

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
7 June 2001 (07.06.2001)

PCT

(10) International Publication Number  
WO 01/41039 A3

(51) International Patent Classification<sup>7</sup>: G06F 1/00, H04L 29/06, G06F 17/60

(74) Agent: VIKSNINS, Ann, S.; Schwegman, Lundberg, Woessner & Kluth, P.O. Box 2938, Minneapolis, MN 55402 (US).

(21) International Application Number: PCT/US00/32774

(22) International Filing Date: 1 December 2000 (01.12.2000)

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, 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, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
60/168,656 2 December 1999 (02.12.1999) US  
09/483,164 14 January 2000 (14.01.2000) US

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

(71) Applicant: SECURE COMPUTING CORPORATION [US/US]; 2675 Long Lake Road, Roseville, MN 55113 (US).

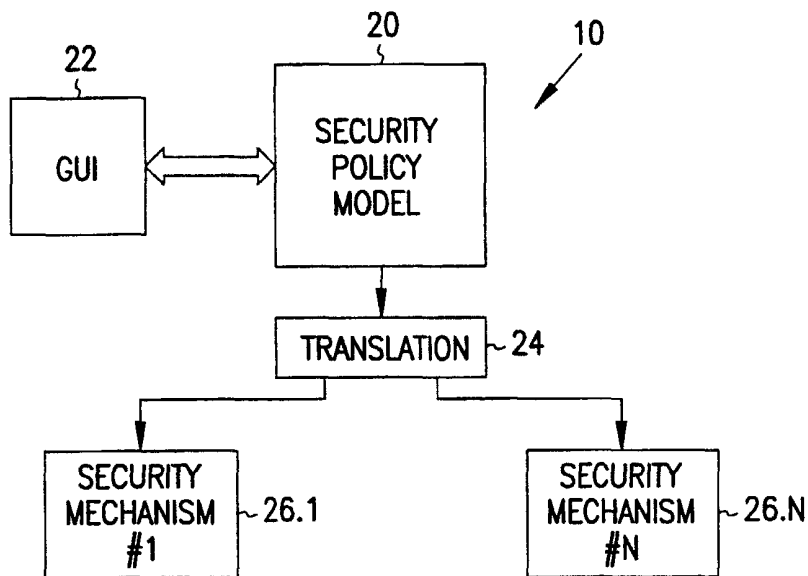
(72) Inventors: THOMSEN, Daniel, Jay; 3565 Cleveland Street N.E., Minneapolis, MN 55418 (US). O'BRIEN, Richard; 9709 Oliver Avenue North, Brooklyn Park, MN 55444 (US). BOGLE, Jessica; 1703 Elm Street, White Bear Lake, MN 55110 (US). PAYNE, Charles; 7135 47th Street Court North, Oakdale, MN 55128 (US).

Published:  
— with international search report

(88) Date of publication of the international search report:  
14 February 2002

[Continued on next page]

(54) Title: SECURITY MANAGEMENT SYSTEM IN AN HETEROGENOUS NETWORK ENVIRONMENT



(57) Abstract: A system and method for defining and enforcing a security policy. Security mechanism application specific information for each security mechanism is encapsulated as a key and exported to a semantic layer. Keys are combined to form key chains within the semantic layer. The key chains are in turn encapsulated as keys and passed to another semantic layer. A security policy is defined by forming key chains from keys and associating users with the key chains. The security policy is translated and exported to the security mechanisms. The security policy is then enforced via the security mechanisms.



WO 01/41039 A3



---

*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/US 00/32774

**A. CLASSIFICATION OF SUBJECT MATTER**  
 IPC 7 G06F1/00 H04L29/06 G06F17/60

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 7 G06F H04L

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 practical, search terms used)  
 EPO-Internal, WPI Data, PAJ, INSPEC

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	THOMSEN D, O'BRIEN R AND PAYNE C: "Napoleon - Network Application Policy Environment" PROCEEDINGS OF THE 4TH ACM WORKSHOP ON ROLE-BASED ACCESS CONTROL, 28 - 29 October 1999, pages 145-152, XP002163998 the whole document ---	1-35
A	VARADHARAJAN V ET AL: "ISSUES IN THE DESIGN OF SECURE AUTHORIZATION SERVICE FOR DISTRIBUTED APPLICATIONS" SYDNEY, NOV. 8 - 12, 1998, NEW YORK, NY: IEEE,US, 1998, pages 874-879, XP000825877 ISBN: 0-7803-4985-7 the whole document --- -/--	1-3,6, 11,14, 22,31

Further documents are listed in the continuation of box C.

Patent family members are listed in 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 document 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  <b>14 August 2001</b>	Date of mailing of the international search report  <b>23 08 2001</b>
----------------------------------------------------------------------------------------	-----------------------------------------------------------------------------

Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer  <b>Sigolo, A</b>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------

## INTERNATIONAL SEARCH REPORT

Inte. onal Application No

PCT/US 00/32774

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>CHANG ET AL: "A Visual language for authorization modeling"            PROCEEDINGS IEEE SYMPOSIUM ON VISUAL LANGUAGES, XX, XX,            23 September 1997 (1997-09-23), pages 110-118, XP002142414            page 110, column 1, line 1 -column 2, line 14</p> <p style="text-align: center;">---</p>	5
A	<p>US 5 826 239 A (EDDY GRAHAM ET AL)            20 October 1998 (1998-10-20)            column 6, line 17 -column 10, line 55</p> <p style="text-align: center;">---</p>	36-38
A	<p>EP 0 854 431 A (IBM)            22 July 1998 (1998-07-22)            column 10, line 12 -column 12, line 27</p> <p style="text-align: center;">-----</p>	36-38

# INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US 00/32774

## Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1.  Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
  
2.  Claims Nos.:  
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
  
3.  Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1.  As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.
2.  As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3.  As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:
  
4.  No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

### Remark on Protest

- The additional search fees were accompanied by the applicant's protest.
- No protest accompanied the payment of additional search fees.

**FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210**

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-35

Method of specifying and enforcing a security policy within a system having one or more security mechanisms

2. Claims: 36-38

Method of controlling workflow in a system having a central policy management system

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 00/32774

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5826239	A	20-10-1998	NONE	
EP 0854431	A	22-07-1998	US 6065009 A	16-05-2000