

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
25 October 2007 (25.10.2007)

PCT

(10) International Publication Number
WO 2007/121361 A3

(51) International Patent Classification:
G08B 23/00 (2006.01)

(21) International Application Number:
PCT/US2007/066645

(22) International Filing Date: 13 April 2007 (13.04.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/279,979 17 April 2006 (17.04.2006) US

(71) Applicant (*for all designated States except US*): **WIN-NOW TECHNOLOGIES, INC.** [US/US]; Three City Place Drive, Suite 770, St. Louis, MO 63141 (US).

(72) Inventors; and

(75) Inventors/Applicants (*for US only*): **LEE, Hojae** [KR/US]; 16350 Valley Oaks Estates Court, Chesterfield, MO 63005 (US). **HARIJONO, Indra Gunawan** [ID/US]; 10504 Copperfield Drive, St. Louis, MO 63123 (US). **NOONEY, Prudhvi Nadh** [IN/US]; 801A Patty Drive, Maryville, IL 62062 (US). **YOON, Uooyeol** [KR/US]; 7719 Ravensridge, St. Louis, MO 63119 (US).

(74) Agents: **KERCHER, Kevin, M.** et al.; Thompson Coburn LLP, One US Bank Plaza, St. Louis, MO 63101 (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, 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).

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

- *with international search report*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
17 April 2008

(54) Title: MALICIOUS ATTACK DETECTION SYSTEM AND AN ASSOCIATED METHOD OF USE

(57) Abstract: A malicious attack detection system and associated method of use is disclosed. This includes receiving and parsing a header frame of a data packet into header information and internet protocol ("IP" or "TCP/IP") addresses, checking the header information for a potential malicious attack condition and if present then a constraint filter result is generated, comparing the internet protocol ("IP") addresses to determine if an internet protocol ("IP") address had been previously received, determining the number of constraint filter results to determine if an incremented count is above a predetermined threshold during a predetermined threshold time period, and dropping at least one data packet based on a determination. Preferably, but not necessarily, the process is carried out at wire-speed meaning when a new data packet arrives, all processing above is complete with regard to the previous data packet.



WO 2007/121361 A3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US07/66645

A. CLASSIFICATION OF SUBJECT MATTER IPC: G08B 23/00(2006.01) USPC: 726/22,23,24,25 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. : 726/22, 23, 24, 25 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, TEXT, NPL, US-PGPUB, USPAT, EPO, JPO, DERWENT		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
☐ 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	“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	
“E” earlier application or patent published on or after the international filing date	“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	
“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)	“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	
“O” document referring to an oral disclosure, use, exhibition or other means	“&” document member of the same patent family	
“P” document published prior to the international filing date but later than the priority date claimed		
Date of the actual completion of the international search 04 February 2008 (04.02.2008)	Date of mailing of the international search report 19 FEB 2008	
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 <i>T. B. Truong</i> T. B. Truong Telephone No. 571-272-3858	