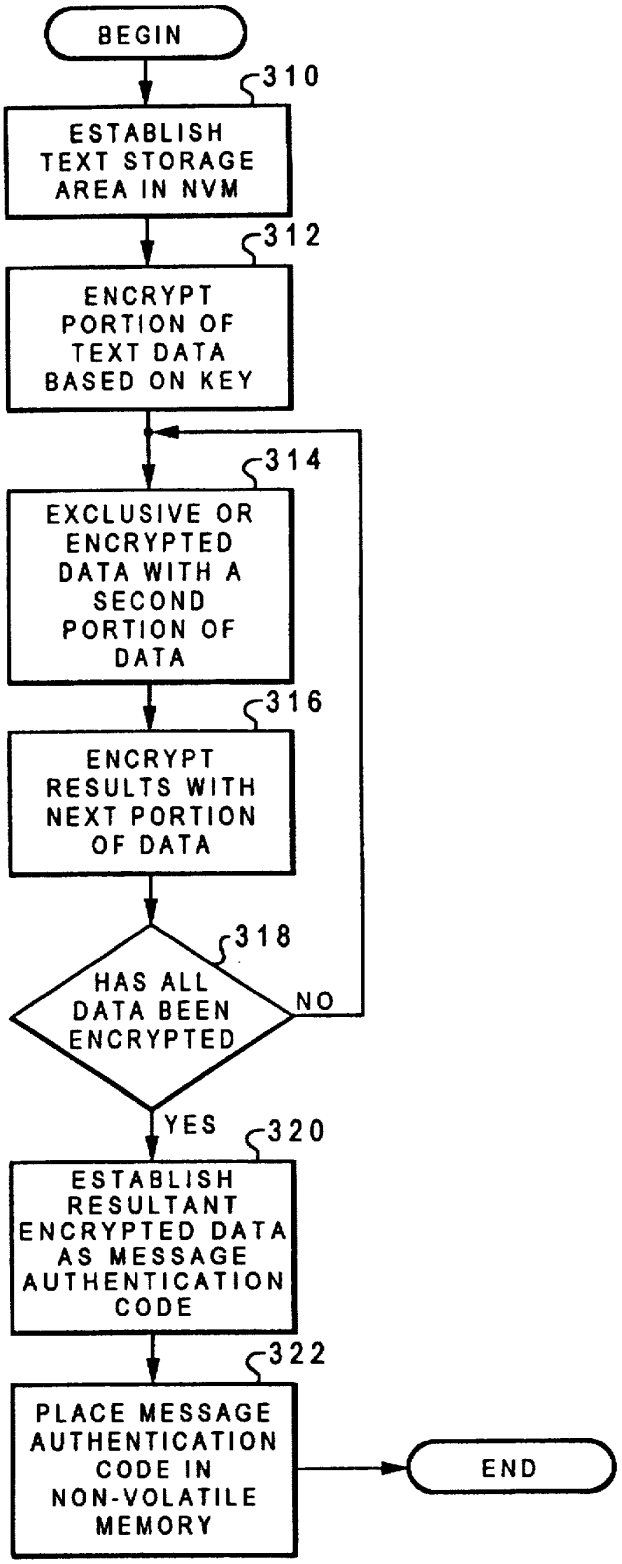


Fig. 3

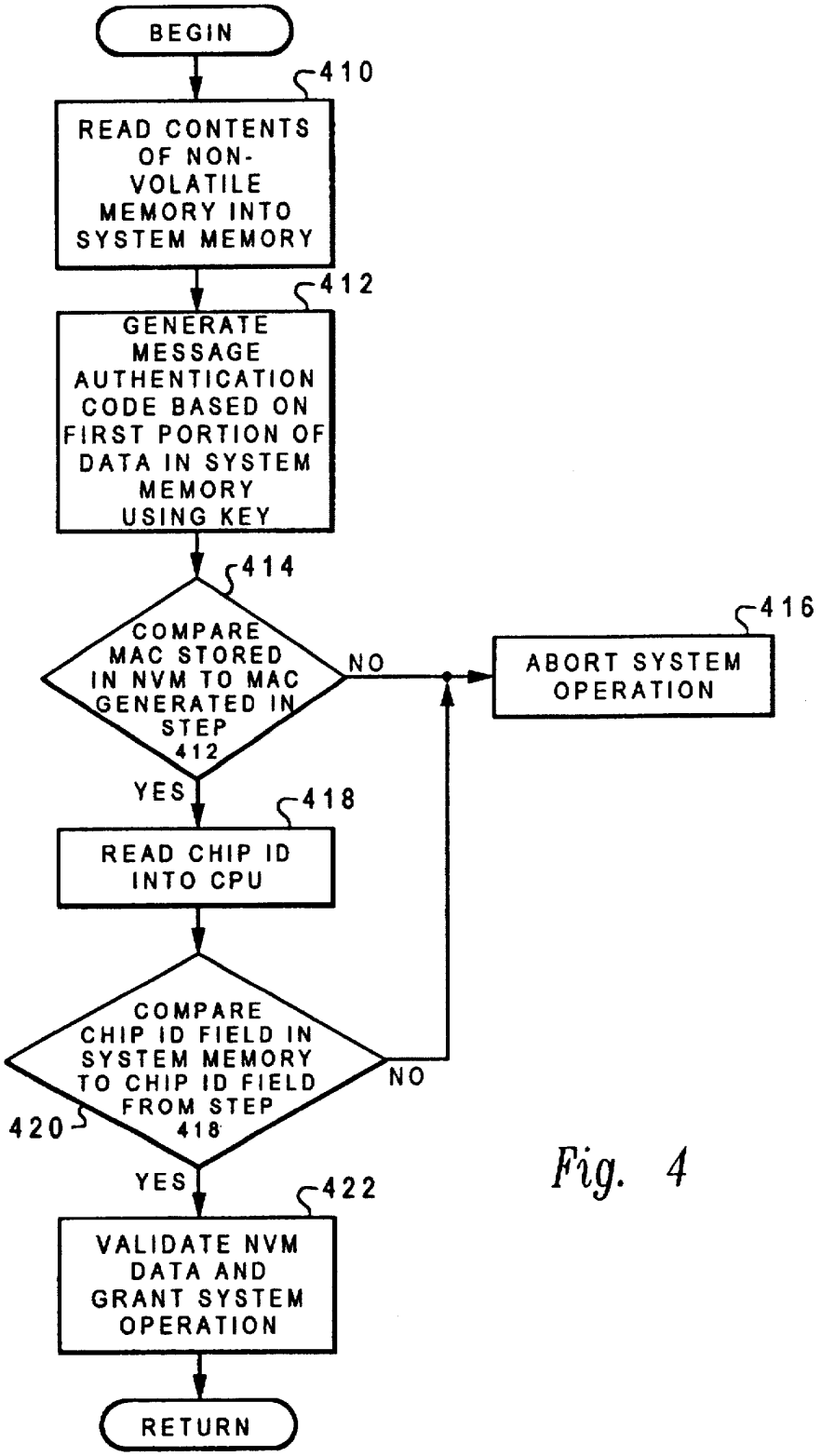


Fig. 4

METHOD AND APPARATUS FOR VALIDATING SYSTEM OPERATION

BACKGROUND OF THE INVENTION

1. Technical Field

The present invention relates, generally, to a computer system having a non-volatile memory and, more specifically, to electronic security information being stored in the non-volatile memory. More specifically, the present invention relates to a computer system having a non-volatile memory with security information written into the non-volatile memory and a way of detecting when that information has been altered so as to prevent operation of the computer system once tampering has been detected.

2. Description of the Related Art

Electronic serial numbers are being employed in more and more electronic devices. These serial numbers are used for multiple purposes ranging from determining whether a device is still under warranty to providing a unique machine identification so that a software key is required to run on that specific machine serial number (this feature is provided in license managers such as NETLS). The objective of providing the electronic serial number is to allow software access to the serial number so that it can be tracked electronically or used as part of the software key encryption algorithm. There is an inherent weakness in the electronic serial number in that the manufacturer of the electronic device wants to control the machine serial number or unique data and that every machine serial number written must be unique. To provide the manufacturer the flexibility to write a different serial number on each machine, the machine is designed with some type of non-volatile memory (NVM) that the manufacturer can write (such as EPROM, PROM, ROS, EEPROM, flash type of memory or a track or header on a tape, DASD or optical diskette). Since the serial number is located in a programmable memory, it is easy for someone else to duplicate the serial number by simply copying the contents of one NVM media to another NVM media or writing a portion of the NVM media. By creating a duplicate serial number machine, all of the software programs that are licensed for the original machine can now be used on the duplicate serial number machine effectively bypassing the license manager checks.

There are multiple ways in which a unique chip identifier can be programmed in a chip and made non changeable. The easiest way is to have a tie up or down signal feed a series of fuses, which in turn feed inputs to a register. These fuses can be blown by a laser as part of the normal chip manufacture process providing a unique chip identifier. The chip fuses are typically blown at the wafer level and contain the lot number, the wafer number, and the chip location on the wafer. Obviously many bits are needed (more than 64) on high volume chips since there is a high percentage of chips that are scrapped and the unique chip identifiers are never used. Chip fuses have been used for many years in DRAM and SRAM designs to select a different portion of the array to be used if found defective by manufacturing. The ability to produce unique chip identifiers is known in the industry.

A second way a unique chip identifier can be built into a module is by using module laser delete chip I/O's. Module laser delete is done in a similar fashion as the chip laser delete in that a tie up or down signal is fed to a series of fuses which in turn go to chip I/O pins and from there to latches in a register. A laser is used to blow the fuse thus causing the data in the latch to be personalized. The register is then made

available to the software. This method reduces the number of bits needed for the unique chip identifier since the chips have already been tested before mounting on the modules and most modules will test good. Again, since a fuse has been blown, it is not possible to duplicate easily another unique chip identifier.

There are several encryption techniques that can be used that can provide the manufacturer the capability to detect any duplication or modification of the non-volatile memory data such as a serial number. One example of the encryption technique is the Message Authentication Code (MAC), which uses the Data Encryption Standard encryption algorithm. The MAC routine is passed a string of text data and an encryption key and returns an 8 byte MAC. Since the DES encryption encrypts 8 bytes at a time and the result of the previous 8 byte encryption is used with the next 8 bytes of encryption, the last 8 bytes of the encryption are dependent on all of the previous text data so any change in any of the previous data will be detected in the last 8 bytes of the encryption (the MAC).

At the time the device is manufactured, the manufacturer will select an 8 byte encryption key that must be kept secret. The unique chip Identifier is included in the text portion of the data to be encrypted along with any other data the manufacturer wants to prevent being modified. A MAC is then generated and written along with the data in the non-volatile memory along with the data. The operating system software program then reads the non-volatile memory and the unique chip identifier from the hardware. If the unique chip identifier found in the text portion of the non-volatile memory does not compare with the one in the hardware, then the text has been altered (probably copied from another machine) and the software program can reject the device as being an invalid device. If the unique chip identifier in the non-volatile memory does match the one in the chip, then the software program verifies that the MAC is correct by generating a new MAC for the text of the non-volatile memory using the same key that was used to generate the MAC in manufacturing and then compares the MAC generated with the MAC in the non-volatile memory. If the MACs compare then the software program is assured that none of the text data that is covered by the MAC has been altered. Since only the manufacturer and the checking software knows the key to create the MAC AND the unique chip identifier is part of the text that created the MAC, it is not possible to alter the text or MAC unless the encryption key is known. Obviously the key must be kept secret and protected by the software and the manufacturer.

Another encryption technique that can be used is RSA where the manufacturer uses a private key to encrypt the text where the unique chip identifier is again included in the text where modification detection is required. A public key is then used by the software program to decrypt the encrypted data and a comparison is made by the software program of the unique chip identifier in the hardware with that in the encrypted text. If there is a match then the text is valid, otherwise the text has been copied from another machine or has been otherwise altered. The advantage of the RSA is that two different keys are used for encryption and decryption and if the public key is known, the private key can not be determined whereas DES uses the same key for encryption and decryption so the software program must hide the key very well. This invention does not rely on any specific encryption technique only on the fact that the manufacturer can control access to the encryption key.

Accordingly, what is needed is a computer system security arrangement using non-volatile memory where critical

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.