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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 September 2006 (28.09.2006)

PCT

(10) International Publication Number
WO 2006/101549 A3

(51) International Patent Classification:
G06F 7/04 (2006.01)

(21) International Application Number:
PCT/US2005/044535

(22) International Filing Date:
5 December 2005 (05.12.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/633,272 3 December 2004 (03.12.2004) US

(71) Applicant *(for all designated States except US)*: **WHITECELL SOFTWARE, INC.** [US/US]; 120 Palmer Drive, Fort Collins, Colorado 80525 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **FANTON, Andrew F.** [US/US]; 14695 Pecos Street, Westminster, Colorado 80020 (US). **GANDEE, John J.** [US/US]; 8500 Coyote Run, Loveland, Colorado 80537 (US). **LUTTON, William H.** [US/US]; 705 Parkview Drive, Fort Collins, Colorado 80525 (US). **HARPER, Edwin L.** [US/US]; 120 Palmer Drive, Fort Collins, Colorado 80525 (US). **GODWIN, Kurt E.** [US/US]; 2833 Logan Drive, Loveland, Colorado 80538 (US). **ROZGA, Anthony A.** [US/US]; 7702 Kit Fox Drive, Wellington, Colorado 80549 (US).

(74) Agent: **DESANCTIS, Michael A.**; Faegre & Benson, LLP, Customer No. 35657, 3200 Wells Fargo Center, 1700 Lincoln Street, Denver, Colorado 80203-4532 (US).

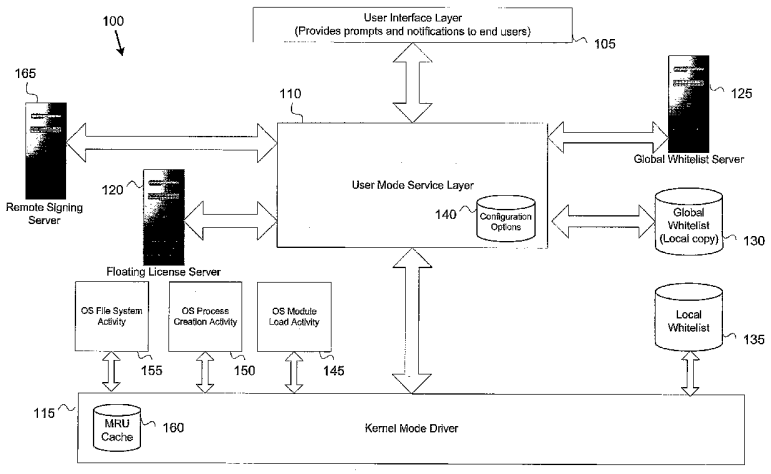
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC,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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) **Title:** SECURE SYSTEM FOR ALLOWING THE EXECUTION OF AUTHORIZED COMPUTER PROGRAM CODE



(57) **Abstract:** Systems and methods are described for allowing the execution of authorized computer program code and for protecting computer systems and networks from unauthorized code execution. In one embodiment, a multi-level proactive whitelist approach is employed to secure a computer system by allowing only the execution of authorized computer program code thereby protecting the computer system against the execution of malicious code such as viruses, Trojan horses, spy-ware, and/or the like. Various embodiments use a kernel-level driver, which intercepts or "hooks" certain system Application Programming Interface (API) calls in order to monitor the creation of processes prior to code execution. The kernel-level driver may also intercept and monitor the loading of code modules by running processes, and the passing of non-executable code modules, such as script files, to approved or running code modules via command line options, for example. Once intercepted, a multi-level whitelist approach may be used to authorize the code execution.

WO 2006/101549 A3

(88) Date of publication of the international search report:
28 December 2006

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.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US05/44535

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **G06F 7/04**(2006.01)

USPC: 726/27
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 726/27

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2002/0099952 A1 (LAMBERT et al) 25 Jul. 2002 (25.07.2002) paragraphs [0010], [0034], [0038],[0044], [0052], [0053], [0055]-[0057], [0062], [0066], [0067], [0071], [0072], [0078], [0080], [0082], [0083], FIGURE 8	1-3, 7-8, 10, 19, 23-27, 29, 38-39, 41, 43-47 --- 4, 9, 11-18, 20-22, 28, 30-37
Y	US 2003/0172167 A1 (JUDGE et al) 11 Sept. 2003 (11.09.2003), paragraph [0208]	4, 9, 11-18, 20-22, 28, 30-37
Y	US 2004/0205167 A1 (GRUMANN) 14 Oct. 2004 (14.10.2004) paragraph [0016]	9, 28
X	US 2003/0135756 A1 (VERMA) 17 June 2003 (17.06.2003) paragraphs [0093]-[0096], FIG. 8	40
P	US 2005/0262558 A1 (USOV) 24 Nov. 2005 (24.11.2005), paragraphs [0040]-[0054]	1-47

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 September 2006 (08.09.2006)	02 OCT 2006
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Emmanuel Moise Telephone No. (571)272-2100

Form PCT ISA/210 (second sheet) (April 2005)