

(19) World Intellectual Property Organization
International Bureau



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

PCT

(10) International Publication Number
WO 2008/092166 A3

(51) International Patent Classification:
H04L 9/00 (2006 01)

[US/US], 20638 Black Road, Los Gatos, California 95033 (US)

(21) International Application Number:
PCT/US2008/052227

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

(22) International Filing Date: 28 January 2008 (28 01 2008)

(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

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/897,577 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)

(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,

(72) Inventor; and

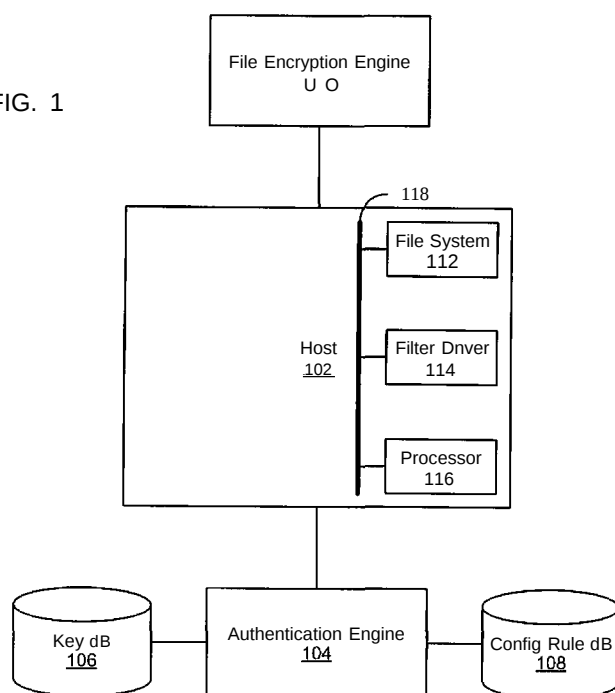
(75) Inventor/Applicant (for US only): **MURRAY, Eric**

[Continued on next page]

(54) Title: FILE ENCRYPTION WHILE MAINTAINING FILE SIZE

100 →

FIG. 1



(57) Abstract: A technique for encrypting a file without changing file size may involve encrypting a first set of a plurality of blocks of a file in a first encryption mode using the first set of encryption keys and/or the first set of configuration rules, and a second set of the plurality of blocks of the file in a second encryption mode using a second set of the encryption keys and/or a second set of the configuration rules without causing the file to increase in size before and after the encryption. Here, the first and the second encryption modes are chosen to be different, so are the first and the second sets of the encryption keys and/or the configuration rules to reduce security risk of the file being encrypted.

WO 2008/092166 A3



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).

— *before the expiration of the time limit for amending the
claims and to be republished in the event of receipt of
amendments*

Published:

— *with international search report*

(88) Date of publication of the international search report:

18 September 2008

INTERNATIONAL SEARCH REPORT

International application No
PCT/US 08/52227

A CLASSIFICATION OF SUBJECT MATTER

IPC(8) - H04L 9/00 (2008 04)

USPC - 713/193

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)
USPC 713/193

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC 713/189.193 | 380/28,37

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

USPTO WEST (PGPUB.USPAT.USOCR.EPABJPAB), GOOGLE Scholars, File system, file, rules, instructions, parameter, encrypting, blocks, metadata, cipher, chain, configuration, storage, key, host

C DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No
Y	US 2006/0232826 A 1 (BAR-EL) 19 October 2006 (19 10 2006) entire document (especially para [0035],[0038],[0049]-[0057],[0061])	1-24
Y	US 2004/0091 114 A 1 (CARTER et al) 13 May 2004 (13 05 2004) (para [0200],[021 3]-[0214],[0269])	1-24
A	US 2003/0108196 A 1 (KIRICHENKO) 12 June 2003 (12 06 2003) entire document	1-24
A	US 2005/0108240 A 1 (BOLOSKY et al) 19 May 2005 (19 07 2005) entire document	1-24

☐ Further documents are listed in the continuation of Box C

* Special categories of cited documents

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search

01 July 2008 (01 07 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 571-273-3201

Authorized officer

Lee W Young

PCT Helpdesk 571-272-4300

PCT OSP 571-272-7774