(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 January 2004 (15.01.2004)

PCT

(10) International Publication Number
WO 2004/004855 A1

(51) International Patent Classification[7]: A63F 13/00

(21) International Application Number:
PCT/US2002/029927

(22) International Filing Date:
19 September 2002 (19.09.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/393,892 5 July 2002 (05.07.2002) US

(71) Applicant *(for all designated States except US)*: **CYBER-SCAN TECHNOLOGY, INC.** [US/US]; 550 Hamilton Avenue, Palo Alto, CA 94301 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **GATTO, Jean-Marie** [FR/GB]; 46 Parkside, 29-46 Knightsbridge, London SW1X 7JP (GB). **BRUNET DE COURSSOU, Thierry** [FR/GB]; 15A Ives Street, London SW3 2ND (GB). **BENEY, Pierre-Jean** [FR/GB]; 9 Queensbury Mews West, London SW7 2DU (GB).

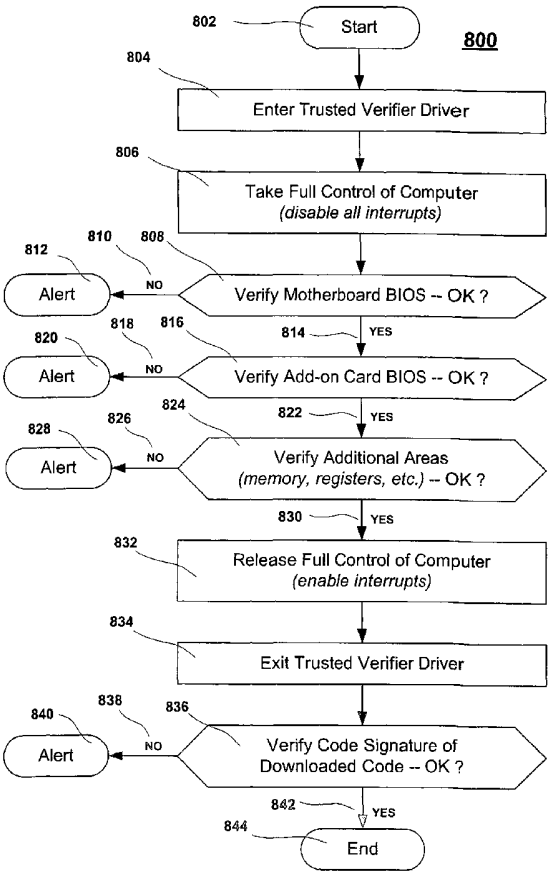
(74) Agent: **YOUNG, Alan, W.**; Young Law Firm, P.C., Suite 106, 4370 Alpine Road, Portola Valley, CA 94028 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),

[Continued on next page]

(54) Title: SECURE GAME DOWNLOAD



(57) Abstract: A method for gaming terminals, gaming kiosks and lottery terminals to ensure that the code-signing verification process of downloaded game software can be trusted. Drivers independently developed from the operating system supplier are embedded within the operating system kernel to verify that the micro-coded hardware components, the BIOS (808), the operating system components and the downloaded game software can be trusted.

WO 2004/004855 A1

Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SECURE GAME DOWNLOAD

FIELD OF THE INVENTION

This invention relates generally to the field of casino gaming terminals, gaming kiosks and lottery gaming terminals.

DESCRIPTION OF THE RELATED ART

On-line download of updated software and new games has been performed routinely with lottery terminals since the on-line capture of lottery slips started to be deployed in the late 1980s. The techniques and procedures have been refined along the years and are now considered as essential features. On the other hand, casino regulators have always been reluctant to introduce on-line download of updated software and of new games for casino gaming machines. Such reluctance stems from concerns relative to unauthorized intrusion and malicious modification of software code. These concerns are understandable, particularly since the late 1990s because of the general trend of constructing gaming terminals using standard PC hardware and PC software platforms that are subject to assault by hackers that are well versed in the techniques for taking advantage of the known weaknesses and flaws of such platforms. Even now with lotteries, the appeal of making use of the broadband public Internet network instead of private networking is considerable, but there are indeed significant security concerns and consequently new plans are blurred with uncertainty.

Although specialized download utilities and software update utilities such as Windows Installer, InstallShield and GetRight include data integrity verification mechanisms to ensure that the downloaded code is not corrupted, there is no mechanism to ensure that the code has not been tampered with. While secure Internet software download technologies such as Authenticode employ powerful PKI (Public Key Infrastructure) code signing, there is no fail-proof mechanism to ensure that the code has not been tampered with at a later stage. Once an authorized properly signed software module has started execution, the operating system does not provide means to verify if the code loaded in memory has not been tampered with to execute fraudulent operations.

Although software corporations like Microsoft have lately shifted their development focus to making their software more stable and very secure, there is always

the risk that an unknown bug or a back door exists somewhere amongst the millions lines of code that would allow someone to perpetrate some form of cheat. Hidden back-doors might be mandated by the United States' NSA (National Security Agency) to be incorporated in operating systems to enable them to monitor terrorism and drug trafficking. Consequently, some corrupt employees or ex-employees having inner knowledge of these back door accesses might be tempted to fraudulently exploit such inner knowledge. Microsoft operating systems and other modern operating systems such as Linux are too complex and constantly changing to consider comprehensive certification by labs traditionally trusted by game regulators for certifying gaming products made by gaming equipment vendors.

Moreover, using strong PKI code signing techniques does not guaranty that the code can be trusted once verified because the "verifying" tool, or the tool that verifies the verifying tool (and so on…) may itself not be trusted.

The approach of the Trusted Computing Platform Alliance (TCPA), whose specification was finalized in January 2001, calls for the creation of a Trusted Platform Module (TPM) that requires a discrete cryptographic processor residing on the PC's motherboard that contains a unique digital signature. Microsoft's security initiative code named "Palladium", on the other hand, uses new forthcoming hardware security features built directly into microprocessors and supporting chipsets being designed by Intel, AMD and National in order to run some form of low-level encryption, and it can also use a TPM-like module for additional encryption. Microprocessors and supporting chipsets that implement Palladium may support a trusted execution mode that allows cryptographically authenticated programs access to a separate memory area. Such microprocessors may be equipped with a security coprocessor, which stores a unique pair of cryptographic keys in a non-volatile memory. Such a microprocessor and coprocessor may then be combined to create a motherboard that implements Palladium functionality. A corresponding software component, called the Trusted Operating Root, works in conjunction with the microprocessor and its coprocessor. The Trusted Operating Root running on the microprocessor and the coprocessor are configured to encrypt data in such a way that no other combination of Trusted Operating Root and coprocessor would be able to decrypt it.

The above security technologies are indeed promising but they require specific hardware that may take several years to be proven and to justify using them in gaming

terminals. Furthermore, there may always persist a lingering distrust of such large corporate software providers such as, for example, Microsoft. Consequently, game regulators tend to hold back the deployment of such technologies, thereby discouraging the early adoption of networked multimedia software technologies as applied to the heavily regulated gaming industry.

SUMMARY OF THE INVENTION

There is no better alternative for casinos and lotteries gaming computer hardware but to adopt standard PC hardware controlled by the latest generation multimedia software from Microsoft, QNX, WindRiver Systems, Unix or from the Linux community. It is, therefore, an object of this invention to provide additional security mechanisms that can perform independent and trusted verification of the Commercial-Off-The-Shelf (COTS) software installed on the gaming terminals that can be trusted because of its precisely defined objectives and the availability of source code for peer review and certification by gaming certification labs.

Gaming terminals, gaming kiosks and lottery terminals are hereafter collectively referenced as gaming machines, for ease of reference.

The most promising approach available today in a COTS multimedia product that offers comprehensive security for preventing unauthorized code from executing, is integrated in Microsoft Windows XP, Windows 2000 and Windows .NET. There are three technologies that address three different layers; namely, (1) Driver Signing, (2) Windows File Protection and (3) Software Restriction Policies. These three technologies cover all but two aspects of possible execution by unauthorized modified software code, that is, (1) by modification of the motherboard BIOS or other add-on boards such as a graphic card with on-board BIOS or a SCSI controller with dedicated on-board BIOS, (2) by modification of an emulated CPU such as downloadable microcode for the Transmeta microprocessor that emulates Intel CPU instructions. The risk with the emulated CPU instructions can be simply avoided by not allowing the use of such emulating microprocessors. It is, therefore, another object of this invention to provide a trusted mechanism to verify that the motherboard BIOS and add-on BIOS are not unauthorized. It is a further object of this invention to provide a trusted mechanism to verify memory content, hardware register content and any form of data storage media. Verification, according to embodiments of the present invention, relies on a hash

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.