(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 July 2005 (28.07.2005)

PCT

(10) International Publication Number
WO 2005/067685 A3

(51) International Patent Classification:
H04L 9/00 (2006.01) *G06F 15/16* (2006.01)

(21) International Application Number:
PCT/US2005/000812

(22) International Filing Date: 10 January 2005 (10.01.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/756,634 12 January 2004 (12.01.2004) US

(71) Applicant *(for all designated States except US)*: **CISCO TECHNOLOGY, INC.** [US/US]; 170 W. Tasman Drive, San Jose, California 95134-1706 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CAM-WINGER, Nancy** [US/US]; 325 Martens Ave., Mountain View, California 94040 (US). **ZHOU, Hao** [CN/US]; 7381 Cheshire Place, Solon, Ohio 44139 (US). **JAKKAHALLI, Padmanabha C.** [IN/US]; 173 Debussy Terrace, Sunnyvale, California 94087 (US). **SALOWEY, Joseph** [US/US]; 106 N 77th Street, Seattle, Washington 98013 (US). **MCGREW, David A.** [US/US]; 14 Hackett Court, Poolesville, Maryland 20837 (US).

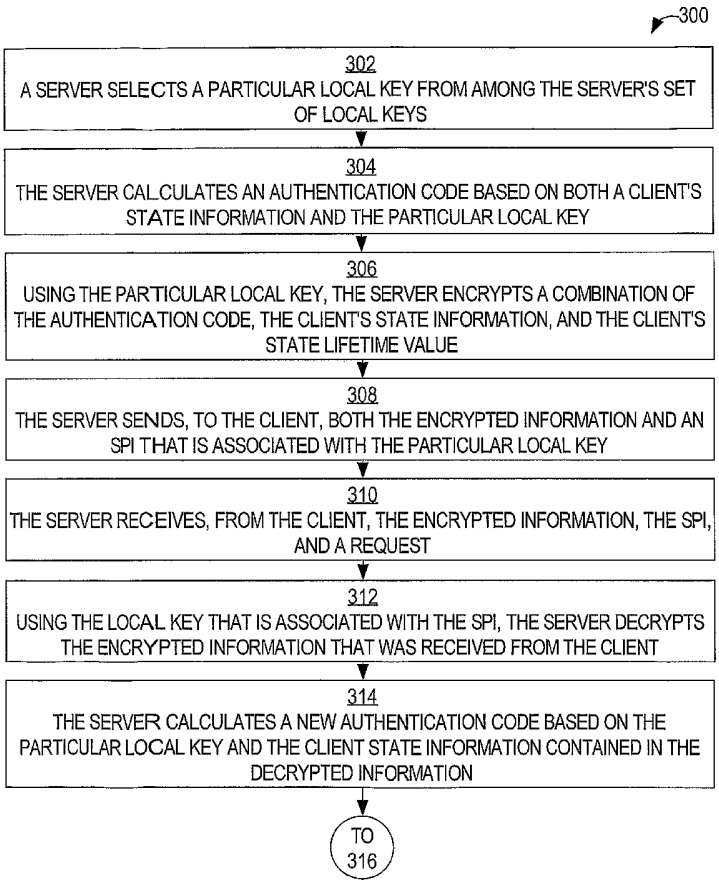
(74) Agents: **NICHOLES, Christian, A.** et al.; HICKMAN PALERMO TRUONG & BECKER LLP, 2055 Gateway Place, Suite 550, San Jose, California 95110-1089 (US).

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

[Continued on next page]

(54) Title: ENABLING STATELESS SERVER-BASED PRE-SHARED SECRETS



(57) Abstract: A method is disclosed for enabling stateless server-based pre-shared secrets. Based on a local key that is not known to a client, a server encrypts the client's state information. The client's state information may include, for example, the client's authentication credentials, the client's authorization characteristics, and a shared secret key that the client uses to derive session keys. By any of a variety of mechanisms, the encrypted client state information is provided to the client. The server may free memory that stored the client's state information. When the server needs the client's state information, the client sends, to the server, the encrypted state information that the client stored. The server decrypts the client state information using the local key. Because each client stores that client's own state information in encrypted form, the server does not need to store any client's state information permanently.

WO 2005/067685 A3

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, MC, 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:

— *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:
27 July 2006

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.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US05/00812

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04L 9/00**(2006.01)
G06F 15/16(2006.01)

USPC: 709/203,226,227,229;713/150,155,168;726/5,10,12,13
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. : 709/203,226,227,229; 713/150,155,168; 726/5, 10, 12, 13

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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6134592 A (MONTULLI) 17 October 2000 (17.10.2000), Abstract; column 2 - column 4.	1-29
A	US 5,961,601 A (IYENGAR) 05 October 1999 (05.10.1999), Abstract; column 9 - column 10, line 32.	1-29
A	US 6,496,932 B1 (TRIEGER) 17 December 2002 (17.12.2002), Abstract; column 3 - column 5, line 15.	1-29

☐ 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

"E" earlier application or patent 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	Date of mailing of the international search report
12 May 2006 (12.05.2006)	14 JUN 2006
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 for Gilberto Barron, Jr. James R. Matthews Telephone No. 571-272-3799

Form PCT/ISA/210 (second sheet) (April 2005)