US 20060101310A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2006/0101310 A1

Diamant et al. (43) Pub. Date: May 11, 2006

(54) DEVICE, SYSTEM AND METHOD FOR VERIFYING INTEGRITY OF SOFTWARE PROGRAMS

(76) Inventors: **Nimrod Diamant**, Kfar Saba (IL); **Gershon Bar-On**, Mizrah Biniamin (IL); **Eliel Louzoun**, Jerusalem (IL); **Fabian Trumper**, Modiin (IL)

Correspondence Address:
PEARL COHEN ZEDEK, LLP
1500 BROADWAY 12TH FLOOR
NEW YORK, NY 10036 (US)

(21) Appl. No.: **10/970,653**

(22) Filed: **Oct. 22, 2004**

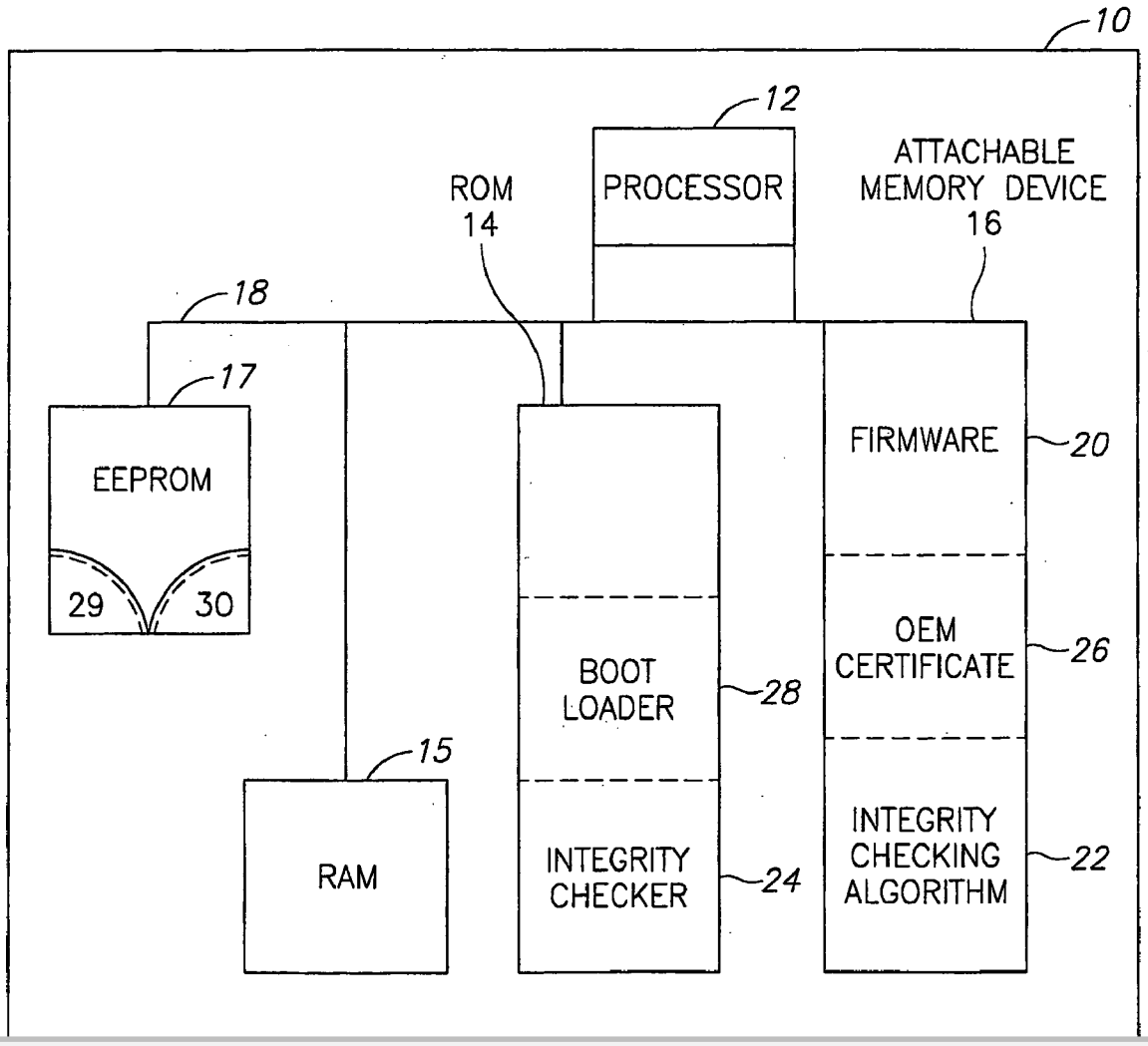
Publication Classification

(51) **Int. Cl.**
G06F 11/00 (2006.01)

(52) **U.S. Cl.** **714/38**

(57) **ABSTRACT**

A method, device and system for using a first verification algorithm or program to evaluate the integrity or authenticity of a second verification program. The first verification program may be stored in a device and may compare a result of such evaluation with a stored expected result. The second verification program may be included in for example an attachable memory unit of the device or other for example add-on memory unit of the device. The second verification program may evaluate the authenticity or integrity of firmware, software, data or other code that is included on the attachable device or elsewhere in the device. If both verification programs confirm the integrity of the respective codes, the firmware or software may be executed or loaded for execution by the device.



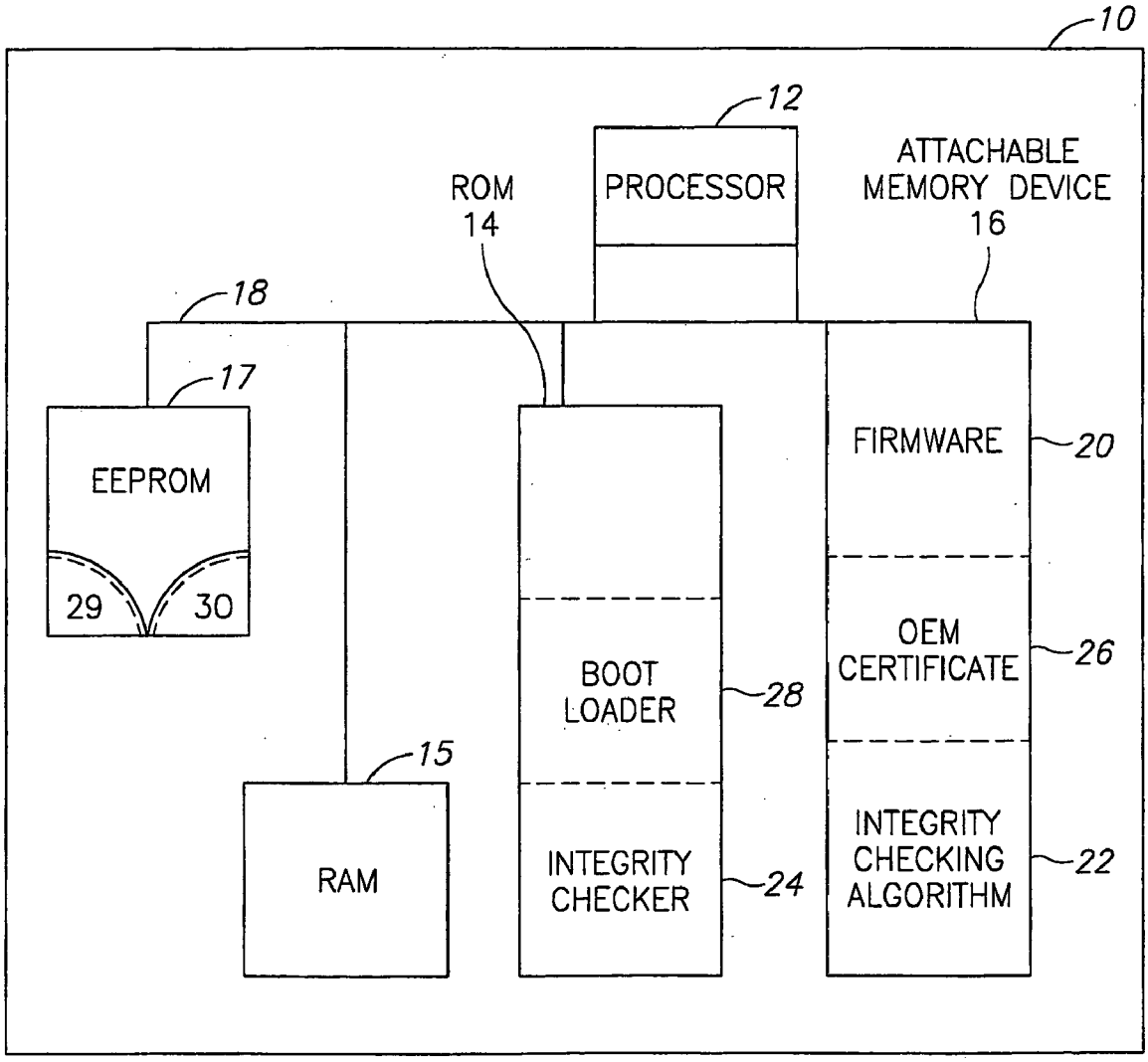


FIG.1

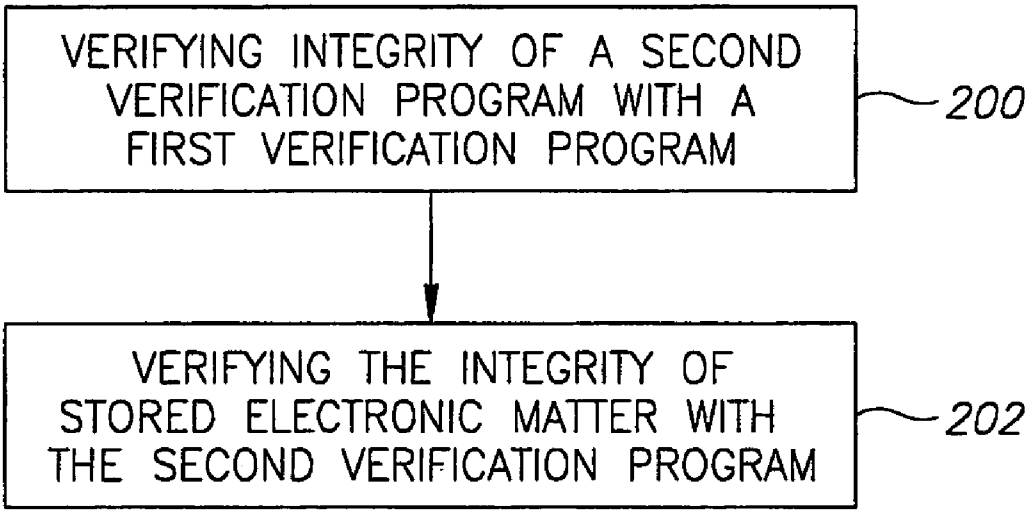


FIG.2

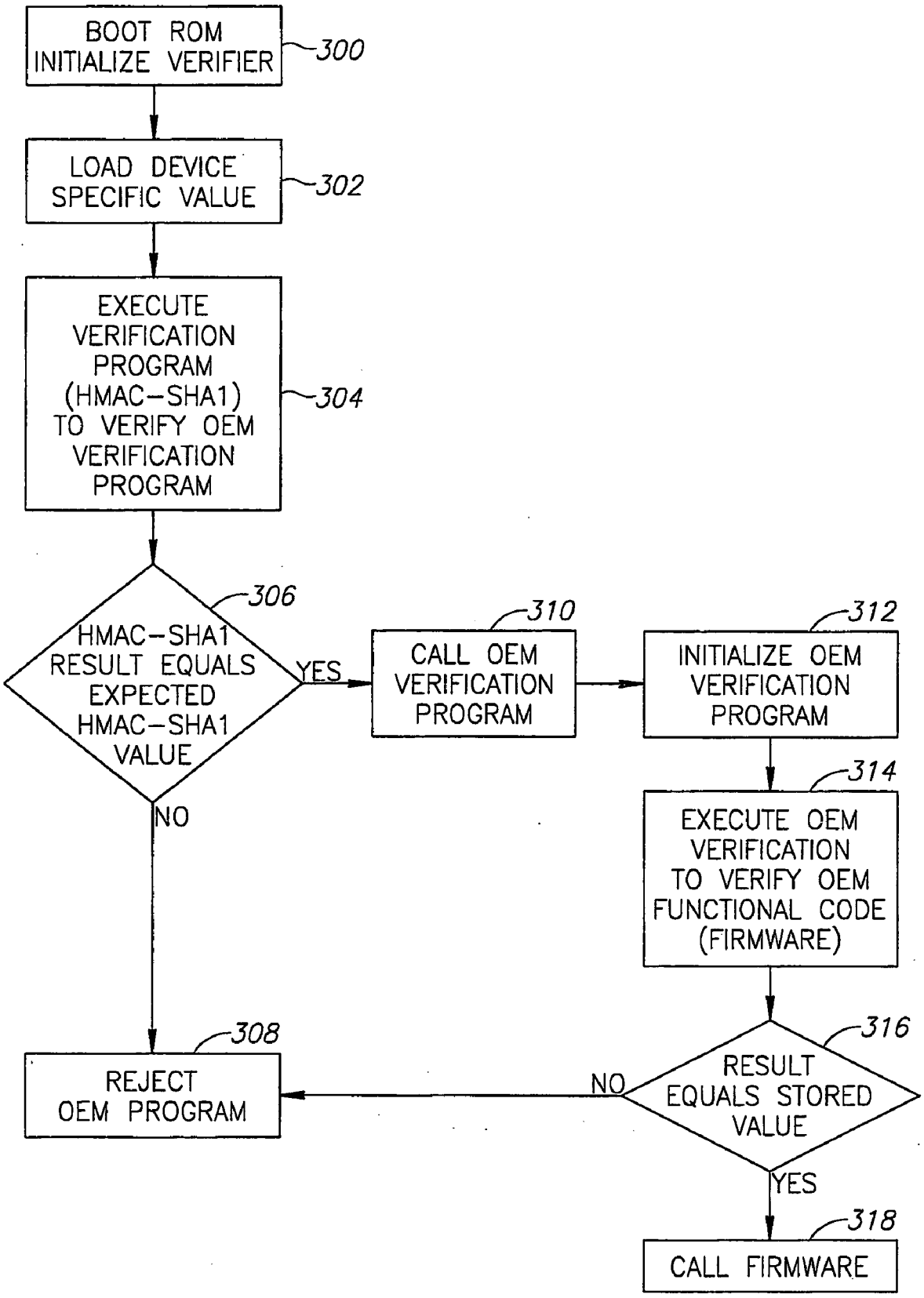


FIG. 3

DEVICE, SYSTEM AND METHOD FOR VERIFYING INTEGRITY OF SOFTWARE PROGRAMS

BACKGROUND OF THE INVENTION

[0001] Devices that include embedded software, instructions or code may run such embedded software from for example read only memory ("ROM") or other memory units. Functionality may be added to such devices by the inclusion in such devices of additional customized or vendor specific functional code, instructions, programs. databases or graphics ("firmware") that may for example be downloaded from a network or otherwise loaded into a memory of a device such as for example random access memory ("RAM"), flash memory units, memory cards, disk on a key or other memory units.

[0002] Code that may for example be stored on a ROM unit may authenticate or verify the completeness or integrity of the firmware or functional code that may be stored on for example another memory unit such as for example an attached memory device, to determine for example that the firmware was not miscopied, corrupted, compromised or otherwise unauthorized for use with a particular device. Such authentication or verification may be performed by various means such as for example integrity checking algorithms or test functions such as for example checksums, cyclic redundancy checks (CRC's) or hash functions stored for example in the ROM code or elsewhere in a device. The results of the execution of such algorithms or test functions may be compared with the expected results that may be stored for example in ROM or in other data storage units of a device. The integrity of the functional program, software, code, data, graphics or other firmware may be confirmed if, for example, the results of the integrity checking algorithm's evaluation of a functional program are equal to a stored value.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] Embodiments of the invention will be understood and appreciated more fully from the following detailed description taken in conjunction with the drawings in which:

[0004] **FIG. 1** is a schematic diagram of components of a device with embedded ROM and stored firmware in accordance with an exemplary embodiment of the invention;

[0005] **FIG. 2** is a flow diagram depicting a method of verifying the integrity of a program in accordance with an exemplary embodiment of the invention; and

[0006] **FIG. 3** is a flow chart of a method in accordance with an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0007] In the following description, various aspects of the present invention will be described. For purposes of explanation, specific configurations and details are set forth in order to provide a thorough understanding of the present invention. However, it will also be apparent to one skilled in the art that the present invention may be practiced without the specific details presented herein. Furthermore, well-

throughout this description. These are merely descriptions of specific embodiments of the invention. The scope of the invention is not limited to the examples given.

[0008] Unless specifically stated otherwise, as apparent from the following discussions, it is appreciated that throughout the specification, discussions utilizing terms such as "processing,""computing,""calculating,""determining," or the like, refer to the action and/or processes of a processor, computer or computing system, or similar electronic or hardware computing device, that manipulates and/or transforms data represented as physical, such as electronic quantities within the computing system's registers and/or memories into other data similarly represented as physical quantities within the computing system's memories, registers or other such information storage, transmission or display devices.

[0009] The processes and displays presented herein are not inherently related to any particular computer, communication device or other apparatus. The desired structure for a variety of these systems will appear from the description below. In addition, embodiments of the present invention are not described with reference to any particular programming language, machine code, etc. It will be appreciated that a variety of programming languages, machine codes, etc. may be used to implement the teachings of the invention as described herein. Embodiments of the invention may be included on a medium or article such as a hard disc, disc on key or other memory unit having stored thereon instruction that when executed implement an embodiment of the invention.

[0010] Reference is made to **FIG. 1**, which is a schematic diagram of components of a device with memory such as for example embedded ROM or other type of storage as well as stored firmware in accordance with an exemplary embodiment of the invention. Device **10** may include a processor **12** that may be connected to, operably linked to or part of a data storage unit such as for example a ROM **14**, electrical erasable read only memory (EEPROM) **17**, random access memory (RAM) **15** and a memory device **16** such as an attachable memory device or another suitable storage device. Other configurations of processor **12** and memory are possible. In some embodiments the storage functions of EEPROM **17** may be filled by other non-volatile memory devices such as ROM, FLASH or battery backed RAM. In some embodiments, one or more buses **18** may connect various components and memory units in device **10**. Memory device **16** may include functionality in addition to memory functionality, such as processing power, communications, etc. In an alternate embodiment, memory device **16** may be included in a remote device, or may be integral to device **10**, and need not be attachable.

[0011] In some embodiments, ROM **14** may be any suitable memory device that is capable of storing a program or other code that is not intended to be erased or written over as part of the function of device **10** in which ROM **14** is held. In some embodiments, ROM **14** may store for example an operating system, code or programs that may for example operate or execute certain basic operations of device **10**. Other programs, instructions or data may be stored on ROM **14**, and data storage units other than ROM **14** may be used.

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.