PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
A63F 5/04, 9/24

A1

(11) International Publication Number: **WO 99/65579**

(43) International Publication Date: 23 December 1999 (23.12.99)

(21) International Application Number: PCT/AU99/00486

(22) International Filing Date: 17 June 1999 (17.06.99)

(30) Priority Data:
60/089,654 17 June 1998 (17.06.98) US

(71) Applicant *(for all designated States except US)*: ARISTOCRAT LEISURE INDUSTRIES PTY. LTD. [AU/AU]; 71 Longueville Road, Lane Cove, NSW 2066 (AU).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: BOND, Eugene, Thomas [US/US]; 6329 Lena King Avenue, Las Vegas, NV 89120 (US).

(74) Agent: F.B. RICE & CO.; 605 Darling Street, Balmain, NSW 2041 (AU).

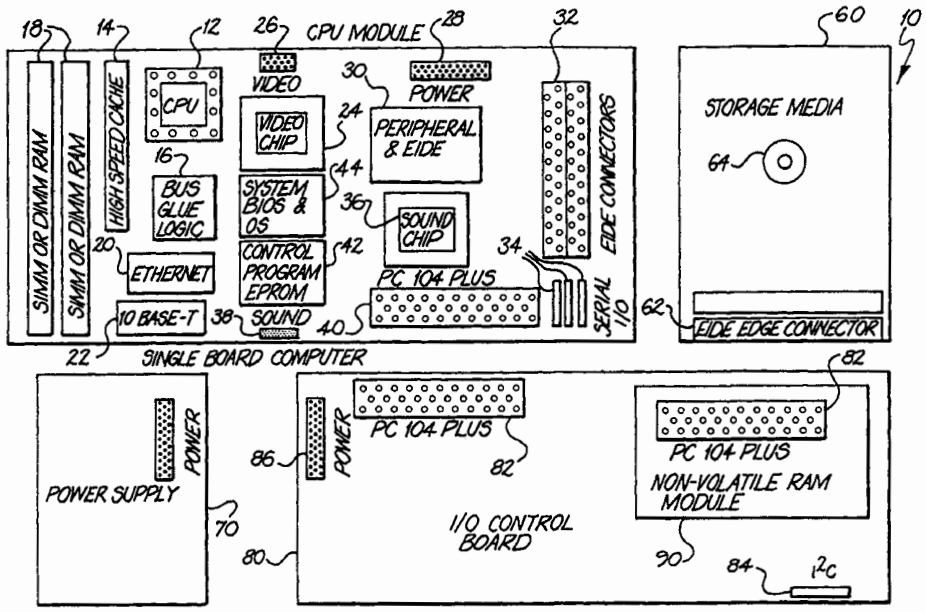
(81) Designated States: AU, JP, NZ, US, ZA, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: SOFTWARE VERIFICATION AND AUTHENTICATION

(57) Abstract

A device for controlling electronic gaming machines comprises a single board computer (SBC) having a microprocessor, memory means, storage means and a ROM (Read Only Memory). The ROM includes: a loader program; verification program; an authentication program; and a presentation program. Additional Mass storage media in communication with the SBC store pre–verified and approved gaming software (program files) and related data files, each of which have a verification signature appended to them. Prior to usage of the gaming software, the program file software or data file is retrieved by the loader program and checked by the verification program which compares the verification signature with a newly calculated verification signature. If the newly calculated signature matches the verification signature, the requested file is deemed to be intact (a validated image). The verification processes ensure that the file has been retrieved in its entirety and is free from corruption caused by storage media faults. If any corruption has occurred, the control device displays an error and the process is halted. After verification, all pending requests for authorization from authentication agents are processed by a queuing means. Each request includes a set of authentication instructions and a reply destination. After queuing, an authentication interpreter processes the validated image pursuant to the requester's instruction. The presentation program reports the resulting authentication identification to the requested destination which either acknowledges or refuses authentication. If acknowledged, the image is used or executed. If refused, an error is displayed and the process is halted.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SOFTWARE VERIFICATION AND AUTHENTICATION

Background of the Invention

This invention relates to ensuring the compliance, integrity and authenticity of microprocessor-based gaming devices utilized in regulated gaming jurisdictions. These devices are commonly referred to as slot machines or video poker machines; however, more recent implementations have combined both aspects and offer a variety of games on a single machine referred to as a multi-game machine. A commonly configured multi-game machine would include a plurality of games such as: keno, poker, slots, blackjack and others. These games can be played separately or be combined together to form new games, games within games, thus pushing the limits of gaming software and hardware capabilities. As the complexity of these gaming devices increases, the difficulty of ensuring regulatory compliance increases.

Typical gaming machines of this type utilize a combination of mechanical devices, electronics, microprocessors and complex software to generate the gaming experience. Some of the common hardware components include a cabinet, handle, jackpot tower, coin acceptor, bill acceptor, credit meters, back-lit glass, reels, monitors, game doors, buttons, payout hoppers, lights and speakers. The electronics include many of the following components: microprocessor, (also referred to as a central processing unit ("CPU")), read only memory (ROM), random access memory (RAM), high speed data bus, peripheral logic chips for serial and parallel ports and driver circuitry for lamps, speakers, video and other devices. Typical software components include: power-up initialization, device drivers, game recovery, state machines (to monitor whether the game is in a state of active play, "sleeping" between active play or off), random number generator, payout routine, credit management, graphics engine, sound, game engine, game data, security, accounting and reporting functions.

In jurisdictions where gaming is legal, use of such gaming devices is regulated by law. This invention is designed to aid in complying with two kinds of gaming regulations: those requiring automated verification of the device's integrity, and those requiring a method of determining the authenticity of the device.

As will be described below, verification and authentication are separate processes. Verification of the gaming software is usually performed

before and during game play. Verification is done initially to make certain that the program code or other data stored in the gaming device is intact and functioning properly by methods known to those skilled in the art. In the case of verification, the gaming device's software is usually required to be check-summed or cyclic redundancy checked (CRC). During program execution (i.e., the course of game play) the software images are periodically re-checked in order to ensure that the storage media in which the program code/data is stored has not become corrupted. This periodic verification is important because media corruption has been known to generate erroneous jackpots.

Occasionally, the software is authenticated, which is typically a process carried out by a third party (other than the manufacturer or the operator/casino) representing the gaming enforcement agency that has jurisdiction over the device. Its purpose is to ensure that the software controlling the game has not been tampered with, and software authentication is usually required after a large jackpot has been obtained by a player. Authentication also verifies that the gaming software was previously examined and approved by the gaming agency in whose jurisdiction the jackpot occurred.

In addition, the casino likes to verify that the software running the game is legitimate particularly if the machine is not earning the expected amount of revenue or in response to player complaints about the behavior of a particular game.

In prior art devices, authentication is usually accomplished by one of two methods. Both methods require the opening of the game, the removal of CPU and the removal of software, typically stored in EPROMS, (Electronically Programmable Read Only Memory) from the CPU. Then, in the first method, the removed EPROMS are compared with a custodial (or master) set of EPROMS which have been kept in a secure location. If the comparison indicates that they are the same, the software is considered to be authentic. The second method involves plugging each EPROM into an electronic authentication device which generates an authentication identification (id) for the image resident in the EPROM. The resulting authentication ids are compared to previously recorded ids for those EPROMS. If they are identical, the software is labeled authentic.

Existing authentication methods are well-suited to prior art devices

which use ROM type storage; and which typically are stand-alone gaming machines. However, with the advent of new storage technologies, increased storage requirements of modern operating systems, and multi-game multimedia gambling devices involving a plurality of gaming machines in communication with each other, the prior art methods are no longer sufficient.

And though Silicon Gaming has invented a method for "authenticating" software stored in other media, it ignores the existing authentication paradigm presently accepted in gaming. Thus, there is a need for a means of verifying and authenticating software stored in modern media that is compatible with existing gaming regulations and practices. It is also believed that such methods should take into account the practice of relating software and modular functionality to EPROMS like prior art systems. The industry is comfortable with having a set of EPROMS for "System" software and a set for each model (comprising unique pay schedule, symbols, and/or play rules), or a set for each game in a multi-game environment. It is further thought that remote authentication is desirable to said agencies. Lastly, it is thought that a method of authentication that does not require the removal of gaming software from the machine is desirable to the operator.

Summary of the Invention

It is an object of the present invention to provide a device for use within a gaming machine, such as a slot machine or a multi-game machine, which allows for continuous verification of gaming software stored in modern media in a manner consistent to that which occurs in EPROM based prior art systems.

Still another object of the present invention is to provide a device for use within a gaming machine, such as a slot machine or a multi-game machine, which allows for verification of data files.

Still another object of the present invention is to provide a method that can be used within a gaming machine, that will allow software authentication without requiring the removal of gaming software (program files) from within the gaming machine.

Still another object of the present invention is to provide a method that allows for authentication of the gaming software (program files) without requiring removal of the central processing unit from the gaming machine.

Still another object of the present invention is to provide a method

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.