US 20050009599A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2005/0009599 A1

Ryan (43) Pub. Date: Jan. 13, 2005

(54) GAMING MACHINE HAVING TARGETED RUN-TIME SOFTWARE AUTHENTICATION

(76) Inventor: **Chad A. Ryan**, Lisle, IL (US)

Correspondence Address:
JENKENS & GILCHRIST, P.C.
225 WEST WASHINGTON
SUITE 2600
CHICAGO, IL 60606 (US)

(21) Appl. No.: **10/616,459**

(22) Filed: **Jul. 9, 2003**

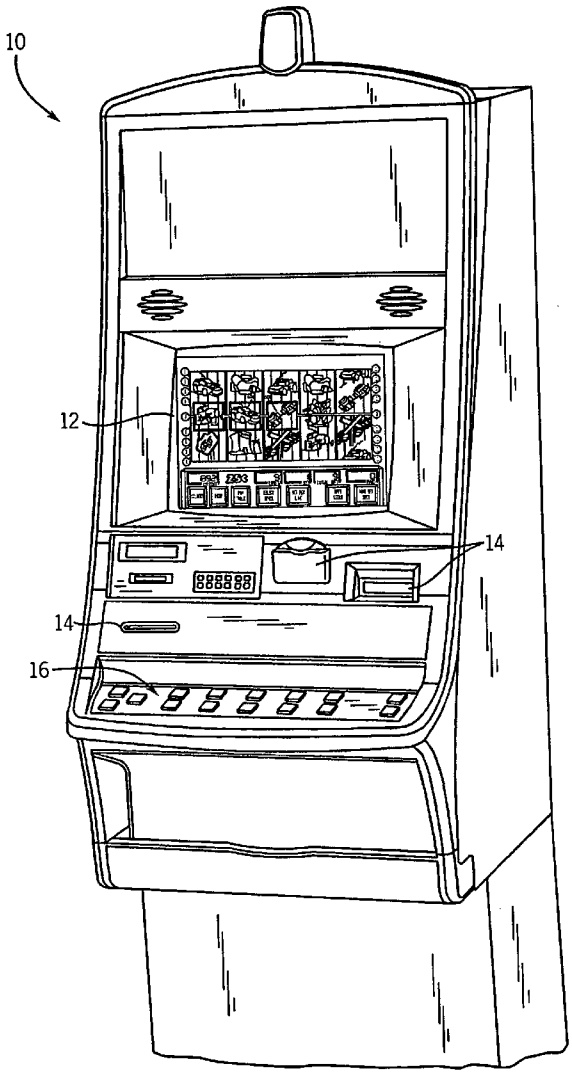
Publication Classification

(51) **Int. Cl.**[7] **A63F 13/00**

(52) **U.S. Cl.** **463/29**

(57) **ABSTRACT**

A gaming machine that authenticates its gaming software substantially continuously and repetitiously while the gaming machine is powered on. A processor, while running the gaming machine's gaming program, determines whether the data in each of a plurality of memories is authentic. The processor may read multiple memories in a parallel fashion while making memory contents authenticity determinations. The processor may also read multiple memories in a serial fashion while making memory contents authenticity determinations. The processor may also read same memories in a parallel fashion and read other memories in a serial fashion while determining the authenticity of each memory's contents. Furthermore, the contents of a memory may be analyzed to decipher between executable data and graphics data such that the executable data's authenticity is determined more often than the graphics data's authenticity



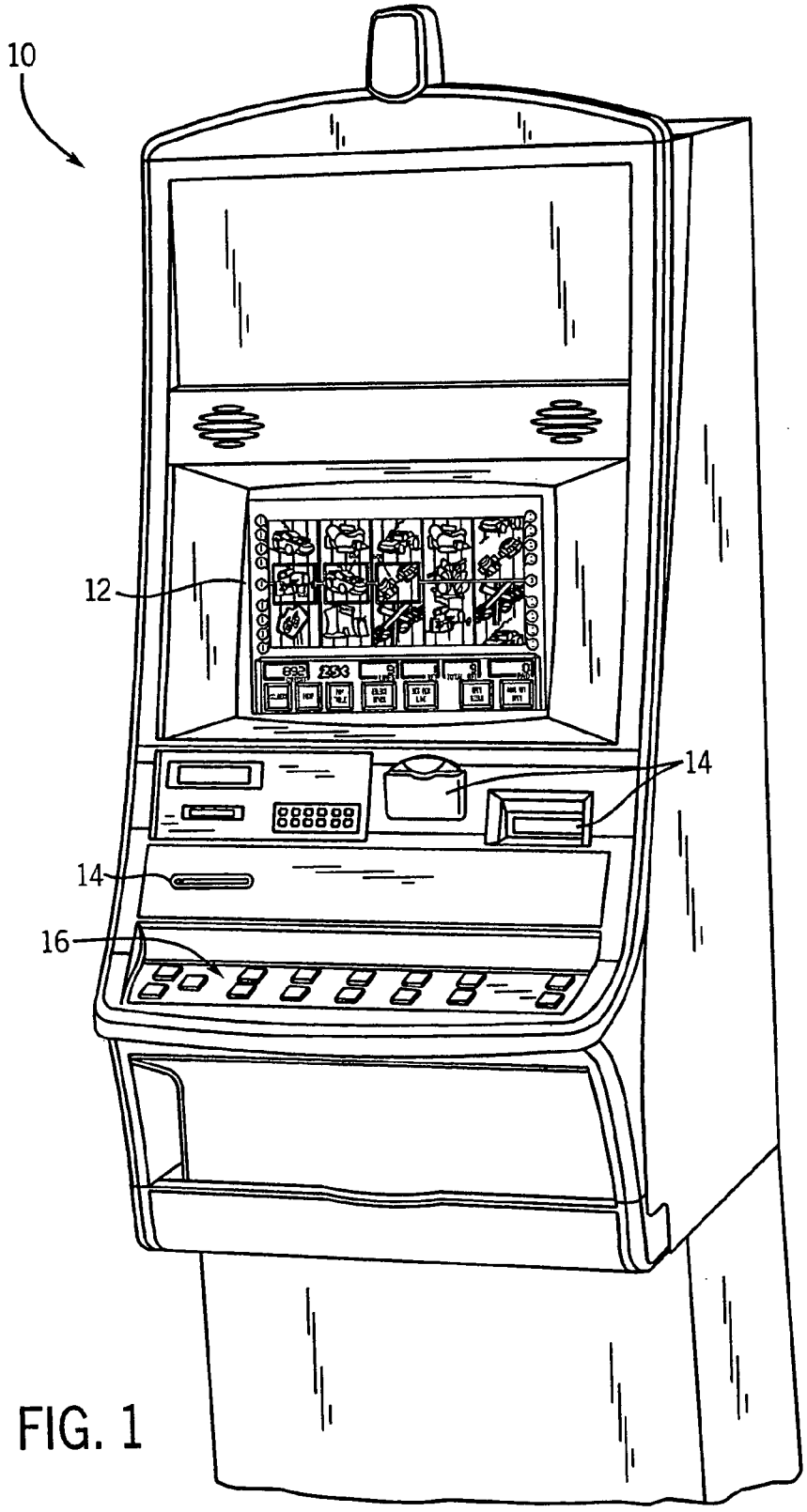


FIG. 1

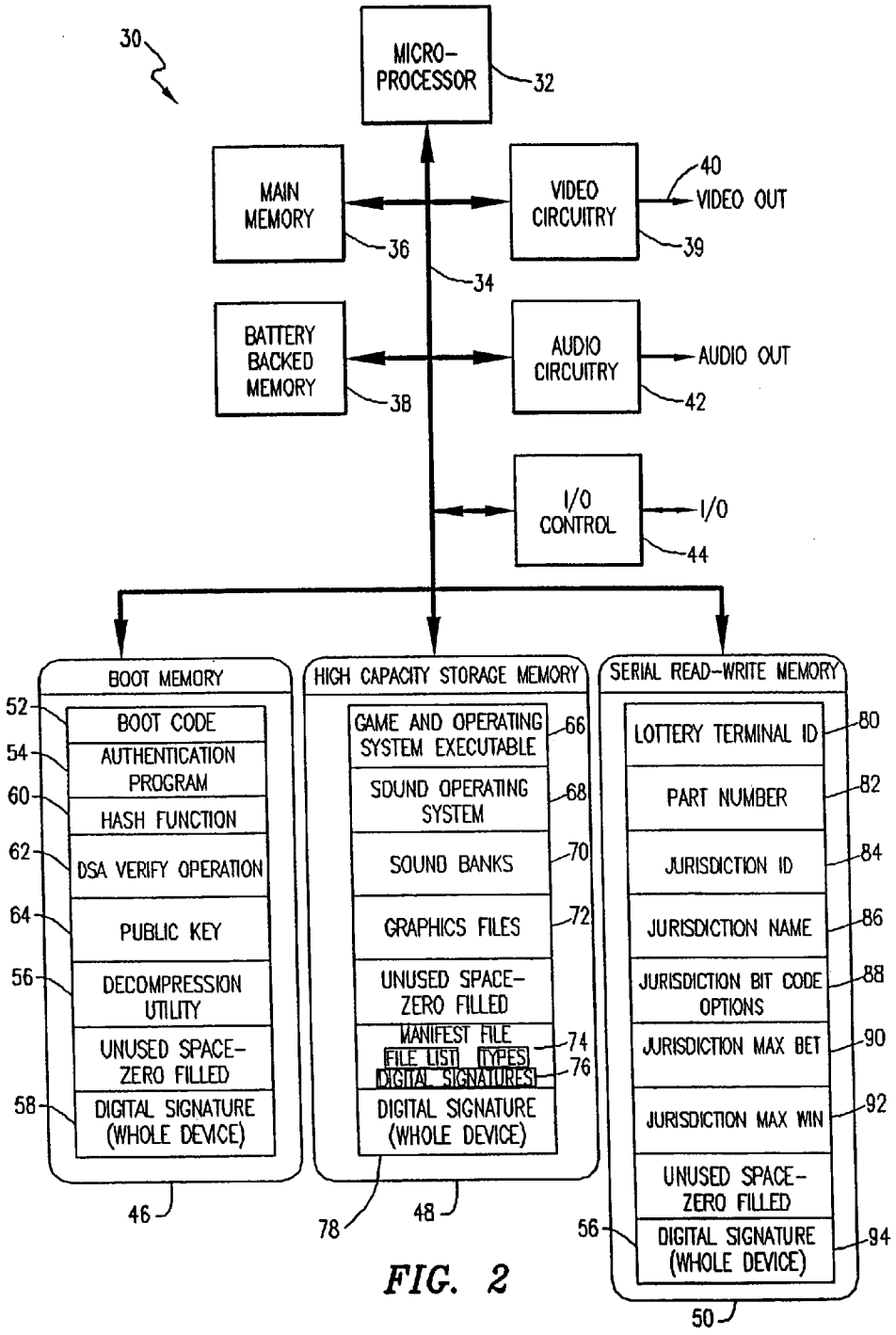


FIG. 2

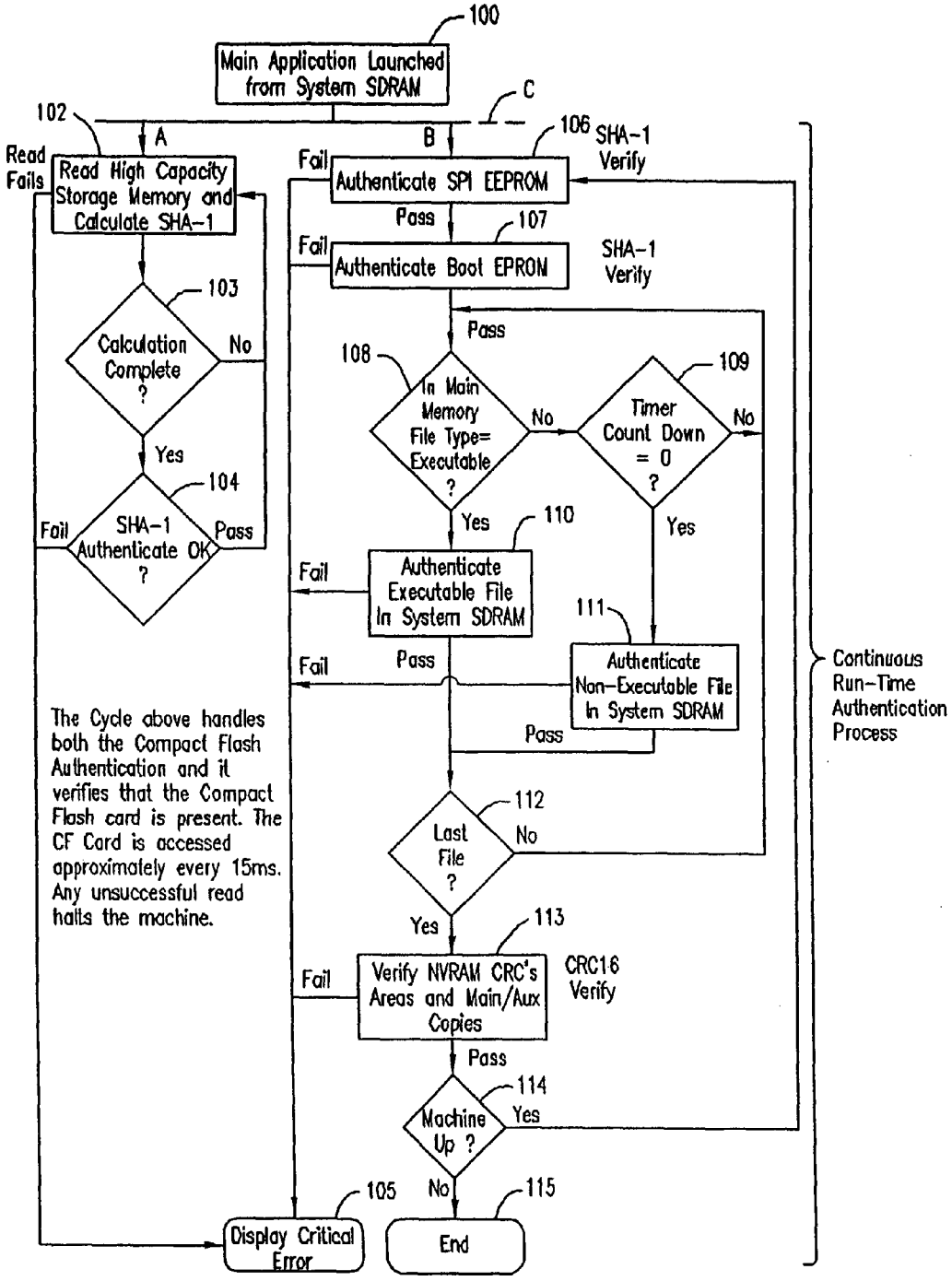


FIG. 3

GAMING MACHINE HAVING TARGETED RUN-TIME SOFTWARE AUTHENTICATION

REFERENCE TO RELATED APPLICATIONS

[0001] This application is related to U.S. patent application Ser. No. 10/119,663 filed on Apr. 10, 2002, entitled "Gaming Software Authentication", and incorporated herein by reference in its entirety.

FIELD OF THE INVENTION

[0002] The present invention relates generally to gaming machines, and more particularly, to software authentication of programs running in a gaming machine.

BACKGROUND OF THE INVENTION

[0003] As a regulatory requirement in virtually all jurisdictions that allow gaming, it is necessary to have a technique to authenticate that the software installed in a gaming machine is tested and approved. In the past, gaming manufacturers have generally used EPROM-based hardware platforms to store program code. As a result, a number of software authentication techniques have been accepted as standards throughout the gaming industry. Depending upon the preferences of the local regulatory agency, these techniques generally include either a Kobetron signature or a hash function based on the data stored in the EPROM device.

[0004] Authentication of software programs basically occurs using two different methods in the field, again determined by the local regulatory agency. In one method, each EPROM is authenticated by a gaming agent prior to being installed in a gaming machine that is to be brought up for play. The EPROMs may be shipped directly to the gaming agency for authentication prior to the install date of the machine, or may be authenticated on the casino floor as the software is being installed in the machine. In another method, authentication is conducted on a spot-check basis wherein a gaming agent periodically visits a casino and picks machines for the removal of software components for authentication.

[0005] Jurisdictional requirements require that storage media containing code or data be authenticated at power-up, continuously or at a periodic rate, or upon occurrence of predetermined events, such as the opening any doors or panels of the gaming device that allows access to internal circuitry. The storage media may be comprised of erasable programmable read-only memory devices (EPROMs), electrically erasable programmable read-only memory devices (EEPROMs), PROMs, CompactFlash storage cards, hard disk drives, CD drives, or substantially any non-volatile memory and in some cases volatile memory (e.g., NVRAM, specialty mask semiconductors, battery backed RAM, SRAM, DRAM, etc.). Storage media comprises a memory device and the data stored thereon. Authentication of storage media is controlled by the gaming device's central processing unit (CPU). However, authentication by the CPU may take more than several minutes due to increasing complexity of the gaming device's software and thus the storage size of the media.

[0006] For example, the majority of gaming machines currently require that a gaming program be authenticated every so often while a gaming machine is running. In some cases, gaming authorities require that a gaming program be authenticated about every ten minutes while the gaming machine is running. To determine the authenticity of a memory device's contents the CPU must read the memory device and perform various calculations and comparisons to determine if the memory device's contents are authentic. Reading many memory devices or large memory devices can use significant CPU time and therefore may negatively affect the responsiveness of the gaming program that a user interacts with. What is needed is a technique for authenticating memory devices associated with a gaming machine that does not affect the gaming program that the user interacts with.

SUMMARY OF THE INVENTION

[0007] Embodiments of the present invention authenticate a gaming machine program, software, firmware, or data (data) stored in memory devices within the gaming machine while the gaming machine is running and interacting with a user. The authentication process does not slow or interfere with the gaming program that interacts with the user. The authentication processes are ongoing and are substantially continuously repetitive. The authentication processes may substantially repeat every 2 minutes to 24 hours. Furthermore, in order to increase the speed of authenticating some of the data, graphics data may be differentiated from executable data so that the authenticity of the executable data can be determined more often than the graphics data.

[0008] It should be understood that for the purposes of this description of exemplary embodiments of the present invention that the gaming machine program may be either compiled or uncompiled. Furthermore the gaming machine program comprises code, files, instructions or programs that are executable in that they direct the gaming machine to do something (hereinafter "executable code"). The gaming machine program further comprises graphics code, files, data, instructions or programs (herein after "graphics data") that have to do with graphics or multimedia applications. Such graphics or multimedia may include, but are not limited to, data or information used to control graphics, animation, or other special effects that move air, move fluids, create smells, create bubbles, create flashing lights, control laser lights, control air pressure, control temperature, control mechanical devices, or control sound devices.

[0009] In an embodiment of the present invention a gaming machine comprises a user interface and a central processing unit (CPU) coupled to the user interface. The CPU comprises a processor. A first memory is coupled to the processor. The first memory is adapted to contain executable program code. The executable program code has both executable instructions and graphics data. A second memory is also coupled to the processor. The second memory stores data. The executable instructions found in the first memory include a plurality of instructions configured to cause the processor to determine the authenticity of the executable program code and the data. The processor, with the aid of the executable instructions, determines the authenticity of the executable program and the data on a substantially continuous, repetitious basis. Furthermore, the authenticity determination of the executable program code might be per-

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.