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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 June 2004 (17.06.2004)

PCT

(10) International Publication Number
WO 2004/051441 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number:
PCT/GB2003/005219

(22) International Filing Date:
28 November 2003 (28.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/313,732 5 December 2002 (05.12.2002) US

(71) Applicant: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, NY 10504 (US).

(71) Applicant *(for MG only)*: **IBM UNITED KINGDOM LIMITED** [GB/GB]; PO Box 41, North Harbour, Portsmouth, Hampshire PO6 3AU (GB).

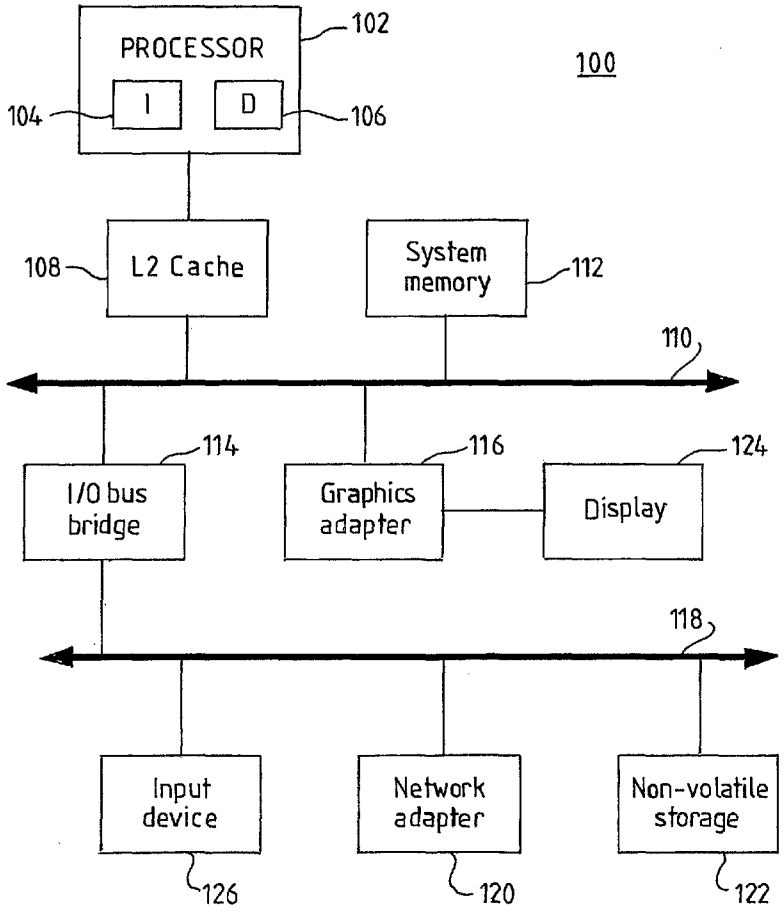
(72) Inventors: **BAFFES, Paul, Thomas**; 8708 Honeysuckle Trail, Austin, TX 78759 (US). **GILFIX, Michael**; 5700 Tapadera Trace Lane, Apartment #221, Austin, TX 78727 (US). **GARRISON, John, Michael**; 4420 Secluded Hollow, Austin, TX 78727 (US). **HSU, Allan**; 2522 Tedbury Court, Centerville, OH 45459 (US). **STADING, Tyron, Jerrod**; 13401 Metric Boulevard, Apartment #135, Austin, TX 78727 (US).

(74) Agent: **WILLIAMS, Julian, David**; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester, Hampshire SO21 2JN (GB).

(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, EG, 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, NI, NO, NZ, OM, PG, PH, PL, PT,

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR RESPONDING TO A COMPUTER INTRUSION



(57) Abstract: A method and system for managing an intrusion on a computer by graphically representing an intrusion pattern of a known past intrusion, and then comparing the intrusion pattern of the known intrusion with a current intrusion. The intrusion pattern may either be based on intrusion events, which are the effects of the intrusion or activities that provide a signature of the type of intrusion, or the intrusion pattern may be based on hardware topology that is affected by the intrusion. The intrusion pattern is graphically displayed with scripted responses, which in a preferred embodiment are presented in pop-up windows associated with each node in the intrusion pattern. Alternatively, the response to the intrusion may be automatic, based on a pre-determined percentage of common features in the intrusion pattern of the known past intrusion and the current intrusion.

WO 2004/051441 A2

RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), 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, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that 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.