PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 29/06 — A1

(11) International Publication Number: WO 99/16225

(43) International Publication Date: 1 April 1999 (01.04.99)

(21) International Application Number: PCT/IL98/00082

(22) International Filing Date: 23 February 1998 (23.02.98)

(30) Priority Data:
121815 22 September 1997 (22.09.97) IL

(71) Applicant *(for all designated States except US)*: SECURITY-7 (SOFTWARE) LTD. [IL/IL]; P.O. Box 107, 20692 Yoqneam (IL).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: ELGRESSY, Doron [IL/IL]; Kish Street 31, 33531 Haifa (IL). JOSPE, Asher [IL/IL]; Nurit Street 39, 42670 Natanya (IL).

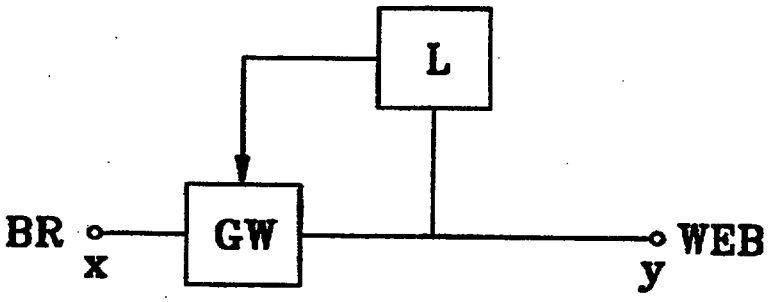
(74) Agents: LUZZATTO, Kfir et al.; Luzzatto & Luzzatto, P.O. Box 5352, 84152 Beer-Sheva (IL).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: METHOD AND SYSTEM FOR THE IDENTIFICATION AND THE SUPPRESSION OF EXECUTABLE OBJECTS

(57) Abstract



A method for processing Executable Objects, comprising: (a) providing analysis means capable of non-interfering analysis of data packets transmitted on a communication line between a browser and an HTTP server on the web, said communication line being established through a gateway; (b) analyzing the handshake between said browser and said server, to detect a "GET_" command sent by the user and an HTTP code sent in response by said server; (c) when such an HTTP code is detected, analyzing the data packets transmitted by said server to said browser, by: (c.1) providing ordering means to order data packets received in non-sequential order, and to forward them in sequential order to header checking means; (c.2) checking the data packets so as to analyze the contents of the header of the Executable Object, and to identify the resources of the system that it needs to employ; (c.3) transmitting to said gateway data representing the resources of the system that the Executable Object needs to utilize; (c.4) providing data packet suppressing means coupled to said gateway, such that if the resources of the system that the Executable Object needs to utilize are not permitted according to the security policy set by the administrator, at least one data packet belonging to the Executable Object is suppressed, altered or damaged, so as to prevent the execution thereof by the browser.