

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
31 July 2008 (31.07.2008)

PCT

(10) International Publication Number
WO 2008/092167 A3

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

(21) International Application Number:
PCT/US2008/052230

(22) International Filing Date: 28 January 2008 (28.01.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/897,783 26 January 2007 (26.01.2007) US

(71) Applicant (for all designated States except US): **INGRIAN NETWORKS, INC.** [US/US]; 350 Convention Way, Second Floor, Redwood City, California 94063 (US).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **MURRAY, Eric** [US/US]; 20638 Black Road, Los Gatos, California 95033 (US).

(74) Agents: **AHMANN, William, F.** et al; Perkins Coie LLP, P.O. Box 2168, Menlo Park, California 94026 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

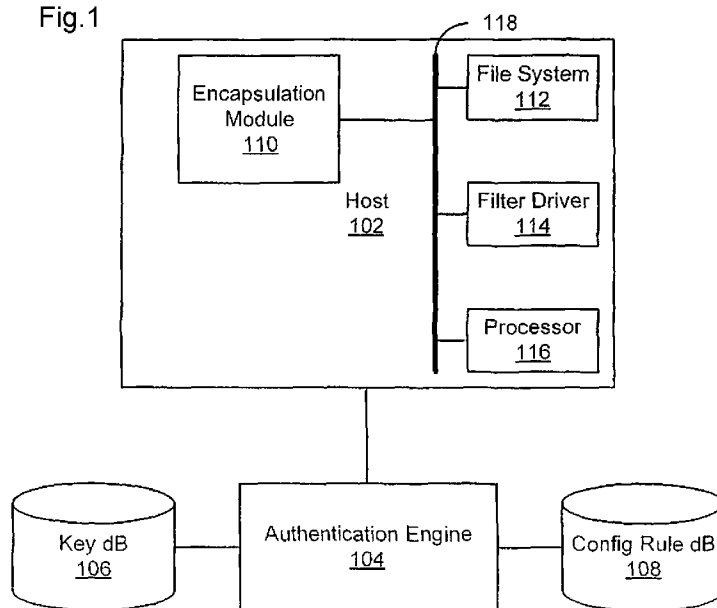
Published:

- with international search report
- 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:
18 September 2008

(54) Title: PROTECTING SECRETS IN AN UNTRUSTED RECIPIENT

Fig.1



(57) Abstract: A technique for protecting secrets may involve enclosing master secret keys in an encapsulation module functioning like an envelope on a host that may run an untrusted operating system. The encapsulation module itself can be obfuscated and protected with various software security techniques, such as anti-debugging techniques, which make reverse-engineering more difficult. Session or file keys could then be derived from the master key stored in the encapsulation module on the host, wherein each of the keys protects a session or a file on the host. Additionally, a code can be provided to prevent the master secret and the keys from being swapped to a non-volatile storage device of the host.

WO 2008/092167 A3

INTERNATIONAL SEARCH REPORT

International application No

PCT/US 08/52230

A CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F 7/04 (2008.04)

USPC - 726/26

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)

IPC(8) G06F 7/04 (2008 04)

USPC 726/26

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
726/1-4, 713/167-171

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

USPTO WEST (PGPB, USPT, EPAB, JPAB), Google

Search Terms Used protect, host, encapsulS, secureS, obfuscateS Modules, unsecurS, untrust\$, unprotectS, volatile, master, key, database, encrypts

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 2005/0010788 A1 (CRAFT) 13 January 2005 (13 01 2005), entire document, especially para [001 1]-[0012], [0032]-[0038], [0043]-[0048] and Figs 2, 3, 5, 9	1-9, 14-18, 20, 23 ----- 10-13, 19, 21-22
Y	US 2004/0039924 A1 (BALDWIN et al) 26 February 2004 (26 02 2004), entire document, especially para [0082], [0091], [0151], [0417], [0422]	10-13, 19, 21-22
A	US 2005/0251680 A1 (BROWN et al) 10 November 2005 (10 11 2005)	1-23

☐ Further documents are listed in the continuation of Box C☐

* Special categories of cited documents	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search

27 June 2008 (27 06 2008)

Date of mailing of the international search report

14 JUL 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 571-273-320 1

Authorized officer

Lee W Young

PCT Helpdesk 571 272-4300
PCT OSP 571-272-7774