

(51) International Patent Classification:  
*H04L 29/06* (2006.01)

US]; 800 Bulfinch Drive, Apt.204, Andover, MA 01810 (US).

(21) International Application Number:  
PCT/US2011/030742(74) Agent: **PICCOLOMINI, Zachary, P.**; Proskauer Rose, LLP, One International Place, Boston, MA 02110 (US).(22) International Filing Date:  
31 March 2011 (31.03.2011)

(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, CL, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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:  
12/770,473 29 April 2010 (29.04.2010) US  
12/770,476 29 April 2010 (29.04.2010) US(71) Applicant (for all designated States except US): **SONUS NETWORKS, INC.** [US/US]; 4 Technology Park Drive, Westford, MA 01886-3141 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **BHARRAT, Shaun, Jaikarran** [US/US]; 6 Ashby Ct., Manalapan, NJ 07726 (US). **JOACHIMPILLAI, Damascene, M.** [CA/US]; 3 Fieldstone Drive, Westford, MA 01886 (US). **KURIAKOSE, Aby** [US/US]; 31 Silverbrooke Circle, Howell, NJ 07731 (US). **LU, Vivian** [US/US]; 182 Concord Road, Westford, MA 01886 (US). **YU, Xiang** [CN/

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: LOOSELY-COUPLED ENCRYPTION FUNCTIONALITY FOR OPERATING SYSTEMS

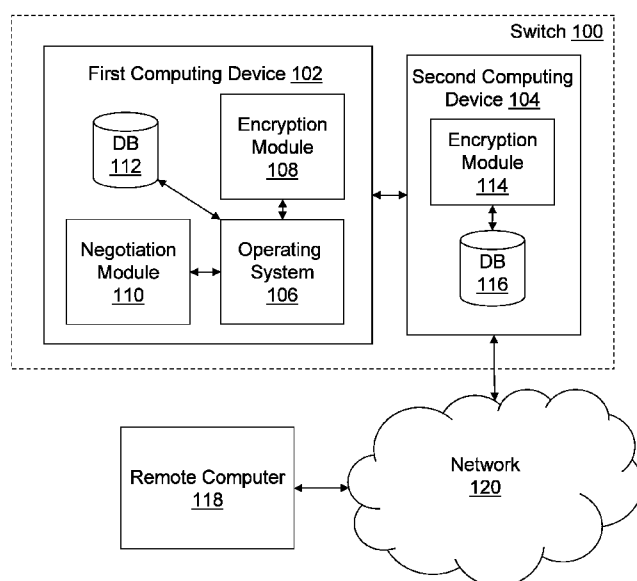


FIG. 1

(57) Abstract: Described are computer-based methods and apparatuses, including computer program products, for loosely-coupled encryption functionality for operating systems. A data packet is processed through one or more internet protocol stack layers to generate a processed data packet. Encryption information is determined that includes parameters for encrypting and decrypting data packets transmitted between the first computing device and the remote computer. A message comprising data indicative of the encryption information is transmitted to a second computing device, wherein an operating system being executed is unaware of a security nature of the transmission. A bypass encryption routine is executed to generate a unencrypted data packet, wherein the bypass encryption routine does not encrypt the processed data packet. The unencrypted data packet is transmitted to the second computing device. The unencrypted data packet is encrypted based on the message transmitted from the first computing device to generate an encrypted data packet.

vice to generate an encrypted data packet.

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

5 January 2012

- *with international search report (Art. 21(3))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 11/30742

## A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - H04L 29/06 (2011.01)

USPC - 713/152

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: 713/152

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
USPC: 713/150; 713/164 (keyword limited - see search terms below)

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

PubWEST (PGPB, USPT, USOC, EPAB, JPAB); GOOGLE; Google Scholar

Terms: encryption, decryption, module, processors, operating, system, loosely, coupled, bypass, negotiate, security, transmit, internet, protocol, socket, layer, ipsec, linux.

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2010/0071055 A1 (Kaniz et al.) 18 March 2010 (18.03.2010), entire document, especially abstract, para [0007], [0008], [0010], [0052], [0069], [0140], [0142], [0143], [0146], [0148], [0149].	1-40
Y	US 2005/0273850 A1 (Freund) 08 December 2005 (08.12.2005), entire document, especially abstract, para [0015], [0017], [0020], [0023], [0048], [0082], [0105].	1-40
A	US 2008/0137848 A1 (Kocher et al.) 12 June 2008 (12.06.2008), entire document, especially abstract, para [0002], [0005], [0020], [0050], [0077], [0088], [0129], [0194].	1-40

☐ 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

"&amp;" document member of the same patent family

Date of the actual completion of the international search

24 October 2011 (24.10.2011)

Date of mailing of the international search report

08 NOV 2011

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