

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
27 December 2007 (27.12.2007)

PCT

(10) International Publication Number
WO 2007/149612 A2

(51) International Patent Classification:
G06F 12/14 (2006.01)

(21) International Application Number:
PCT/US2007/064949

(22) International Filing Date: 26 March 2007 (26.03.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/785,723 24 March 2006 (24.03.2006) US

(71) Applicant: **EXPLOIT PREVENTION LABS, INC.**
[US/US]; PO Box 755, New Kingstown, PA 17072 (US).

(72) Inventors: **THOMPSON, Roger, John**; 1650 Emerald Ridge, Marietta, GA 30062 (US). **MOSHER, Gregory, Andrew**; 4157 Kindewood Court, Roswell, GA 30075 (US).

(74) Agents: **ROSANDER, Wesley, C.** et al.; Workman Nydegger, 1000 Eagle Gate Tower, 60 East South Temple, Salt Lake City, UT 84111 (US).

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, 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, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, MT, 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:
— *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.

(54) Title: SOFTWARE VULNERABILITY EXPLOITATION SHIELD

(57) Abstract: This paper describes a mechanism for minimizing the exploitation of vulnerabilities on software installed on a computing system. At a transport layer (e.g., transmission communication protocol (TCP) sockets layer), network traffic is monitored using a security component installed on a target computer. When a message destined for the computing system is received, data included in the message is compared with exploit evidence used to identify malicious code. The exploit evidence is provided to the security component by security service that gathers information about the malicious code. Based on the comparison of data in the message with the exploit evidence, rules are identified that instruct the security component to take an appropriate action on the message received.



WO 2007/149612 A2