

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been
filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.);

DOCKET NO. 2:22-cv-00322	DATE FILED 8/19/2022	U.S. DISTRICT COURT Eastern District of Texas
PLAINTIFF LIONRA TECHNOLOGIES LIMITED		DEFENDANT FORTINET, INC.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 7,302,708	11/27/2007	Lionra Technologies Limited
2 7,685,436	3/23/2010	Lionra Technologies Limited
3 7,921,323	4/5/2011	Lionra Technologies Limited
4 8,566,612	10/22/2013	Lionra Technologies Limited
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Print

Save As...

Reset

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been
filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.);

DOCKET NO. 2:22-cv-305	DATE FILED 8/8/2022	U.S. DISTRICT COURT Eastern District of Texas
PLAINTIFF LIONRA TECHNOLOGIES LIMITED		DEFENDANT CISCO SYSTEMS, INC.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 7,916,630	3/29/2011	Lionra Technologies Limited
2 8,566,612	10/22/2013	Lionra Technologies Limited
3 7,921,323	4/5/2011	Lionra Technologies Limited
4 7,302,708	11/27/2007	Lionra Technologies Limited
5 7,685,436	3/23/2010	Lionra Technologies Limited

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Print

Save As...

Reset



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/798,074	11/27/2007	7302708	7162-0110	5321

68085 7590 11/07/2007
HARRIS CORPORATION
C/O DARBY & DARBY PC
P.O. BOX 770
CHURCH STREET STATION
NEW YORK, NY 10008-0770

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 707 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Vincent Joseph Kovarik JR., Grant, FL;

Electronic Patent Application Fee Transmittal				
Application Number:		10798074		
Filing Date:		11-Mar-2004		
Title of Invention:		ENFORCING COMPUTER SECURITY UTILIZING AN ADAPTIVE LATTICE MECHANISM		
First Named Inventor/Applicant Name:		Vincent Joseph Kovarik		
Filer:		Robert Joseph Sacco/Joyce Dougherty		
Attorney Docket Number:		7162-0110		
Filed as Large Entity				
Utility Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	1501	1	1440	1440
Publication fee for republication	1505	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Printed copy of patent - no color	8001	2	3	6
Total in USD (\$)				1746

Electronic Acknowledgement Receipt

EFS ID:	2309108
Application Number:	10798074
International Application Number:	
Confirmation Number:	5321
Title of Invention:	ENFORCING COMPUTER SECURITY UTILIZING AN ADAPTIVE LATTICE MECHANISM
First Named Inventor/Applicant Name:	Vincent Joseph Kovarik
Customer Number:	68085
Filer:	Robert Joseph Sacco/Joyce Dougherty
Filer Authorized By:	Robert Joseph Sacco
Attorney Docket Number:	7162-0110
Receipt Date:	11-OCT-2007
Filing Date:	11-MAR-2004
Time Stamp:	16:48:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	\$ 1746
RAM confirmation Number	1822
Deposit Account	080870
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 and 1.17	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	01277263.pdf	480875	no	1
			91215bdb777c6a24d065a5ea0190992a903c48d5		
Warnings:					
Information:					
2	Fee Worksheet (PTO-06)	fee-info.pdf	8474	no	2
			e67c79fefa2dd17461627109a64ae15826a27a2		
Warnings:					
Information:					
Total Files Size (in bytes):			489349		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
 or **Fax (571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

39207 7590 08/29/2007

SACCO & ASSOCIATES, PA
 P.O. BOX 30999
 PALM BEACH GARDENS, FL 33420-0999

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/798,074	03/11/2004	Vincent Joseph Kovarik JR.	7162-0110	5321

TITLE OF INVENTION: ENFORCING COMPUTER SECURITY UTILIZING AN ADAPTIVE LATTICE MECHANISM

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1400	\$300	\$0	\$1700	11/29/2007

EXAMINER	ART UNIT	CLASS-SUBCLASS
SHAIFER HARRIMAN, DANT B	2134	726-026000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list
 (1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
 (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1. DARBY & DARBY
 2. ROBERT J. SACCO
 3. _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

HARRIS CORPORATION

MELBOURNE, FL

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☒ Issue Fee
☒ Publication Fee (No small entity discount permitted)
☒ Advance Order - # of Copies 2

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 08-0870 (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____

Date 10-11-07

Typed or printed name Robert J. Sacco

Registration No. 35,667

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	FILE WRAPPER LOCATION
10/798,074		2134	21M1

Correspondence Address / Fee Address Change

The following fields have been set to Customer Number 68085 on 10/03/2007

- Correspondence Address

The address of record for Customer Number 68085 is:

HARRIS CORPORATION
C/O DARBY & DARBY PC
P.O. BOX 770
CHURCH STREET STATION
NEW YORK, NY 10008-0770



Approved for use through 07/31/2006. OMB 0851-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known

Application Number	10/798,074
Filing Date	March 11, 2004
First-Named Inventor	KOVARIK, JR.
Art Unit	2109
Examiner Name	Dant B. Shaifer-Harriman
Attorney Docket Number	7162-0110

Sheet	1	of	2
-------	---	----	---

U. S. PATENT DOCUMENTS

[illegible]

FOREIGN PATENT DOCUMENTS

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	1 ^o
		Country Code ² Number ⁴ Kind Code ³ (if known)	MM-DD-YYYY			
/DS/		WO 03/088018	10/23/2003	RAYTHEON CO.		

Examiner Signature	/Dant Shaifer Harriman/	Date Considered	4/4/07
-----------------------	-------------------------	--------------------	--------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. *Applicant's unique citation designation number (optional). *See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 801.04. *Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). *For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. *Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. *Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

39207 7590 08/29/2007

SACCO & ASSOCIATES, PA
P.O. BOX 30999
PALM BEACH GARDENS, FL 33420-0999

EXAMINER

SHAIFER HARRIMAN, DANT B

ART UNIT

PAPER NUMBER

2134

DATE MAILED: 08/29/2007

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/798,074	03/11/2004	Vincent Joseph Kovarik JR.	7162-0110	5321

TITLE OF INVENTION: ENFORCING COMPUTER SECURITY UTILIZING AN ADAPTIVE LATTICE MECHANISM

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1400	\$300	\$0	\$1700	11/29/2007

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. **PROSECUTION ON THE MERITS IS CLOSED.** THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. **THIS STATUTORY PERIOD CANNOT BE EXTENDED.** SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

- A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.
- B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

- A. Pay TOTAL FEE(S) DUE shown above, or
- B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450**
or Fax **(571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

39207 7590 08/29/2007

SACCO & ASSOCIATES, PA
P.O. BOX 30999
PALM BEACH GARDENS, FL 33420-0999

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/798,074	03/11/2004	Vincent Joseph Kovarik JR.	7162-0110	5321

TITLE OF INVENTION: ENFORCING COMPUTER SECURITY UTILIZING AN ADAPTIVE LATTICE MECHANISM

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1400	\$300	\$0	\$1700	11/29/2007

EXAMINER	ART UNIT	CLASS-SUBCLASS
SHAIFER HARRIMAN, DANT B	2134	726-026000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
- (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☐ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/798,074	03/11/2004	Vincent Joseph Kovarik JR.	7162-0110	5321

39207	7590	08/29/2007
-------	------	------------

SACCO & ASSOCIATES, PA
P.O. BOX 30999
PALM BEACH GARDENS, FL 33420-0999

EXAMINER	
SHAIFER HARRIMAN, DANT B	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 08/29/2007

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 707 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 707 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

6

Notice of Allowability	Application No.	Applicant(s)	
	10/798,074	KOVARIK, VINCENT JOSEPH	
	Examiner	Art Unit	
	Dant B. Shaifer - Harriman	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--
 All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 07/12/2007.
2. ☒ The allowed claim(s) is/are 1 & 3-11 & 19, renumbered as claims 1-17.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

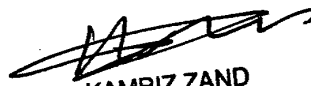
Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|---|--|
| <ol style="list-style-type: none"> 1. ☒ Notice of References Cited (PTO-892) 2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948) 3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____ 4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material | <ol style="list-style-type: none"> 5. ☐ Notice of Informal Patent Application 6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____ 7. ☐ Examiner's Amendment/Comment 8. ☒ Examiner's Statement of Reasons for Allowance 9. ☐ Other _____ |
|---|--|


KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

DETAILED ACTION

Response to Amendment

- 1. Claims: 2 & 12 are cancelled.***
- 2. Claims: 1 & 3-11 & 13 – 19 are pending respectively.***

Allowable Subject Matter

- 3. Claims: 1 & 3-11 & 13 – 19 are allowable, and the rejections made on 1 & 3-11 & 13 – 19 claims are withdrawn.***

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dant B. Shaifer - Harriman whose telephone number is 571-272-7910. The examiner can normally be reached on Monday - Thursday: 8:00am - 5:30pm Alt. Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

D.S.H.


KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

Notice of References Cited	Application/Control No. 10/798,074	Applicant(s)/Patent Under Reexamination KOVARIK, VINCENT JOSEPH	
	Examiner Dant B. Shaifer - Harriman	Art Unit 2134	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,970,246	10-1999	Moughani et al.	717/128
*	B	US-5,887,065	03-1999	Audebert, Yves	713/172
*	C	US-2004/0193891	09-2004	Ollila, Juha	713/182
*	D	US-2005/0229000	10-2005	Shoji et al.	713/182
*	E	US-2004/0123159	06-2004	Kerstens et al.	713/202
*	F	US-2004/0107345	06-2004	Brandt et al.	713/171
*	G	US-2004/0044655	03-2004	Cotner et al.	707/003
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

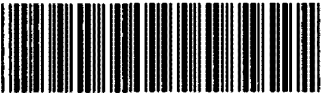
FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims 	Application/Control No. 10798074	Applicant(s)/Patent Under Reexamination KOVARIK, VINCENT JOSEPH
	Examiner Shaifer - Harriman , Dant B	Art Unit 2134

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant			☐ CPA			☐ T.D.			☐ R.1.47		
CLAIM		DATE									
Final	Original	08/15/2007									
1	1	=									
	2	-									
2	3	=									
3	4	=									
4	5	=									
5	6	=									
6	7	=									
7	8	=									
8	9	=									
9	10	=									
10	11	=									
	12	-									
11	13	=									
12	14	=									
13	15	=									
14	16	=									
15	17	=									
16	18	=									
17	19	=									

Search Notes 	Application/Control No. 10798074	Applicant(s)/Patent Under Reexamination KOVARIK, VINCENT JOSEPH
	Examiner Shaifer - Harriman , Dant B	Art Unit 2109

SEARCHED			
Class	Subclass	Date	Examiner
709	229	4/9/2007	dsh
713	201	4/5/2007	dsh
713	166	4/5/2007	dsh
726	23	4/9/2007	dsh
709	219	4/9/2007	dsh

SEARCH NOTES			
Search Notes		Date	Examiner
East Search (see attached) <i>, NPL search, EIC NPL search</i>		4/5/2007- 4/9/2007	dsh
Inventor Search, reveiwed related applications (see attached)		4/3/2007	dsh
Consolted with Mr. Matt Heneghan, AU=2134		4/9/2007	dsh

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
713	201	08/16/2007	dsh
713	166	08/16/2007	dsh
709	229	08/16/2007	dsh
709	219	08/16/2007	dsh
726	23	08/16/2007	dsh
713		08/16/2007	dsh
726		08/16/2007	dsh
380		08/16/2007	dsh

Please Scan
[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) | [Purchase History](#) | [Cart](#)

Welcome United States Patent and Trademark Office

[View Selected Items](#)[BROWSE](#)[SEARCH](#)[IEEE XPLORE GUIDE](#)

Results for "(((cascade or cascaded or order or ordered or sequence)and (access or entry) and (security or secu... "



Your search matched 12 of 1632036 documents. You selected 12 items.

 Display Format: ☐ Citation ☒ Citation & Abstract

Article Information

View: 1-12 | [View](#)

» Download Citations

Citation & Abstract

ASCII Text

» [Learn more](#)

» Key

IEEE JNL IEEE Journal or Magazine

IEE JNL IEE Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IEE CNF IEE Conference Proceeding

IEEE STD IEEE Standard

1. A temporal access control mechanism for database systems

Bertino, E.; Bettini, C.; Ferrari, E.; Samarati, P.

[Knowledge and Data Engineering, IEEE Transactions on](#)

Volume: 8 Issue: 1 Feb 1996

Page(s): 67-80

Digital Object Identifier 10.1109/69.485637

Summary: The paper presents a discretionary access control model in which authorization is automatically revoked when the associated interval expires. The proposed model provides rules for the.....

[AbstractPlus](#) | [References](#) | Full Text: [PDF](#) [IEEE JNL](#)

2. A logic for state transformations in authorization policies

Yun Bai; Varadharajan, V.

[Computer Security Foundations Workshop, 1997. Proceedings., 10th](#)

10-12 Jun 1997

Page(s): 173-182

Digital Object Identifier 10.1109/CSFW.1997.596810

Summary: In a multi-user information-sharing system, an authorization policy provides and control access to system, applications and information. In the real world, an authorization temporal properties. That is, it needs to be

[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)

3. Biometric identification through speaker verification over telephone lines

Gonzalez-Rodriguez, J.; Gruz-Llanas, S.; Ortega-Garcia, J.

[Security Technology, 1999. Proceedings. IEEE 33rd Annual 1999 International Carnat on](#)
1999

Page(s): 238-242

Digital Object Identifier 10.1109/CCST.1999.797919

Summary: In this paper, the identity of a remote user is verified through his voice by a telephone in order to gain access to a specific system or service. We have used state-independent speaker modeling algorithms, likelihood

[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)

4. A fast automaton-based method for detecting anomalous program behaviors

Sekar, R.; Bendre, M.; Dhurjati, D.; Bollineni, P.

[Security and Privacy, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on](#)
2001

Page(s): 144-155

Digital Object Identifier 10.1109/SECPRI.2001.924295

Summary: Anomaly detection on system call sequences has become perhaps the most approach for detecting novel intrusions. A natural way for learning sequences is to use automaton (FSA). However previous research indicates that FSA-learning.....

[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)

5. **Performance analysis on new biometric gait motion model**
 ChewYean Yam; Nixon, M.S.; Carter, J.N.
Image Analysis and Interpretation, 2002. Proceedings. Fifth IEEE Southwest Symposium
 2002
 Page(s): 31-34
 Digital Object Identifier 10.1109/IAI.2002.999884
Summary: Recognising people by the way they walk and/or run is new. A novel analysis is invariant to human gait of walking and running is developed based on the concept of coupled oscillators and the biomechanics of human walking and.....
[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)
6. **Design validation of ZCSP with SPIN**
 Beaudenon, V.; Encrenaz, E.; Desbarbieux, J.-L.
Application of Concurrency to System Design, 2003. Proceedings. Third International
 18-20 June 2003
 Page(s): 102- 110
 Digital Object Identifier 10.1109/CSD.2003.1207704
Summary: We consider the problem of specifying a model of the zero copy secured purpose of LTL verification with the SPIN model checker. ZCSP is based on direct memory access. Data is directly read/written in user space memory, decreasing latency.....
[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)
7. **sTuples: semantic tuple spaces**
 Khushraj, D.; Lassila, O.; Finin, T.
Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004 Annual International Conference on
 22-26 Aug. 2004
 Page(s): 268- 277
 Digital Object Identifier 10.1109/MOBIC.2004.1331733
Summary: Tuple spaces offer a coordination infrastructure for communication between entities by providing a logically shared memory along with data persistence, transaction support as well as temporal and spatial decoupling - properties that make them suitable for mobile and ubiquitous computing.....
[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)
8. **A first step towards formal verification of security policy properties for RBAC**
 Drouineaud, M.; Bortin, M.; Torrini, P.; Sohr, K.
Quality Software, 2004. QSIC 2004. Proceedings. Fourth International Conference on
 8-9 Sept. 2004
 Page(s): 60- 67
 Digital Object Identifier 10.1109/QSIC.2004.1357945
Summary: Considering the current expansion of IT-infrastructure, the security of the infrastructure becomes increasingly important. Therefore, assuring certain security properties of systems by formal methods is desirable. So far in security research.....
[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)
9. **Analysis and Modeling of Advanced PIM Architecture Design Tradeoffs**
 Upchurch, E.; Sterling, T.; Brockman, J.
Supercomputing, 2004. Proceedings of the ACM/IEEE SC2004 Conference
 06-12 Nov. 2004
 Page(s): 12- 12
 Digital Object Identifier 10.1109/SC.2004.11
Summary: A major trend in high performance computer architecture over the last two decades is the migration of memory in the form of high speed caches onto the microprocessor semiconductor. Where temporal locality in the computation is high, caches prove to be effective.....
[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)
10. **Token based path authorization at interconnection points between hybrid network and lambda grid**
 Gommans, L.; de Laat, C.; Meijer, R.
Broadband Networks, 2005 2nd International Conference on

3-7 Oct. 2005

Page(s): 1378- 1385 Vol. 2

Digital Object Identifier 10.1109/ICBN.2005.1589768

Summary: In order to provide cost effective transport services for highly demanding applications, National Research Networks (NRNs) are considering additional types of network infrastructures. Next to traditional IP access.....

[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)

11. A Scalable and Intrusion-tolerant Digital Time-stamping System

Tulone, D.

[Communications, 2006. ICC '06. IEEE International Conference on](#)

Volume: 5 June 2006

Page(s): 2357-2363

Digital Object Identifier 10.1109/ICC.2006.255122

Summary: Secure digital time-stamps play a crucial role in many applications that require correctness of time-sensitive information. Well-known time-stamping systems are based on linking schemes which provide a relative temporal order by linking requests.....

[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)

12. Ubiquitous Semantic Space: A context-aware and coordination middleware for Ubiquitous Computing

Sudha, R.; Rajagopalan, M.R.; Selvanayagi, M.; Selvi, S.Thamarai

[Communication Systems Software and Middleware, 2007. COMSWARE 2007. 2nd International Conference on](#)

7-12 Jan. 2007

Page(s): 1-7

Digital Object Identifier 10.1109/COMSWA.2007.382562

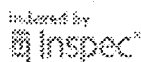
Summary: Ubiquitous Computing poses the challenge of increased communication, coordination, and functionality. In a highly dynamic and widely connected ubiquitous environment, coordination to the network (synchronous communication) is very difficult.....

[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)

[View: 1-12](#) | [View Search Results](#)

[Help](#) [Contact Us](#) [Privacy & Cookies](#)

© Copyright 2006 IEEE - All Rights Reserved




[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) | [Purchase History](#) | [Cart](#)

Welcome United States Patent and Trademark Office

View Selected Items

BROWSE

SEARCH

IEEE XPLORE GUIDE

Results for "(((sequence or order or ordered or cascade or cascaded) and (access or entry) and (secure or securit... "



Your search matched 733 of 1632036 documents. You selected 25 items.

Display Format: ☐ Citation ☒ Citation & Abstract

Article Information

View: 1-25 | [View](#)

» Download Citations

Citation & Abstract

ASCII Text

» Learn more

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

1. An n-grid model for group authorization

Wen-Gong Shieh; Weems, B.; Kavi, K.M.

Computer Security Applications Conference, 1990., Proceedings of the Sixth Annual 3-7 Dec 1990

Page(s): 384-392

Digital Object Identifier 10.1109/CSAC.1990.143813

Summary: The n-grid model for group authorization and access control extends the N representation of two-dimensional partial orders and incorporates the implicit authorize model. The n-grid is a representation of multi-dimensional partial

[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)

2. A temporal access control mechanism for database systems

Bertino, E.; Bettini, C.; Ferrari, E.; Samarati, P.

Knowledge and Data Engineering, IEEE Transactions on

Volume: 8 Issue: 1 Feb 1996

Page(s): 67-80

Digital Object Identifier 10.1109/69.485637

Summary: The paper presents a discretionary access control model in which authorize temporal intervals of validity. An authorization is automatically revoked when the associated interval expires. The proposed model provides rules for the

[AbstractPlus](#) | [References](#) | Full Text: [PDF](#) [IEEE JNL](#)

3. Reducing manpower intensive tasks through automation of security technologies

Carback, R.T.

Security Technology, 1995. Proceedings. Institute of Electrical and Electronics Engineers, 1995 International Carnahan Conference on

18-20 Oct 1995

Page(s): 331-339

Digital Object Identifier 10.1109/CCST.1995.524932

Summary: Security in today's government and commercial environments is changing. To provide manpower against security threats is diminishing. Risk management is preferred avoidance. In order for management to ensure that the appropriate

[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)

Multiple intelligent agent supported Internet security system: issues, current solutions, and proposed approach

Lin Zeng; Huaqing Wang; Lee, M.K.O.

Intelligent Processing Systems, 1997. ICIPS '97. 1997 IEEE International Conference

Volume: 1 28-31 Oct 1997

Page(s): 920-922 vol.1

Digital Object Identifier 10.1109/ICIPS.1997.672965

Summary: The Internet has become a common target to attack because of security concerns. Incidents, such as attempted and successful intrusions, have grown dramatically. Studies have shown that many individuals and companies are abstaining

[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)

Search string:

(cascade or cascaded or sequence or order or ordered) and

(access or entry) and

(security or secure or authorize or authorization)

5. **Specifying application-level security in workflow systems**
 Olivier, M.S.; van de Riet, R.P.; Gudes, E.
Database and Expert Systems Applications, 1998. Proceedings. Ninth International W
 25-28 Aug 1998
 Page(s): 346-351
 Digital Object Identifier 10.1109/DEXA.1998.707423
Summary: A workflow process involves the execution of a set of related activities over a specific task. Security requires that such activities may only be performed by authorized order to enforce such requirements, access to the u.....
[AbstractPlus](#) | Full Text: [PDF](#) IEEE CNF
6. **A contextual role-based access control authorization model for electronic patient**
 Motta, G.H.M.B.; Furuie, S.S.
Information Technology in Biomedicine, IEEE Transactions on
 Volume: 7 Issue: 3 Sept. 2003
 Page(s): 202- 207
 Digital Object Identifier 10.1109/TITB.2003.816562
Summary: The design of proper models for authorization and access control for electronic record (EPR) is essential to a wide scale use of EPR in large health organizations. In this paper, we propose a contextual role-based access control authorization model.....
[AbstractPlus](#) | [References](#) | Full Text: [PDF](#) IEEE JNL
7. **Human computer interaction through consolidation and visualization for order entry**
 Toyoda, S.; Niki, N.; Nishitani, H.
Engineering in Medicine and Biology Society, 2003. Proceedings of the 25th Annual International Conference of the IEEE
 Volume: 2 17-21 Sept. 2003
 Page(s): 1280- 1283 Vol.2
 Digital Object Identifier 10.1109/IEMBS.2003.1279500
Summary: In this paper, we propose a human computer interaction model through consolidation and visualization for order entry systems. This model makes effective use of the patient data features 1) the consolidation of order data, 2) the visualization.....
[AbstractPlus](#) | Full Text: [PDF](#) IEEE CNF
8. **Secure access to corporate resources in a multi-access perspective: needs, problems and solutions**
 Casole, M.; Yi Cheng
Personal Mobile Communications Conference, 2003. 5th European (Conf. Publ. No. 4)
 22-25 April 2003
 Page(s): 482- 489
Summary: The modern businessman needs to access corporate resources constantly and from any location, thus improving effectiveness. In order to accomplish this, a number of technologies allow mobile users to be connected to some kind of network.....
[AbstractPlus](#) | Full Text: [PDF](#) IEEE CNF
9. **A first step towards formal verification of security policy properties for RBAC**
 Drouineaud, M.; Bortin, M.; Torrini, P.; Sohr, K.
Quality Software, 2004. QSIC 2004. Proceedings. Fourth International Conference on
 8-9 Sept. 2004
 Page(s): 60- 67
 Digital Object Identifier 10.1109/QSIC.2004.1357945
Summary: Considering the current expansion of IT-infrastructure, the security of the infrastructure becomes increasingly important. Therefore, assuring certain security properties of systems by formal methods is desirable. So far in security.....
[AbstractPlus](#) | Full Text: [PDF](#) IEEE CNF
10. **Database security - concepts, approaches, and challenges**
 Bertino, E.; Sandhu, R.
Dependable and Secure Computing, IEEE Transactions on
 Volume: 2 Issue: 1 Jan.-March 2005

Page(s): 2- 19

Digital Object Identifier 10.1109/TDSC.2005.9

Summary: As organizations increase their reliance on, possibly distributed, information technology in their daily business, they become more vulnerable to security breaches even as they gain efficiency advantages. Though a number of techniques, such....

[AbstractPlus](#) | Full Text: [PDF](#) [IEEE JNL](#)

11. Security service adaptation for embedded service systems in changing environments

Illner, S.; Pohl, A.; Krumm, H.

Industrial Informatics, 2004. INDIN '04. 2004 2nd IEEE International Conference on
24-26 June 2004

Page(s): 457- 462

Digital Object Identifier 10.1109/INDIN.2004.1417387

Summary: Distributed embedded applications increasingly operate in changing environments. The application security depends on the type and properties of the currently used communication services and employed devices. While vulnerabilities, threats, and

[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)

12. Random-access control mechanisms using adaptive traffic load in ALOHA and CSMA for EDGE

Rivero-Angeles, M.E.; Lara-Rodriguez, D.; Cruz-Perez, F.A.

Vehicular Technology, IEEE Transactions on

Volume: 54 Issue: 3 May 2005

Page(s): 1160- 1186

Digital Object Identifier 10.1109/TVT.2005.844657

Summary: In this paper, three random access control mechanisms based on the well known ALOHA, NP-CSMA, and 1P-CSMA protocols are presented. The basic idea is to limit the number of transmissions and retransmissions at high traffic loads in order to maintain a high throughput....

[AbstractPlus](#) | [References](#) | Full Text: [PDF](#) [IEEE JNL](#)

13. New authentication method for mobile centric communications

Hongyuan Chen; Sivakumar, T.V.L.N.

Vehicular Technology Conference, 2005. VTC 2005-Spring. 2005 IEEE 61st

Volume: 5 30 May-1 June 2005

Page(s): 2780- 2784 Vol. 5

Digital Object Identifier 10.1109/VETECS.2005.1543853

Summary: This paper proposes a new authentication scheme for accessing contents of applications in both mobile device and Internet. A user first divide all the contents, send applications in both mobile device and the Internet into four groups....

[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)

14. Job-centric security model for open collaborative environment

Demchenko, Y.; de Laat, C.; Gommans, L.; Oudenaarde, B.; Tokmakoff, A.; Snijders, J.

Collaborative Technologies and Systems, 2005. Proceedings of the 2005 International

15-20 May 2005

Page(s): 69- 77

Digital Object Identifier 10.1109/ISCST.2005.1553296

Summary: This paper describes the design and development of a flexible, customer-centric infrastructure for open collaborative environments. The experiences were gained within the collaboratory.nl project. The work is based on extensive research....

[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)

15.

Exploiting Hierarchical Identity-Based Encryption for Access Control to Pervasive Information

Hengartner, U.; Steenkiste, P.

Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm International Conference on

05-09 Sept. 2005

Page(s): 384- 396

Digital Object Identifier 10.1109/SECURECOMM.2005.18

Summary: Access control to confidential information in pervasive computing environment is challenging for multiple reasons: First, a client requesting access might not know which are necessary in order to be granted access to the requested information.....

[AbstractPlus](#) | Full Text: [PDF](#) IEEE CNF

16. A Multi-dimension Rule Update in a TCAM-based High-Performance Network Set

Hae-Jin Jeong; Il-Seop Song; Taeck-Geun Kwon; Yoo-Kyoung Lee

Advanced Information Networking and Applications, 2006. AINA 2006. 20th International Conference on
Volume: 2 18-20 April 2006

Page(s): 62- 66

Digital Object Identifier 10.1109/AINA.2006.37

Summary: Network security systems such as firewall and intrusion prevention system use packet classification rule to allow or protect the network traffic. In addition, they are for multi-gigabit speed in order to deploy the current Internet.....

[AbstractPlus](#) | Full Text: [PDF](#) IEEE CNF

17. Frameworks for Secured Business Process Management Systems

Haeng-Kon Kim; Roger Y. Lee; Hae-Sool Yang

Software Engineering Research, Management and Applications, 2006. Fourth International Conference on
09-11 Aug. 2006

Page(s): 57- 65

Digital Object Identifier 10.1109/SERA.2006.38

Summary: This paper formally defines a role-driven security and access control model and process in order eventually to provide a theoretical basis for realizing the secured business process management systems. That is, we propose a graphical representation.....

[AbstractPlus](#) | Full Text: [PDF](#) IEEE CNF

18. Design of security state machine of access control for control object based on II

Bin Duan; Bing Liu

Power Engineering Society General Meeting, 2006. IEEE
18-22 June 2006

Page(s): 3 pp.-

Digital Object Identifier 10.1109/PES.2006.1709328

Summary: Access control with identity authentication becomes crucial for critical circuit operation in the substation automation system. According to IEC 61850, the implementation of control policy depends on a virtual access view. But the state.....

[AbstractPlus](#) | Full Text: [PDF](#) IEEE CNF

19. Security Constraints in Access Control of Information System Using UML Language

Ane ta Poniszewska-Maranda

Enabling Technologies: Infrastructure for Collaborative Enterprises, 2006. WETICE '06. International Workshops on
June 2006

Page(s): 332-337

Digital Object Identifier 10.1109/WETICE.2006.58

Summary: Process of security administration in an information system is a complex task. Constraints should be expressed in order to define in the proper way the security policy. Constraints can be classified into two groups. The first.....

[AbstractPlus](#) | Full Text: [PDF](#) IEEE CNF

20. Quantifiable Security Metrics for Large Scale Heterogeneous Systems

Syed Naqvi; Michel Riguidel

Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International Conference on
Oct. 2006

Page(s): 209-215

Digital Object Identifier 10.1109/CCST.2006.313452

Summary: The exponential growth of information technology and the prospect of increased access to the computing, communications, and storage resources have made these systems vulnerable to attacks. Use of heterogeneous devices and communication links.....

[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)

21. Security for FTTx Optical Access Networks

Walid Shawbaki; Ahmed Kamal

[Local Computer Networks, Proceedings 2006 31st IEEE Conference on](#)
Nov. 2006

Page(s): 221-228

Digital Object Identifier 10.1109/LCN.2006.322103

Summary: Passive optical networks (PONs) is the answer to increasing demand on b enabler for Fiber To The x (FTTx) implementation, where x can be Home (FTTH), Curl Building (FTTB). However, PONs use shared fiber link with broadcast a.....

[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)

22. Chaotic functions for generating binary sequences and their suitability in Multip

Mandi, Mahalinga V.; Murali, R.; Haribhat, K.N.

[Communication Technology, 2006. ICCT '06. International Conference on](#)
Nov. 2006

Page(s): 1-4

Digital Object Identifier 10.1109/ICCT.2006.341812

Summary: Chaotic sequences have good correlation properties and they can be used sequences in Spread Spectrum Communication. Chaotic functions are highly sensitive condition and exhibit non-linear behavior. In Chaotic spread spectrum com.....

[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)

23. Concurrency Control using Subject- and Purpose-Oriented (SPO) View

Enokido, Tomoya; Takizawa, Makoto

[Availability, Reliability and Security, 2007. ARES 2007. The Second International Conf](#)
10-13 April 2007

Page(s): 454-464

Digital Object Identifier 10.1109/ARES.2007.60

Summary: In information systems, multiple transactions issued by subjects manipulate conflicting way. Conflicting access requests from multiple transactions have to be serial various ways to order multiple access requests like FIFO.....

[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)

24. Context-Aware Access Control Making Access Control Decisions Based on Con

Lachmund, Sven; Walter, Thomas; Gomez, Laurent; Bussard, Laurent; Olk, Eddy

[Mobile and Ubiquitous Systems - Workshops, 2006. 3rd Annual International Conferer](#)
17-21 July 2006

Page(s): 1-8

Digital Object Identifier 10.1109/MOBIQW.2006.361782

Summary: In ubiquitous computing environments access control decisions have to be changes of the situation or state of an entity, in order to properly adjust to these changing need of manual interaction. A solution to this challenge is.....

[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)

25. Role-based Concurrency Control in a Subject- and Purpose-Oriented (SPO) View

Enokido, Tomoya; Barolli, Valbona; Takizawa, Makoto

[Advanced Information Networking and Applications, 2007. AINA '07. 21st International](#)
21-23 May 2007

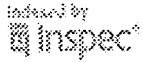
Page(s): 171-178

Digital Object Identifier 10.1109/AINA.2007.124

Summary: In information systems, processes have to be scheduled to share a limited resource objects like memory and CPU with other processes. In database systems, co requests from multiple transactions have to be serialized. There are.....

[AbstractPlus](#) | Full Text: [PDF](#) [IEEE CNF](#)

[View: 1-25](#) | [View Search Results](#)



[Help](#) [Contact Us](#) [Privacy & ;](#)

© Copyright 2006 IEEE -



[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

Search: ☒ The ACM Digital Library ☐ The Guide

(sequence or order or ordered or cascade or cascaded) and (a

THE ACM DIGITAL LIBRARY

[Feedb](#)

** Search String same as for IEEE search **

Terms used:

sequence or order or ordered or cascade or cascaded and access or entry and secure or security or authoriz

Sort results by

Display results

[Save results to a Binder](#)

[Search Tips](#)

☐ Open results in a new window

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

1 [A taxonomy for secure object-oriented databases](#)



Martin S. Olivier, Sebastiaan H. von Solms

March 1994

ACM Transactions on Database Systems (TODS), Volume 19 Issue 1

Publisher: ACM Press

Full text available: [pdf\(3.05 MB\)](#)

Additional Information: [full citation](#), [abstract](#), [referen](#)

This paper proposes a taxonomy for secure object-oriented databases in order to clarify the issi indicates some implications of the various choices one may make when designing such a databi relational databases. The object-oriented database model is more complex than the relational n databases are more complex than ...

Keywords: formal security models, information security, multilevel secure databases, object-o

2 [The relational model for database management: version 2](#)

E. F. Codd

January 1990 Book

Publisher: Addison-Wesley Longman Publishing Co., Inc.

Full text available: [pdf\(28.61 MB\)](#)

Additional Information: [full citation](#), [abstract](#), [referen](#)

From the Preface (See Front Matter for full Preface)

An important adjunct to precision is a sound theoretical foundation. The relational model is solid logic and the theory of relations. This book, however, does not dwell on the theoretical foundati that I now perceive as important for database users, and therefore for DBMS vendors. My perce

3 [A model of OASIS role-based access control and its support for active security](#)



Jean Bacon, Ken Moody, Walt Yao

November 2002

ACM Transactions on Information and System Security (TISSEC), Volume 5

Publisher: ACM Press

Full text available: [pdf\(352.06 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [referen](#)

OASIS is a role-based access control architecture for achieving secure interoperation of service: to allow autonomous management domains to specify their own access control policies and to ii Services define roles and implement formally specified policy to control role activation and serv appropriate context, in order to activat ...

Keywords: Certificates, OASIS, RBAC, distributed systems, policy, role-based access control, s

4 Propagation of authorizations in distributed database systems



Pierangela Samarati, Paul Ammann, Sushil Jajodia

November 1994

Proceedings of the 2nd ACM Conference on Computer and communication

Publisher: ACM Press

Full text available: pdf(1.40 MB)

Additional Information: [full citation](#), [abstract](#), [reference](#)

We consider the propagation of authorizations in distributed database systems. If no constraint then the authorization states at different sites may evolve inconsistently. A standard solution is appear as if they had occurred in some serial order at a single site, perhaps via an atomic comr result in authorization changes ...

5 Cryptography and data security

Dorothy Elizabeth Robling Denning

January 1982 Book

Publisher: Addison-Wesley Longman Publishing Co., Inc.

Full text available: pdf(19.47 MB)

Additional Information: [full citation](#), [abstract](#), [reference](#)

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prol have come to rely on these systems to process and store data, we have also come to wonder a

Data security is the science and study of methods of protecting data in computer and communi

6 A rule-based framework for role-based delegation and revocation



Longhua Zhang, Gail-Joon Ahn, Bei-Tseng Chu

August 2003

ACM Transactions on Information and System Security (TISSEC), Volume 6

Publisher: ACM Press

Full text available: pdf(1.05 MB)

Additional Information: [full citation](#), [abstract](#), [reference](#)

Delegation is the process whereby an active entity in a distributed environment authorizes anot systems, a user often needs to act on another user's behalf with some subset of his/her rights. requirements with ad-hoc mechanisms by compromising existing disorganized policies or simply there is a strong need in the large, distrib ...

Keywords: Role, access control, delegation, revocation, rule-based

7 Access control with IBM Tivoli access manager



Günter Karjoth

May 2003

ACM Transactions on Information and System Security (TISSEC), Volume 6

Publisher: ACM Press

Full text available: pdf(367.07 KB)

Additional Information: [full citation](#), [abstract](#), [reference](#)

Web presence has become a key consideration for the majority of companies and other organiz the Web is increasingly being regarded as an extension of the organization itself, directly integr takes place, security grows in importance. IBM Tivoli Access Manager offers a shared infrastruc technologies that have begun to emerge in the com ...

Keywords: Access control, WWW security, Web servers, authorization management

8 Fast detection of communication patterns in distributed executions

Thomas Kunz, Michiel F. H. Seuren

November 1997 **Proceedings of the 1997 conference of the Centre for Advanced Studies c**

Publisher: IBM Press

Full text available:  pdf(4.21 MB)

Additional Information: [full citation](#), [abstract](#), [referen](#)

Understanding distributed applications is a tedious and difficult task. Visualizations based on pr understanding of the execution of the application. The visualization tool we use is Poet, an ever these diagrams are often very complex and do not provide the user with the desired overview c repeated occurrences of n on-trivial commun ...

9 Access control: On the modeling and analysis of obligations

 Keith Irwin, Ting Yu, William H. Winsborough

October 2006 **Proceedings of the 13th ACM conference on Computer and communicatio**

Publisher: ACM Press

Full text available:  pdf(230.18 KB)

Additional Information: [full citation](#), [abstract](#), [referen](#)

Traditional security policies largely focus on access control requirements, which specify who car control requirements, the availability of services in many applications often further imposes obl taken by a subject in the future as a condition of getting certain privileges at present. However, policies are concerning the security ...

Keywords: obligations, policy

10 Macintosh human interface guidelines

Apple Computer, Inc.

January 1992 Book

Publisher: Addison-Wesley Publishing Company

Full text available:  pdf(37.61 MB)

Additional Information: [full citation](#), [abstract](#), [referen](#)

Macintosh Human Interface Guidelines describes the way to create products that optimize the ii explains the whys and hows of the Macintosh interface in general terms and specific details.

Macintosh Human Interface Guidelines helps you link the philosophy behind the Macintosh inter Examples from a wide range of Macintosh products show good human interface design, includin

11 Limitations of the Kerberos authentication system

 S. M. Bellovin, M. Merritt

October 1990 **ACM SIGCOMM Computer Communication Review**, Volume 20 Issue 5

Publisher: ACM Press

Full text available:  pdf(1.12 MB)

Additional Information: [full citation](#), [abstract](#), [citations](#),

The Kerberos authentication system, a part of MIT's Project Athena, has been adopted by other number of limitations and some weaknesses. Some are due to specifics of the MIT environment discuss a number of such problems, and present solutions to some of them. We also demonstr needed in some cases.

12 A calculus for access control in distributed systems

 Martin Abadi, Michael Burrows, Butler Lampson, Gordon Plotkin

September 1993 **ACM Transactions on Programming Languages and Systems (TOPLAS)**, v

Publisher: ACM Press

Full text available:  pdf(1.94 MB)

Additional Information: [full citation](#), [abstract](#), [referen](#)

We study some of the concepts, protocols, and algorithms for access control in distributed syst principal may come to believe that another principal is making a request, either on his own or c

for access control lists and theories for deciding whether requests should be granted.

Keywords: cryptographic protocols, cryptography, modal logic

13 Approaches to fault-tolerant and transactional mobile agent execution---an algorithmic view

 Stefan Pleisch, André Schiper

September 2004 **ACM Computing Surveys (CSUR)**, Volume 36 Issue 3

Publisher: ACM Press

Full text available:  pdf(946.94 KB)

Additional Information: [full citation](#), [abstract](#), [reference](#)

Over the past years, mobile agent technology has attracted considerable attention, and a significant development in mobile agent technology, reliability mechanisms such as fault tolerance and transaction processing in the field of fault-tolerant and transactional mobile agent execution and thus at guiding the reader to existing approaches. It starts with a discussion ...

Keywords: ACID, Byzantine failures, agreement problem, asynchronous system, commit, crash replication, security, transaction

14 Query evaluation techniques for large databases

 Goetz Graefe

June 1993

ACM Computing Surveys (CSUR), Volume 25 Issue 2

Publisher: ACM Press

Full text available:  pdf(9.37 MB)

Additional Information: [full citation](#), [abstract](#), [reference](#)

Database management systems will continue to manage large data volumes. Thus, efficient algorithms and sequences will be required to provide acceptable performance. The advent of object-oriented databases. On the contrary, modern data models exacerbate the problem: In order to manipulate large set systems manipulate simple records, query-processing ...

Keywords: complex query evaluation plans, dynamic query evaluation plans, extensible database operator model of parallelization, parallel algorithms, relational database systems, set-matching

15 Secure operating systems: Towards a VMM-based usage control framework for OS kernel

 Min Xu, Xuxian Jiang, Ravi Sandhu, Xinwen Zhang

June 2007

Proceedings of the 12th ACM symposium on Access control models and technologies

Publisher: ACM Press

Full text available:  pdf(485.61 KB)

Additional Information: [full citation](#), [abstract](#), [reference](#)

Protecting kernel integrity is one of the fundamental security objectives in building a trustworthy operating system. Various approaches and systems have been proposed and developed. However, access control models must capture important security requirements such as continuous policy enforcement and mutable protection mechanisms in these systems reside in the ...

Keywords: UCON, VMM, access control, authorization, kernel integrity, operating system protection

16 UIO: a uniform I/O system interface for distributed systems

 David R. Cheriton

January 1987

ACM Transactions on Computer Systems (TOCS), Volume 5 Issue 1

Publisher: ACM Press

Full text available:  pdf(3.20 MB)

Additional Information: [full citation](#), [abstract](#), [reference](#)

A uniform I/O interface allows programs to be written relatively independently of specific I/O system

available in a distributed environment. Ideally, the interface provides this uniform access without performance. However, a uniform interface does not arise from careful design of individual system paper, the UIO (unif...

17 Peer-to-peer infrastructure: Pastiche: making backup cheap and easy

 Landon P. Cox, Christopher D. Murray, Brian D. Noble

December 2002 **ACM SIGOPS Operating Systems Review**, Volume 36 Issue 51

Publisher: ACM Press

Full text available:  pdf(1.65 MB)

Additional Information: [full citation](#), [abstract](#), [reference](#)

Backup is cumbersome and expensive. Individual users almost never back up their data, and this presents *Pastiche*, a simple and inexpensive backup system. *Pastiche* exploits excess disk capacity and costs. Each node minimizes storage overhead by selecting peers that share a significant amount of data, and peers with high overhead ...

18 Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure

 Albert Levi, M. Ufuk Caglayan, Cetin K. Koc

February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7

Publisher: ACM Press

Full text available:  pdf(532.64 KB)

Additional Information: [full citation](#), [abstract](#), [reference](#)

Certification is a common mechanism for authentic public key distribution. In order to obtain a network of certificates, which is called public key infrastructure (PKI), and verify the certificates. Nested certification is a novel methodology for efficient certificate path verification. Basic idea is other certificates ...

Keywords: Digital certificates, key management, nested certificates, public key infrastructure

19 Distributed operating systems

 Andrew S. Tanenbaum, Robbert Van Renesse

December 1985 **ACM Computing Surveys (CSUR)**, Volume 17 Issue 4

Publisher: ACM Press

Full text available:  pdf(5.49 MB)

Additional Information: [full citation](#), [abstract](#), [reference](#)

Distributed operating systems have many aspects in common with centralized ones, but they also have differences. This paper introduces distributed operating systems, and especially to current university research about distributed operating systems and how it is distinguished from a computer network, various key design issues are examined in some detail ...

20 Access management for distributed systems: Role-based cascaded delegation

 Roberto Tamassia, Danfeng Yao, William H. Winsborough

June 2004 **Proceedings of the ninth ACM symposium on Access control models and mechanisms**

Publisher: ACM Press

Full text available:  pdf(218.61 KB)

Additional Information: [full citation](#), [abstract](#), [reference](#)

We propose *role-based cascaded delegation*, a model for delegation of authority in decentralized systems. Role-based cascaded delegation combines the advantages of role-based trust management with those of cascaded delegation. Implementation of role-based cascaded delegation using Hierarchical Certificate-Based Encryption. The long role-based delegation chain is captured ...

Keywords: RBAC, access control, delegation, trust management

Set	Items	Description
S1	327854	(COMPUTER?(2N)SYSTEM? ? OR NETWORK? OR DISTRIBUT? OR ETHER-NET? OR INTERNET OR INTRANET? OR LAN OR LANS OR WAN OR WANS OR WLAN? ? OR VLAN? ? (7N) (CONTROL? OR REGULAT? OR DIRECT? OR M-ANAG? OR ADMINISTRAT? OR SUSTAIN? OR ORDER??? OR MAINTAIN? OR SUPERVIS???)
S2	248932	(PROTECT? OR SECUR? OR GUARD? OR FORTIF? OR SHIELD? OR ENF-ORC?) (3N) (ACCESS? OR ENTRY OR ENTRIE? ? OR USE??? OR UTILI? OR USING)
S3	195926	(ORDER?())SET? ? OR SEQUEN? OR PATTERN? OR ORDER?) (5N) (LEVE-L? OR STEP? ? OR STAGE? OR TIER?? ? OR OPERATION? OR FUNCTION? OR COMMAND?)
S4	26666	S3(5N) (TIME? ? OR TIMING OR TEMPORAL? OR CLOCK? OR DURATIO-N? OR EVENT? OR SCHEDUL? OR OCCASION? OR DAY? ? OR HOUR? ? OR MINUTE? ? OR SECOND? ? OR PERIOD?)
S5	33021	S3:S4(5N) (SECOND? OR COUPLE OR 2ND OR 2 OR DUAL?? OR TWICE OR ANOTHER? OR TWO OR DIFFERENT OR PAIR OR MORE(2N)ONE OR ADD-ITIONAL)
S6	8606	S4:S5(5N) (PERFORM? OR EXECUT? OR IMPLEMENT? OR OPERATE? ? - OR OPERATING OR ENACT? OR HANDL? OR (CARRY? OR CARRIE? ?) ()OUT OR COMPLET? OR ENABL? OR ALLOW?)
S7	25	S6 AND S2 AND S1

File 350:Derwent WPIX 1963-2007/UD=200752
(c) 2007 The Thomson Corporation

File 347:JAPIO Dec 1976-2007/Mar(Updated 070809)
(c) 2007 JPO & JAPIO

7/69,K/2 (Item 2 from file: 350)

DIALOG(R) File 350:Derwent WPIX

(c) 2007 The Thomson Corporation. All rts. reserv.

0015035617 - Drawing available

WPI ACC NO: 2005-383609/200539

XRPX Acc No: N2005-310943

Trail/path protection function enhancement method in synchronous optical network, involves mapping content of bytes of section overhead into path overhead bytes at low/high order level, for handling protective resources

Patent Assignee: ALCATEL (COGE)

Inventor: CAZZANIGA G; SESTITO V

Patent Family (3 patents, 33 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
US 20050099941	A1	20050512	US 2004822667	A	20040413	200539 B
EP 1531566	A1	20050518	EP 2003292866	A	20031112	200539 E
CN 1617476	A	20050518	CN 200410042594	A	20040525	200558 E

Priority Applications (no., kind, date): EP 2003292866 A 20031112

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
--------	------	-----	----	-----	--------------

US 20050099941	A1	EN	16	7	
----------------	----	----	----	---	--

EP 1531566	A1	EN			
------------	----	----	--	--	--

Regional Designated States, Original: AL AT BE BG CH CY CZ DE DK EE ES FI
FR GB GR HU IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR

Alerting Abstract US A1

NOVELTY - The content of bytes of section overhead are mapped in a linear multiplex section protection (MSP) N:l trail protection function by protocol exchange, into path overhead (POH) bytes at low order and/or high order level, so as to allow handling of multiple protective resources shared among different working resources in both end-to-end handling and intermediate handling.

DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

- 1.network element;
- 2.trail/path protection function enhancement program; and
- 3.computer readable medium storing trail/path protection function enhancement program.

USE - For enhancing trail/path **protection** function in **synchronous** optical network (SONET) and synchronous digital hierarchy (SDH) network.

ADVANTAGE - Enhances the features of standardized protection scheme. Eliminates requirement of operating system application to the operator, thereby improving traffic **management** reliability in **network**.

DESCRIPTION OF DRAWINGS - The figure shows the schematic diagram of the network elements.

NEa, NEb network elements

Title Terms/Index Terms/Additional Words: TRAILING; PATH; PROTECT; FUNCTION
; ENHANCE; METHOD; SYNCHRONOUS; OPTICAL; NETWORK; MAP; CONTENT; BYTE;
SECTION; OVERHEAD; LOW; HIGH; ORDER; LEVEL; HANDLE; RESOURCE

Class Codes

International Classification (Main): G01R-031/08

International Classification (+ Attributes)

IPC + Level Value Position Status Version
H04J-0003/14 A I R 20060101
H04Q-0011/04 A N R 20060101
H04J-0003/14 C I R 20060101
H04Q-0011/04 C N R 20060101
US Classification, Issued: 370907000, 370228000

File Segment: EPI;
DWPI Class: T01; W01
Manual Codes (EPI/S-X): T01-F02C2; T01-N02B2C; T01-S03; W01-A06A1;
W01-A06C1; W01-A06E
Alerting Abstract ...USE - For enhancing trail/path **protection** function
in **synchronous** optical network (SONET) and synchronous digital hierarchy
(SDH) network...

...standardized protection scheme. Eliminates requirement of operating
system application to the operator, thereby improving traffic **management**
reliability in **network** .

Original Publication Data by Authority

Original Abstracts:

...protocol exchange into POH bytes of the path overhead in SDH or SONET,
at Low **Order** and/or High **Order level** , so as to **allow** the
handling of **more** than **one** protecting **resource** shared **among**
different working resources, both in end-to-end handling and in
intermediate handling...

...in SDH or SONET, at Low Order and/or High Order level, so as to **allow**
the **handling** of **more** than **one** protecting resource shared among
different working resources, both in **end - to -end handling** and in
intermediate **handling**. >

Claims:

...protocol exchange into POH bytes of the path overhead in SDH or SONET,
at Low **Order** and/or High **Order level** , so as to **allow** the
handling of **more** than **one** protecting **resource** shared **among**
different working resources, both in end-to-end handling and in
intermediate handling...

...protocol exchange into POH bytes of the path overhead in SDH or SONET,
at Low **Order** and/or High **Order level** , so as to **allow** the **handling**
of more than one protecting resource shared among **different** working
resources, both in **end-to-end handling** and in **intermediate handling**.
>

7/69,K/5 (Item 5 from file: 350)
 DIALOG(R) File 350:Derwent-WPIX
 (c) 2007 The Thomson Corporation. All rts. reserv.

0014416207 - Drawing available
 WPI ACC NO: 2004-606295/200459
 Related WPI Acc No: 2004-634023; 2004-634025
 XRPX Acc No: N2004-479628

Coprocessor e.g. graphics processing unit, task scheduling method, involves processing tasks by coprocessor in order indicated by run list, where coprocessor switches to next task in event of occurrence of any switching event

Patent Assignee: GOSSALIA A B (GOSS-I); MICROSOFT CORP (MICT); PRONOVOST S (PRON-I)
 Inventor: GOSALIA A B; GOSSALIA A B; LANGLEY B; LANGLEY B L; NAGASE H; PRONOVOST S

Patent Family (9 patents, 35 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
EP 1450258	A2	20040825	EP 20043544	A	20040217	200459 B
JP 2004252983	A	20040909	JP 200442173	A	20040218	200459 E
US 20040187122	A1	20040923	US 2003448399	P	20030218	200463 E
			US 2003448400	P	20030218	
			US 2003448402	P	20030218	
			US 2003474513	P	20030529	
			US 2004763778	A	20040122	
US 20040187135	A1	20040923	US 2003448399	P	20030218	200463 E
			US 2003448400	P	20030218	
			US 2003448402	P	20030218	
			US 2004777797	A	20040212	
US 20040231000	A1	20041118	US 2003448400	P	20030218	200477 E
			US 2004779272	A	20040213	
US 20050168472	A1	20050804	US 2003448399	P	20030218	200552 E
			US 2003748362	A	20031230	
			US 200589856	A	20050325	
CN 1609812	A	20050427	CN 200410039767	A	20040213	200558 E
IN 200400206	I1	20060331	IN 2004DE206	A	20040213	200625 NCE
IN 200400207	I1	20060303	IN 2004DE207	A	20040213	200639 E

Priority Applications (no., kind, date): US 200589856 A 20050325; US 2004779272 A 20040213; IN 2004DE206 A 20040213; US 2004777797 A 20040212; US 2003748362 A 20031230; US 2003474513 P 20030529; US 2003448399 P 20030218; US 2003448400 P 20030218; US 2003448402 P 20030218; US 2004763778 A 20040122

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
EP 1450258	A2	EN	64	26	
Regional Designated States, Original: AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR					
JP 2004252983	A	JA	145		
US 20040187122	A1	EN			Related to Provisional US 2003448399
					Related to Provisional US 2003448400
					Related to Provisional US 2003448402
					Related to Provisional US 2003474513
US 20040187135	A1	EN			Related to Provisional US 2003448399
					Related to Provisional US 2003448400
					Related to Provisional US 2003448402
US 20040231000	A1	EN			Related to Provisional US 2003448400
US 20050168472	A1	EN			Related to Provisional US 2003448399
					Continuation of application US

2003748362
IN 200400206 I1 EN
IN 200400207 I1 EN

Alerting Abstract EP A2

NOVELTY - The method involves generating a run list by a CPU, where the list comprises a list of tasks to be processed by a coprocessor. The run list is delivered to a scheduler process that prepares the tasks on the run list. The tasks are processed by the coprocessor in an order indicated by the run list. The coprocessor switches to a next task on the run list, when a switching event e.g. page fault, occurs while processing a task.

DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

- 1.a computer readable medium comprising computer executable instructions for carrying out a method for scheduling task for processing in a coprocessor
- 2.a modulated data signal carrying computer executable instructions for use in performing a method for scheduling task for processing in a coprocessor
- 3.a graphics processing unit for performing a method of scheduling tasks for processing in a coprocessor.

USE - Used in a computer system for scheduling tasks that are processed in a coprocessor e.g. a graphics processing unit that performs three-dimensional graphics calculation to support application e.g. games and computer aided design.

ADVANTAGE - The method provides the run list and allows the coprocessor to switch immediately from one task to the next, on the occurrence of a switching event, without waiting for CPU intervention, thus providing the CPU with more processing time for other functions and enhancing coprocessor efficiency and power.

DESCRIPTION OF DRAWINGS - The drawing shows a scheduling model.

Title Terms/Index Terms/Additional Words: GRAPHIC; PROCESS; UNIT; TASK; SCHEDULE; METHOD; ORDER; INDICATE; RUN; LIST; SWITCH; EVENT; OCCUR

Class Codes

International Classification (Main): G06F, G06F-009/38, G09G-005/14

(Additional/Secondary): G06T-001/20, G09G-005/393, G06F-009/46

International Classification (+ Attributes)

IPC + Level Value Position Status Version

G06F-0009/46	A	I	R	20060101
G06F-0009/48	A	I	R	20060101
G06F-0009/50	A	I	R	20060101
H04N-0007/16	A	I	R	20060101
H04N-0007/173	A	I	R	20060101
G06F-0009/46	C	I	R	20060101
H04N-0007/16	C	I	R	20060101
H04N-0007/173	C	I	R	20060101

US Classification, Issued: 718100000, 718104000, 725132000, 725133000, 725140000, 725141000, 725152000, 345543000

File Segment: EngPI; EPI;

DWPI Class: T01; P85

Manual Codes (EPI/S-X): T01-C04D; T01-M02B; T01-S03

Original Publication Data by Authority

Original Abstracts:

...any one or more of (1) executing rendering commands sent to the coprocessor in a **different order** than they were **submitted** by **applications** ; (2) preempting the coprocessor during **scheduling** of non-interruptible hardware; (3) **allowing** user mode drivers to build work items using command buffers in a way that **does** not compromise **security** ; (4) preparing DMA **buffers** for execution while the coprocessor is busy executing a previously prepared DMA buffer; (5) resuming...

...in a computer environment having a main processing unit for executing an operating system and **an application** , a **system** memory, and a graphics processing unit having an aperture that maps, in a tiled manner, between a portion...

7/69,K/6 (Item 6 from file: 350)

~~DIAGRAM (R) File 350: Derwent: WPIX~~

(c) 2007 The Thomson Corporation. All rts. reserv.

0013999657 - Drawing available

WPI ACC NO: 2004-180864/200417

XRPX Acc No: N2004-143794

Device for copy-protected distribution of electronic documents via public electronic data network e.g. the internet, with time-limited access to reconstruction server for reconstruction of encrypted document

Patent Assignee: BRAINSHIELD TECHNOLOGIES INC (BRAI-N)

Inventor: WITTKOETTER E; WITTKOTTER E

Patent Family (4 patents, 100 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
WO 2004015952	A2	20040219	WO 2003EP8606	A	20030804	200417 B
DE 10335943	A1	20040603	DE 10335943	A	20030804	200436 E
AU 2003266962	A1	20040225	AU 2003266962	A	20030804	200456 E
US 20040181688	A1	20040916	US 2003635798	A	20030805	200461 E

Priority Applications (no., kind, date): DE 10236061 A 20020806

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
--------	------	-----	----	-----	--------------

WO 2004015952	A2	DE	32	2	
---------------	----	----	----	---	--

National Designated States, Original: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DK DM DZ EC 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 OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW

Regional Designated States, Original: AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR HU IE IT KE LS LU MC MW MZ NL OA PT RO SD SE SI SK SL SZ TR TZ UG ZM ZW

AU 2003266962 A1 EN Based on OPI patent WO 2004015952

Alerting Abstract WO A2

NOVELTY - The device has a number of subscriber terminals (10), each assigned to a user, configured for loading access of an electronic document via the electronic data network, a number of loading accesses carried out for associated electronic file sections, at least one loading access effected from a different subscriber terminal assigned to a different user, with electronic operational sequence instruction data provided by an instruction data server unit (24) required for performing the loading accesses. The received file sections are encrypted according to the operational sequence instruction data to prevent use of the electronic document before reconstruction via a reconstruction server unit (30), coupled for a limited time access to a decryption unit (16,18) within the subscriber terminal.

DESCRIPTION - An INDEPENDENT CLAIM for a method for copy-protected distribution of electronic documents via a public electronic data network is also included.

USE - The device is **used** for copy- **protected** distribution of electronic documents to subscriber terminals connected to a public electronic data network, e.g. the internet.

ADVANTAGE - Device protects distributed electronic documents from being read by unauthorized network users.

DESCRIPTION OF DRAWINGS - The figure shows a schematic block circuit diagram of a device for copy-protected distribution of electronic documents via electronic data network. (Drawing includes non-English language text).

10 Subscriber terminals

14 Publication unit

16,18 Decryption unit
24 Instruction data server unit
30 Reconstruction server unit

Title Terms/Index Terms/Additional Words: DEVICE; COPY; PROTECT; DISTRIBUTE
; ELECTRONIC; DOCUMENT; PUBLIC; DATA; NETWORK; TIME; LIMIT; ACCESS;
RECONSTRUCT; SERVE; ENCRYPTION

Class Codes

International Classification (Main): H04L-012/22, H04L-029/06, H04L-009/00
(Additional/Secondary): H04L-009/32
US Classification, Issued: 713201000

File Segment: EPI;
DWPI Class: T01
Manual Codes (EPI/S-X): T01-N01D2; T01-N02B1

Alerting Abstract ...USE - The device is **used** for copy- **protected** distribution of electronic documents to subscriber terminals connected to a public electronic data network, e...

Original Publication Data by Authority

Original Abstracts:

...of electronic documents of a predetermined document data structure in a publicly accessible electronic data **network**, particularly **the** Internet. Said device comprises: a number of subscriber terminal units (10), which are at least...

...to carry out the number of loading accesses, the subscriber terminal units obtain electronic operational **sequence** instruction **data**, **which** are **created** in a document-specific and/or subscriber-specific manner, from an instruction data unit (24), particularly...and configured for combining the encrypted form with a reconstruction file in order to generate **the** electronic document **for** display by the display unit in an unencrypted form that can be used by the...

Claims:

...and that represent an encrypted form of said electronic document, at least one of said **downloads** **being** **from** said second computer and at least one of said downloads being from said third computer...

7/69,K/7 (Item 7 from file: 350)

DIALOG(R) File-350:Derwent WPIX

(c) 2007 The Thomson Corporation. All rts. reserv.

0013865161 - Drawing available

WPI ACC NO: 2004-043742/200404

Related WPI Acc No: 2005-423933; 2006-510379

XRPX Acc No: N2004-035314

Hardware processor for Internet protocol based storage network appliance, provides remote direct memory access capability on IP and Ethernet network, using transmission control protocol, STCP and UDP protocol

Patent Assignee: PANDYA A (PAND-I); PANDYA A A (PAND-I)

Inventor: PANDYA A; PANDYA A A

Patent Family (13 patents, 99 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
WO 2003104943	A2	20031218	WO 2003US18386	A	20030610	200404 B
US 20040010545	A1	20040115	US 2002388407	P	20020611	200406 E
			US 2003458855	A	20030610	
US 20040010612	A1	20040115	US 2002388407	P	20020611	200406 E
			US 2003459674	A	20030610	
US 20040030757	A1	20040212	US 2002388407	P	20020611	200412 E
			US 2003459297	A	20030610	
US 20040030770	A1	20040212	US 2002388407	P	20020611	200412 E
			US 2003459350	A	20030610	
US 20040030806	A1	20040212	US 2002388407	P	20020611	200412 E
			US 2003459019	A	20030610	
US 20040037299	A1	20040226	US 2002388407	P	20020611	200416 E
			US 2003458844	A	20030610	
US 20040037319	A1	20040226	US 2002388407	P	20020611	200416 E
			US 2003459349	A	20030610	
AU 2003251492	A1	20031222	AU 2003251492	A	20030610	200445 E
US 20040165588	A1	20040826	US 2002388407	P	20020611	200457 E
			US 2003458844	A	20030610	
			US 2003458855	A	20030610	
			US 2003459019	A	20030610	
			US 2003459297	A	20030610	
			US 2003459349	A	20030610	
			US 2003459350	A	20030610	
			US 2003459674	A	20030610	
			WO 2003US18386	A	20030610	
			US 2004783890	A	20040220	
US 20040210320	A1	20041021	US 2002388407	P	20020611	200470 E
			US 2003458844	A	20030610	
			US 2003458855	A	20030610	
			US 2003459019	A	20030610	
			US 2003459297	A	20030610	
			US 2003459349	A	20030610	
			US 2003459350	A	20030610	
			US 2003459674	A	20030610	
			WO 2003US18386	A	20030610	
			US 2004783890	A	20040220	
			US 2004845345	A	20040512	
EP 1573454	A2	20050914	EP 2003757485	A	20030610	200560 E
			WO 2003US18386	A	20030610	
JP 2006516054	W	20060615	WO 2003US18386	A	20030610	200639 E
			JP 2004511951	A	20030610	

Priority Applications (no., kind, date): US 2004845345 A 20040512; US 2004783890 A 20040220; US 2003459674 A 20030610; US 2003459350 A

20030610; US 2003459349 A 20030610; US 2003459297 A 20030610; US
 2003459019 A 20030610; US 2003458855 A 20030610; US 2003458844 A
 20030610; WO 2003US18386 A 20030610; US 2002388407 P 20020611

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing	Notes
WO 2003104943	A2	EN	232	52		
National Designated States, Original: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC 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 OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZM ZW						
Regional Designated States, Original: AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR HU IE IT KE LS LU MC MW MZ NL OA PT RO SD SE SI SK SL SZ TR TZ UG ZM ZW						
US 20040010545	A1	EN				Related to Provisional US 2002388407
US 20040010612	A1	EN				Related to Provisional US 2002388407
US 20040030757	A1	EN				Related to Provisional US 2002388407
US 20040030770	A1	EN				Related to Provisional US 2002388407
US 20040030806	A1	EN				Related to Provisional US 2002388407
US 20040037299	A1	EN				Related to Provisional US 2002388407
US 20040037319	A1	EN				Related to Provisional US 2002388407
AU 2003251492	A1	EN				Based on OPI patent WO 2003104943
US 20040165588	A1	EN				Related to Provisional US 2002388407
						C-I-P of application US 2003458844
						C-I-P of application US 2003458855
						C-I-P of application US 2003459019
						C-I-P of application US 2003459297
						C-I-P of application US 2003459349
						C-I-P of application US 2003459350
						C-I-P of application US 2003459674
						C-I-P of application WO 2003US18386
US 20040210320	A1	EN				Related to Provisional US 2002388407
						C-I-P of application US 2003458844
						C-I-P of application US 2003458855
						C-I-P of application US 2003459019
						C-I-P of application US 2003459297
						C-I-P of application US 2003459349
						C-I-P of application US 2003459350
						C-I-P of application US 2003459674
						C-I-P of application WO 2003US18386
						C-I-P of application US 2004783890
EP 1573454	A2	EN				PCT Application WO 2003US18386
						Based on OPI patent WO 2003104943
Regional Designated States, Original: AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR						
JP 2006516054	W	JA	64			PCT Application WO 2003US18386
						Based on OPI patent WO 2003104943

Alerting Abstract WO A2

NOVELTY - The hardware processor provides remote **direct** memory access capability on **Internet** protocol (IP) **network** and **Ethernet network** using transmission **control** protocol (TCP), STCP and UDP protocol.

DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

1. switching system;
2. network appliance;
3. chip set;

4. hardware implemented ISCSI/IP storage controller ;
5. host processor;
6. host;
7. multi-port hardware processor;
8. integrated circuit hardware processor;
9. remote direct memory access operating method;
10. iSCSI stack;
11. TCP/IP stack;
12. IP processor;
13. multiprocessor system;
14. TCP/IP processor engine;
15. IP storage processor engine;
16. TCP/IP processor;
17. hardware implemented IP network application processor;
18. transport level RDMA function execution method;
19. peer system;
20. cluster of server;
21. CPU;
22. packet scheduler and sequencer;
23. classification resource;
24. Internet protocol packet scheduling and sequencing method;
25. hardware data processing classifier engine;
26. hardware classifier engine method;
27. storage flow and RDMA controller ;
28. commands scheduling and sequencing method;
29. RDMA method;
30. data processing apparatus;
31. session index;
32. session cache and memory complex;
33. session memory;
34. transport layer RDMA protocol execution method;

- 35.server;
- 36.hardware processor manufacturing method;
- 37.IP storage area network switching system line card;
- 38.gate controller ;
- 39.storage area network management appliance; and
40. network .

USE - Hardware processor for Internet protocol (IP) based storage network **appliance** (claimed) and switching system (claimed). Also used in **network management**, bandwidth **management**, **firewall** and security applications.

ADVANTAGE - Reduces TCP/IP protocol stack overhead sharply and enables high line rate storage and data transport solution based on IP. Provides features to **terminate TCP** traffic **carrying** the storage and data payload. Thereby eliminates the TCP/IP networking stack overhead. Allows packets to pass through from input to output with minimal latency. Enables high line rate storage or data traffic carried over IP.

DESCRIPTION OF DRAWINGS - The figure shows a block diagram of the IP network application processor.

Title Terms/Index Terms/Additional Words: HARDWARE; PROCESSOR; PROTOCOL; BASED; STORAGE; NETWORK; APPLIANCE; REMOTE; DIRECT; MEMORY; ACCESS; CAPABLE; IP; TRANSMISSION; CONTROL

Class Codes

International Classification (+ Attributes)

IPC + Level Value Position Status Version

G05B-0015/00	A	I		R	20060101
G06F-0013/10	A	I	F	B	20060101
G06F-0015/173	A	I		R	20060101
G06F-0015/177	A	I		R	20060101
H04L-0012/56	A	I		R	20060101
H04L-0029/06	A	I		R	20060101
H04L-0029/08	A	I		R	20060101
G05B-0015/00	C	I		R	20060101
G06F-0015/16	C	I		R	20060101
H04L-0012/56	C	I		R	20060101
H04L-0029/06	C	I		R	20060101
H04L-0029/08	C	I		R	20060101

US Classification, Issued: 709203000, 709230000, 709213000, 709217000, 709223000, 709220000, 709250000, 709212000, 370401000, 370395500, 370469000, 370395520, 370389000, 700001000

File Segment: EPI;

DWPI Class: T01; W01

Manual Codes (EPI/S-X): T01-F05E; T01-H01B1A; T01-N02A1; T01-N02A3C; W01-A03B; W01-A06E1; W01-A06G2; W01-A06G5E

Hardware processor for Internet protocol based storage network appliance, provides remote direct memory access capability on IP and Ethernet network, using transmission control protocol, STCP and UDP protocol

Alerting Abstract ...NOVELTY - The hardware processor provides remote

direct memory access capability on **Internet** protocol (IP) **network** and **Ethernet network** using transmission **control** protocol (TCP), STCP and UDP protocol....switching system; network appliance; chip set; **hardware** implemented iSCSI/IP storage **controller** ; host processor; host; multi-port hardware processor; integrated circuit hardware processor; remote direct memory access...

...classification resource; Internet protocol packet scheduling and sequencing method; hardware data processing classifier engine; hardware **classifier** engine method; storage flow and **RDMA controller** ; **commands scheduling** and **sequencing** method; RDMA method; data processing apparatus; session index; session cache and memory complex; session memory; transport layer RDMA protocol execution method; server; hardware processor manufacturing method; IP storage area **network** switching system line card; gate **controller** ; storage area **network management** appliance; and **network** .

...

...USE - Hardware processor for Internet protocol (IP) based storage network **appliance** (claimed) and switching system (claimed). Also used in **network management** , bandwidth **management** , **firewall** and security applications.

...

...enables high line rate storage and data transport solution based on IP. Provides features to **terminate** **TCP** traffic **carrying** the storage and data payload. Thereby eliminates the TCP/IP networking stack overhead. Allows packets

Original Publication Data by Authority

Original Abstracts:

...Une architecture fournit des possibilites de transport et de traitement de paquets de Protocole **Internet** (**IP**) depuis la couche 2 par la terminaison totale TCP/IP et l'inspection complete de...

Claims:

...comprising a hardware processor providing remote direct memory access capability for enabling data transfer using **TCP** over IP **networks** , said processor being programmable and sending and receiving data packets' also having identification information based...

...What is claimed is:1. A hardware processor providing remote **direct** memory access capability on an IP **network** and using a TCP, SCTP or UDP protocol, or a combination of **any** of the foregoing, over IP **networks** .

...

...packets;b. a session memory for storing IP session information;c. at least one memory **controller** for **controlling** memory accesses;d. at least one media interface for coupling to at least one network...a peer, memory regions reserved for RDMA;l. recording said memory regions reserved for RDMA in an RDMA database and **maintaining** said database;m. executing operations provided by RDMA capability;n. executing security management functions;o...

...I claim:1. A **security** system comprising a **network** ,said network comprising one or more networked systems of one or more types,a plurality...

...said hardware processor comprising a protocol processing engine to do transport layer protocol processing; or a programmable rule processing engine to analyze **network** traffic for rule matching or **taking** actions on matched rules or a combination thereof; or a security processing engine to do encryption, decryption, authorization or authentication or a combination thereof **using** standard or proprietary **security** protocols; or a packet classification engine to classify the network traffic; or a packet processing

7/69,K/8 (Item 8 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2007 The Thomson Corporation. All rts. reserv.

0013706078 - Drawing available
WPI ACC NO: 2003-803229/200375
XRPX Acc No: N2003-643888

Computer-based maintenance resource system in industrial facility, has operation interface which receives operation data for scheduling and assigning resources to execute job plan

Patent Assignee: FRISINA F (FRIS-I)

Inventor: FRISINA F

Patent Family (1 patents, 1 countries)

Patent			Application			
Number	Kind	Date	Number	Kind	Date	Update
US 20030187865	A1	20031002	US 2002368022	P	20020327	200375 B
			US 2002147344	A	20020515	

Priority Applications (no., kind, date): US 2002368022 P 20020327; US 2002147344 A 20020515

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 20030187865	A1	EN	42	28	Related to Provisional US 2002368022

Alerting Abstract US A1

NOVELTY - The system executes a job planning software for producing job plan or work orders, based on the information supplied by a user. An operation interface receives operation data related to generated job plan or work order, for scheduling and assigning resources to execute job plan or protection request.

DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

- 1.job plan preparation method;
- 2.computer generated work order approved method.

USE - For maintaining resources in industrial or commercial facility using computer.

ADVANTAGE - The operation input and requirement are fully integrated with maintenance resource allocation and planning requirements by using operation interface, hence work orders are issued only after achieving necessary approvals and operation input.

DESCRIPTION OF DRAWINGS - The figure shows the block diagram of the computer-based maintenance resource system.

- 1 computer
- 4 standard database
- 5 work order database
- 6 integration software component
- 8 operation requirement database

Title Terms/Index Terms/Additional Words: COMPUTER; BASED; MAINTAIN; RESOURCE; SYSTEM; INDUSTRIAL; FACILITY; OPERATE; INTERFACE; RECEIVE; DATA; SCHEDULE; ASSIGN; EXECUTE; JOB; PLAN

Class Codes

International Classification (Main): G06F-007/00
US Classification, Issued: 707102000

File Segment: EPI;
DWPI Class: T01

Manual Codes (EPI/S-X): T01-J05A2B; T01-J05B4P; T01-N01A2

Original Publication Data by Authority

Original Abstracts:

A computer based maintenance resource **management system** has an **operations** software component with access to historical operations requirements such that job plans for the current...

Claims:

...program, and means for integrating the operations data into the job plan and/or work **order** for use in **scheduling and** assigning resources to **execute** the job plan and/or **protection request.**>

DIALOG(R) File 350:Derwent.WPIX

0013565781 - Drawing available

Related WPI Acc No: 2003-660044; 2007-024009

Data network management and service provider using command line interface framework, transmits command sequences to corresponding managed data network entity, for execution of command line interface actions in entity

Inventor: CHAN D W; KATZ F; LANDRY K E D; MURRAY C; MURRAY C W; NGO C N;
ZABIHI A

Patent			Application			
Number	Kind	Date	Number	Kind	Date	Update
US 20030115304	A1	20030619	US 2002115900	A	20020405	200362
CA 2365436	A1	20030619	CA 2365436	A	20011219	200362
EP 1322066	A2	20030625	EP 2002293097	A	20021213	200362
US 7113989	B2	20060926	US 2002115900	A	20020405	200663
EP 1322066	B1	20061220	EP 2002293097	A	20021213	200702
DE 60216885	E	20070201	DE 60216885	A	20021213	200722
			EP 2002293097	A	20021213	
DE 60216885	T2	20070705	DE 60216885	A	20021213	200744
			EP 2002293097	A	20021213	

Patent Details

Regional Designated States, Original: AL AT BE BG CH CY CZ DE DK EE ES FI
FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR

Regional Designated States, Original: DE ES FR GB IT

Alerting Abstract US A1

DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

- USE - For managing data networks such as wireless local area network

(LAN) comprising data switching equipments, routers, bridge, access nodes providing multiplexing function, remote access servers (RAS), distribution nodes providing demultiplexing function, customer premise equipment (CPE) and for controlling software applications such as inventory reporting, configuration **management**, statistics gathering, performance reporting, fault **management**, **network surveillance**, **service provisioning**, **billing and accounting** and **security enforcement** using command line interface framework.

ADVANTAGE - Provides automatic entry of CLI command in dictionary and support for multi-vendor equipment by using multiple CLI command vocabularies and dictionaries. Reduces data **network** entity **management costs and time and improves development and maintenance of the network management** and service provisioning solution.

DESCRIPTION OF DRAWINGS - The figure shows the block diagram of the data **network management** and service provisioning command line interface framework.

200 managed object server
510 **managed data network** entity
520 CLI processor
540 communication module

Title Terms/Index Terms/Additional Words: DATA; NETWORK; MANAGEMENT; SERVICE; COMMAND; LINE; INTERFACE; FRAMEWORK; TRANSMIT; SEQUENCE; CORRESPOND; ENTITY; EXECUTE; ACTION

Class Codes

International Classification (+ Attributes)

IPC + Level Value Position Status Version

G06F-0015/173 A I F B 20060101
H04L-0012/24 A I R 20060101
H04L-0012/24 A I F B 20060101
H04L-0012/24 A I F 20060101
G06F-0015/16 C I F B 20060101
H04L-0012/24 C I R 20060101
H04L-0012/24 C I F B 20060101
H04L-0012/24 C I 20060101
H04L-0012/24 C I B 20060101

US Classification, Issued: 709223000, 709222000, 709224000, 709220000, 709223000, 370241000, 370254000, 707100000

File Segment: EPI;

DWPI Class: T01; W01

Manual Codes (EPI/S-X): T01-F05B; T01-N02A2; W01-A06B5A; W01-A06E

Data network management and service provider using command line interface framework, transmits command sequences to corresponding managed data network entity, for execution of command line interface actions in entity

Alerting Abstract ...entries holding vocabulary and grammar specifications of commands used in interacting with at least one **managed data network** entity (510), on receiving request for CLI actions to be performed from a managed object...

...method of interacting with **managed data network** entity; and method of providing dictionary of CLI commands...

...USE - For **managing data networks** such as wireless local area **network** (LAN) comprising data switching equipments, routers, bridge, access nodes providing multiplexing function, remote access servers...

...function, customer premise equipment (CPE) and for controlling software applications such as inventory reporting, configuration **management**, statistics gathering, performance reporting, fault **management**, **network** surveillance, service provisioning, billing and accounting and **security enforcement** using command line interface framework...

...support for multi-vendor equipment by using multiple CLI command vocabularies and dictionaries. Reduces data **network** entity **management** costs and time and improves development and maintenance of the **network management** and service provisioning solution...

...DESCRIPTION OF DRAWINGS - The figure shows the block diagram of the data **network management** and service provisioning command line interface framework...

...510 **managed** data **network** entity...

Original Publication Data by Authority

Original Abstracts:

A method of interacting with a **managed** data **network** entity is provided. The method includes a sequence of steps. A change in the operational state of the **managed** data **network** entity is detected. A CLI dictionary entry is retrieved from a CLI dictionary associated with...

...Based on the retrieved CLI dictionary entry, CLI commands are extracted therefrom to configure the **managed** data **network** entity to reflect the detected change in the operational state. A CLI command sequence is...

...the extracted CLI commands. Each CLI command in the command sequence is sent to the **managed** data **network** entity for execution. CLI command responses are monitored. Based on a successful execution of CLI...

...commands in the CLI command sequence are sent for execution. The solution provides automated configuration **management** of data **network** entities from different vendors when SNMP is not a viable option. The automation eliminates manual CLI command entry in providing **network management** and service provisioning solutions, provides support for multi-vendor equipment by processing multiple CLI command vocabulary and grammar specifications in the CLI command dictionary. The solution reduces data **network** entity **management** costs, downtime, and training time for analysts. The advantages are derived from the ability to...

...data network entities with human readable code greatly improving the development and maintenance of the **network management** and service provisioning solution...

...A method of interacting with a **managed** data **network** entity is provided. The method includes a sequence of steps. A change in the operational state of the **managed** data **network** entity is detected. A CLI dictionary entry is retrieved from a CLI dictionary associated with...

...Based on the retrieved CLI dictionary entry, CLI commands are extracted therefrom to configure the **managed** data **network** entity to reflect the detected change in the operational state. A CLI command sequence is...

...the extracted CLI commands. Each CLI command in the command sequence is sent to the **managed** data **network** entity for execution. CLI command responses are monitored. Based on a successful execution of CLI...

...commands in the CLI command sequence are sent for execution. The

solution provides automated configuration **management** of data **network** entities from different vendors when SNMP is not a viable option. The automation eliminates manual CLI command entry in providing **network management** and service provisioning solutions, provides support for multi-vendor equipment by processing multiple CLI command vocabulary and grammar specifications in the CLI command dictionary. The solution reduces data **network** entity **management** costs, downtime, and training time for analysts. The advantages are derived from the ability to...

...data network entities with human readable code greatly improving the development and maintenance of the **network management** and service provisioning solution...

...A method of interacting with a **managed** data **network** entity is provided. The method includes a sequence of steps. A change in the operational state of the **managed** data **network** entity is detected. A CLI dictionary entry is retrieved from a CLI dictionary associated with...

...Based on the retrieved CLI dictionary entry, CLI commands are extracted therefrom to configure the **managed** data **network** entity to reflect the detected change in the operational state. A CLI command sequence is...

...the extracted CLI commands. Each CLI command in the command sequence is sent to the **managed** data **network** entity for execution. CLI command responses are monitored. Based on a successful execution of CLI...

...commands in the CLI command sequence are sent for execution. The solution provides automated configuration **management** of data **network** entities from different vendors when SNMP is not a viable option. The automation eliminates manual CLI command entry in providing **network management** and service provisioning solutions, provides support for multi-vendor equipment by processing multiple CLI command vocabulary and grammar specifications in the CLI command dictionary. The solution reduces data **network** entity **management** costs, downtime, and training time for analysts. The advantages are derived from the ability to...

...data network entities with human readable code greatly improving the development and maintenance of the **network management** and service provisioning solution.

Claims:

Network management and service provisioning Command Line Interface (CLI) framework, comprising: **a.** a processor responsive to...

...holding vocabulary and grammar specifications of a plurality of commands used in interacting with at **least** one **managed** data network entity; and **c.** a communications module sending in sequence for execution and...

...of commands generated in response to the notification as specified in the plurality of dictionary **entries** **wherein** a network management and service provisioning solution is provided making abstraction of the **at least one** managed data network entity...

...A Command Line Interface (CLI) **framework** **for** a network manager (NM) that manages a plurality of managed entities **of** a communication network, comprising: a CLI dictionary (530) holding vocabulary and grammar specifications for all...

...sequence of commands required to configure a managed entity that said managed object represents in **response** to **said event** and handling **execution** of **said** sequence of commands at said managed entity; and a communications module (540) for transmitting said sequence of commands to

said managed entity for execution, and interpreting results **received** from said managed **entity**, wherein a network management and service provisioning solution is provided making abstraction of the type of...

...I/we **claim** : **1** . A network management and service provisioning Command Line Interface (CLI) framework, comprising: a. a processor...

...entries holding vocabulary and grammar specifications of a plurality of commands used in interacting with **at least one** managed data network entity; and c. a communications module sending in sequence for execution and...

...of commands generated in response to the notification as specified in the plurality of dictionary **entries** wherein a network management and service provisioning solution is provided making abstraction of the **at least one** managed data network entity...

...We claim:1. A Command Line Interface (CLI) framework **component of** a Network Management System (**NMS**), the NMS managing a plurality **of** field **installed** managed communications network entities **of** a communications network, **each** field **installed** managed communications network entity being represented and modeled by an associated managed object instance stored...

...database associated with the NMS, the CLI framework component comprising: a. a CLI dictionary codifying **a plurality of** managed communications network entity-specific **CLI** commands and maintaining at least one **mapping** between **the** managed communications network entity-specific CLI commands **and** a corresponding managed object type;b. a generic processor executing coded logic to: i. detect...

...responsive to the detected event selectively generate a sequence of CLI commands required to configure **the** field **installed** managed communications network entity **associated** with said managed object instance by consulting the CLI dictionary;iii. handle execution of said sequence of CLI commands at **said** field **installed** managed communications network entity, including interpreting CLI command execution results received from **said** field **installed** managed communications network entity; andiv. generating an error report based on an unsuccessful execution...

...the execution results; andc. a communications module transmitting said sequence of CLI commands to **said** field **installed** managed communications network entity to be executed thereon, and conveying the execution results received from **said** field **installed** managed communications network entity to the generic **processor**, wherein a network management and service provisioning solution is provide **making** abstraction **of** managed communications network entity types.

7/69,K/24 (Item 24 from file: 350)

~~DIALOG(R)File=350:Derwent.WPIX~~

(c) 2007 The Thomson Corporation. All rts. reserv.

0008061777 - Drawing available

WPI ACC NO: 1997-157344/199715

XRPX Acc No: N1997-129878

Access control method for resources in distributed systems - involves obtaining object references that include unforgeable numbers and supplying these references to server objects

Patent Assignee: SUN MICROSYSTEMS INC (SUNM)

Inventor: NESSETT D M; TOCK T D

Patent Family (8 patents, 8 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
EP 762289	A2	19970312	EP 1996306020	A	19960816	199715 B
JP 9251425	A	19970922	JP 1996234642	A	19960819	199748 E
TW 314609	A	19970901	TW 1996112101	A	19961003	199803 E
KR 1997012183	A	19970329	KR 199634970	A	19960819	199815 E
US 5742759	A	19980421	US 1995516671	A	19950818	199823 E
CN 1149797	A	19970514	CN 1996113317	A	19960817	200123 E
EP 762289	B1	20040721	EP 1996306020	A	19960816	200449 E
DE 69632938	E	20040826	DE 69632938	A	19960816	200456 E
			EP 1996306020	A	19960816	

Priority Applications (no., kind, date): EP 1996306020 A 19960816; US 1995516671 A 19950818

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
EP 762289	A2	EN	13	3	
Regional Designated States,Original: DE FR GB IT					
JP 9251425	A	JA	14		
TW 314609	A	ZH			
US 5742759	A	EN	14		
EP 762289	B1	EN			
Regional Designated States,Original: DE FR GB IT					
DE 69632938	E	DE			
					Application EP 1996306020
					Based on OPI patent EP 762289

Alerting Abstract EP A2

The access control method involves a user operating at a display device (107) and establishes a authenticated link to the computer (101). The computer or the system has a client object (117) and a number of server objects (119,121). When the user logs on the client object obtains details of the associated membership group (123).

The client object can communicate with the server objects to identify objects that will be required. The server objects return a reference that includes an unforgeable number. When the user makes a print request, it passes the object reference. The print server uses these to obtain approved access to other servers.

ADVANTAGE - Provides simple and efficient "delegation" handling of user access rights.

Title Terms/Index Terms/Additional Words: ACCESS; CONTROL; METHOD; RESOURCE ; DISTRIBUTE; SYSTEM; OBTAIN; OBJECT; REFERENCE; NUMBER; SUPPLY; SERVE

Class Codes

International Classification (Main): G06F-001/00, G06F-012/00, G06F-012/14, G06F-015/00, H04L-009/00
(Additional/Secondary): G06F-013/00, G06F-017/21, G06F-009/46, G09C-001/00

, H04L-009/32
US Classification, Issued: 395187010, 395800280, 395800300, 395200330,
395200490, 395200550, 395200590, 711163000

File Segment: EngPI; EPI;
DWPI Class: T01; P85
Manual Codes (EPI/S-X): T01-F05G5; T01-H01C2; T01-H07C5A; T01-J05B4A
Access control method for resources in distributed systems...

Original Titles:

...Method and system for **securely controlling access** to system resources in a **distributed system**...

...Method and system for **securely controlling access** to system resources in a **distributed system**...

...METHOD AND SYSTEM FOR **CONTROLLING SECURITY OF ACCESS TO SYSTEM RESOURCE IN DISTRIBUTED SYSTEM**...

...Method and system for facilitating access **control** to system resources in a **distributed computer system** .

Original Publication Data by Authority

Original Abstracts:

Embodiments of the present invention provide an improve method and system for **securely controlling access to resources in a distributed computer system** . One **embodiment of the present invention** stores and binds a group identification to a target object and then uses...
...Embodiments of the present invention provide an improved method and system for **securely controlling access to resources in a distributed computer system** . One **embodiment of the present invention** stores and binds a group identification to a target object and then uses membership checking to determine whether a client...

...the present invention avoids performing costly cryptographic operations in order to verify access rights of **requesting** objects, as was common in some prior art systems. A **second embodiment** of the present invention stores and binds a group identification to a target object...

Claims:

1. A method executed in a **computer system for controlling access to system resources in a distributed computer system** , the **method** comprising the steps of: sending a request from a client object to a spreadsheet server...

...A method executed in a **computer system (101) for controlling access to system resources in a distributed computer system** comprising:

 sending a request (201) from a client object (117) to a spreadsheet server object to bind a group identifier to a spreadsheet object;
 under **control** of the spreadsheet server object;
 obtaining a **spreadsheet object (205)**;
 storing the group identifier with the spreadsheet object (207);
 generating an unforgeable checksum (209);
 storing the unforgeable checksum with the spreadsheet object (209);
 sending the...A method executed in a **computer system** for facilitating access **control** to system resource in a **distributed computer system** , the **distributed computer system** including a first server object, a target object, a client object and a second server...

...of the objects belonging to one or more specified groups of objects residing in the **computer system**, the method comprising the steps of:under **control** of the first server object,storing a group identifier associated with the target object in...

...group of object in the computer system with access privileges to the target object;under **control** of the second server object,sending an **access** request to the **first** server object requesting access to **the target object**, the **access request** including a second server principal identifier which identifies a principal operating the second server object;under...

...target object, the target object reference indicating a location of the target object in the **computer system**;under **control** of the client object,locating a second server object which operates on behalf of a

7/69,K/21 (Item 21 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2007 The Thomson Corporation. All rts. reserv.

0008978289 - Drawing available

WPI ACC NO: 1998-532222/199845

Related WPI Acc No: 1998-532211; 1998-532223; 1998-532433; 1999-024004;
2002-470358

XRPX Acc No: N1998-415231

Dynamic client registry for distribution of information over network - in which information from client entities on different networks is organized for selective sharing

Patent Assignee: BURNS T A (BURN-I); BUTMAN R A (BUTM-I); DOUGHERTY J C (DOUG-I); KMEC M D (KMIE-I); MALONE T J (MALO-I); PFN INC (PFNP-N); RAMACHANDRAN R (RAMA-I)

Inventor: BURNS T A; BUTMAN R A; DOUGHERTY J C; KMEC M D; MALONE T J; RAMACHANDRAN R

Patent Family (5 patents, 80 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
WO 1998043184	A1	19981001	WO 1998US5731	A	19980324	199845 B
AU 199867701	A	19981020	AU 199867701	A	19980324	199909 E
US 6026430	A	20000215	US 1997828833	A	19970324	200016 E
EP 1019850	A1	20000719	EP 1998913067	A	19980324	200036 E
			WO 1998US5731	A	19980324	
JP 2002515156	W	20020521	JP 1998545903	A	19980324	200236 E
			WO 1998US5731	A	19980324	

Priority Applications (no., kind, date): US 1997828833 A 19970324

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
WO 1998043184	A1	EN	132	47	
National Designated States,Original: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM GW HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW					
Regional Designated States,Original: AT BE CH DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW					
AU 199867701	A	EN			Based on OPI patent WO 1998043184
EP 1019850	A1	EN			PCT Application WO 1998US5731
					Based on OPI patent WO 1998043184
Regional Designated States,Original: AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					
JP 2002515156	W	JA	128		PCT Application WO 1998US5731
					Based on OPI patent WO 1998043184

Alerting Abstract WO A1

The registry is used to organise information from client entities on different networks for selective sharing, and includes a computer for storing a dynamic client registry and resource locators containing function names.

A web server causes the computer to respond to the resource locators by loading the function name indicated. A database management program organises the dynamic client registry.

USE - Providing **control** over **distribution**, redistribution, **access security**, filtering, organizing and display of information across disparate networks.

ADVANTAGE - Enables selective transmission of valuable information in manner which allows for control or replication and publication of information.

Title Terms/Index Terms/Additional Words: DYNAMIC; CLIENT; REGISTER;
DISTRIBUTE; INFORMATION; NETWORK; ENTITY; ORGANISE; SELECT; SHARE

Class Codes

International Classification (Main): G06F-015/00, G06F-015/16, G06F-017/30
(Additional/Secondary): G06F-012/00, G06F-012/14, G06F-013/00
US Classification, Issued: 709203000, 709217000, 709225000, 709227000,
709238000, 709239000, 709249000

File Segment: EPI;

DWPI Class: T01

Manual Codes (EPI/S-X): T01-D01; T01-H07C5E; T01-J05B4M

Alerting Abstract ...USE - Providing control over distribution ,
redistribution, access security , filtering, organizing and display of
information across disparate networks...

Original Publication Data by Authority

Original Abstracts:

...to resource locators directed to it and to direct the database
management program in organizing the dynamic client registry; several
secondary computers networked with the first, each having a disk for
storing a dynamic group registry and resource...

...resource locators directed to it and to direct the database management
program in organizing the dynamic client registry; several secondary
computers networked with the first, each having a disk for storing a
dynamic group registry and resource...

...locators directed to it and to direct the database management program in
organizing the dynamic client registry; several secondary computers
networked with the first, each having a disk for storing a dynamic group
registry and resource...

Claims:

...for execution in the client side communications server in each secondary
computer so that communications between the first computer and each
secondary computer cause the selected predetermined functions to be
executed dynamically in order to store and index information in the
dynamic client registry for selective access by each secondary
computer.

7/69,K/19 (Item 19 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2007 The Thomson Corporation. All rts. reserv.

0009798320 - Drawing available

WPI ACC NO: 2000-087497/200007

Related WPI Acc No: 1999-561717

XRPX Acc No: N2000-068688

Security system for business use computer

Patent Assignee: DMW WORLDWIDE INC (DMWW-N); HARTLEY B V (HART-I);

INNERWALL INC (INNE-N); KNIGHT E (KNIG-I); MAVROS C (MAVR-I); REYNOLDS

K (REYN-I); ZYMBALUK G (ZYMB-I)

Inventor: HARTLEY B V; KNIGHT E; MAVROS C; REYNOLDS K; ZYMBALUK G

Patent Family (5 patents, 82 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
WO 1999066383	A2	19991223	WO 1999US13476	A	19990615	200007 B
AU 199945682	A	20000105	AU 199945682	A	19990615	200024 E
US 20020026591	A1	20020228	US 199891270	P	19980615	200220 E
			US 1999333547	A	19990615	
			US 2001834334	A	20010412	
US 6889168	B2	20050503	US 199891270	P	19980615	200531 E
			US 1999333547	A	19990615	
			US 2001834334	A	20010412	
US 20050171737	A1	20050804	US 199891270	P	19980615	200552 E
			US 1999333547	A	19990615	
			US 2001834334	A	20010412	
			US 2005100714	A	20050407	

Priority Applications (no., kind, date): US 2005100714 A 20050407; US 2001834334 A 20010412; US 1999333547 A 19990615; US 199891270 P 19980615

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
--------	------	-----	----	-----	--------------

WO 1999066383	A2	EN	37	15	
---------------	----	----	----	----	--

National Designated States, Original: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK 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 MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW

Regional Designated States, Original: AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ UG ZW

AU 199945682	A	EN			Based on OPI patent WO 1999066383
--------------	---	----	--	--	-----------------------------------

US 20020026591	A1	EN			Related to Provisional US 199891270 Continuation of application US
----------------	----	----	--	--	---

1999333547					
US 6889168	B2	EN			Related to Provisional US 199891270 Continuation of application US

1999333547					
US 20050171737	A1	EN			Related to Provisional US 199891270 Continuation of application US

1999333547					
					Continuation of application US

2001834334					
					Continuation of patent US 6889168

Alerting Abstract WO A2

NOVELTY - Security module of the system under direction from processor (12) accesses and analyzes selected portions of the computer comprising unix server (10) to identify vulnerabilities. Utility module under direction from processor performs various utility functions with regard to

computer, in response to identified vulnerabilities.

DESCRIPTION - Security information for performing analysis of computer is stored in security system memory (30). The security system is connected to the computer comprising unix server (10) via (18). The reporting module of the system provides status information to GUI with regard to operations of the system. The security module includes at least one of configuration mode which performs initial analysis of the **computer system** acquire configuration information, **directory** checking module analyzing **directories** and files in system memory (13) to determine if security initial files have been tampered, user **manager** module, integrity checking module, **network** checking module and a password checking module. The utility module is chosen from user manager module, file removal module, file marking module, and scheduling module. An INDEPENDENT CLAIM is also included for method of providing a security assessment for computer system.

USE - For business use computer.

ADVANTAGE - Enables manually marking certain critical files and analyzing the marked files to detect tampering when directory check module is activated. Enables scheduling automated performance of functions and providing reports to the system user in a number of different formats.

DESCRIPTION OF DRAWINGS - The figure shows block diagram of security system.

- 10 Unix server
- 12 Processor
- 13 System memory
- 18 Via
- 30 Security system memory

Title Terms/Index Terms/Additional Words: SECURE; SYSTEM; BUSINESS; COMPUTER

Class Codes

International Classification (Main): G06F, G06F-011/30, G06F-012/14, G06F-015/00

(Additional/Secondary): H04L-009/00

US Classification, Issued: 713201000, 709224000, 702186000, 702186000, 713201000

File Segment: EPI;

DWPI Class: T01

Manual Codes (EPI/S-X): T01-H07C5A; T01-J12C

Security system for business use computer

Alerting Abstract ...security module includes at least one of configuration mode which performs initial analysis of the **computer system** acquire configuration information, **directory** checking module analyzing **directories** and files in system memory (13) to determine if security initial files have been tampered, user **manager** module, integrity checking module, **network** checking module and a password checking module. The utility module is chosen from user manager...

Original Publication Data by Authority

Original Abstracts:

...identify, notify, and possibly correct, vulnerabilities and discrepancies. The security system includes a number of **security** tools and **utilities** in order to **perform** these functions. The **security** system includes the capability to identify the system configuration and once this is done performs different processes to analyze the **computer system directories**, locate **vulnerabilities** in the files or

directories , check the network access , do analysis of the users or groups which have access to the computer system and check the permissions ...

...identify, notify, and possibly correct, vulnerabilities and discrepancies. The security system includes a number of security tools and utilities in order to perform these functions . The security system includes the capability to identify the system configuration and once this is done performs different processes to analyze the computer system directories , locate vulnerabilities in the files or directories , check the network access, do analysis of the users or groups which have access to the computer system and check the permissions which these parties have been granted, and analyze passwords of the...

...security analysis computer system to identify, notify, and possibly correct, vulnerabilities and discrepancies. The security system includes a number of security tools and utilities in order to perform these functions. The security system includes the capability to identify the system configuration and once this is done performs different processes to analyze the computer system directories , locate vulnerabilities in the files or directories , check the network access, do analysis of the users or groups which have access to the computer system and check the permissions which these parties have been granted, and analyze passwords of the...

...to identify, notify, and possibly correct, vulnerabilities and discrepancies. The security system includes a number of security tools and utilities in order to perform these functions. The security system includes the capability to identify the system configuration and once this is done performs different processes to analyze the computer system directories , locate vulnerabilities in the files or directories , check the network access, do analysis of the users or groups which have access to the computer system and check the permissions which these parties have been granted, and analyze passwords of the users. The utilities include...

...to permanently remove files from the computer system, mark particular files to be analyzed, as well as schedule the security tests to be performed at predetermined times...

...des vulnerabilites et des anomalies. Ce systeme de securite comporte un certain nombre d'outils de securite et d'utilitaires destines a executer ces fonctions. Il a la capacite d'identifier la configuration du systeme et, cela fait, d'effectuer differentes operations pour analyser les repertoires, localiser les vulnerabilites dans les fichiers ou les directoires, verifier l'accès réseau...

...permanence des fichiers du systeme, de marquer des fichiers particuliers a analyser et de planifier les essais de securite a executer a des moments predetermines.

Claims:

...said security system comprising: at least one security module which under direction from the processor accesses and analyzes selected portions of the computer apparatus to identify vulnerabilities; at least one utility module which under...

...performs various utility functions with regards to the computer apparatus in response to the identified vulnerabilities ; and a security system memory which contains security information for performing the analysis of the computer apparatus...

...1. A computer security system, comprising: a configuration/set-up module that operates under **direction** of a processor of a **computer system** and that identifies **security critical files** of the **computer system**; a **directory** checking module that operates under **direction** of the processor and that **identifies unauthorized** changes to the security critical files; and a **user manager** module that operates **under direction** of the processor and that identifies unauthorized **access** to the **security critical files**.

...

...said security system comprising: at least one security module which under direction from the processor **accesses** and analyzes selected **portions** of the computer apparatus to identify vulnerabilities; at least one utility module which under the direction from the processor, performs various **utility** functions with **regards** to the computer apparatus in response to the identified vulnerabilities; and a security system memory

7/69,K/18 (Item 18 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2007 The Thomson Corporation. All rts. reserv.

0010023825 - Drawing available

WPI ACC NO: 2000-328317/200028

XRPX Acc No: N2000-247139

Computer system hardware resource sharing method for business application, involves selecting at least one system operating mode and operation interval

Patent Assignee: SAVVY FRONTIERS PROPERTY TRUST (SAVV-N)

Inventor: WEBER H J

Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
US 6052781	A	20000418	US 1997803636	A	19970221	200028 B

Priority Applications (no., kind, date): US 1997803636 A 19970221

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 6052781	A	EN	36	26	

Alerting Abstract US A

NOVELTY - The computer system's hardware resources are configured to select at least one of primary and secondary system operating modes. At least one of two operation intervals is selected during an initial ROM-BIOS **controlled** POST sequence of **computer system**, preferably before BOOT of OS.

DESCRIPTION - A computational portion, a random access memory portion and an operator interface portion of the computer system's hardware resources are shared between user-1 and user-2. Hard disk drive (HDD0) (90-1) and HDD1 (90-2) are interlinked with the hardware resources. Operating system software of user-1, user-2 are respectively maintained on HDD0 and HDD1. The primary system operating mode enables the user-1 to access the HDD0 while denying functional access to HDD1. Secondary system operating mode enables user-2 to access HDD1 while denying functional access to HDD0. The operation interval includes the respective user and system operating mode. An INDEPENDENT CLAIM is also included for the computer system hardware resource sharing apparatus.

USE - For business and office application, for students for enabling at least two non-current users to exercise functionally separate operational access to hardware resources while maintaining substantially incorruptible OS and program software integrity for each user.

ADVANTAGE - The two hard disk drives are electrically disassociated and independently operable only by an intended user. Non-intended user cannot access the unique hard disk drive. Even massive errors such as disk reformat does not occur. OS on each HDD may be nearly identical or entirely different. When the user accesses the computer system, corresponding HDD is also accessed. Any other HDD is operationally set aside and **secured** against **access** through password **protection** during boot by unique removable media device or through hardware selection devices such as key switch or user ID data card.

DESCRIPTION OF DRAWINGS - The figure shows the arrangement of PC including operator selectable hard disk drive exclusion.

90-1 HDD0

90-2 HDD1

Title Terms/Index Terms/Additional Words: COMPUTER; SYSTEM; HARDWARE; RESOURCE; SHARE; METHOD; BUSINESS; APPLY; SELECT; ONE; OPERATE; MODE;

INTERVAL

Class Codes

International Classification (Main): G06F-013/00

US Classification, Issued: 713200000, 713002000, 713100000

File Segment: EPI;

DWPI Class: T01

Manual Codes (EPI/S-X): T01-F02C2; T01-F05B2; T01-H05A

Alerting Abstract ...modes. At least one of two operation intervals is selected during an initial ROM-BIOS **controlled** POST sequence of **computer system**, preferably before BOOT of OS...computer system, corresponding HDD is also accessed. Any other HDD is operationally set aside and **secured** against **access** through password **protection** during boot by unique removable media device or through hardware selection devices such as key...

Original Publication Data by Authority

Claims:

...enables at least two non-concurrent users to exercise functionally separate operational access to the **computer system's hardware resources** while **maintaining** substantially **incorruptible** operating system and program software integrity for each user, comprising steps of: sharing a common...

...at least a first hard disk drive and a second hard disk drive with the **computer system's hardware resources**; **maintaining the first user's** operating system software **and** program files on the first hard disk drive; maintaining the second user's operating system software and program **files** on the second hard disk **drive**; configuring the **computer system's hardware resources** to enable a selectable one of at least a first system operating...

...system operating mode, and a second interval of operation including the second user and the **second system operating mode during an initial ROM-BIOS controlled POST sequence of the computer system and** preferably prior to a BOOT of **the operating system.**>

7/69,K/13 (Item 13 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2007 The Thomson Corporation. All rts. reserv.

0013129049 - Drawing available
WPI ACC NO: 2003-211125/200320
XRPX Acc No: N2003-168269

Stand-alone security system for controlling access to secured information and self-service functionality for sponsor organization for Web-based and IVR-based self-service functions

Patent Assignee: BURCHARD W (BURC-I); EDWARDS B T (EDWA-I); HARRIS S A (HARR-I); HUMANA INC (HUMA-N); KEINSLEY B E (KEIN-I); LATIMER E W (LATI-I); LAWHEAD A L (LAWH-I); LIGHT E P (LIGH-I); ROSENBERG S (ROSE-I); SMITHSON M A (SMIT-I); STANLEY C (STAN-I); TOWNSEND D L (TOWN-I); WEBER L S (WEBE-I)
Inventor: BURCHARD W; EDWARDS B T; HARRIS S A; KEINSLEY B E; LATIMER E W; LAWHEAD A L; LIGHT E P; ROSENBERG S; SMITHSON M A; STANLEY C; TOWNSEND D L; WEBER L S

Patent Family (6 patents, 100 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
WO 2003017096	A1	20030227	WO 2002US25272	A	20020812	200320 B
US 20030154403	A1	20030814	US 2001311821	P	20010814	200355 E
			US 2002216664	A	20020812	
EP 1417574	A1	20040512	EP 2002768461	A	20020812	200431 E
			WO 2002US25272	A	20020812	
AU 2002331022	A1	20030303	AU 2002331022	A	20020812	200452 E
JP 2005500617	W	20050106	WO 2002US25272	A	20020812	200505 E
			JP 2003521939	A	20020812	
IN 200400289	P4	20051209	WO 2002US25779	A	20020814	200604 E
			IN 2004CN289	A	20040212	

Priority Applications (no., kind, date): US 2002216664 A 20020812; US 2001311821 P 20010814

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
WO 2003017096	A1	EN	176	30	
National Designated States,Original: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC 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 OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW					
Regional Designated States,Original: AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SK SL SZ TR TZ UG ZM ZW					
US 20030154403	A1	EN			Related to Provisional US 2001311821
EP 1417574	A1	EN			PCT Application WO 2002US25272 Based on OPI patent WO 2003017096
Regional Designated States,Original: AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR					
AU 2002331022	A1	EN			Based on OPI patent WO 2003017096
JP 2005500617	W	JA	280		PCT Application WO 2002US25272 Based on OPI patent WO 2003017096
IN 200400289	P4	EN			PCT Application WO 2002US25779

Alerting Abstract WO A1

NOVELTY - Sponsor organizations e.g. healthcare companies, use the stand-alone security system for controlling access to secured information by clients that access the company's data and other resources

over a distributed information retrieval system e.g. WWW.

DESCRIPTION - The secured logon application is a stand-alone **security** system which controls **access** to **secured** information and self-service functionality for a sponsor organization via a secure, externally managed, dynamic menuing program that provides for controlled access to resources e.g. secured information and self-service functionality of the sponsor organization. It can be implemented using commercially available computer equipment and programming languages, and used for web-based and IVR-based self-service functions.

USE - Web-based **security** applications for providing controlled access to sponsor organisation's data and other resources.

ADVANTAGE - Secured logon application can have differences in configuration depending upon the sponsor organization, and can be integrated and blended into a web site between an unsecured section of the site and a secured section of the site.

DESCRIPTION OF DRAWINGS - The drawing shows the relationship between an entity, a user, what the user can do e.g. business functions, and what data the user can perform those functions on (access identifiers).

Title Terms/Index Terms/Additional Words: STAND; SECURE; SYSTEM; CONTROL; ACCESS; INFORMATION; SELF; SERVICE; FUNCTION; ORGANISE; WEB; BASED

Class Codes

International Classification (Main): G06F-011/30, G06F-015/00, G06F-009/445
(Additional/Secondary): G06F-015/173, G06F-017/00, G06F-017/60,
G06F-007/00, H04L-009/00

US Classification, Issued: 713201000, 709223000

File Segment: EPI;

DWPI Class: T01

Manual Codes (EPI/S-X): T01-J12C; T01-N01D1A; T01-N02B1B; T01-S01C

Stand-alone security system for controlling access to secured information and self-service functionality for sponsor organization for Web-based and IVR-based self...

Original Titles:

WEB-BASED **SECURITY** WITH CONTROLLED **ACCESS** TO DATA AND RESOURCES...

...WEB-BASED **SECURITY** WITH CONTROLLED **ACCESS** TO DATA AND RESOURCES...

...Web-based **security** with controlled **access** to data and resources...

...WEB-BASED **SECURITY** WITH CONTROLLED **ACCESS** TO DATA AND RESOURCES...

Alerting Abstract ...NOVELTY - Sponsor organizations e.g. healthcare companies, **use** the stand-alone **security** system for controlling **access** to **secured** information by clients that access the company's data and other resources over a distributed...

DESCRIPTION - The secured logon application is a stand-alone **security** system which controls **access** to **secured** information and self-service functionality for a sponsor organization via a secure, externally managed, dynamic...

... **USE** - Web-based **security** applications for providing controlled access to sponsor organisation's data and other resources

Original Publication Data by Authority

Original Abstracts:

A stand-alone security system controlling access to secured information and self-service functionality for a sponsor organization, usable for Web-based and IVR-based self-service functions, having five primary facets: (1) control of access to secured information (2) enabling access to users having indirect and direct relationships with the sponsor organization (3) distribution of security administration from a central information technology resource to users of the security system, (4) support for integration into different environments, and (5) support for system integrators. Key components of access control...

...A stand-alone security system controlling access to secured information and self-service functionality for a sponsor organization, usable for Web-based and IVR-based self-service functions, having five primary facets: (1) control of access to secured information and self-service functionality for a sponsor organization, (2) enabling access to users having indirect relationships to the sponsor organization and to users having a direct relationship with the sponsor organization, (3) distribution of security administration from a central information technology resource to various users of the security system, (4) support for integration into different kinds of environments, and (5) support for system integrators. Key components of access control include (1) association...

...who handles day-to-day security administration for the employer. Facet (3) enables multiple levels of distribution, including enabling one organization to delegate its rights to another organization...

...A stand-alone security system controlling access to secured information and self-service functionality for a sponsor organization, usable for Web-based and IVR-based self-service functions, having five primary facets: (1) control of access to secured information (2) enabling access to users having indirect and direct relationships with the sponsor organization (3) distribution of security administration from a central information technology resource to users of the security system, (4) support for integration into different environments, and (5) support for system integrators. Key components of access control include (1) association of a userID with one specific person, (2) identification of keys...

...un systeme RVI et presentant cinq facettes principales: (1) surveillance de l'acces aux informations securisees, (2) acces aux utilisateurs ayant un lien indirect et direct avec l'organisation de parrainage, (3) distribution de l'administration de securite a partir d'une ressource de technologie d'information centrale aux utilisateurs du systeme securise, (4) support dans le cadre de l'integration a differents environnements, (5) support aux integrateurs de systemes. Les composants cles de la surveillance de l'acces sont constitues de (1) l'association d'une...

Claims:

We claim: 1. A stand-alone security system controlling access to secured information and self-service functionality for a sponsor organization, comprising: means for controlling access to secured information and self-service functionality for the sponsor organization; means for enabling access to users who have indirect relationships to the sponsor organization as well as to users who have a direct relationship with the sponsor organization; means for distributing security administration from a central information technology resource to various users of the security system; means for supporting integration into different kinds of environments; and means for supporting

system integrators who need to interface with and use information in the security system in order to execute their business functions.>

7/69,K/12 (Item 12 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2007 The Thomson Corporation. All rts. reserv.

0013158471 - Drawing available
WPI ACC NO: 2003-241263/200324
Related WPI Acc No: 2003-362270
XRPX Acc No: N2003-192073

Interfacing method for security processor used in online transactions over networks e.g. Internet, in which macro- security operations are used for communicating tasks and results between host and security processors

Patent Assignee: CAVIUM NETWORKS (CAVI-N); CAVIUM NETWORKS INC (CAVI-N)
Inventor: AHMED K E; CARLSON D A; HUSSAIN M R; KESSLER R E; SANZONE R A;
VARGA M D

Patent Family (4 patents, 33 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
EP 1282025	A2	20030205	EP 200216424	A	20020722	200324 B
JP 2003216591	A	20030731	JP 2002215500	A	20020724	200351 E
TW 576963	A	20040221	TW 2002116472	A	20020724	200455 E
US 6789147	B1	20040907	US 2001307643	P	20010724	200459 E
			US 200125512	A	20011219	

Priority Applications (no., kind, date): US 2001307643 P 20010724; US 200125512 A 20011219

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
EP 1282025	A2	EN	22	10	
Regional Designated States, Original: AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR					
JP 2003216591	A	JA	64		
TW 576963	A	ZH			
US 6789147	B1	EN			Related to Provisional US 2001307643

Alerting Abstract EP A2

NOVELTY - A processor includes execution units to process requests for security operations, and output results of the requests to output data structures associated with the requests within a remote memory based on pointers stored in the requests.

DESCRIPTION - The method involves communicating tasks and results between a host processor and a security coprocessor having a number of execution units. A host processor can transfer the type of tasks, in particular macro security operations, to the security processor. The security coprocessor having multiple execution units receives requests and provides results through a continuous flow mechanism. The received requests are treated as independent of each other, are **distributed** to available multiple **execution** units in- **order**, can be macro-security **operations**, can take **different** amounts of **time** to **complete** and can be **completed** /returned out-of-order.

INDEPENDENT CLAIMS are included for

- 1.a method executing on a host processor;
- 2.a processor including a number of execution units;
- 3.a system comprising a host processor coupled to a system bus;
- 4.a machine readable medium storing instructions for executing the

method.

USE - Processing **security** operations in online sales for business-to-business and **business** -to-customer over communications networks e.g. Internet.

ADVANTAGE - Macro- **security** operations can be **used** with different techniques for communicating **tasks** and results between **a** host processor and a security processor.

DESCRIPTION OF DRAWINGS - The drawing shows an exemplary establishment of a secure SSL 3.0 session according to an embodiment of the invention.

401 Client

403 Server

407, 409, 423, 425 Security operations

Title Terms/Index Terms/Additional Words: INTERFACE; METHOD; SECURE; PROCESSOR; TRANSACTION; NETWORK; MACRO; OPERATE; COMMUNICATE; TASK; RESULT; HOST

Class Codes

International Classification (Main): G06F-001/00, G06F-015/16, G06F-009/00

(Additional/Secondary): G06F-012/00, G06F-013/00, G06F-015/177,

G06F-009/38

US Classification, Issued: 710200000, 713200000, 712034000

File Segment: EPI;

DWPI Class: T01; W01

Manual Codes (EPI/S-X): T01-D01; T01-M05; T01-N01A2A; T01-N02B1B; T01-S03; W01-A05A

Interfacing method for security processor used in online transactions over networks e.g. Internet, in which macro- security operations are used for communicating tasks and results between host and security processors

Alerting Abstract ...a continuous flow mechanism. The received requests are treated as independent of each other, are **distributed** to available multiple **execution** units in- **order** , can be macro-security **operations** , can take **different** amounts of **time** to **complete** and can be **completed** /returned out-of-order...

... **USE** - Processing **security** operations in online sales for business-to- **business** and **business** -to-customer over communications networks e.g. Internet...

...**ADVANTAGE** - Macro- **security** operations can be **used** with different techniques for communicating **tasks** and results between **a** host processor and a security processor

Original Publication Data by Authority

Claims:

...for security operations from a host memory, wherein the number of requests are in an **order** within the host **memory** ; **distributing** , by the request unit, the **number** of requests for the security operations to a number of execution units, wherein the distribution...

...for security operations from a host memory, wherein the number of requests are in an **order** within the host memory; **distributing** , by the request unit, the number of requests for the security operations to a number of execution **units** , wherein the **distribution** is based on **availability** of the number of execution units; processing the number of

requests for the security operations...

7/69,K/10 (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2007 The Thomson Corporation. All rts. reserv.

0013416971 - Drawing available
WPI ACC NO: 2003-507459/200348
XRPX Acc No: N2003-403057

Computer system operated in security trading system providing reference market for processing orders has pre-match control unit for executing order against quote if order matches quote

Patent Assignee: DEUT BOERSE AG (DEBO-N)
Inventor: GOMBER P; MAURER K; ZICKWOLFF M
Patent Family (2 patents, 27 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
EP 1321870	A1	20030625	EP 2001129858	A	20011214	200348 B
US 20030177086	A1	20030918	US 2002307506	A	20021202	200362 E

Priority Applications (no., kind, date): EP 2001129858 A 20011214

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing	Notes
EP 1321870	A1	EN	28	8		

Regional Designated States, Original: AL AT BE CH CY DE DK ES FI FR GB GR
IE IT LI LT LU LV MC MK NL PT RO SE SI TR

Alerting Abstract EP A1

NOVELTY - A pre-match control unit (255) is used for determining whether an order matches a quote. The pre-match control unit may be arranged for executing the order against the quote if the order matches the quote or automatically forwarding the order to the reference market for execution if the order does not match the quote.

DESCRIPTION - INDEPENDENT CLAIMS are included for:

1.a method of operating a computer system for processing orders in a security trading system

USE - For processing orders in a **security** trading system providing a reference market, in which orders are matched with quotes for execution purposes.

ADVANTAGE - Provides such internalization functionality without the need to re-submit an order that could not be internalized, to the order book.

DESCRIPTION OF DRAWINGS - The drawing illustrates a system according to a preferred embodiment of the invention.

255 pre-match control unit

Title Terms/Index Terms/Additional Words: COMPUTER; SYSTEM; OPERATE; SECURE ; TRADE; REFERENCE; MARKET; PROCESS; ORDER; PRE; MATCH; CONTROL; UNIT; EXECUTE

Class Codes

International Classification (Main): G06F-017/60
US Classification, Issued: 705037000

File Segment: EPI;
DWPI Class: T01
Manual Codes (EPI/S-X): T01-J05A2F; T01-N01A2F

Alerting Abstract ...a method of operating a **computer system** for processing orders in a security trading system...

...USE - For processing orders in a **security** trading system providing a reference market, in which orders are matched with quotes for execution...

Original Publication Data by Authority

Original Abstracts:

The invention provides a method of operating a **computer system** for processing **orders** in a security trading system providing a reference market, and a corresponding computer system. A message that indicates a...

...The invention provides a method of operating a **computer system** for processing **orders** in a security trading **system providing** a reference **market**, and a corresponding **computer system**. A message that indicates a (private) quote is received. The quote includes quote parameters defining...

...invention therefore provides an integrated internalization functionality in a security trading system leading to best **execution** of **orders**, to price- **time** priority consistency, order **book** consistency, full transparency and fairness.

Claims:

Computer system operated in a security trading system (260) providing a reference market, the **computer system being arranged** for processing **orders** and **comprising**: means for receiving a message indicating a quote, the quote including quote parameters implicitly defining...

...1. Computer system operated in a security trading system (260) providing a reference market, the **computer system** being arranged **for processing orders** and comprising: means for receiving a message indicating a quote, the quote including **quote parameters** implicitly defining a buy **limit order** and a sell limit order; a quote storage (250) for storing the quote parameters; means...

7/69,K/9 (Item 9 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2007 The Thomson Corporation. All rts. reserv.

0013565781 - Drawing available

WPI ACC NO: 2003-660043/200362

Related WPI Acc No: 2003-660044; 2007-024009

XRPX Acc No: N2003-526333

Data network management and service provider using command line interface framework, transmits command sequences to corresponding managed data network entity, for execution of command line interface actions in entity

Patent Assignee: ALCATEL CANADA INC (COGE); CHAN D W (CHAN-I); KATZ F (KATZ-I); LANDRY K E D (LAND-I); MURRAY C (MURR-I); NGO C N (NGOC-I); ZABIHI A (ZABI-I)

Inventor: CHAN D W; KATZ F; LANDRY K E D; MURRAY C; MURRAY C W; NGO C N; ZABIHI A

Patent Family (7 patents, 32 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
US 20030115304	A1	20030619	US 2002115900	A	20020405	200362 B
CA 2365436	A1	20030619	CA 2365436	A	20011219	200362 E
EP 1322066	A2	20030625	EP 2002293097	A	20021213	200362 E
US 7113989	B2	20060926	US 2002115900	A	20020405	200663 E
EP 1322066	B1	20061220	EP 2002293097	A	20021213	200702 E
DE 60216885	E	20070201	DE 60216885	A	20021213	200722 E
			EP 2002293097	A	20021213	
DE 60216885	T2	20070705	DE 60216885	A	20021213	200744 E
			EP 2002293097	A	20021213	

Priority Applications (no., kind, date): CA 2365436 A 20011219; US 2002115900 A 20020405

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 20030115304	A1	EN	13	7	
CA 2365436	A1	EN			
EP 1322066	A2	EN			

Regional Designated States,Original: AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR

EP 1322066 B1 EN

Regional Designated States,Original: DE ES FR GB IT

DE 60216885	E	DE	Application	EP 2002293097
			Based on OPI patent	EP 1322066
DE 60216885	T2	DE	Application	EP 2002293097
			Based on OPI patent	EP 1322066

Alerting Abstract US A1

NOVELTY - A command line interface (CLI) processor (520) processes the CLI dictionary entries holding vocabulary and grammar specifications of commands used in interacting with at least one **managed data network** entity (510), on receiving request for CLI actions to be performed from a managed object server (MOS) (200). A communication module (540) transmits each CLI command sequence to corresponding network entity, for execution.

DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

- 1.method of interacting with managed data network entity; and
- 2.method of providing dictionary of CLI commands.

USE - For **managing data networks** such as wireless local area **network**

(LAN) comprising data switching equipments, routers, bridge, access nodes providing multiplexing function, remote access servers (RAS), distribution nodes providing demultiplexing function, customer premise equipment (CPE) and for controlling software applications such as inventory reporting, configuration **management**, statistics gathering, performance reporting, fault **management**, **network surveillance**, **service provisioning**, **billing and accounting and security enforcement using** command line interface framework.

ADVANTAGE - Provides automatic entry of CLI command in dictionary and support for multi-vendor equipment by using multiple CLI command vocabularies and dictionaries. Reduces data **network entity management costs and time and improves development and maintenance of the network management** and service provisioning solution.

DESCRIPTION OF DRAWINGS - The figure shows the block diagram of the data **network management** and service provisioning command line interface framework.

200 managed object server
510 **managed data network** entity
520 CLI processor
540 communication module

Title Terms/Index Terms/Additional Words: DATA; NETWORK; MANAGEMENT; SERVICE; COMMAND; LINE; INTERFACE; FRAMEWORK; TRANSMIT; SEQUENCE; CORRESPOND; ENTITY; EXECUTE; ACTION

Class Codes

International Classification (+ Attributes)

IPC + Level Value Position Status Version

G06F-0015/173 A I F B 20060101
H04L-0012/24 A I R 20060101
H04L-0012/24 A I F B 20060101
H04L-0012/24 A I F 20060101
G06F-0015/16 C I F B 20060101
H04L-0012/24 C I R 20060101
H04L-0012/24 C I F B 20060101
H04L-0012/24 C I 20060101
H04L-0012/24 C I B 20060101

US Classification, Issued: 709223000, 709222000, 709224000, 709220000, 709223000, 370241000, 370254000, 707100000

File Segment: EPI;

DWPI Class: T01; W01

Manual Codes (EPI/S-X): T01-F05B; T01-N02A2; W01-A06B5A; W01-A06E

Data network management and service provider using command line interface framework, transmits command sequences to corresponding managed **data network entity**, **for execution of command line interface actions in entity**

Alerting Abstract ...entries holding vocabulary and grammar specifications of commands used in interacting with at least one **managed data network entity** (510), on receiving request for CLI actions to be performed from a managed object...

...method of interacting with **managed data network entity**; and method of providing dictionary of CLI commands...

...USE - For **managing data networks** such as wireless local area **network** (LAN) comprising data switching equipments, routers, bridge, access nodes providing multiplexing function, remote access servers...

...function, customer premise equipment (CPE) and for controlling software applications such as inventory reporting, configuration **management**, statistics gathering, performance reporting, fault **management**, **network** surveillance, service provisioning, billing and accounting and **security enforcement** using command line interface framework...

...support for multi-vendor equipment by using multiple CLI command vocabularies and dictionaries. Reduces data **network** entity **management** costs and time and improves development and maintenance of the **network management** and service provisioning solution...

...DESCRIPTION OF DRAWINGS - The figure shows the block diagram of the data **network management** and service provisioning command line interface framework...

...510 **managed** data **network** entity...

Original Publication Data by Authority

Original Abstracts:

A method of interacting with a **managed** data **network** entity is provided. The method includes a sequence of steps. A change in the operational state of the **managed** data **network** entity is detected. A CLI dictionary entry is retrieved from a CLI dictionary associated with...

...Based on the retrieved CLI dictionary entry, CLI commands are extracted therefrom to configure the **managed** data **network** entity to reflect the detected change in the operational state. A CLI command sequence is...

...the extracted CLI commands. Each CLI command in the command sequence is sent to the **managed** data **network** entity for execution. CLI command responses are monitored. Based on a successful execution of CLI...

...commands in the CLI command sequence are sent for execution. The solution provides automated configuration **management** of data **network** entities from different vendors when SNMP is not a viable option. The automation eliminates manual CLI command entry in providing **network management** and service provisioning solutions, provides support for multi-vendor equipment by processing multiple CLI command vocabulary and grammar specifications in the CLI command dictionary. The solution reduces data **network** entity **management** costs, downtime, and training time for analysts. The advantages are derived from the ability to...

...data network entities with human readable code greatly improving the development and maintenance of the **network management** and service provisioning solution...

...A method of interacting with a **managed** data **network** entity is provided. The method includes a sequence of steps. A change in the operational state of the **managed** data **network** entity is detected. A CLI dictionary entry is retrieved from a CLI dictionary associated with...

...Based on the retrieved CLI dictionary entry, CLI commands are extracted therefrom to configure the **managed** data **network** entity to reflect the detected change in the operational state. A CLI command sequence is...

...the extracted CLI commands. Each CLI command in the command sequence is sent to the **managed** data **network** entity for execution. CLI command responses are monitored. Based on a successful execution of CLI...

...commands in the CLI command sequence are sent for execution. The

solution provides automated configuration **management** of data **network** entities from different vendors when SNMP is not a viable option. The automation eliminates manual CLI command entry in providing **network management** and service provisioning solutions, provides support for multi-vendor equipment by processing multiple CLI command vocabulary and grammar specifications in the CLI command dictionary. The solution reduces data **network** entity **management** costs, downtime, and training time for analysts. The advantages are derived from the ability to...

...data network entities with human readable code greatly improving the development and maintenance of the **network management** and service provisioning solution...

...A method of interacting with a **managed** data **network** entity is provided. The method includes a sequence of steps. A change in the operational state of the **managed** data **network** entity is detected. A CLI dictionary entry is retrieved from a CLI dictionary associated with...

...Based on the retrieved CLI dictionary entry, CLI commands are extracted therefrom to configure the **managed** data **network** entity to reflect the detected change in the operational state. A CLI command sequence is...
...the extracted CLI commands. Each CLI command in the command sequence is sent to the **managed** data **network** entity for execution. CLI command responses are monitored. Based on a successful execution of CLI...

...commands in the CLI command sequence are sent for execution. The solution provides automated configuration **management** of data **network** entities from different vendors when SNMP is not a viable option. The automation eliminates manual CLI command entry in providing **network management** and service provisioning solutions, provides support for multi-vendor equipment by processing multiple CLI command vocabulary and grammar specifications in the CLI command dictionary. The solution reduces data **network** entity **management** costs, downtime, and training time for analysts. The advantages are derived from the ability to...

...data network entities with human readable code greatly improving the development and maintenance of the **network management** and service provisioning solution.

Claims:

Network management and service provisioning Command Line Interface (CLI) framework, comprising: **a.** a processor responsive to...

...holding vocabulary and grammar specifications of a plurality of commands used in interacting with at **least** one **managed** data network entity; and **c.** a communications module sending in sequence for execution and...

...of commands generated in response to the notification as specified in the plurality of dictionary **entries** wherein a network management and service provisioning solution is provided making abstraction of the **at least one** managed data network entity...

...A Command Line Interface (CLI) **framework** for a network manager (NM) that manages a plurality of managed entities of a communication network, comprising: a CLI dictionary (530) holding vocabulary and grammar specifications for all...

...sequence of commands required to configure a managed entity that said managed object represents in **response** to **said event** and handling **execution** of **said** sequence of commands at said managed entity; and a communications module (540) for transmitting said sequence of commands to

said managed entity for execution, and interpreting results **received** from said managed **entity**, **wherein** a network management and service provisioning solution is provided making abstraction of the type of...

...I/we **claim** : **1** . A network management and service provisioning Command Line Interface (CLI) framework, comprising: a. a processor...

...entries holding vocabulary and grammar specifications of a plurality of commands used in interacting with **at least one** managed data network entity; and c. a communications module sending in sequence for execution and...

...of commands generated in response to the notification as specified in the plurality of dictionary **entries wherein** a network management and service provisioning solution is provided making abstraction of the **at least one** managed data network entity...

...We claim:1. A Command Line Interface (CLI) framework **component of** a Network Management System (**NMS**), the NMS managing a plurality **of field installed** managed communications network entities **of** a communications network, **each field installed** managed communications network entity being represented and modeled by an associated managed object instance stored...

...database associated with the NMS, the CLI framework component comprising: a. a CLI dictionary codifying **a plurality of** managed communications network entity-specific **CLI** commands and maintaining at least one **mapping** between **the** managed communications network entity-specific CLI commands **and** a corresponding managed object type;b. a generic processor executing coded logic to: i. detect...

...responsive to the detected event selectively generate a sequence of CLI commands required to configure **the field installed** managed communications network entity **associated** with said managed object instance by consulting the CLI dictionary;iii. handle execution of said sequence of CLI commands at **said field installed** managed communications network entity, including interpreting CLI command execution results received from **said field installed** managed communications network entity; andiv. generating an error report based on an unsuccessful execution...

...the execution results; andc. a communications module transmitting said sequence of CLI commands to **said field installed** managed communications network entity to be executed thereon, and conveying the execution results received from **said field installed** managed communications network entity to the generic **processor**, **wherein** a network management and service provisioning solution is provide **making abstraction of** managed communications network entity types.

Set	Items	Description
S1	1569864	COMPUTER?(2N)SYSTEM? ? OR NETWORK? OR DISTRIBUT? OR ETHERNET? OR INTERNET OR INTRANET? OR LAN OR LANS OR WAN OR WANS OR WLAN? ? OR VLAN? ?
S2	14742	S1(5N)(PROTECT? OR SECUR? OR GUARD? OR FORTIF? OR SHIELD? - OR ENFORC?) (3N)(ACCESS? OR ENTRY OR ENTRIE? ? OR USE??? OR UTILI? OR USING)
S3	3481	S2(5N)(ENFORC? OR CONTROL? OR REGULAT? OR DIRECT? OR MANAG? OR ADMINISTRAT? OR SUSTAIN? OR ORDER??? OR MAINTAIN? OR SUPERVIS???)
S4	195926	(ORDER?())SET? ? OR SEQUEN? OR PATTERN? OR ORDER?) (5N)(LEVEL? OR STEP? ? OR STAGE? OR TIER?? ? OR OPERATION? OR FUNCTION? OR COMMAND?)
S5	26666	S4(5N)(TIME? ? OR TIMING OR TEMPORAL? OR CLOCK? OR DURATION? OR EVENT? OR SCHEDUL? OR OCCASION? OR DAY? ? OR HOUR? ? OR MINUTE? ? OR SECOND? ? OR PERIOD?)
S6	33021	S4:S5(5N)(SECOND? OR COUPLE OR 2ND OR 2 OR DUAL?? OR TWICE OR ANOTHER? OR TWO OR DIFFERENT OR PAIR OR MORE(2N)ONE OR ADDITIONAL)
S7	5876	S6(5N)(PERFORM? OR EXECUT? OR IMPLEMENT? OR OPERATE? ? OR - OPERATING OR ENACT? OR HANDL? OR (CARRY? OR CARRIE? ?)())OUT OR COMPLET? OR ENABL? OR ALLOW?)
S8	54114	(PRESELECT? OR PRE()SELECT? OR (SELECT? OR PICK??? OR CHOOSE? OR DESIGNAT? OR CHOSEN OR IDENT?)())BEFORE? OR PREDETERMIN? OR PRE()(DETERMIN? OR SPECIF?) (5N)(ACCESS? OR ENTRY OR ENTRIE? ? OR USE??? OR UTILI?)
S9	1	S3 AND S7 AND S8
S10	126	S3 AND ENFORC?(3N)SECUR?
S11	3	S10 AND S8
S12	2	S2:S3 AND S7 AND S8
S13	1	S12 NOT (S9 OR S11)
S14	22	S2:S3 AND S4:S5 AND S8
S15	19	S14 NOT (S9 OR S11:S13)
S16	126817	(DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR TRANSFER? OR TRANSMI? OR BEAM??? OR LOAD??? OR POST??? ?) (5N)(- SEARCH? OR RESEARCH? OR RETRIEV? OR INQUIR? OR QUERY? OR QUERIE? ? OR REQUEST? OR ASK???)
S17	274804	(RETRIEV? OR RECEIV??? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR DOWNLOAD? OR FETCH??? OR ACCESS?) (5N)(SEARCH? OR RESEARCH? OR RETRIEV? OR INQUIR? OR QUERY? OR QUERIE? ? OR REQUEST? OR ASK???)
S18	4	S15 AND S16:S17
S19	15	S15 NOT S18
S20	13	AU=(KOVARIK V? OR KOVARIK, V?)
S21	0	(VINCENT OR VINCE OR VINNIE) (2N) KOVARIK
S22	1	S20 AND S2:S3

File 350:Derwent WPIX 1963-2007/UD=200752
(c) 2007 The Thomson Corporation
File 347:JAPIO Dec 1976-2007/Mar(Updated 070809)
(c) 2007 JPO & JAPIO

*Abstract lat. files
(2)*

*** Your Assignee ****

11/69,K/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2007 The Thomson Corporation. All rts. reserv.

0015307045 - Drawing available
WPI ACC NO: 2005-657227/200567
XRPX Acc No: N2005-538483

Secure access method in computer system, involves granting access request only, if access request does not complete prohibited temporal access pattern and minimum access level for base node does not exceed

predetermined access level

Patent Assignee: HARRIS CORP (HARO)

Inventor: KOVARIK V J

Patent Family (5 patents, 40 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
US 20050204131	A1	20050915	US 2004798074	A	20040311	200567 B
CA 2499986	A1	20050911	CA 2499986	A	20050309	200567 E
EP 1577735	A2	20050921	EP 20055394	A	20050311	200567 E
JP 2005259146	A	20050922	JP 200565879	A	20050309	200567 E
CN 1667544	A	20050914	CN 200510054559	A	20050311	200607 E

Priority Applications (no., kind, date): US 2004798074 A 20040311

Patent Details

Number	Kind	Lañ	Pg	Dwg	Filing Notes
US 20050204131	A1	EN	18	10	
CA 2499986	A1	EN			
EP 1577735	A2	EN			

Regional Designated States, Original: AL AT BA BE BG CH CY CZ DE DK EE ES
FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK NL PL PT RO SE SI SK TR YU
JP 2005259146 A JA 17

Alerting Abstract US A1

NOVELTY - The method involves determining if **access** request from entity with **predetermined access** level, completes a prohibited temporal access pattern for entity. A minimum access level established for base node (110) is compared to **predetermined access** level. The **access** request is granted only, if the access request does not complete the access pattern and minimum **access** level does not exceed **predetermined access** level.

DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

- 1.method for restricting access to computer system; and
- 2.computer system.

USE - For secure access computer system.

ADVANTAGE - Enables maintaining the access authorities for each user dynamically, thereby allowing system objects to have multiple level of access classification based on historical access by each user.

DESCRIPTION OF DRAWINGS - The figure shows the data primitives and hierarchical graph for secure access to computer system.

- 1021-1024 object types
- 1041-1043 system functions
- 110 base node
- 112 higher level node

Title Terms/Index Terms/Additional Words: SECURE; ACCESS; METHOD; COMPUTER; SYSTEM; REQUEST; COMPLETE; PROHIBIT; TEMPORAL; PATTERN; MINIMUM; LEVEL; BASE; NODE; PREDETERMINED

Class Codes

International Classification (Main): G06F-001/00, G06F-012/14, H04L-009/00
US Classification, Issued: 713166000

File Segment: EPI;

DWPI Class: T01; W01

Manual Codes (EPI/S-X): T01-H01C2; T01-J12C; T01-N02B1B; W01-A06E1C

...complete prohibited temporal access pattern and minimum access level for
base node does not exceed predetermined access level

Original Titles:

...Method and system enforcing computer security utilizing an
adaptive lattice mechanism...

... ENFORCING COMPUTER SECURITY UTILIZING ADAPTIVE LATTICE MECHANISM...

... Enforcing computer security utilizing an adaptive lattice mechanism
...NOVELTY - The method involves determining if access request from
entity with predetermined access level, completes a prohibited temporal
access pattern for entity. A minimum access level established for base node
(110) is compared to predetermined access level. The access request
is granted only, if the access request does not complete the access pattern
and minimum access level does not exceed predetermined access level.

Original Publication Data by Authority

Original Abstracts:

...the computer system a request from an entity (using 1002). The entity
can have a predetermined access authorization level for access to a
first base node (110) representing an information type (102) or a
computer system function (104). The system...

...access pattern for the entity. The system also compares a minimum access
level established for the first base node to the predetermined access
authorization level assigned to the entity. Thereafter, the system can
grant the access request only if the minimum access level for the first
base node does not exceed to the predetermined access authorization
level.

...

...the computer system a request from an entity (using 1002). The
entity can have a predetermined access authorization level for access
to a first base node (110) representing an information type
(102) or a computer system function (104). The system
determines if the access request completes a prohibited temporal...

...entity. The system also compares a minimum access level established for
the first base node to the predetermined access authorization level
assigned to the entity. Thereafter, the system can grant the access
request only if the minimum access level for the first base node does
not exceed to the predetermined access authorization level.

Claims:

...the steps of:receiving in said computer system a request from an entity
with a predetermined access level for access to a first base node
representing at least one of an information type and a computer system
function;determining...

...for said entity; and comparing a minimum access level established for said first base node to said **predetermined access** level; and granting said **access** request **only if** it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said **predetermined access** level.

...

...computer system, comprising the steps of: receiving in said computer system a request from an **entity** with a **predetermined access** level for **access** to a first base node representing at least one of an information type and a **computer system** function; determining **if** said **access** request completes a prohibited temporal access pattern for said entity; and comparing a minimum access level established for said first base node to said **predetermined access** level; **and** granting said **access** request **only if** it does not complete a prohibited temporal access pattern for said entity, and said **minimum access** level for said first base node **does** not exceed said **predetermined access** level.

13/69,K/1 (Item 1 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2007 The Thomson Corporation. All rts. reserv.

0001862168

WPI ACC NO: 1979-K8815B/197947

Authenticating identity of user of information system - transferring terminal user authentication pattern with identification number to host data processing system

Patent Assignee: IBM CORP (IBMC)

Inventor: MATYAS S M; MEYER C H W

Patent Family (5 patents, 5 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
EP 5179	A	19791114	EP 1979101038	A	19790405	197947 B
US 4218738	A	19800819	US 1978903286	A	19780505	198036 E
CA 1111563	A	19811027				198148 E
EP 5179	B	19830518	EP 1979101038	A	19790405	198321 E
DE 2965420	G	19830707				198328 E

Priority Applications (no., kind, date): EP 1979101038 A 19790405; US 1978903286 A 19780505

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
EP 5179	A	EN			
Regional Designated States,Original: DE FR GB IT					
CA 1111563	A	EN			
EP 5179	B	EN			
Regional Designated States,Original: DE FR GB IT					

Alerting Abstract EP A

A process confirms the identity of a terminal user provided with an identification number and a secret password in a system providing data communication between a terminal and a host data processing system each having cryptographic appts. The identification number and password are used at the terminal to obtain a terminal user authentication pattern which is transferred with the identification number from the terminal to the host d.p.s.

At the host d.p.s. an operation is performed in accordance with a predetermined number provided by the host and the terminal user identification number to obtain a terminal user first verification pattern. The latter is compared with a second verification pattern obtained at the host d.p.s. in accordance with a **predetermined** terminal **user** test pattern provided at the host d.p.s. and the terminal user authentication pattern.

The process authenticates the identity of a terminal user provided with an identification number and a secret password more securely than customary.

Title Terms/Index Terms/Additional Words: AUTHENTICITY; IDENTIFY; USER; INFORMATION; SYSTEM; TRANSFER; TERMINAL; PATTERN; NUMBER; HOST; DATA; PROCESS

Class Codes

International Classification (Main): G06F-013/00

(Additional/Secondary): G06F-003/00, G07C-011/00, H04K-001/00

US Classification, Issued: 380025000, 340825310, 364DIG002, 364222200, 364222500, 364228400, 364234000, 364235000, 364236200, 364236300, 364238300, 364248100, 364248200, 364259000, 364259200, 380045000

File Segment: EPI;
DWPI Class: T01; T05

Alerting Abstract ...a second verification pattern obtained at the host d.p.s. in accordance with a **predetermined** terminal **user** test pattern provided at the host d.p.s. and the terminal user authentication pattern...

Original Publication Data by Authority

Original Abstracts:

...authentication processing. This is accomplished by providing terminal user identification numbers and passwords and a **predetermined number** at the host data processing system. A first initialization operation is performed at the host...

...in accordance with the terminal user identification numbers and passwords to obtain terminal user authentication **patterns**. A **second** initialization **operation** is **performed** at the host **data** processing **system** in **accordance** with the **predetermined** number and the terminal **user** identification numbers to obtain terminal **user** first **verification** patterns. A third initialization operation is performed at the host data processing system in accordance...

...during authentication processing and for generating test patterns during the secure run is disclosed which **uses** a variation of the host computer master **key** to reduce risk of **compromise** of total **system** **security**. The **use** of a variant of the host master key prevents system programmers and/or computer operators...

?

18/69,K/1 (Item 1 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2007 The Thomson Corporation. All rts. reserv.

0016174489 - Drawing available

WPI ACC NO: 2006-706129/200673

XRPX Acc No: N2006-555460

Security apparatus for use in telecommunication system, has computer for providing user authorization by comparing authorization user input to security code based on retrieved user profile

Patent Assignee: ACCESSLINE COMMUNICATIONS CORP (ACCE-N)

Inventor: EPLER F A; KNIGHT J M; STENSBERG P A; ZHUK O V

Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
US 7106845	B1	20060912	US 2000604283	A	20000626	200673 B

Priority Applications (no., kind, date): US 2000604283 A 20000626

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 7106845	B1	EN	27	11	

Alerting Abstract US B1

NOVELTY - The apparatus has a database storing a user profile indicating a set of security modes selectable by the user. A computer communicates with the database to receive telecommunication data transmissions. The computer stores selected security mode in the user profile corresponding to the user. The computer provides user authorization by comparing authorization user input to a security code based on the **retrieved** user profile.

DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

- 1.a method of providing security for a telecommunication system
- 2.a computer-readable signal bearing medium storing instructions for a computer for providing security for a telecommunication system
- 3.a user prompt signal for providing security for a telecommunication system.

USE - Used in a telecommunication system for telecommunication company, professional service provider such as doctor, lawyer and accountant, financial institution such as bank and securities broker and insurance company.

ADVANTAGE - The computer compares the authorization user input to the security code based on the **retrieved** user profile to provide user authorization, thus effectively providing user security and access to the telecommunication system.

DESCRIPTION OF DRAWINGS - The drawing shows a block diagram of a suitable environment employing a dynamic security system.

Title Terms/Index Terms/Additional Words: SECURE; APPARATUS; TELECOMMUNICATION; SYSTEM; COMPUTER; USER; AUTHORISE; COMPARE; INPUT; CODE; BASED; **RETRIEVAL** ; PROFILE

Class Codes

International Classification (+ Attributes)

IPC + Level Value Position Status Version

H04M-0003/42 A I F B 20060101

US Classification, Issued: 379207110, 379201120, 379189000, 455410000

File Segment: EPI;

DWPI Class: T01; W01

Manual Codes (EPI/S-X): T01-N02B1B; T01-S03; W01-A05B; W01-C02B6

Security apparatus for use in telecommunication system, has computer for providing user authorization by comparing authorization user input to security code based on retrieved user profile

Alerting Abstract ...provides user authorization by comparing authorization user input to a security code based on the **retrieved** user profile....**ADVANTAGE** - The computer compares the authorization user input to the security code based on the **retrieved** user profile to provide user authorization, thus effectively providing user security and access to the ...

Title Terms.../Index Terms/Additional Words: **RETRIEVAL** ;

Original Publication Data by Authority

Original Abstracts:

...typically only the user would know. Another level of security employs voice fingerprinting or voice **pattern** recognition. Yet another **level** employs a N by M matrix of random numbers, from which a **user** selects numbers from **predetermined** positions to generate a current security code. Various levels of security may be performed on...

Claims:

...user profile corresponds to the user, in response to a telecommunications call from the user, **retrieve** the at least one user profile, receive authorization user input, and provide user authorization by comparing the received authorization user input to a security code based on the **retrieved** user profile, wherein the security code is an automatically and dynamically generated user security code...

...wherein the plurality of security modes includes a current time sequence recognition mode wherein the **user** security code is based on **predetermined** numerical sequence based on an hour of day, day of week, day of month and...

* AU/INN srch - your Assignee/INN

22/69,K/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2007 The Thomson Corporation. All rts. reserv.

0015307045 - Drawing available
WPI ACC NO: 2005-657227/200567
XRPX Acc No: N2005-538483

Secure access method in computer system, involves granting access request only, if access request does not complete prohibited temporal access pattern and minimum access level for base node does not exceed predetermined access level

Patent Assignee: HARRIS CORP (HARO)

Inventor: KOVARIK V J

Patent Family (5 patents, 40 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
US 20050204131	A1	20050915	US 2004798074	A	20040311	200567 B
CA 2499986	A1	20050911	CA 2499986	A	20050309	200567 E
EP 1577735	A2	20050921	EP 20055394	A	20050311	200567 E
JP 2005259146	A	20050922	JP 200565879	A	20050309	200567 E
CN 1667544	A	20050914	CN 200510054559	A	20050311	200607 E

Priority Applications (no., kind, date): US 2004798074 A 20040311

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 20050204131	A1	EN	18	10	
CA 2499986	A1	EN			
EP 1577735	A2	EN			

Regional Designated States, Original: AL AT BA BE BG CH CY CZ DE DK EE ES
FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK NL PL PT RO SE SI SK TR YU
JP 2005259146 A JA 17

Alerting Abstract US A1

NOVELTY - The method involves determining if access request from entity with predetermined access level, completes a prohibited temporal access pattern for entity. A minimum access level established for base node (110) is compared to predetermined access level. The access request is granted only, if the access request does not complete the access pattern and minimum access level does not exceed predetermined access level.

DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

- 1.method for restricting access to computer system; and
- 2.computer system.

USE - For secure access computer system .

ADVANTAGE - Enables maintaining the access authorities for each user dynamically, thereby allowing system objects to have multiple level of access classification based on historical access by each user.

DESCRIPTION OF DRAWINGS - The figure shows the data primitives and hierarchical graph for secure access to computer system .

- 1021-1024 object types
- 1041-1043 system functions
- 110 base node
- 112 higher level node

Title Terms/Index Terms/Additional Words: SECURE; ACCESS; METHOD; COMPUTER; SYSTEM; REQUEST; COMPLETE; PROHIBIT; TEMPORAL; PATTERN; MINIMUM; LEVEL; BASE; NODE; PREDETERMINED

Class Codes

International Classification (Main): G06F-001/00, G06F-012/14, H04L-009/00
US Classification, Issued: 713166000

File Segment: EPI;

DWPI Class: T01; W01

Manual Codes (EPI/S-X): T01-H01C2; T01-J12C; T01-N02B1B; W01-A06E1C

Secure access method in computer system, involves granting access request only, if access request does not complete prohibited temporal access pattern and minimum access...

Original Titles:

...Method and system enforcing computer security utilizing an adaptive lattice mechanism...

Inventor: KOVARIK V J

Alerting Abstract ... USE - For secure access computer system .
...

...DESCRIPTION OF DRAWINGS - The figure shows the data primitives and hierarchical graph for secure access to computer system .

Original Publication Data by Authority

Inventor name & address:

KOVARIK V J ...

... Kovarik, Vincent Joseph, Jr ...

... KOVARIK VINCENT JOSEPH JR ...

... Kovarik, Vincent Joseph JR

Original Abstracts:

Method and apparatus for ensuring secure access to a computer system (1000). The method can begin with the step of receiving in the computer system a request from an entity...

...Method and apparatus for ensuring secure access to a computer system (1000). The method can begin with the step of receiving in the computer system a request from an entity (using 1002). The entity can have a predetermined access authorization level for access to a first...

Claims:

A method for secure access to a computer system, comprising the steps of:receiving in said computer system a request from an entity with a predetermined...

...1. A method for secure access to a computer system, comprising the steps of:receiving in said computer system a request from an entity with a predetermined access level for access to a first base node representing at least one of an information type and a...
?

Set	Items	Description
S1	883612	COMPUTER?(2N) (SYSTEM? ? OR SECUR?) OR NETWORK? OR DISTRIBUT? OR ETHERNET? OR INTERNET OR INTRANET? OR LAN OR LANS OR WAN OR WANS OR WLAN? ? OR VLAN? ?
S2	14705	S1(7N) ((PROTECT? OR SECUR? OR GUARD? OR FORTIF? OR SHIELD?-) (5N) (ACCESS? OR ENTRY OR ENTRIE? ? OR USE??? OR UTILI? OR USING))
S3	3588	S2(7N) (ENFORC? OR CONTROL? OR REGULAT? OR DIRECT? OR MANAG? OR ADMINISTRAT? OR SUSTAIN? OR ORDER??? OR MAINTAIN? OR SUPERVIS???)
S4	374666	(ORDER?())SET? ? OR SEQUEN? OR PATTERN? OR ORDER?OR SEQUENTIAL? OR SERIE?? OR SERIAL?? OR IN()ORDER? OR CONTIGU? OR CONSECUT? OR SERIAT? OR STEPWISE? OR CONSECUT? OR ONE()AFTER(2W-) (OTHER OR ANOTHER)) (5N) (LEVEL? OR STEP? ? OR STAGE? OR TIER?? ? OR OPERATION? OR FUNCTION? OR COMMAND?)
S5	47231	S4(5N) (TIME? ? OR TIMING OR TEMPORAL? OR CLOCK? OR DURATION? OR EVENT? OR SCHEDUL? OR OCCASION? OR DAY? ? OR HOUR? ? OR MINUTE? ? OR SECOND? ? OR PERIOD?)
S6	90467	S4:S5(7N) (SECOND? OR COUPLE OR 2ND OR 2 OR DUAL?? OR TWICE OR ANOTHER? OR TWO OR DIFFERENT OR PAIR OR MORE(2N)ONE OR ADDITIONAL)
S7	17781	S6(7N) (PERFORM? OR EXECUT? OR IMPLEMENT? OR OPERATE? ? OR - OPERATING OR ENACT? OR HANDL? OR (CARRY? OR CARRIE? ?) ()OUT OR COMPLET? OR ENABL? OR ALLOW?)
S8	70957	(PRESELECT? OR PRE()SELECT? OR (SELECT? OR PICK??? OR CHOOSE? OR DESIGNAT? OR CHOSEN OR IDENT?) ()BEFORE? OR PREDETERMIN? OR PRE() (DETERMIN? OR SPECIF?)) (5N) (ACCESS? OR ENTRY OR ENTRIE? ? OR USE??? OR UTILI?)
S9	101478	(DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR TRANSFER? OR TRANSMI? OR BEAM??? OR LOAD??? OR POST??? ?) (5N) (- SEARCH? OR RESEARCH? OR RETRIEV? OR INQUIR? OR QUERY? OR QUERIE? ? OR REQUEST? OR ASK???)
S10	211155	(RETRIEV? OR RECEIV??? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR DOWNLOAD? OR FETCH??? OR ACCESS?) (5N) (SEARCH? OR RESEARCH? OR RETRIEV? OR INQUIR? OR QUERY? OR QUERIE? ? OR REQUEST? OR ASK???)
S11	6	S2:S3(100N)S7(100N)S8(100N)S9:S10
S12	15	S2:S3(100N)S4:S5(100N)S8(100N)S9:S10
S13	18	S11:S12
S14	5	AU=(KOVARIK V? OR KOVARIK, V?)
S15	3	(VINCENT OR VINCE OR VINNIE) (2N)KOVARIK
S16	0	S14:S15(100N)S1(100N)S2:S3
S17	0	S14:S15(100N)S4(100N)S8(100N)S9:S10
S18	0	S14:S15(100N)S1
File 348:EUROPEAN PATENTS 1978-2007/ 200732		
(c) 2007 European Patent Office		
File 349:PCT FULLTEXT 1979-2007/UB=20070809UT=20070802		
(c) 2007 WIPO/Thomson		

Full Text Pat. Files

13/5,K/17 (Item 9 from file: 349)
(DIALOG(R) File 349:PCT:FULLTEXT)
(c) 2007 WIPO/Thomson. All rts. reserv.

00571474 **Image available**
COMPUTER NETWORK INTRUSION DETECTION
DETECTION D'INTRUSION DANS UN RESEAU INFORMATIQUE

Patent Applicant/Assignee:
VISA INTERNATIONAL SERVICE ASSOCIATION,
DIEP Thanh A,

Inventor(s):
DIEP Thanh A,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200034847 A1 20000615 (WO 0034847)
Application: WO 99US29080 19991207 (PCT/WO US9929080)
Priority Application: US 98208617 19981208

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM 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 MD
MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG
US UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ TZ UG ZW AM AZ BY KG KZ MD RU
TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG
CI CM GA GN GW ML MR NE SN TD TG

Main International Patent Class (v7): G06F-001/00

Publication Language: English

Fulltext Availability:

Detailed Description

Claims

Fulltext Word Count: 11423

English Abstract

Detecting harmful or illegal intrusions into a computer network or into restricted portions of a computer network uses statistical analysis to match user commands and program names with a template sequence. Discrete correlation matching and permutation matching are used to match sequences. The result of the match is input to a feature builder and then a modeler to produce a score. The score indicates possible intrusion. A sequence of user commands and program names and a template sequence of known harmful commands and program names from a set of such templates are retrieved. A closeness factor indicative of the similarity between the user command sequence and a template sequence is derived from comparing the two sequences. The user command sequence is compared to each template sequence in the set of templates thereby creating multiple closeness or similarity measurements. These measurements are examined to determine which sequence template is most similar to the user command sequence. A frequency feature associated with the user command sequence and the most similar template sequence is calculated. It is determined whether the user command sequence is a potential intrusion into restricted portions of the computer network by examining output from a modeler using the frequency feature as one input.

French Abstract

L'invention concerne la detection d'intrusions nuisibles ou illegales dans un reseau informatique ou dans des parties reservees dudit reseau, qui consiste a utiliser des analyses statistiques pour comparer des commandes d'utilisateur et des noms de programmes a une sequence modele. Une correspondance de correlation et une correspondance de permutation discretes servent a comparer des sequences. Le resultat de la correspondance est introduit dans un realisateur de caracteristiques,

puis dans un modeliseur pour etabliir une cote, laquelle permet d'indiquer une intrusion possible. Une sequence de commandes d'utilisateur et de noms de programmes, ainsi qu'une sequence modele de commandes et de noms de programmes nuisibles provenant de tels modeles sont recherchees. Un facteur de proximite, indiquant la similitude entre la sequence de commandes d'utilisateur et la sequence modele, est deduit de la comparaison des deux sequences. La sequence de commandes d'utilisateur est comparee a chaque sequence modele de l'ensemble de modeles. On etablit ainsi plusieurs mesures de proximite ou de similitude. L'examen de ces mesures permet de determiner la sequence modele qui presente le plus de similitudes avec la sequence de commandes d'utilisateur. Une caracteristique de frequence, associee a la sequence de commandes d'utilisateur et a la sequence modele qui presente le plus de similitudes, est calculee. On determine si la sequence de commandes d'utilisateur constitue une intrusion potentielle dans des parties reservees du reseau informatique en examinant le resultat d'un modeliseur au moyen de la caracteristique de frequence en tant qu'une entree.

Fulltext Availability:
Detailed Description

Detailed Description

... set of templates is created and can be added to whenever a newly identified suspicious **command** sequence is discovered. The process of generating templates of command sequences is then complete.

Related...

...is analyzed, the program selects the first template from
1 4
template set 14, and **retrieves** the next template in the second iteration, as described below in step 5 1 0...

...Y selection can be based on other criteria such as frequency, importance, or length.

At **step** 506 input **sequence** X ...input sequence X being analyzed
1 5
as shown in FIG. 5. Template Y' is **retrieved** at step 602. Examples of other features are the number of audit records processed for...

...all sequences entered by the same user during time period T. Preferably, the duration of **time** period T used in this **step** is greater than the **sequence** length of the input **sequence** from **step** 306.

io Thus, if the user input **sequence** contains **commands** and program names entered by a user over 30 minutes, time period T is preferably...

...program to calculate an average occurrence or frequency level dynamically without having to store and **retrieve** from memory the multiple values that would be needed to calculate a static average. A...

Examination: 051130 A2 Date of request for examination: 20051005
Change: 060517 A2 Title of invention (German) changed: 20060517
Change: 060517 A2 Title of invention (English) changed: 20060517
Change: 060517 A2 Title of invention (French) changed: 20060517
Change: 061213 A2 Title of invention (German) changed: 20061213
Change: 061213 A2 Title of invention (English) changed: 20061213
Change: 061213 A2 Title of invention (French) changed: 20061213
Grant: 070516 B1 Granted patent

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200442	575
CLAIMS B	(English)	200720	404
CLAIMS B	(German)	200720	390
CLAIMS B	(French)	200720	436
SPEC A	(English)	200442	6252
SPEC B	(English)	200720	5715
Total word count - document A			6828
Total word count - document B			6945
Total word count - documents A + B			13773

...SPECIFICATION phone carried by the user exists in registered specific area where the user makes a **request** for a video information **distribution** service to be provided and the traffic of the radio channel connected to the mobile phone carried by the **user** is lower than the **predetermined** threshold, video information about the specific area is distributed from the video contents server to the mobile phone based on push technology, so that the **user** can **securely** be **distributred** with, for example, video information of commercial, guidance or the like about the specific area...

...a predetermined time period, but displaying the distributed video information is restricted within the predetermined **time in order** to prevent the **function** of the mobile phone from be occupied with displaying the distributed video information. After the...

...SPECIFICATION phone carried by the user exists in registered specific area where the user makes a **request** for a video information **distribution** service to be provided and the traffic of the radio channel connected to the mobile phone carried by the **user** is lower than the **predetermined** threshold, video information about the specific area is distributed from the video contents server to the mobile phone based on push technology, so that the **user** can **securely** be **distributred** with, for example, video information of commercial, guidance or the like about the specific area...

...a predetermined time period, but displaying the distributed video information is restricted within the predetermined **time in order** to prevent the **function** of the mobile phone from be occupied with displaying the distributed video information. After the...

Set	Items	Description
S1	12454539	COMPUTER?(2N) (SYSTEM? ? OR SECUR?) OR NETWORK? OR COMPUTER? OR DISTRIBUT? OR ETHERNET? OR INTERNET OR INTRANET? OR LAN OR LANS OR WAN OR WANS OR WLAN? ? OR VLAN? ?
S2	22262	S1(7N) ((PROTECT? OR SECUR? OR GUARD? OR FORTIF? OR SHIELD?-) (5N) (ACCESS? OR ENTRY? OR ENTRIE? ? OR ENTREE? OR USE??? OR - UTILI? OR USING))
S3	6211	S2(7N) (ENFORC? OR CONTROL? OR REGULAT? OR DIRECT? OR MANAG? OR ADMINISTRAT? OR SUSTAIN? OR ORDER??? OR MAINTAIN? OR SUPE- RVIS???)
S4	475945	(ORDER?()) SET? ? OR SEQUEN? OR PATTERN? OR ORDER? OR SEQUENT- IAL? OR SERIE?? OR SERIAL?? OR IN() ORDER? OR CONTIGU? OR CO- NSECUT? OR SERIAT? OR STEPWISE? OR CONSECUT? OR ONE() AFTER(2W-) (OTHER OR ANOTHER)) (5N) (LEVEL? OR STEP? ? OR STAGE? OR TIER?? ? OR OPERATION? OR FUNCTION? OR COMMAND?)
S5	38489	S4(5N) (TIME? ? OR TIMING OR TEMPORAL? OR CLOCK? OR DURATIO- N? OR EVENT? OR SCHEDUL? OR OCCASION? OR DAY? ? OR HOUR? ? OR MINUTE? ? OR SECOND? ? OR PERIOD?)
S6	64248	S4:S5(7N) (SECOND? OR COUPLE OR 2ND OR 2 OR DUAL?? OR TWICE OR ANOTHER? OR TWO OR DIFFERENT OR PAIR OR MORE(2N) ONE OR ADD- ITIONAL)
S7	5797	S6(7N) (PERFORM? OR EXECUT? OR IMPLEMENT? OR OPERATE? ? OR - OPERATING OR ENACT? OR HANDL? OR (CARRY? OR CARRIE? ?) () OUT OR COMPLET? OR ENABL? OR ALLOW?)
S8	4102	(PRESELECT? OR PRE() SELECT? OR (SELECT? OR PICK??? OR CHOO- SE? OR DESIGNAT? OR CHOSEN OR IDENT?) () BEFORE? OR PREDETERMIN? OR PRE() (DETERMIN? OR SPECIF?)) (5N) (ACCESS? OR ENTRY OR ENTR- IE? ? OR USE??? OR UTILI?)
S9	144801	(DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR T- RANSFER? OR TRANSMI? OR BEAM??? OR LOAD??? OR POST??? ?) (5N) (- SEARCH? OR RESEARCH? OR RETRIEV? OR INQUIR? OR QUERY? OR QUER- IE? ? OR REQUEST? OR ASK???)
S10	489980	(RETRIEV? OR RECEIV??? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR DOWNLOAD? OR FETCH??? OR ACCESS?) (5N) (SEARCH? OR RESEARCH? OR RETRIEV? OR INQUIR? OR QUERY? OR QUERIE? ? OR REQUEST? OR ASK- ???)
S11	0	S2:S3 AND S7 AND S8
S12	1	S2:S3 AND S4:S5 AND S8
S13	0	S7 AND S8 AND S9:S10
S14	150	AU=(KOVARIK V? OR KOVARIK, V?)
S15	0	(VINCENT OR VINCE OR VINNIE) (2N) KOVARIK
S16	21	S14 AND S1:S3
S17	0	S16 AND S4 AND S8
S18	0	S16 AND S9:S10
S19	15	RD S16 (unique items)
File	2:INSPEC 1898-2007/Aug W1	(c) 2007 Institution of Electrical Engineers
File	6:NTIS 1964-2007/Aug W3	(c) 2007 NTIS, Intl Cpyrght All Rights Res
File	8:EI Compendex(R) 1884-2007/Aug W1	(c) 2007 Elsevier Eng. Info. Inc.
File	34:SciSearch(R) Cited Ref Sci 1990-2007/Aug W3	(c) 2007 The Thomson Corp
File	35:Dissertation Abs Online 1861-2007/Jul	(c) 2007 ProQuest Info&Learning
File	56:Computer and Information Systems Abstracts 1966-2007/Aug	(c) 2007 CSA.
File	60:ANTE: Abstracts in New Tech & Engineer 1966-2007/Jul	(c) 2007 CSA.
File	62:SPIN(R) 1975-2007/Jul W5	(c) 2007 American Institute of Physics

*Abstract Npl. files
* Nothing found*

File 65:Inside Conferences 1993-2007/Aug 17
 (c) 2007 BLDSC all rts. reserv.
File 95:TEME-Technology & Management 1989-2007/Aug W2
 (c) 2007 FIZ TECHNIK
File 99:Wilson Appl. Sci & Tech Abs 1983-2007/Jul
 (c) 2007 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2007/Aug 13
 (c) 2007 The Gale Group
File 144:Pascal 1973-2007/Jul W5
 (c) 2007 INIST/CNRS
File 239:Mathsci 1940-2007/Sep
 (c) 2007 American Mathematical Society
File 256:TecInfoSource 82-2007/Nov
 (c) 2007 Info.Sources Inc
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
 (c) 2006 The Thomson Corp
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
 (c) 2002 The Gale Group

Set	Items	Description
S1	21442996	COMPUTER?(2N) (SYSTEM? ? OR SECUR?) OR NETWORK? OR COMPUTER? OR DISTRIBUT? OR ETHERNET? OR INTERNET OR INTRANET? OR LAN OR LANs OR WAN OR WANS OR WLAN? ? OR VLAN? ?
S2	283082	S1(7N) ((PROTECT? OR SECUR? OR GUARD? OR FORTIF? OR SHIELD?-) (5N) (ACCESS? OR ENTRY OR ENTRIE? ? OR USE??? OR UTILI? OR US- ING))
S3	84610	S2(7N) (ENFORC? OR CONTROL? OR REGULAT? OR DIRECT? OR MANAG? OR ADMINISTRAT? OR SUSTAIN? OR ORDER??? OR MAINTAIN? OR SUPE- RVIS???)
S4	307166	(ORDER?())SET? ? OR SEQUEN? OR PATTERN? OR ORDER?OR SEQUENT- IAL? OR SERIE?? OR SERIAL?? OR IN()ORDER? OR CONTIGU? OR CO- NSECUT? OR SERIAT? OR STEPWISE? OR CONSECUT? OR ONE()AFTER(2W-) (OTHER OR ANOTHER)) (5N) (LEVEL? OR STEP? ? OR STAGE? OR TIER?? ? OR OPERATION? OR FUNCTION? OR COMMAND?)
S5	23579	S4(5N) (TIME? ? OR TIMING OR TEMPORAL? OR CLOCK? OR DURATIO- N? OR EVENT? OR SCHEDUL? OR OCCASION? OR DAY? ? OR HOUR? ? OR MINUTE? ? OR SECOND? ? OR PERIOD?)
S6	33087	S4:S5(7N) (SECOND? OR COUPLE OR 2ND OR 2 OR DUAL?? OR TWICE OR ANOTHER? OR TWO OR DIFFERENT OR PAIR OR MORE(2N)ONE OR ADD- ITIONAL)
S7	4917	S6(7N) (PERFORM? OR EXECUT? OR IMPLEMENT? OR OPERATE? ? OR - OPERATING OR ENACT? OR HANDL? OR (CARRY? OR CARRIE? ?) ()OUT OR COMPLET? OR ENABL? OR ALLOW?)
S8	9378	(PRESELECT? OR PRE()SELECT? OR (SELECT? OR PICK??? OR CHOO- SE? OR DESIGNAT? OR CHOSEN OR IDENT?) ()BEFORE? OR PREDETERMIN? OR PRE() (DETERMIN? OR SPECIF?)) (5N) (ACCESS? OR ENTRY OR ENTR- IE? ? OR USE??? OR UTILI?)
S9	0	S2:S3(100N)S7(100N)S8
S10	5	S2:S3(100N)S4(100N)S8
File 275:	Gale Group Computer DB(TM)	1983-2007/Jul 24 (c) 2007 The Gale Group
File 621:	Gale Group New Prod. Annou. (R)	1985-2007/Aug 13 (c) 2007 The Gale Group
File 636:	Gale Group Newsletter DB(TM)	1987-2007/Aug 16 (c) 2007 The Gale Group
File 16:	Gale Group PROMT(R)	1990-2007/Aug 16 (c) 2007 The Gale Group
File 160:	Gale Group PROMT(R)	1972-1989 (c) 1999 The Gale Group
File 148:	Gale Group Trade & Industry DB	1976-2007/Aug 14 (c) 2007 The Gale Group
File 624:	McGraw-Hill Publications	1985-2007/Aug 17 (c) 2007 McGraw-Hill Co. Inc
File 15:	ABI/Inform(R)	1971-2007/Aug 17 (c) 2007 ProQuest Info&Learning
File 647:	CMP Computer Fulltext	1988-2007/Sep W2 (c) 2007 CMP Media, LLC
File 674:	Computer News Fulltext	1989-2006/Sep W1 (c) 2006 IDG Communications
File 696:	DIALOG Telecom. Newsletters	1995-2007/Aug 16 (c) 2007 Dialog
File 369:	New Scientist	1994-2007/Jul W5 (c) 2007 Reed Business Information Ltd.
File 810:	Business Wire	1986-1999/Feb 28 (c) 1999 Business Wire
File 813:	PR Newswire	1987-1999/Apr 30 (c) 1999 PR Newswire Association Inc
File 610:	Business Wire	1999-2007/Aug 17 (c) 2007 Business Wire.
File 613:	PR Newswire	1999-2007/Aug 17

*Full Text
Npl. files*

(c) 2007 PR Newswire Association Inc

10/3,K/5 (Item 1 from file: 813)
DIALOG(R) File 813:PR Newswire
(c) 1999 PR Newswire Association Inc. All rts. reserv.

0877285 LA039
NOVELL LAUNCHES ITS NEXT GENERATION OPEN TRANSACTION PROCESSING MONITOR -
TUXEDO SYSTEM 6.1

DATE: October 31, 1995 08:36 EST WORD COUNT: 1,163

...a fast and
efficient way to create event-based communications, enabling businesses
to trigger a **series** of processing **steps** across multiple applications in
response to **pre - specified** events;

-- Enhanced **network security** through **Access Control Lists**
(ACLs),
which provide user or group-level authorization to individual TUXEDO
services.

TUXEDO is...

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
		S74 and ((user or entity) near6 (secure or security or authorized or authorization or valid\$6)	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/11 21:15
		S74 and ((user or entity) near6 (secure or security or authorized or authorization or valid\$6) near6 (request or initiat\$ or ask\$3 or query\$3 or queries or inquir\$3 or requisition) near6 ((pre ADJ determined) or (pre ADJ defined) or preselect\$ or preset or preprogrammed or preplaced or presett\$3 or preestablished or predetermined or predefined or predesignate\$ or preloaded) near6 (compar\$4 or comparative or compari\$ or comparable or contrast) near6 (allow\$3 or grant\$3 or approv\$2 or consent or permission or signoff or sign\$3 adj off or permit\$ or certif\$))	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/11 21:12
		S74 and (user or entity) near6 (secure or security or authorized or authorization or valid\$6) near6 (request or initiat\$ or ask\$3 or query\$3 or queries or inquir\$3 or requisition) near6 ((pre ADJ determined) or (pre ADJ defined) or preselect\$ or preset or preprogrammed or preplaced or presett\$3 or preestablished or predetermined or predefined or predesignate\$ or preloaded) near6 (compar\$4 or comparative or compari\$ or comparable or contrast) near6 (allow\$3 or grant\$3 or approv\$2 or consent or permission or signoff or sign\$3 adj off or permit\$ or certif\$)	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/11 21:11
		"254457"	USPAT	OR	ON	2007/04/09 15:20
		S59 and compar\$4 or equal\$2 adj match\$3 or correspond\$3	USPAT	OR	ON	2007/04/09 14:03

EAST Search History

		receiv\$3 or reception or accept\$3 or get or getting or got or import\$3 or download\$3 or down adj load\$3 or retriev\$3 or fetch\$3 or acquir\$3 or obtain\$3 or take or taking or took or upgrade or update or replace or change or transfer or transferr\$3 or transference or transference or telnet or FTP\$ or copy\$3 or copied or copies or up adj (grade or date) or get or gets or getting	USPAT	OR	ON	2007/08/15 13:31
L1	0	(receiv\$3) with (request) with (predetermined) with (node) with (information ADJ type) with (computer ADJ system ADJ function) with (temporal) with (access) with (compar\$3) with (minimum) with (grant\$3) with (prohibit\$3) with (exceed\$3) with (deny\$3) with (completes).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 15:39
L2	0	(receiv\$3) and (request) and (predetermined) and (node) and (information ADJ type) and (computer ADJ system ADJ function) and (temporal) and (access) and (compar\$3) and (minimum) and (grant\$3) and (prohibit\$3) and (exceed\$3) and (deny\$3) and (complet\$3).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:01
L3	265199	(receiv\$3 and request and predetermined and node and (information ADJ type) and (computer ADJ system ADJ function) and temporal and access and compar\$3 and minimum and grant\$3 and prohibit\$3 and exceed\$3 and deny\$3and complet\$3).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:04
L4	4033	(receiv\$3 and request and predetermined and node and (information ADJ type) and (computer ADJ system ADJ function) and temporal and access and compar\$3 and minimum and grant\$3 and prohibit\$3 and exceed\$3 and deny\$3and complet\$3).clm. and ("713".clas. or "726".clas. or "380".clas.)	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:05

EAST Search History

L5	74276	(receiv\$3 and request and predetermined and node and (information ADJ type) and (computer ADJ system ADJ function) and temporal and access and compar\$3 and minimum and grant\$3 and prohibit\$3 and exceed\$3 and deny\$3and complet\$3).clm.	US-PGPUB; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:04
L6	1735	(receiv\$3 and request and predetermined and node and (information ADJ type) and (computer ADJ system ADJ function) and temporal and access and compar\$3 and minimum and grant\$3 and prohibit\$3 and exceed\$3 and deny\$3and complet\$3).clm. and ("713".clas. or "726".clas. or "380".clas.)	US-PGPUB; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:28
L7	0	(receiv\$3 with request with predetermined with node with (information ADJ type) with (computer ADJ system ADJ function) with temporal with access with compar\$3 with minimum with grant\$3 with prohibit\$3 with exceed\$3 with deny\$3 with complet\$3).clm.	US-PGPUB; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:08
L8	0	((higher ADJ level) and node and arrang\$3 and (tree ADJ hierarchy) and interface and receiv\$3 and request and entity and predetermined and access and (predetermined ADJ access ADJ table) and process\$3 and den\$4). clm.	US-PGPUB; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:15
L9	0	((higher ADJ level) with node with arrang\$3 with (tree ADJ hierarchy) with interface with receiv\$3 with request with entity with predetermined with access with (predetermined ADJ access ADJ table) with process\$3 with den\$4). clm.	US-PGPUB; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:18

EAST Search History

L10	0	((higher ADJ level) with node with arrang\$3 with (tree ADJ hierarchy) with interface with receiv\$3 with request with entity with predetermined with access with (predetermined ADJ access ADJ table) with process\$3 with den\$4 with minimum with updat\$3 with aggregation with compar\$6).clm.	US-PGPUB; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:19
L11	0	((higher ADJ level) and node and arrang\$3 and (tree ADJ hierarchy) and interface and receiv\$3 and request and entity and predetermined and access and (predetermined ADJ access ADJ table) and process\$3 and den\$4 and minimum and updat\$3 and aggregation and compar\$6).clm.	US-PGPUB; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:22
L12	26423	"713".clas. "726".clas. "380".clas.	US-PGPUB; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:23
L13	0	8 and 12	US-PGPUB; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:23
L14	0	9 and 12	US-PGPUB; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:23
L15	0	10 and 12	US-PGPUB; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:23
L16	0	11 and 12	US-PGPUB; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:23
L17	3608	709/229.ccls. or 713/201.ccls. or 713/166.ccls. or 726/23.ccls. or 709/219.ccls.	US-PGPUB; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:29
L18	0	17 and 1	US-PGPUB; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:29
L19	0	17 and 2	US-PGPUB; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:29
L20	270	17 and 3	US-PGPUB; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:30
L21	45	17 and 4	US-PGPUB; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:30

EAST Search History

L22	270	17 and 5	US-PGPUB; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:30
L23	45	17 and 6	US-PGPUB; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 16:31
S1	27	"6014628"	US-PGPUB; USPAT	OR	ON	2007/04/03 07:42
S2	3	"7020717"	US-PGPUB; USPAT	OR	ON	2007/04/03 07:44
S3	2	"7126470"	US-PGPUB; USPAT	OR	ON	2007/04/03 07:48
S4	19	"5733418"	US-PGPUB; USPAT	OR	ON	2007/04/03 10:21
S5	1	"20020138322"	US-PGPUB; USPAT	OR	ON	2007/04/03 11:41
S6	22	"6023765"	US-PGPUB; USPAT	OR	ON	2007/04/03 16:51
S7	10	"5,429,736"	US-PGPUB; USPAT	OR	ON	2007/04/04 08:01
S8	3	"0044655"	US-PGPUB; USPAT	OR	ON	2007/04/04 08:02
S9	1	2004/0044655	US-PGPUB; USPAT	OR	ON	2007/04/04 08:02
S10	1	"20040044655"	US-PGPUB; USPAT	OR	ON	2007/04/04 10:15
S11	0	wo03/088018	US-PGPUB; USPAT	OR	ON	2007/04/04 10:16
S12	0	wo03088018	US-PGPUB; USPAT	OR	ON	2007/04/04 10:16
S13	1	"03088018"	US-PGPUB; USPAT	OR	ON	2007/04/04 10:17
S14	6	"088018"	US-PGPUB; USPAT	OR	ON	2007/04/04 10:18
S15	0	03/088018	US-PGPUB; USPAT	OR	ON	2007/04/04 10:18
S16	0	03/088018	US-PGPUB; USPAT	OR	ON	2007/04/04 10:22
S17	0	wo03/088018	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/04 10:23

EAST Search History

S18	0	wo03088018	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/04 10:23
S19	3	"03088018"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/04 10:24
S20	2	"20040044655"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/05 16:19
S21	0	713/201.CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/05 16:22
S22	0	713/201.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/05 16:22
S23	415	713/166.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/05 16:25
S24	12	"6334121"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/05 16:29
S25	8	("6334121").URPN.	USPAT	OR	ON	2007/04/05 16:55

EAST Search History

S26	23	"6345361"	USPAT	OR	ON	2007/04/05 16:56
S27	22	("6345361").URPN.	USPAT	OR	ON	2007/04/05 17:13
S28	12	"6405202"	USPAT	OR	ON	2007/04/09 08:09
S29	26	"6408391"	USPAT	OR	ON	2007/04/09 08:28
S30	9	"6446206"	USPAT	OR	ON	2007/04/09 08:43
S31	10	"6446077"	USPAT	OR	ON	2007/04/09 09:19
S32	3	"6453418"	USPAT	OR	ON	2007/04/09 11:28
S33	221	726/23.ccls.	USPAT	OR	ON	2007/04/09 15:19
S34	100	S33 and (receiving and request and computer and system)	USPAT	OR	ON	2007/04/09 11:35
S35	63	S33 and (temporal or (time and interval))	USPAT	OR	ON	2007/04/09 11:35
S36	5	("20010047420" "5974496" "6529706" "6741841" "6904449").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/04/09 11:37
S37	1	("2001/0047420").URPN.	USPAT	OR	ON	2007/04/09 11:38
S38	25	("6484203").URPN.	USPAT	OR	ON	2007/04/09 12:25
S39	0	("7200656").URPN.	USPAT	OR	ON	2007/04/09 12:26
S40	0	("7200656").URPN.	USPAT	OR	ON	2007/04/09 12:26
S41	0	("7200656").URPN.	USPAT	OR	ON	2007/04/09 12:26
S42	10	S33 and (temporal)	USPAT	OR	ON	2007/04/09 12:28
S43	5	("6826697").URPN.	USPAT	OR	ON	2007/04/09 13:20
S44	0	("7181733").URPN.	USPAT	OR	ON	2007/04/09 13:21
S45	165	S33 and ((request and (user or entity) and in and computer and system) or (receiving and (user or entity) and in and computer and system))	USPAT	OR	ON	2007/04/09 13:26
S46	14	S33 and ((request same (user or entity) same in same computer same system) or (receiving same (user or entity) same in same computer same system))	USPAT	OR	ON	2007/04/09 13:26
S47	76	S45 and ((predetermined and access and level) or (minimum and access and level))	USPAT	OR	ON	2007/04/09 13:28
S48	5	S47 and ((temporal and access and pattern) or (temporal))	USPAT	OR	ON	2007/04/09 13:30
S49	38	("6324647").URPN.	USPAT	OR	ON	2007/04/09 13:30
S50	38	("6324647").URPN.	USPAT	OR	ON	2007/04/09 13:31
S51	0	("7178166").URPN.	USPAT	OR	ON	2007/04/09 13:40
S52	2739	709/219.ccls.	USPAT	OR	ON	2007/04/09 13:42

8/16/2007 4:37:35 PM

Page 7

C:\Documents and Settings\dshaiferharriman\My Documents\EAST\Workspaces\10798074.wsp

EAST Search History

S53	599	S52 and (receiving and request and computer and system and entity)	USPAT	OR	ON	2007/04/09 13:43
S54	239	S53 and ((predetermined and access and entity) and (minimum and access level))	USPAT	OR	ON	2007/04/09 13:45
S55	451	S53 and ((predetermined and access and entity) or (minimum and access and level) or (authorization) or (authentication))	USPAT	OR	ON	2007/04/09 13:46
S56	15	S55 and (((temporal) or (temporal and access and pattern))	USPAT	AND	ON	2007/04/09 13:52
S57	15	S55 and (((temporal) or (temporal and access and pattern))	USPAT	OR	ON	2007/04/09 13:55
S58	3149461	receiv\$3 or accept\$3 or get or getting or got or import\$3 or download\$3 or down adj load\$3 or retriev\$3 or fetch\$3 or acquir\$3 or obtain\$3	USPAT	OR	ON	2007/04/09 14:13
S59	3125668	S58 and (Analyze, Authority, hierarchy, limit\$5 modification, restrict\$3 or access\$3 or secur\$3 or authori\$6 or right or privilege or unauthori\$6 or verif\$7 or entitl\$5 or recogni\$4 or protect\$3 or control\$3 or safeguard\$3 OR confine or confining or confined or filter\$3 or lock\$3 access control, access levels, access rights, access privileges (authority role, position, job, rank) adj profile, tier authority clearances, need to know,view rights role-based access control (RBAC) firewall, fire adj wall, screening router, security agent, security interface authenti\$6, confirm\$5, substantiat\$3, valid\$5 or identif\$7 or phras or code or entitl\$5 or recogni\$4 or access\$3 password or pass adj word secur\$3 or gatekeep\$3 certif\$6 or compar\$4)	USPAT	OR	ON	2007/04/09 13:58
S60	2051	709/229.ccls.	USPAT	OR	ON	2007/04/09 14:15
S61	2050	S60 and (receiving and request in computer and system)	USPAT	OR	ON	2007/04/09 14:14

EAST Search History

S62	1049	S61 and ((authorization) or (authentication) or (pretdetermined and access and level) or (minimum and access and level))	USPAT	OR	ON	2007/04/09 14:19
S63	0	"10254457"	USPAT	OR	ON	2007/04/09 15:19
S64	8	"254457"	USPAT	OR	ON	2007/04/11 07:34
S65	1	"0044655"	USPAT	OR	ON	2007/04/11 07:35
S66	0	"20040044655"	USPAT	OR	ON	2007/04/11 07:35
S67	1	"2004/0044655"	USPAT	OR	ON	2007/04/11 07:35
S68	1	2004/0044655	USPAT	OR	ON	2007/04/11 07:36
S69	0	"20040044655"	USPAT	OR	ON	2007/04/11 07:36
S70	1	"20040044655"	US-PGPUB; USPAT	OR	ON	2007/04/11 07:36
S71	104635	(temporal)	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/11 19:57
S72	14825	S71 and (secure or security or authorized or authorize)	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/11 19:59
S73	11547	S72 and (access or (access ADJ control) or access\$ble or entry or entrance)	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/11 20:14
S74	57343	(sequence or sequenced or ordered or order or successive or interval or time temporal) ADJ (access or (access ADJ control) or entry or validation or permission)	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/11 20:26
S75	438457	(sequence or sequenced or ordered or order or successive or interval or time temporal) with (access or (access ADJ control) or entry or validation or permission)	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/11 20:25
S76	235020	(sequence or sequenced or ordered or order or successive or interval or time temporal) near3 (access or (access ADJ control) or entry or validation or permission)	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/11 20:25

EAST Search History

S77	0	S74 and ((user or entity) near6 (secure or security or authorized or authorization or valid\$6) near6 (request or initiat\$ or ask\$3 or query\$3 or queries or inquir\$3 or requisition) near6 ((pre ADJ determined) or (pre ADJ defined) or preselect\$ or preset or preprogrammed or preplaced or presett\$3 or preestablished or predetermined or predefined or predesignate\$ or preloaded) near6 (compar\$4 or comparative or compari\$ or comparable or contrast) near6 (allow\$3 or grant\$3 or approv\$2 or consent or permission or signoff or sign\$3 adj off or permit or permitting or permitt or certif\$))	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/11 21:18
S78	0	S74 and ((user or entity) near6 (secure or security or authorized or authorization or valid\$6) near6 (request or initiat\$ or ask\$3 or query\$3 or queries or inquir\$3 or requisition) near6 ((pre ADJ determined) or (pre ADJ defined) or preselect\$ or preset or preprogrammed or preplaced or presett\$3 or preestablished or predetermined or predefined or predesignate\$ or preloaded) near6 (compar\$4 or comparative or compari\$ or comparable or contrast))	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/11 21:14
S79	0	S74 and ((user or entity) near6 (secure or security or authorized or authorization or valid\$6) near6 (request or initiat\$ or ask\$3 or query\$3 or queries or inquir\$3 or requisition) near6 ((pre ADJ determined) or (pre ADJ defined) or preselect\$ or preset or preprogrammed or preplaced or presett\$3 or preestablished or predetermined or predefined or predesignate\$ or preloaded) near6 (compar\$4 or comparable or contrast))	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/11 21:15

EAST Search History

S80	10765	S74 and ((user or entity) near6 (secure or security or authorized or authorization or valid\$6))	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/11 21:15
S81	10098	S80 and (request or initiat\$ or ask\$3 or query\$3 or queries or inquir\$3 or requisition)	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/11 21:15
S82	6968	S81 and ((pre ADJ determined) or (pre ADJ defined) or preselect\$ or preset or preprogrammed or preplaced or presett\$3 or preestablished or predetermined or predefined or predesignate\$ or preloaded)	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/11 21:16
S83	5799	S82 and (compar\$4 or comparative or compari\$ or comparable or contrast)	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/11 21:17
S84	5722	S83 and (allow\$3 or grant\$3 or approv\$2 or consent or permission or signoff or sign\$3 adj off or permit or permitting or permitt or certif\$)	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/11 21:18
S85	54156	"713"/.clas. or "726"/.clas. or "380"/.clas.	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/11 21:20
S86	1058	S84 and S85	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/11 21:24
S87	101	S86 and temporal	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	ON	2007/08/16 15:03
S88	21	"6711615"	USPAT	OR	ON	2007/08/15 13:31



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO
10/798,074	03/11/2004	2134	770	7162-0110

CONFIRMATION NO. 5321

39207
SACCO & ASSOCIATES, PA
P.O. BOX 30999
PALM BEACH GARDENS, FL33420-0999

REPLACEMENT FILING RECEIPT

Date Mailed: 07/16/2007

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please write to the Office of Initial Patent Examination's Filing Receipt Corrections. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Vincent Joseph Kovarik JR., Grant, FL;

Assignment For Published Patent Application

Harris Corporation, Melbourne, FL

Power of Attorney: The patent practitioners associated with Customer Number 39207

Domestic Priority data as claimed by applicant

Foreign Applications

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 05/27/2004

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US10/798,074**

Projected Publication Date: Not Applicable

Non-Publication Request: No

Early Publication Request: No

Title

Preliminary Class

713

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

**RECEIVED
CENTRAL FAX CENTER**

JUL 12 2007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appln. No.	:	10/798,074	Confirmation No.	:	5321
First Named Inventor	:	KOVARIK, Jr.			
Filed	:	March 11, 2004			
TC/A.U.	:	2109			
Examiner	:	SHAIFER HARRIMAN			
Docket	:	7162-0110			
Customer No.	:	39207			

Via Facsimile 571-273-8300

Mail Stop Amendment
Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT

Sir:

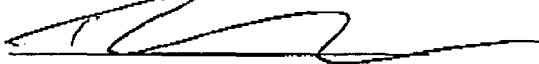
In response to the Office Action dated April 18, 2007, please amend the above-identified application as follows:

Amendments to the Claims are reflected in the listing of claims which begin on page 2 of this paper.

Remarks/arguments begin on page 7 of this paper.

Certificate of Transmission

I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office, Fax No. (571)273-8300 on 7-12-07. Typed or printed name of person signing this certificate: **ROBERT J. SACCO**



{00016049;2}

Appln. No.: 10/798,074
Amdt. dated: July 12, 2007
Reply to Office Action dated: April 18, 2007

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for secure access to a computer system, comprising the steps of:

receiving in said computer system a request from an entity with a predetermined access level for access to a first base node representing at least one of an information type and a computer system function;

determining if said access request completes a prohibited temporal access pattern for said entity; and

comparing a minimum access level established for said first base node to said predetermined access level; and

granting said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level; and

denying said request if said access request completes a prohibited temporal access pattern for said entity.

2. (Cancelled)

3. (Original) The method according to claim 1, further comprising the step of denying said request if said minimum access level for said first base node exceeds said predetermined access level for said entity.

4. (Original) The method according to claim 1, further comprising the steps of:

logically organizing said computer system in the form of a tree hierarchy having a plurality of leaf nodes and higher-level nodes;

{00016049;2}

Appln. No.: 10/798,074
Amdt. dated: July 12, 2007
Reply to Office Action dated: April 18, 2007

defining a plurality of said base nodes as comprising respectively a plurality of leaf nodes of said tree hierarchy; and

defining said higher-level nodes as aggregations of said base nodes.

5. (Original) The method according to claim 4 further comprising the step of identifying within said hierarchy any higher-level nodes that are aggregations comprising said first base node.
6. (Original) The method according to claim 5, further comprising the step of identifying within said hierarchy any nodes that comprise children of any generation of said higher-level nodes that are aggregations comprising said first base node.
7. (Original) The method according to claim 6, further comprising the step of updating a minimum required entity access level for any base nodes that comprise children of any generation of said higher-level nodes that are aggregations comprising said first base node.
8. (Original) The method according to claim 7, wherein said updating step further comprises the steps of:
 - comparing said entity's predetermined access level against the minimum required access level of said higher-level nodes that are aggregations comprising said first base node; and
 - updating a minimum required access level of any said base node that is also a member of any aggregation comprising said first base node if a minimum required access level for said higher-level node comprising said aggregation has a required access level that is higher than said entity's predetermined access level.
9. (Original) The method according to claim 1, further comprising the steps of:
 - comparing said entity's predetermined access level against the minimum required access level of at least one higher-level node that is an aggregation of base nodes including said first base node; and

{00016049;2}

Appln. No.: 10/798,074
Amdt. dated: July 12, 2007
Reply to Office Action dated: April 18, 2007

updating a minimum required access level of any said base node that is also a member of any aggregation comprising said first base node if a minimum required access level for said higher-level node comprising said aggregation has a required access level that is higher than said entity's predetermined access level.

10. (Currently Amended) A method for restricting access to a computer system having a plurality of logical base nodes representing at least one of an information type and a computer system function, and a plurality of higher-level nodes arranged together with said base nodes in the form of a tree hierarchy, comprising the steps of:

receiving in said computer system a request from an entity with a predetermined access level for access to a first base node;

determining if said access request completes a prohibited temporal access pattern for said entity; and

comparing a minimum access level established for said first base node to said predetermined access level; and

granting said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level; and

denying said request if said access request completes a prohibited temporal access pattern for said entity.

11. (Currently Amended) A secure computer system comprising:

a plurality of logical base nodes representing at least one of an information type and a computer system function;

a plurality of higher-level nodes arranged together with said base nodes in the form of a tree hierarchy;

a computer system interface capable of receiving a request from an entity with a predetermined access level for access to a first base node;

a temporal access table;

{00016049;2}

Appln. No.: 10/798,074
Amdt. dated: July 12, 2007
Reply to Office Action dated: April 18, 2007

processing means programmed for comparing said access request to said temporal access table to determine if said access request completes a prohibited temporal access pattern for said entity, and for comparing a minimum access level established for said first base node to said predetermined access level; and

wherein said processing means denies said request if said access request completes a prohibited temporal access pattern for said entity and grants said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level.

12. (Cancelled)

13. (Original) The secure computer system according to claim 11, wherein said processing means denies said request if said minimum access level for said first base node exceeds said predetermined access level for said entity.

14. (Original) The secure computer system according to claim 11 wherein said higher-level nodes are aggregations of said base nodes.

15. (Original) The secure computer system according to claim 14 wherein said processing means identifies within said hierarchy any higher-level nodes that are aggregations comprising said first base node.

16. (Original) The secure computer system according to claim 15 wherein said computer processing means identifies within said hierarchy any nodes that comprise children of any generation of said higher-level nodes that are aggregations comprising said first base node.

17. (Original) The secure computer system according to claim 16 wherein said processing means updates a minimum required entity access level for any base nodes that comprise children of any generation of said higher-level nodes that are aggregations comprising said first base node.

{00016049;2}

Appln. No.: 10/798,074
Amdt. dated: July 12, 2007
Reply to Office Action dated: April 18, 2007

18. (Original) The secure computer system according to claim 17 wherein said processing means compares said entity's predetermined access level against the minimum required access level of said higher-level nodes that are aggregations comprising said first base node; and

automatically updates a minimum required access level of any said base node that is also a member of any aggregation comprising said first base node if a minimum required access level for said higher-level node comprising said aggregation has a required access level that is higher than said entity's predetermined access level.

19. (Original) The secure computer system according to claim 11 wherein said processing means compares said entity's predetermined access level against the minimum required access level of at least one higher-level node that is an aggregation of base nodes including said first base node; and

updates a minimum required access level of any said base node that is also a member of any aggregation comprising said first base node if a minimum required access level for said higher-level node comprising said aggregation has a required access level that is higher than said entity's predetermined access level.

{00016049;2}

Appln. No.: 10/798,074
Amdt. dated: July 12, 2007
Reply to Office Action dated: April 18, 2007

Remarks/Arguments

These remarks are in response to the Office Action dated April 18, 2007. This reply is timely filed. At the time of the Office Action, claims 1-19 were pending in the application. Claims 1, 10, and 11-19 were rejected under 35 U.S.C. §101. Claims 1-9 and 10-19 have been rejected under 35 U.S.C. 102(e). The rejections are set out in more detail below.

I. Claim Rejections Under 35 U.S.C. §101

Claims 1, 10, and 11-19 were rejected under 35 U.S.C. §101, citing the claimed invention is directed to non-statutory subject matter. In this regard, the Examiner states that the subject matter recited in independent claims 1, 10, and 11 lacks a practical application since the subject matter fails to produce a useful, concrete, and tangible result. More specifically, the Examiner notes that the claimed subject matter provides for the granting of an entity's request if and only if, the entity doesn't complete a temporal access pattern, and the entity's predetermined access level meets the minimum access level of the first base node. The Examiner asserts that this conditional statement yields a tangible result only if access is granted, and therefore makes for a non-tangible result. In response, Applicants have amended the subject matter of independent claims 1 and 10 to include the following conditional statement: "denying said request if said access request completes a prohibited temporal access pattern for said entity." Applicants have also amended the subject matter of independent claim 11 to include the following phrase: "wherein said processing means denies said request if said access request completes a prohibited temporal access pattern for said entity". Applicants believe that the currently amended independent claims 1, 10, 11 overcome the Examiners rejection under 35 U.S.C. §101.

II. Brief Review of Applicants' Invention

Prior to addressing the Examiner's rejections on the art, a brief review of the Applicants' invention is appropriate. The invention relates to a method and apparatus

{00016049;2}

Appln. No.: 10/798,074
Amdt. dated: July 12, 2007
Reply to Office Action dated: April 18, 2007

for using an adaptive lattice mechanism to enforce computer security. See paragraph [0023]. Generally, the method involves receiving in the computer system a request from an entity. See paragraphs [0009], [0033] and FIG. 6. The entity can be a user or a process and can have a predetermined access authorization level for access to a first base node representing an information type or a computer system function. See paragraph [0009]. The method also involves determining if the access request completes a prohibited temporal access pattern for the entity. See paragraphs [0009], [0033] and FIG. 6.

In this regard, it should be appreciated that a temporal access pattern is defined by a temporal relation between two or more nodes. See paragraph [0028]. A temporal relation is an inter-propositional relation that communicates the ordering in time of events. See paragraph [0028] and FIG. 1. For example, a prohibited temporal access pattern of a node A is defined by a temporal relation between an item N_1 and an item N_2 , e.g., $N_1 \rightarrow N_2$. Thus, a temporal ordering at node A exists that the item N_1 is accessed before the item N_2 . So, for the security policy associated with node A to be activated, not only must the item N_1 and item N_2 be accessed but they must be accessed in the order indicated by the temporal relation.

If it is determined that the access request completes a prohibited temporal access pattern for the entity, then the request is rejected. See paragraphs [0009], [0033] and FIG. 6. Otherwise, the method continues with a comparison of a minimum access level established for the first base node to the predetermined access authorization level assigned to the entity. See paragraphs [0009], [0035] and FIG. 6. If the minimum access level for the first base node does not exceed to the predetermined access authorization level, then access request is granted. See paragraphs [0009], [0035] and FIG. 6. However, if the minimum access level for the first base node exceeds the predetermined access authorization level assigned to the entity, then the access request is denied. See paragraphs [0009], [0035] and FIG. 6.

{00016049;2}

Appln. No.: 10/798,074
Amdt. dated: July 12, 2007
Reply to Office Action dated: April 18, 2007

III. Claim Rejections Under 35 U.S.C. §102(e)

Claims 1-9 and 10-19 have been rejected under 35 U.S.C. §102(e) as being taught by U.S. Patent Publication No. 2004/0044655 to Cotner ("Cotner"). Cotner discloses and teaches a method of controlling access to a relational database. See paragraphs [0009], [0053], [0072]-[0084] and FIG. 7B. The method includes receiving a user request for data from the database, in which the request includes a request to perform a database operation and a user security label. See paragraphs [0009], [0073] and FIG. 7B. User security information is determined from the user security label. See paragraphs [0009], [0074] and FIG. 7B. In response to the user request, rows of data are retrieved from a table in the database that satisfy the database operation, in which the rows each have a security label. See paragraphs [0009], [0074] and FIG. 7B. The method further includes determining row security information for each of the retrieved rows based on the row's security label. See paragraphs [0009], [0074] and FIG. 7B. For each retrieved row the method determines whether the user is authorized to access the row based on the user security information and the row security information. See paragraphs [0009], [0074] and FIG. 7B. Only the rows for which the user is determined to have authorization to access are returned to the user. See paragraph [0009] and FIG. 7B.

A. Independent Claims 1 and 10

Claim 1 concerns a method for secure access to a computer system. Claim 10 concerns a method for restricting access to a computer system having logical base nodes representing an information type and/or a computer system function. Claims 1, 10 recite in relevant part "determining if an access request completes a prohibited temporal access pattern for an entity". Claims 1, 10 also recite in relevant part "granting the access request only if it does not complete a prohibited temporal access pattern for the entity". Claims 1, 10 further recite in relevant part "denying the request if the access request completes a prohibited temporal access pattern for said entity."

{00016049;2}

Appin. No.: 10/798,074
Amdt. dated: July 12, 2007
Reply to Office Action dated: April 18, 2007

Upon review of the Cotner reference, it becomes readily apparent that it fails to disclose and/or teach the step of "determining if an access request completes a prohibited temporal access pattern for an entity". It also becomes readily apparent that the Cotner reference fails to disclose and/or teach granting or denying an access request based on the outcome of the determination step. Instead, the Cotner reference teaches a method for controlling access to a relational database based solely on security levels. See paragraphs [0009], [0053], [0072]-[0084] and FIG. 7B. Accordingly, a person skilled in the art may interpret the Cotner reference as failing to teach temporal access patterns and an access request control technique utilizing temporal access patterns.

It should be noted that the Examiner opines that paragraph [0034] of the Cotner reference discloses and/or teaches the step of "determining if an access request completes a prohibited temporal access pattern for an entity". However, Applicants have reviewed the cited paragraph [0034] and can find no such teaching. In this regard, it should be appreciated that the cited paragraph [0034] discloses and teaches user security labels identifying certain security levels, such as top secret, secret, and unclassified. The cited paragraph [0034] also discloses and teaches permitting access to data by determining if the user has the proper security level to view the data. In effect, the cited paragraph [0034] fails to disclose and/or teach an access request control technique that involves determining if an access request completes a prohibited temporal access pattern for an entity.

In view of the forgoing, the Cotner reference fails to disclose and teach the steps recited in claims 1, 10. Accordingly, Applicants request reconsideration and allowance of pending claims 1, 10. Claims 3-9 are believed to be in condition for allowance at least by virtue of their dependence upon an allowable base claim. Accordingly, reconsideration and allowance of claims 3-9 is also requested.

B. Independent Claim 11

Claim 11 concerns a secure computer system. Claim 11 recites in relevant part "a secure computer system comprising a temporal access table." Claim 11 also recites

{00016049;2}

Appln. No.: 10/798,074
Amdt. dated: July 12, 2007
Reply to Office Action dated: April 18, 2007

in relevant part "a secure computer system comprising a processing means programmed for comparing an access request to the temporal access table to determine if the access request completes a prohibited temporal access pattern for an entity." Claim 11 further recites in relevant part that the "processing means denies the request if the access request completes a prohibited temporal access pattern for the entity and grants the access request only if it does not complete a prohibited temporal access pattern for the entity."

Upon review of the Cotner reference, it becomes readily apparent that it fails to disclose and/or teach a secure computer system comprising a temporal access table. It also becomes readily apparent that the Cotner reference fails to disclose and/or teach a processing means programmed for comparing an access request to the temporal access table to determine if the access request completes a prohibited temporal access pattern for an entity. Instead, the Cotner reference teaches a secure computer system configured for controlling access to a relational database based solely on security levels. See paragraphs [0009], [0053], [0072]-[0084] and FIG. 7B. Accordingly, a person skilled in the art may interpret the Cotner reference as failing to teach temporal access patterns and a means for implementing an access request control technique utilizing temporal access patterns.

It should be noted that the Examiner opines that paragraphs [00030] and [0034] of the Cotner reference disclose and/or teach a temporal access table. However, Applicants have reviewed the cited paragraphs [00030], [0034] and can find no such teaching.

In view of the forgoing, the Cotner reference fails to disclose and teach the subject matter claimed in claim 11. Accordingly, Applicants request reconsideration and allowance of pending claim 11. Claims 13-19 are believed to be in condition for allowance at least by virtue of their dependence upon an allowable base claim. Accordingly, reconsideration and allowance of claims 13-19 is also requested.

{00016049;2}

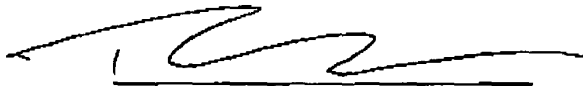
Appln. No.: 10/798,074
Amdt. dated: July 12, 2007
Reply to Office Action dated: April 18, 2007

IV. Conclusion

Applicants have made every effort to present claims which distinguish over the prior art, and it is believed that all claims are in condition for allowance. Nevertheless, Applicants invite the Examiner to call the undersigned if it is believed that a telephonic interview would expedite the prosecution of the application to an allowance. In view of the foregoing remarks, Applicants respectfully request reconsideration and prompt allowance of the pending claims.

Respectfully submitted,

7-12-07
Date



Robert J. Sacco
Registration No. 35,667
SACCO & ASSOCIATES, P.A.
P.O. Box 30999
Palm Beach Gardens, FL 33420-0999
Tel: 561-626-2222

{00016049;2}

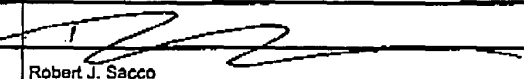
PTO/SB/21 (04-07)

Approved for use through 09/30/2007. OMB 0651-0031

U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM (to be used for all correspondence after initial filing)	Application Number	11/798,074	RECEIVED CENTRAL FAX CENTER JUL 12 2007
	Filing Date	March 11, 2004	
	First Named Inventor	KOVARIK, JR.	
	Art Unit	2109	
	Examiner Name	SHAIFER HARRIMAN	
Total Number of Pages in This Submission	14	Attorney Docket Number	7162-0110

ENCLOSURES (Check all that apply)		
☐ Fee Transmittal Form ☐ Fee Attached ☒ Amendment/Reply ☐ After Final ☐ Affidavits/declaration(s) ☐ Extension of Time Request ☐ Express Abandonment Request ☐ Information Disclosure Statement ☐ Certified Copy of Priority Document(s) ☐ Reply to Missing Parts/Incomplete Application ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53	☐ Drawing(s) ☐ Licensing-related Papers ☐ Petition ☐ Petition to Convert to a Provisional Application ☐ Power of Attorney, Revocation ☐ Change of Correspondence Address ☐ Terminal Disclaimer ☐ Request for Refund ☐ CD, Number of CD(s) _____ ☐ Landscape Table on CD	☐ After Allowance Communication to TC ☐ Appeal Communication to Board of Appeals and Interferences ☐ Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) ☐ Proprietary Information ☐ Status Letter ☒ Other Enclosure(s) (please identify below): PTO/SB/39
Remarks Please charge any deficiencies, or credit any overpayment to Dep. Acct. 08-0870.		
SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT		
Firm Name	SACCO & ASSOCIATES, P.A.	
Signature		
Printed name	Robert J. Sacco	
Date	July 12, 2007	Reg. No. 35,667

CERTIFICATE OF TRANSMISSION/MAILING	
I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:	
Signature	
Typed or printed name	Robert J. Sacco
Date	July 12, 2007

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

RECEIVED
CENTRAL FAX CENTER

JUL 12 2007

Doc Code: PD.TO.AUTH

PTO/SB/39 (04-07)

Approved for use through 09/30/2007. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**AUTHORIZATION TO PERMIT
ACCESS TO APPLICATION BY
PARTICIPATING OFFICES**Send completed form to: Commissioner for Patents
P.O. Box 1450, Alexandria, VA 22313-1450

COMPLETE IF KNOWN	
Application Number	10/798074
Filing Date	March 11, 2004
First Named Inventor	KORVARIK, JR.
Art Unit	2109
Examiner Name	SHAFER HARRIMAN
Attorney Docket Number	7162-0110

The undersigned hereby grants the USPTO authority under the Trilateral Document Access (TDA) Program to provide the European Patent Office (EPO) access to the above-identified patent application, entitled:

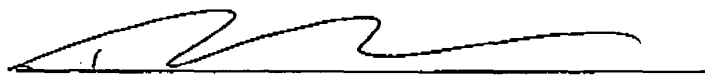
ENFORCING COMPUTER SECURITY UTILIZING AN ADAPTIVE LATTICE
MECHANISM

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the application-as-filed with respect to: 1) the above-identified application, 2) any foreign application to which the above-identified application claims priority under 35 USC 119(a)-(d), and 3) any U.S. application from which benefit is sought in the above-identified application.

This written authorization should be submitted prior to the filing of a subsequent foreign application with the EPO in which priority is claimed to the above-identified application.

No fee will be charged under 37 CFR 1.19(b)(1) for providing the EPO with an electronic copy of the above-identified application.

This form must be signed by an authorized party in accordance with 37 CFR 1.14(c).



Signature

Robert J. Sacco

Printed or Typed Name

Attorney

Title

7-12-07

Date

561-626-2222

Telephone Number

35,667

Registration Number, if applicable

This collection of information is required by 37 CFR 1.14(h). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process an application). Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 8 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 10/798,074		Filing Date 03/11/2004		☐ To be Mailed	
APPLICATION AS FILED – PART I										
(Column 1)			(Column 2)			SMALL ENTITY ☐ OR		OTHER THAN SMALL ENTITY		
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)			
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A				
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A				
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A				
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X \$ =			X \$ =				
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$ =			X \$ =				
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).									
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
* If the difference in column 1 is less than zero, enter "0" in column 2.										
TOTAL			TOTAL							
APPLICATION AS AMENDED – PART II										
(Column 1)			(Column 2)			SMALL ENTITY OR		OTHER THAN SMALL ENTITY		
AMENDMENT	07/12/2007	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	* 17	Minus	** 20	= 0	X \$ =		OR	X \$50=	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X \$ =		OR	X \$200=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
	TOTAL ADD'L FEE					TOTAL ADD'L FEE				
TOTAL			TOTAL			0				
AMENDMENT	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(i))	*	Minus	**	=	X \$ =		OR	X \$ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$ =		OR	X \$ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
	TOTAL ADD'L FEE					TOTAL ADD'L FEE				
TOTAL			TOTAL							
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.										

Legal Instrument Examiner:
peggy s. yarborough

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

74

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/798,074	03/11/2004	Vincent Joseph Kovarik JR.	7162-0110	5321

39207 7590 04/18/2007
SACCO & ASSOCIATES, PA
P.O. BOX 30999
PALM BEACH GARDENS, FL 33420-0999

EXAMINER

SHAIFER HARRIMAN, DANT B

ART UNIT	PAPER NUMBER
----------	--------------

2109

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/798,074	KOVARIK, VINCENT JOSEPH	
	Examiner	Art Unit	
	Dant B. Shaifer - Harriman	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 3/11/2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-19 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 3/11/2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) ☒ Notice of References Cited (PTO-892) | 4) ☐ Interview Summary (PTO-413) |
| 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) ☒ Information Disclosure Statement(s) (PTO/SB/08) | 5) ☐ Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>3/11/2004, 3/27/06</u> | 6) ☐ Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims(s) 11-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 USC 101. They are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. They are, at best, functional descriptive material *per se*.

Claim 1, 10, 11 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims(s) 1, 10, 11 are directed to a method and secure computer system where a request is received in a computer system, the entity (i.e. the user or the system) that made the request has a predetermined access level that is compared to a minimum access level that is established by the first base node; the entity is also checked to see if it completes a temporal access pattern, if the entity does complete a temporal access pattern, and the entity's predetermined access pattern meets the minimum access level of the first base node, then the entity's request is granted.

This claimed subject matter lacks a practical application of a judicial exception (law of nature, abstract idea, naturally occurring phenomenon) since it fails to produce a useful, concrete and tangible result.

Specifically, the claimed subject matter does not produce a tangible result because the claimed subject matter fails to produce a result that is limited to having real world value rather than a result that may be interpreted to be abstract in nature as, for example, a thought, a computation, or manipulated data. More specifically, the claimed subject matter provides for the granting of an entity's request if and only if, the entity doesn't complete a temporal access pattern, and the entity's predetermined access level meets the minimum access level of the first base node. This conditional statement yields only a tangible result if access is granted, but otherwise access isn't granted, this is what makes for a non-tangible result. This produced result remains in the abstract and, thus, fails to achieve the required status of having real world value.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claim(s) 1-9 & 10-19 are rejected under 35 U.S.C. 102(e) as being taught by Cotner (PGPub # US 2004/0044655 A1) hereinafter Cotner.

Cotner teaches:

Claim #1

A method for secure access to a computer system, comprising the steps of:

- receiving in said computer system a request from an entity with a predetermined access level for access to a first base node representing at least one of an information type and a computer system function (Paragraph: 0085), the examiner notes that the user or entity requests an update to the data in the database, this is equivalent to a computer system receiving a request and a first base node is of either a information type(i.e. data in data row) and a computer system function (i.e. the actual computer function that updates the row data in the row).

- determining if said access request completes a prohibited temporal access pattern for said entity(Paragraph: 0034), the examiner notes that by the fact that a user can or administrator can update the security label from Secret to Top Secret over a period of time based on the type of work or clearance that is needed to work on the project, it is inherent that this is a temporal access pattern.
- and comparing a minimum access level established for said first base node to said predetermined access level(Paragraph: 0039), the examiner notes that the user security level must be greater or equal to the row's security level, this is equivalent to the first base node minimum access level doesn't exceed the predetermined access level of the user or entity.
- and granting said access request only if it does not complete a prohibited temporal access pattern for said entity(Paragraph: 0034), the examiner notes that by the fact that a user can or administrator can update the security label from Secret to Top Secret over a period of time based on the type of work or clearance that is needed to work on the project, it is inherent that this is a temporal access pattern.
- and said minimum access level for said first base node does not exceed said predetermined access level(Paragraph: 0039), the examiner notes that the user security level must be greater or equal to the row's security level, this is equivalent to the first base node minimum access level doesn't exceed the predetermined access level of the user or entity.

The examiner further notes that claims 1 and 10 are duplicates and that claims 10 is the implementation of claim 1 on the method, which when implement produces the same result.

Claim #2

The method according to claim 1, further comprising the step of denying said request if said access request completes a prohibited temporal access pattern for said entity, (Paragraph: 0038 & 0039, the examiner notes that by the fact that a user or administrator can update the security label from Secret to Top Secret over a period of time based on the type of work or access clearance that is needed to work on the project, it is inherent that this is a completed temporal access pattern.

The examiner further notes that claims 2 and 12 are duplicates and that claims 12 is the implementation of claim 2 on the method, which when implement produces the same result.

Claim # 3

The method according to claim 1, further comprising the step of denying said request if said minimum access level for said first base node exceeds said predetermined access level for said entity, (Paragraph: 0039, the examiner notes that the users security label is greater than or equal to the row's security label is the same as the entity or user meeting the minimum access level of the first base node.

The examiner further notes that claims 3 and 13 are duplicates and that claims 13 is the implementation of claim 3 on the method, which when implement produces the same result.

Claim #4

The method according to claim 1, further comprising the steps of: logically organizing said computer system in the form of a tree hierarchy having a plurality of leaf nodes and higher-level nodes; defining a plurality of said base nodes as comprising respectively a plurality of leaf nodes of said tree hierarchy; and defining said higher-level nodes as aggregations of said base nodes, (Paragraphs: 0057, the examiner notes that the keywords "leaf node and higher level security level node" describes a tree hierarchy, which contains both higher level nodes and leaf nodes per se.

The examiner further notes that claims 4 and 14 are duplicates and that claims 14 is the implementation of claim 4 on the method, which when implement produces the same result.

Claim #5

The method according to claim 4 further comprising the step of identifying within said hierarchy any higher-level nodes that are aggregations comprising said first base node, (Paragraph: 0057 & Figure 4, the examiner notes that the rainbow (higher leaf node) is composed of a multitude of colors including sunset, which is the first base node in this case.

The examiner further notes that claims 5 and 15 are duplicates and that claims 15 is the implementation of claim 5 on the method, which when implement produces the same result.

Claim #6

The method according to claim 5, further comprising the step of identifying within said hierarchy any nodes that comprise children of any generation of said high-level nodes that are aggregations comprising said first base node, (Paragraph: 0057 & 0058 & Figure 4, the examiner notes that the rainbow (higher leaf node) is composed of a multitude of colors including sunset, which is the first base node in this case.

The examiner further notes that claims 6 and 16 are duplicates and that claims 16 is the implementation of claim 6 on the method, which when implement produces the same result.

Claim #7

The method according to claim 6, further comprising the step of updating a minimum required entity access level for any base nodes that comprise children of any generation of said higher-level nodes that are aggregations comprising said first base node, (Paragraph: 0058 & Figure 4 & 0085 & Figure 8A, the examiner notes that if the data is changed or updated in the row, for example the column headings are changed from secret to top secret, then the corresponding users (entity) security level is updated as well (i.e. sunset(first base node) to rainbow), then the user that initiated the update

will be able to access the top secret data at a rainbow security level or at a higher color access control level.

The examiner further notes that claims 7 and 17 are duplicates and that claims 17 is the implementation of claim 7 on the method, which when implement produces the same result.

Claim #8

The method according to claim 7, wherein said updating step further comprises the steps of: comparing said entity's predetermined access level against the minimum required access level of said higher-level nodes that are aggregations comprising said first base node; and updating a minimum required access level of any said base node that is also a member of any aggregation comprising said first base node if a minimum required access level for said higher-level node comprising said aggregation has a required access level that is higher than said entity's predetermined access level, (Paragraph: 0058 & Figure 4 & 0085 & Figure 8A, the examiner notes that if the data is changed or updated in the row, for example the column headings are changed from secret to top secret, then the corresponding users (entity) security level is updated as well (i.e. sunset(first base node) to rainbow), then the user that initiated the update will be able to access the top secret data at a rainbow security level or at a higher color access control level.

The examiner further notes that claims 8 and 18 are duplicates and that claims 18 is the implementation of claim 8 on the method, which when implement produces the same result.

Claim #9

The method according to claim 1, further comprising the steps of: comparing said entity's predetermined access level against the minimum required access level of at least one higher-level node that is an aggregation of base nodes including said first base node; and updating a minimum required access level of any said base node that is also a member of any aggregation comprising said first base node if a minimum required access level for said higher-level node comprising said aggregation has a required access level that is higher than said entity's predetermined access level, (Paragraph: 0058 & Figure 4 & 0085 & Figure 8A, the examiner notes that if the data is changed or updated in the row, for example the column headings are changed from secret to top secret, then the corresponding users(entity) security level is updated as well (i.e. sunset(first base node) to rainbow), then the user that initiated the update will be able to access the top secret data at a rainbow security level or at a higher color access control level.

The examiner further notes that claims 9 and 19 are duplicates and that claims 19 is the implementation of claim 9 on the method, which when implement produces the same result.

Claim #11

A secure computer system comprising: a plurality of logical base nodes representing at least one of an information type and a computer system function; a

plurality of higher-level nodes arranged together with said base nodes in the form of a tree hierarchy; a computer system interface capable of receiving a request from an entity with a predetermined access level for access to a first base node; a temporal access table; processing means programmed for comparing said access request to said temporal access table to determine if said access request completes a prohibited temporal access pattern for said entity, and for comparing a minimum access level established for said first base node to said predetermined access level and wherein said processing means grants said access requests only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level, (Paragraphs: 0030 & 0034, the examiner notes that a security table which relates a user identification and security table, change with time based on the project type and sensitivity level associated with the project, therefore it is inherent that a security table in fact is a temporal access table. The examiner further notes that to one of ordinary skill in the art, that a database is constructed in a software language and can only be implemented on a computer or computer system, thus it is inherent that a computer system and software will employ an interface for interaction with the user or administrator.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dant B. Shaifer - Harriman whose telephone number is 571-272-7910. The examiner can normally be reached on Monday - Thursday: 8:00am - 5:30pm Alt.Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Del Sole can be reached on 571-272-1130. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



KIMBERLY D. NGUYEN
PRIMARY EXAMINER

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known

Application Number	10/798074
Filing Date	3/11/04
First Named Inventor	KOVARIK
Art Unit	2109
Examiner Name	Dant B. Shaifer - Harriman
Attorney Docket Number	7162-0110

Sheet	1	of	1
-------	---	----	---

U. S. PATENT DOCUMENTS

[illegible]

FOREIGN PATENT DOCUMENTS

[illegible]

Examiner Signature	/Dant Shaifer Harriman/
-----------------------	-------------------------

Date Considered	4/9/2007
-----------------	----------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶ Applicant is to place a check-mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, Washington, DC 20231.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Express Mail Label:
EV 417207036 US



Approved for use through 07/31/2006. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known

Application Number	10/798,074
Filing Date	March 11, 2004
First/Named Inventor	KOVARIK, JR.
Art Unit	2109
Examiner Name	Dant B. Shaifer-Harriman
Attorney Docket Number	7162-0110

U. S. PATENT DOCUMENTS

[illegible]

FOREIGN PATENT DOCUMENTS

FOREIGN PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear
		Country Code ³ Number ⁴ Kind Code ⁵ (if known)	MM-DD-YYYY		
/DS/		WO 03/088018	10/23/2003	RAYTHEON CO.	

Examiner Signature	/Dant Shaifer Harriman/	Date Considered	4/4/07
-----------------------	-------------------------	--------------------	--------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>		Complete if Known	
		Application Number	10/798,074
		Filing Date	March 11, 2004
		First Named Inventor	KOVARIK, JR.
		Art Unit	2109 → 2109
		Examiner Name	Dant B. Shaifer - Harriman
Sheet 2 of 2	Attorney Docket Number	7162-0110	

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
/DS/		MEADOWS, C., "Extending the Brewer-Nash Model to a Multilevel Context" IEEE, Proceedings of the Symposium on Research in Security and Privacy. Oakland, May 7-9, 1990	
/DS/		STICKEL, M., "Elimination of Inference Channels by Optimal Upgrading" Research in Security and Privacy, 1994. 1994 IEEE Computer Society Symposium in Oakland, CA, May 16-18, IEEE Comput. Soc, 16 May, 2004, pages 168-174	
/DS/		DENNING, D., "A Lattice Model of Secure Information Flow" COMMUNICATIONS OF THE ACM, Vol. 19, No. 5, May 1976, pp 236-243.	
/DS/		NULL, L., et al., "A Unified Approach for Multilevel Database Security Based on Inference Engines" SIGCSE BULLETIN, ACM, New York, NY Feb. 23, 1989, pp 108-111	
/DS/		SAMARATI, et al., "Access Control: Policies, Models, and Mechanisms" Lecture Notes in Computer Science, Springer Verlag, New York, NY Vol. 2171, June 2003, pp 137-196	
/DS/		SANDHU, R., "Lattice-Based Access Control Models" Online: URL: http://doi.ieeecomputersociety.org/10.1109/2.241422 retrieved on 10/25/2005	
/DS/		BREWER, D., et al., "The Chinese Wall Security Policy" Proceedings of the Symposium on Security and Privacy. Oakland, May 1-3, 1989, Washington, IEEE Comp. Soc. Press, US	
/DS/		SANDHU, R., "The Typed Access Matrix Model" IEEE, Proceedings of the Computer Society Symposium on Research in Security and Privacy. Oakland, May 4-6, 1992, Los Alamitos, IEEE Comp. Soc. Press, US., Vol. SYMP. 13, May 4, 1992, pp. 122-136	

Examiner Signature	/Dant Shaifer Harriman/	Date Considered	4/4/07
--------------------	-------------------------	-----------------	--------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.
This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Notice of References Cited	Application/Control No. 10/798,074	Applicant(s)/Patent Under Reexamination KOVARIK, VINCENT JOSEPH	
	Examiner Dant B. Shaifer - Harriman	Art Unit 2109	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2004/0044655 A1	03-2004	Cotner et al.	707/003
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes 	Application/Control No. 10798074	Applicant(s)/Patent Under Reexamination KOVARIK, VINCENT JOSEPH
	Examiner Shaifer - Harriman , Dant B	Art Unit 2109

SEARCHED			
Class	Subclass	Date	Examiner
709	229	4/9/2007	dsh
713	201	4/5/2007	dsh
713	166	4/5/2007	dsh
726	23	4/9/2007	dsh
709	219	4/9/2007	dsh

SEARCH NOTES		
Search Notes	Date	Examiner
East Search (see attached)	4/5/2007- 4/9/2007	dsh
Inventor Search, reveiwed related applications (see attached)	4/3/2007	dsh
Consolted with Mr. Matt Heneghan, AU=2134	4/9/2007	dsh

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov



Bib Data Sheet

CONFIRMATION NO. 5321

SERIAL NUMBER 10/798,074	FILING OR 371(c) DATE 03/11/2004 RULE	CLASS 713	GROUP ART UNIT 2109	ATTORNEY DOCKET NO. 7162-0110	
APPLICANTS Vincent Joseph Kovarik JR., Grant, FL;					
** CONTINUING DATA *****					
** FOREIGN APPLICATIONS *****					
IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** 05/27/2004					
Foreign Priority claimed ☐ yes ☒ no		STATE OR COUNTRY FL ✓	SHEETS DRAWING 10 ✓	TOTAL CLAIMS 19 ✓	INDEPENDENT CLAIMS 3 ✓
35 USC 119 (a-d) conditions ☐ yes ☒ no ☐ Met after met					
Verified and Acknowledged <i>D. B. Schaffer-Hawkins DSH</i> Examiner's Signature Initials					
ADDRESS 39207					
TITLE Enforcing computer security utilizing an adaptive lattice mechanism					
FILING FEE RECEIVED 770	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:		☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit		

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2051	709/229.ccls.	USPAT	OR	ON	2007/04/09 14:15
L2	2050	L1 and (receiving and request in computer and system)	USPAT	OR	ON	2007/04/09 14:14
L3	1049	L2 and ((authorization) or (authentication) or (pretdetermined and access and level) or (minimum and access and level))	USPAT	OR	ON	2007/04/09 14:19
L5	0	"10254457"	USPAT	OR	ON	2007/04/09 15:19
L6	8	"254457"	USPAT	OR	ON	2007/04/09 15:20
S1	27	"6014628"	US-PGPUB; USPAT	OR	ON	2007/04/03 07:42
S2	3	"7020717"	US-PGPUB; USPAT	OR	ON	2007/04/03 07:44
S3	2	"7126470"	US-PGPUB; USPAT	OR	ON	2007/04/03 07:48
S4	19	"5733418"	US-PGPUB; USPAT	OR	ON	2007/04/03 10:21
S5	1	"20020138322"	US-PGPUB; USPAT	OR	ON	2007/04/03 11:41
S6	22	"6023765"	US-PGPUB; USPAT	OR	ON	2007/04/03 16:51
S7	10	"5,429,736"	US-PGPUB; USPAT	OR	ON	2007/04/04 08:01
S8	3	"0044655"	US-PGPUB; USPAT	OR	ON	2007/04/04 08:02
S9	1	2004/0044655	US-PGPUB; USPAT	OR	ON	2007/04/04 08:02
S10	1	"20040044655"	US-PGPUB; USPAT	OR	ON	2007/04/04 10:15
S11	0	wo03/088018	US-PGPUB; USPAT	OR	ON	2007/04/04 10:16
S12	0	wo03088018	US-PGPUB; USPAT	OR	ON	2007/04/04 10:16
S13	1	"03088018"	US-PGPUB; USPAT	OR	ON	2007/04/04 10:17
S14	6	"088018"	US-PGPUB; USPAT	OR	ON	2007/04/04 10:18
S15	0	03/088018	US-PGPUB; USPAT	OR	ON	2007/04/04 10:18
S16	0	03/088018	US-PGPUB; USPAT	OR	ON	2007/04/04 10:22

EAST Search History

S17	0	wo03/088018	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/04 10:23
S18	0	wo03088018	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/04 10:23
S19	3	"03088018"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/04 10:24
S20	2	"20040044655"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/05 16:19
S21	0	713/201.CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/05 16:22
S22	0	713/201.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/05 16:22
S23	415	713/166.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/05 16:25

EAST Search History

S24	12	"6334121"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/04/05 16:29
S25	8	("6334121").URPN.	USPAT	OR	ON	2007/04/05 16:55
S26	23	"6345361"	USPAT	OR	ON	2007/04/05 16:56
S27	22	("6345361").URPN.	USPAT	OR	ON	2007/04/05 17:13
S28	12	"6405202"	USPAT	OR	ON	2007/04/09 08:09
S29	26	"6408391"	USPAT	OR	ON	2007/04/09 08:28
S30	9	"6446206"	USPAT	OR	ON	2007/04/09 08:43
S31	10	"6446077"	USPAT	OR	ON	2007/04/09 09:19
S32	3	"6453418"	USPAT	OR	ON	2007/04/09 11:28
S33	221	726/23.ccls.	USPAT	OR	ON	2007/04/09 15:19
S34	100	S33 and (receiving and request and computer and system)	USPAT	OR	ON	2007/04/09 11:35
S35	63	S33 and (temporal or (time and interval))	USPAT	OR	ON	2007/04/09 11:35
S36	5	("20010047420" "5974496" "6529706" "6741841" "6904449").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/04/09 11:37
S37	1	("2001/0047420").URPN.	USPAT	OR	ON	2007/04/09 11:38
S38	25	("6484203").URPN.	USPAT	OR	ON	2007/04/09 12:25
S39	0	("7200656").URPN.	USPAT	OR	ON	2007/04/09 12:26
S40	0	("7200656").URPN.	USPAT	OR	ON	2007/04/09 12:26
S41	0	("7200656").URPN.	USPAT	OR	ON	2007/04/09 12:26
S42	10	S33 and (temporal)	USPAT	OR	ON	2007/04/09 12:28
S43	5	("6826697").URPN.	USPAT	OR	ON	2007/04/09 13:20
S44	0	("7181733").URPN.	USPAT	OR	ON	2007/04/09 13:21
S45	165	S33 and ((request and (user or entity) and in and computer and system) or (receiving and (user or entity) and in and computer and system))	USPAT	OR	ON	2007/04/09 13:26
S46	14	S33 and ((request same (user or entity) same in same computer same system) or (receiving same (user or entity) same in same computer same system))	USPAT	OR	ON	2007/04/09 13:26

EAST Search History

S47	76	S45 and ((predetermined and access and level) or (minimum and access and level))	USPAT	OR	ON	2007/04/09 13:28
S48	5	S47 and ((temporal and access and pattern) or (temporal))	USPAT	OR	ON	2007/04/09 13:30
S49	38	("6324647").URPN.	USPAT	OR	ON	2007/04/09 13:30
S50	38	("6324647").URPN.	USPAT	OR	ON	2007/04/09 13:31
S51	0	("7178166").URPN.	USPAT	OR	ON	2007/04/09 13:40
S52	2739	709/219.ccls.	USPAT	OR	ON	2007/04/09 13:42
S53	599	S52 and (receiving and request and computer and system and entity)	USPAT	OR	ON	2007/04/09 13:43
S54	239	S53 and ((predetermined and access and entity) and (minimum and access level))	USPAT	OR	ON	2007/04/09 13:45
S55	451	S53 and ((predetermined and access and entity) or (minimum and access and level) or (authorization) or (authentication))	USPAT	OR	ON	2007/04/09 13:46
S56	15	S55 and ((temporal) or (temporal and access and pattern))	USPAT	AND	ON	2007/04/09 13:52
S57	15	S55 and ((temporal) or (temporal and access and pattern))	USPAT	OR	ON	2007/04/09 13:55



PALM INTRANET

Day : Tuesday
Date: 4/3/2007
Time: 07:12:33

Inventor Name Search Result

Your Search was:

Last Name = KOVARIK

First Name = VIN

Application#	Patent#	Status	Date Filed	Title	Inventor Name
09135389	6014628	150	08/17/1998	METHOD AND SYSTEM FOR TRACKING ANY ENTITY THROUGH ANY SET OF PROCESSES UTILIZING A TEMPORAL PROJECTION	KOVARIK JR., VINCENT J.
60065811	Not Issued	159	11/14/1997	METHODOLOGY FOR DESIGNING AND CONFIGURING LOW EARTH ORBITING SATELLITE COMMUNICATION SYSTEM	KOVARIK, VINCE
60066924	Not Issued	159	11/28/1997	METHODOLOGY FOR DESIGNING AND CONFIGURING LOW EARTH ORBITING SATELLITE COMMUNICATION SYSTEM	KOVARIK, VINCE
09677072	7020717	150	09/29/2000	A SYSTEM AND METHOD FOR RESYNCHRONIZING INTERPROCESS COMMUNICATIONS CONNECTION BETWEEN CONSUMER AND PUBLISHER APPLICATIONS BY USING A SHARED STATE MEMORY AMONG MESSAGE TOPIC SERVER AND MESSAGE ROUTERS	KOVARIK, VINCENT
60156605	Not Issued	159	09/29/1999	METHOD FOR RE-SYNCHRONIZING INTER-PROCESS COMMUNICATIONS IN A DISTRIBUTED MESSAGE SYSTEM	KOVARIK, VINCENT
10814032	7126470	150	03/31/2004	WIRELESS AD-HOC RFID TRACKING SYSTEM	KOVARIK, VINCENT J.
06386370	4728862	150	06/08/1982	A METHOD FOR ACHIEVING IGNITION OF A LOW	KOVARIK, VINCENT J.

				VOLTAGE GAS DISCHARGE DEVICE	
<u>07249813</u>	<u>4942339</u>	250	09/27/1988	INTENSE STEADY STATE ELECTRON BEAM GENERATOR	KOVARIK, VINCENT J.
<u>08646149</u>	<u>5733418</u>	250	05/07/1996	SPUTTERING METHOD AND APPARATUS	KOVARIK, VINCENT J.
<u>60064128</u>	Not Issued	159	11/03/1997	SOFTWARE ENGINE FOR OBJECT TRACKING SYSTEM	KOVARIK, VINCENT J.
<u>10798074</u>	Not Issued	30	03/11/2004	Enforcing computer security utilizing an adaptive lattice mechanism	KOVARIK, VINCENT JOSEPH

Inventor Search Completed: No Records to Display.

Search Another: Inventor	Last Name	First Name	Search
	kovarik	vin	

To go back use Back button on your browser toolbar.

Back to [PALM](#) | [ASSIGNMENT](#) | [OASIS](#) | [Home page](#)



IFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No. : 10/798,074 Confirmation No. 5321
Applicant : KOVARIK, JR.
Filed : March 11, 2004
TC/A.U. : 2131
Examiner :

Docket No. : 7162-0110
Customer No. : 39207

TRANSMITTAL LETTER

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Please find enclosed for filing:

- ✓ Supplemental Information Disclosure Statement
- ✓ PTO Forms SB08A and SB08B
- ✓ Copy of European Search Report; References
- ✓ Other: Postcard Receipt
- ✓ Please charge any deficiencies or credit any overpayments to Deposit Acct. No. 08-0870.

Respectfully submitted,

Date: Mar. 22, 2006

Robert J. Sacco
Registration No. 35,667
SACCO & ASSOCIATES, P.A.
P.O. Box 30999
Palm Beach Gardens, FL 33420-0999
Tel: 561-626-2222

Certificate Under 37 C.F.R. 1.8(a)

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on Mar. 22, 2006. Typed name of person signing this certificate: ROBERT J. SACCO

{00009419;}



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No. : 10/798,074 Confirmation No. 5321
Applicant : KOVARIK, JR.
Filed : March 11, 2004
TC/A.U. : 2131
Examiner :
Docket No. : 7162-0110
Customer No. : 39207

**SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT
PURSUANT TO 37 CFR 1.97**

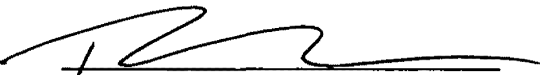
Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Pursuant to the Duty to Disclose under 37 C.F.R. §1.56, the references cited on the accompanying forms PTO SB08A and SB08B are hereby brought to the attention of the Examiner for independent evaluation. The references were cited in part in a search report drawn up by the European Patent Office on a corresponding European Patent application. A copy of the Search Report is enclosed, which satisfies the requirement for a brief explanation of relevance of foreign language documents. This paper is submitted in accordance with 37 CFR 1.97(b)(3). A fee is not required for consideration of these documents. However, should a fee be deemed to be due by the Commissioner, such fee should be charged to Deposit Account No. 08-0870.

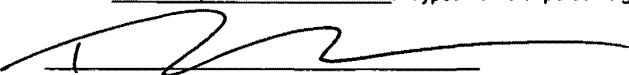
Respectfully submitted,

Date: Mar. 22, 2006


Robert J. Sacco
Registration No. 35,667
SACCO & ASSOCIATES, P.A.
P.O. Box 30999
Palm Beach Gardens, FL 33420-0999
Tel: 561-626-2222

Certificate Under 37 C.F.R. 1.8(a)

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on Mar. 22, 2006. Typed name of person signing this certificate: ROBERT J. SACCO


{00009419;}



PTO/SB/08A (07-05)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known

Application Number	10/798,074
Filing Date	March 11, 2004
First Named Inventor	KOVARIK, JR.
Art Unit	2131
Examiner Name	
Attorney Docket Number	7162-0110

Sheet 1 of 2

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
		US- 2002/0138322	09/26/2002	UMEZAWA, et al.	
		US- 6,023,765	02/08/2002	KUHN	
		US- 2004/0044655	03/04/2004	COTNER, et al.	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T ⁶
		Country Code ³ Number ⁴ Kind Code ⁵ (if known)				
		WO 03/088018	10/23/2003	RAYTHEON CO.		

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)		Complete if Known	
		Application Number	10/798,074
		Filing Date	March 11, 2004
		First Named Inventor	KOVARIK, JR.
		Art Unit	2131
		Examiner Name	
Sheet 2	of 2	Attorney Docket Number	7162-0110

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
		MEADOWS, C., "Extending the Brewer-Nash Model to a Multilevel Context" IEEE, Proceedings of the Symposium on Research in Security and Privacy. Oakland, May 7-9, 1990	
		STICKEL, M., "Elimination of Inference Channels by Optimal Upgrading" Research in Security and Privacy, 1994. 1994 IEEE Computer Society Symposium in Oakland, CA, May 16-18, IEEE Comput. Soc, 16 May, 2004, pages 168-174	
		DENNING, D., "A Lattice Model of Secure Information Flow" COMMUNICATIONS OF THE ACM, Vol. 19, No. 5, May 1976, pp 236-243.	
		NULL, L., et al., "A Unified Approach for Multilevel Database Security Based on Inference Engines" SIGCSE BULLETIN, ACM, New York, NY Feb. 23, 1989, pp 108-111	
		SAMARATI, et al., "Access Control: Policies, Models, and Mechanisms" Lecture Notes in Computer Science, Springer Verlag, New York, NY Vol. 2171, June 2003, pp 137-196	
		SANDHU, R., "Lattice-Based Access Control Models" Online: URL: http://doi.ieeeecomputersociety.org/10.1109/2.241422 > retrieved on 10/25/2005	
		BREWER, D., et al., "The Chinese Wall Security Policy" Proceedings of the Symposium on Security and Privacy. Oakland, May 1-3, 1989, Washington, IEEE Comp. Soc. Press, US	
		SANDHU, R., "The Typed Access Matrix Model" IEEE, Proceedings of the Computer Society Symposium on Research in Security and Privacy. Oakland, May 4-6, 1992, Los Alamitos, IEEE Comp. Soc. Press, US., Vol. SYMP. 13, May 4, 1992, pp. 122-136	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

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

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
23 October 2003 (23.10.2003)

PCT

(10) International Publication Number
WO 03/088018 A2(51) International Patent Classification⁷: G06F 1/00

(21) International Application Number: PCT/US03/10751

(22) International Filing Date: 9 April 2003 (09.04.2003)

(25) Filing Language: English

(26) Publication Language: English

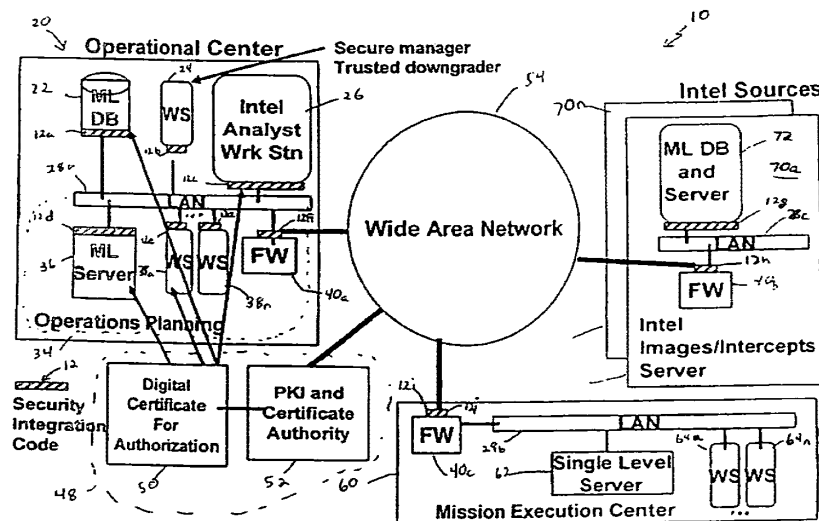
(30) Priority Data:
60/372,489 12 April 2002 (12.04.2002) US
Not furnished 1 April 2003 (01.04.2003) US(71) Applicant: RAYTHEON COMPANY [US/US]; 141
Spring Street, Lexington, MA 02421 (US).(72) Inventor: KUNG, Kenneth, C.; 19029 Vickie Avenue,
Cerritos, CA 90703 (US).(74) Agents: DURKEE, Paul, D. et al.; Daly, Crowley & Mof-
ford, LLP, 275 Turnpike Street, Suite 101, Canton, MA
02021 (US).(81) Designated States (national): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,CZ, DE, DK, DM, DZ, EC, 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, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD,
SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ,
VC, VN, YU, ZA, ZM, ZW.(84) Designated States (regional): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,
SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM,
GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— as to the identity of the inventor (Rule 4.17(i)) for the fol-
lowing designations AE, AG, AL, AM, AT, AU, AZ, BA, BB,
BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK,
DM, DZ, EC, 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, NI, NO, NZ,
OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM,
TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.
ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ,

[Continued on next page]

(54) Title: SYSTEM AND TECHNIQUES TO BIND INFORMATION OBJECTS TO SECURITY LABELS



(57) Abstract: A method to providing multilevel security for a data object requested by a workstation user includes providing a security label for the data object, associating security rules including a security clearance level for the data object with the security label, binding the security label to the data object, validating the correctness of the security label, associating the user's security clearance level with at least one user certificate, verifying the at least one user certificate, and determining whether the user has clearance to receive the requested data.

BEST AVAILABLE COPY



UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, 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, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations

Published:

- without international search report and to be republished upon receipt of that report

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.

SYSTEM AND TECHNIQUES TO BIND INFORMATION OBJECTS TO SECURITY LABELS

5 FIELD OF THE INVENTION

This invention relates generally to multilevel security systems and more particularly to systems and techniques to bind data objects to security labels.

BACKGROUND OF THE INVENTION

10 In commercial and military information technology applications, it is often desirable to control access to information having different levels of security. In a multilevel secure computer system, where not all users are trusted to handle all data objects, mandatory access control mechanisms are often used to enforce a multilevel security policy. The mandatory access control mechanisms determine whether a particular
15 user has the proper privilege (via his or her security clearance level or other privilege indicator) to access a data object.

In conventional secure operating systems, a security label is often associated with specific data files. These files are protected by the secure operating system. However, when these files are exported from the operating system, the receiving system cannot
20 always ascertain the trustworthiness of the security label and the file. Without this trust, all users must be trusted at a level equal to the highest clearance level in order to see to see all information within the system. This is an expensive solution and unworkable when operating in joint or coalition military environments. Conventional methods to protect information in transit include encrypting the data with a different key for each security
25 level. This protection stops as soon as the information is decrypted at an information receiving system.

It would, therefore, be desirable to control the distribution of data objects within a multilevel security system. It would be further desirable to securely bind a security label to an object and enforce a multilevel security policy in a distributed environment.

30

SUMMARY OF THE INVENTION

In accordance with the present invention, a method to providing multilevel security for a data object requested by a workstation user includes providing a security label for the data object, associating security rules including a security clearance level for the data

object with the security label, binding the security label to the data object, validating the correctness of the security label, associating the user's security clearance level with at least one user certificate, verifying at least one user certificate, and determining whether the user has clearance to receive the requested data.

5 With such an arrangement, a low cost multilevel security system is provided which controls the distribution of data objects within a multilevel security system by securely binding a security label to a data object and enforcing the associated security rules in a distributed environment. In addition, the multilevel security protection is extended into the respective operating systems and provides finer access control for granting the user access
10 privilege based on both security levels and the handling instructions (e.g., no foreign access, but releasable to UK, Canada and Australia). The multilevel security protection can be applied to individual files, paragraphs, sentences, words, and the data bit level.

BRIEF DESCRIPTION OF THE DRAWINGS

15 The foregoing features of this invention, as well as the invention itself, may be more fully understood from the following description of the drawings in which:

FIG.- 1 is a block diagram of a multilevel security, multilevel protection (MLS/MLP) system including security integration code and information network according to the invention;

20 FIG. 2 is a flow diagram illustrating the steps to login to the MLS/MLP system of FIG. 1, and to request and receive data objects;

FIG. 3 is a flow diagram illustrating the steps to launch an application and receive a remote data object from the MLS/MLP system of FIG. 1;

25 FIG. 4 is a flow diagram illustrating the steps to enforce the security rules included in a security label provided by the MLS/MLP system of FIG. 1;

FIG. 5 is a flow diagram illustrating the steps to issue a mission execution order using the MLS/MLP system of FIG. 1.

FIG. 6 is a schematic diagram of a multilevel secured data object includes a security label, data object, and digital signature according to the invention;

30 FIG. 7 is an exemplary representation of multiple levels of security in an electronic document modeled as a collection of eXtensible Markup Language (XML) tags according to the invention;

FIG. 7A is an exemplary XML Security Label data type definition for the Security Label of FIG. 7;

FIGs. 8 and 8A illustrate a set of security levels and a set of categories combined to form a partial ordering; and

5 FIG. 9 illustrates authorized and unauthorized transactions accessing secure data objects

DETAILED DESCRIPTION OF THE INVENTION

Before providing a detailed description of the invention, it may be helpful to define
10 some of the terms used in the description. As used herein, "security integration code" refers to a distributed application, which provides some of the multilevel security, multilevel protection functions described below. The functions of the security integration code can be distributed over the various workstations, platforms, database engines, and network components. A multilevel security, multilevel protection system is also referred
15 to as a MLS/MLP system.

As used herein, the term "data object" includes a file, part of a file, a paragraph, a sentence, a word, a database field, or a column or a row in a relational database table. The data object (also referred to as an information object) can also include an image and, if distinguishable, a portion of an image.

20 The term "security label," as used herein, refers to data associated with a particular data object which includes one or more security rules, for example a security level classification, and can optionally include restrictions, caveats, handling instructions and other security related data for controlling access to the data object. A data object having a associated security label is referred to as a secure data object.

25 The term "hierarchical components" refers to a security structure having a linear order such as TOP SECRET, SECRET, classified and unclassified classifications. The term "non-hierarchical components" refers to, for example, classifications such as, "nofor" (non-releasable to foreigners), "nuclear" (related to nuclear weapons), "intel" (related to intelligence activities) which are not put in any linear order.

30 The term "caveats," as used herein, refers to additional rules and restrictions placed on how data objects may be used, by the "owner" or provider of the object. The restrictions can include a list of users to whom the object can be released. These additional rules and restrictions are placed in the security label.

Referring now to Fig. 1, an exemplary multilevel security, multilevel protection system 10 includes an operational center 20 having at least one intelligence (Intel) analyst workstation 26 (also referred to as a user workstation, an Intel workstation or an application workstation) coupled to a local area network (LAN) 28a and running a portion 12c of a distributed application referred to as security integration code 12. The operational center 20 further includes a multilevel protection database (ML DB) 22 (also referred to as a multilevel security database MLS DB), and a secure manager trusted downgrader work station 24, each of which is coupled to LAN 28 and running portions of the security integration code 12a and 12b respectively. The operational center 20 further includes an operations planning component 34 having a multilevel protection sever (MLServer) 36, a plurality of workstations (WS) 38a-38n and a firewall 40a, each of which is coupled to LAN 28 and running further portions of the security integration code 12d, 12e and 12f respectively. The firewall 40a is further coupled to a wide area network (WAN) 54 via the portion of the security integration code 12f.

The operational center 20 is coupled to a PKI infrastructure 48 comprising a certificate authority 52 which provides a plurality of digital certificates 50 to the workstations and servers of the operational center 20. A plurality of intelligence (Intel) sources 70a-70n (generally referred to as Intel source 70) are coupled to the operational center 20 and to a mission execution center 60 through the WAN 54. Each Intel source 70 includes a multilevel protection database (ML DB) 72 coupled to a LAN 28c which is coupled to a firewall 40b. Each Intel source 70 collects information from related sources and files the information in the local database. Secure access to the Intel sources 70 provides aggregation of the data from various agencies. The firewall 40b is further coupled to a wide area network (WAN) 54. Both the (ML DB) 72 and the firewall 40b include portions of the security integration code 12g, and 12h respectively.

The mission execution center 60 includes a single level server 62 coupled to a LAN 28b which is coupled to a firewall 40c. The single level server 62 classifies information at one security level, regardless of the true classification of data due to the underlying system inability to protect data at multiple security levels. The firewall 40b is further coupled to a wide area network (WAN) 54. The firewall 40c includes security integration code 12i

The LANs 28a-28c can be hardwired or secure wireless LANS using 802.x protocols. The WAN 54 interconnects the mission execution center 60, the operational center 20 and one or more Intel source 70 by one or more logical links typically

implemented using secure Internet protocols, for example IPSEC. Data leaving the operational center 20 can be encrypted and can be encrypted again when entering the WAN 54. The servers 36, 62, and 72 include portions of the security integration code 12 to control the distribution of data objects having security labels before processing of the data objects by services and resources on the servers 36, 62, and 72. Each portion of the security integration code 12a-12i can be viewed as a security integration code processor securely networked together to control the distribution of data objects.

It will be appreciated by those of ordinary skill in the art that the exemplary multilevel security, multilevel protection system 10 includes can include personal computers and other hardware devices, which can operate workstations, databases and servers providing resources. It will be appreciated by those of ordinary skill in the art that the connections among the various components in the operations center 20 can include but is not limited to routers, bridges and other networking components resulting in alternative network topologies. The operating system and firewalls 40 are augmented with the security integration code 12 to protect data from unauthorized intrusion.

The security integration code 12a-12i (collectively referred to as the security integration code 12) is implemented on various computing platforms and network components of the multilevel security, multilevel protection system 10 as a distributed application. The security integration code 12 has a component which runs on at least one intel analyst work station 26 and the secure manager trusted downgrader workstation 24. Portions of the security integration code also run on the firewalls 40, the ML DB 22, the ML server 36, and operations planning workstations 38.

The security integration code 12 provides the protection processing of the secure data objects. The security integration code 12 can be implemented at several levels in the host processors, workstations, file servers, or any computer that processes secure data objects. The security integration code 12 can be located for example in the network protocol stack or at the interface between the operating system and the network interface. In operation, the security integration code 12 detects data objects having security labels leaving or entering the workstation, server, network devices, etc. The security integration code 12 guarantees that no unauthorized information can bypass the security integration check provided by the security integration code 12 (described in further detail in conjunction with FIGs. 3, and 7-9).

In a first embodiment, the security integration code 12 is inserted in the network protocol stack. As the secure data objects enter a computer system through the network connection, the secure data objects pass through the network protocol stack. Before information is passed from the protocol layer through the security integration code 12 to a higher layer protocol, the security integration code 12 checks the access rights of a user requesting the data object from the Intel workstation 26 and with security rules included in an eXtensible Markup Language (XML) security label carried within the information content. If the user is not allowed to view the information represented by the security label, the content of that information is not passed to the user. In the network layer, checking is performed to assure that the XML security label is included in each network packet including secure data objects to allow validation and security rule enforcement. In particular, if the security integration code 12 checking is implemented in the transport layer (e.g., TCP or UDP protocols), then the XML security label is included in each transport layer protocol data unit.

The security label is inserted into the appropriate protocol data unit (e.g., network packet or transport protocol data unit) for information leaving the workstation. The security clearance level in the security label is the security clearance level of the current user on the host machine. If the underlying workstation operating system supports the multilevel security mechanisms, then the security label is securely passed from the operating system to the security integration code 12. If the underlying operating system is trusted to pass the security label to the security integration code 12, then the appropriate security label will be provided by the security integration code 12. The operating system is multilevel secure (MLS) if it is trusted to associate security label to the data. Additional XML security labels could be embedded within the data (i.e., a security label is attached to data within a file). Additional security labels include information on how to handle the data, for example, an instruction providing that the data may be downgraded in 5 years from January 3, 2003.

In a second embodiment, the security integration code 12 is implemented within each underlying operating system interface to the network and the network communication protocol stack on the corresponding server, workstation or database. Secure data objects leaving the operating system and entering the network include security labels having the appropriate security clearance levels. If the underlying operating system is not multilevel secure, then the security clearance level of the data is

the security clearance level of the user logon session. Alternatively, the highest clearance level of the user is used for the security label. If the underlying operating system is a multilevel secure system, then the security level of the process calling the network communication stack is used as its security label.

5 In a third embodiment specifically designed to operate with the Apple Computer OS, an approach similar to the Apple Computer File Management Tool Kit is used. In Apple Operating System, each time a user wishes to open, close, modify, create, or manipulate a file, the action must be passed to the file management tool kit. In this particular embodiment, the security integration code 12 is integrated with the file
10 management tool kit to provide access to the secure data objects and associated security labels.

 In processing the access control check, the security integration code 12 matches the user's session security level with the security level included in the security label, for example an XML security label (described in further detail in conjunction with FIGs. 7
15 and 7A). A dominance relationship (as described in further detail in conjunction with FIGs. 8 and 8A) is used in the processing of the security label. However, the processing for the caveat handling instruction within the security label is determined prior to generating the instructions. For example, the handling instructions could include the instruction that content is releasable to Canadian and UK, but not other
20 foreigners. The security integration code 12 ascertains whether the user on the host machine is a US, Canadian, or UK citizen. To handle this type of caveat handling instructions, the security integration code 12 knows the meaning of the handling instruction when the security label is created. Logic is added to the security integration code to handle special handling instructions.

25 In operation, a mandatory access control mechanism implemented by the security integration code 12 determines the correct access control only if the security label of the data object is presented without any tampering, and can be trusted. Mandatory access control is a department of Defense (DoD) term that indicates the access control is required to meet the security policy, and is not at the discretion of the users. In one embodiment, an
30 extensible markup language (XML), a secure hashing algorithm, and a digital signature are used to bind a data object to its security label. The data objects can be individual data (record) in a database, a view in a database, a specific word, a specific paragraph, a specific file, digital image; or any combination of electronic representation of digital

information. The security label associated with each secure data object is used to enforce the mandatory access control rules stated by the security policy.

5 The secure manager trusted downgrader workstation 24 manages the security of the MLS/MLP system 10. The secure manager trusted downgrader work station 24 runs special code to change the embedded security level to a lower or another level, without violating the security policy. It is understood that the secure manager trusted downgrader workstation 24 can be implemented perform the trusted downgrade function on a separate workstation. The secure manager trusted downgrader workstation 24 collects the audit information from various platforms within the operational center 20, performs trusted
10 downgrading and performs an intrusion detection function. The intrusion detection system detects malicious activities within the operation center 20. A new security label is generated by the secure manager trusted downgrader work station 24 for binding with data objects to provide secure data objects. The new security label is associated with the data object when the downgrade is approved.

15 By providing a mechanism for securely binding the security label to an object, the security policy is enforced in a distributed environment. The security label includes both the clearance-level (hierarchical levels), and the compartments (non-hierarchical caveats). The mandatory access control mechanism operating on each workstation can validate the correctness of the security label for any data object arriving at the workstation and
20 determine whether the user on that workstation has the proper clearance to receive the data object.

When the data object includes classified data, it is labeled with the highest classification included within that data object. The security label includes a hierarchical level plus a set of non-hierarchical handling instructions. The security label is then used
25 by the mandatory access control code (enforced by security integration code 12) to determine whether the user on the workstation has the proper clearance to access the data object.

The security integration code 12 checks the mandatory access control, and the security integration code 12 must have the assurance that the security label has not been
30 tampered either during transit or storage of the security label.

In one embodiment an extensible markup language (XML) is used to define the data object and its associated security label, and digitally sign the hash value that is derived from the data object and its security label. The digital signature prevents corruption or

tampering of the data and the security label. It is signed and verified by the security integration code 12 at the sending node and receiving node, respectively. In one embodiment, the signing process includes the following four steps. First, XML elements are used to define the boundary of the data object for which the security label is assigned.

5 Next, the security label includes the hierarchical and non-hierarchical components. The security label usually includes the security clearance level derived from the login session for the workstation originating the request for information. XML provides the processing instruction on how to interpret the security label. The processing instruction can be placed before the data object, within the data object or at the end of the data object. The XML

10 notation attribute defines the application (i.e., Security Integration Code, the hashing algorithm, and digital signature mechanism) needed to do the processing. Next, a hashing algorithm is used to derive a digital digest from the security label and the data object. Finally, a digital signature is used to sign the digital digest.

An exemplary scenario for a multilevel security (MLS) application as implemented

15 with the present invention includes one or more Intel operator in the operation center running applications on the Intel Analyst workstation 26. In conjunction with the application, the Intel operator accesses information from the MLS database 22 and MLS file server 36. The Intel operator can also use a collaboration tool, which interrogates remote centers, e.g. Intel sources 70, for additional information and retrieves the

20 information, and transmits the information to local operational center 20. The Intel operator aggregates information from the above sources to determine the situation, before issuing a subsequent course of action. The course of action is subsequently transmitted to the mission execution center 60.

The information that the Intel Operator requests from the MLS DB 22 and ML File

25 Server 36 is delivered in the form of secure data objects each having an associated security label. The security integration code 12 checks the security label after the data and security label are returned to the workstation. Mandatory access control check is performed to meet the MLS/MLP (multilevel protection) rules. Security label caveats and handling rules are enforced. After these checks explicitly grant access, the information is passed to

30 the application program that made the original request on the user's behalf. The Intel operator uses the information to do the analysis. Intel operator writes data out to the database, file server, or sends message via the network. Data leaving the workstation is associated with a security label equal to the security level of the log in session of the user.

If data leaving is taken from the database and file server, the corresponding security label that come with the data is also attached. The generation and attachment of security labels are performed by the security integration code 12. Collaboration and data mining tools determine whether additional information should be retrieved from remote locations (e.g., Intel sources 70).

In one embodiment, the system 10 the workstations, servers and databases operate on trusted operating systems, (for example, Trusted Solaris, Secure Linux, etc.). In this embodiment, trusted handshaking is used between security integration code 12 and the underlying operating system. A secure protocol, for example, IPSEC (Internet standard) is used to protect transmission among workstations having security integration code 12. Firewalls 40 are also IPSEC enabled. These measures protect all communication paths. The security integration code 12 is non-bypassable as is required in the MLS/MLP system 10. The security integration code 12 intercepts any data requests from the user workstation to the database or data files. The security integration code 12 can be hosted onto trusted UNIX platforms, and the trusted code is tied to the underlying trusted operating system.

It will be appreciated by those of ordinary skill in the art that the data objects can be encrypted or alternatively encrypted in transit to provide a higher level of security, but the system does not require any use of encryption to provide multilevel security. Transmission among workstations, databases, and file servers that are local or remote can be encrypted. Collaboration and data mining tools make initial requests to remote sites. When the data object is returned, the now secure data object includes the security label. When information is returned to the Intel Operator on the workstation, the security integration code performs the mandatory access control, caveats, and handling instruction checks.

Information transmitted among the MLS components is protected with IPSEC protocol. Traffic leaving or entering the Operation Center must be protected with IPSEC at the firewall (FW). IPSEC protects the confidentiality of information, and integrity of the security label. It will be appreciated by those of ordinary skill in the art that other secure protocol in addition to IPSEC may be used to provide security for the transmitted information.

Referring now to FIG. 2, a flow diagram illustrates a process for user login to the MLS/MLP system 10 of FIG. 1 and to launch a requested application. The process begins at step 120, after which at step 122 the user, here an Intel analyst, logs onto the

workstation, by specifying a login ID, password, security level for the session, and role for the session in conjunction a request for access to a data object. The login procedure can also include biometric information provided by the analyst. At step 124, as part of the log in process, the Intel analyst inserts an identification document, for example
5 a government issued smart card. The smart card includes a set of digital certificates. A certificate authority service or software component issues the digital certificate adapted to be stored on a smart card. The digital certificate includes the user's security clearance level, for example, TOP SECRET, Secret, Confidential, Unclassified; clearance caveats, for example, COMSEC, Nuclear, U.S. Citizen; authorizations, for example, work on
10 project XY123; and permitted roles, for example, system admin, security officer, air traffic control, tomahawk missile operator. The digital certificate can also include information related to the user's identity.

At step 126, the public key infrastructure (PKI) and one or more certificate authorities are accessed to authenticate the user's certificate. At step 128 it is determined
15 whether the digital certificate is valid and that the digital certificate is not on the certificate revocation list. If the digital certificate is valid and not on the certificate revocation list processing continues at step 130, otherwise processing continues at step 132.

At step 130, the analyst's login and role are transferred to the portion of the security integration code 12 on the Intel workstation 26 to be used at step 144 to enforce
20 security rules. Processing continues at step 136. At step 131, the analyst requests a specific data object from ML File Server 36 or ML DB 22. It will be appreciated by those of ordinary skill in the art that the request may be an explicit request for the specific data object or the request can result for the action of an application program execution on the Intel workstation 26.

25 At step 132, the user's login session is dropped because the digital certificate has been revoked or the user's login request is not within predetermined security parameters. Processing terminates at step 134, after the login failure audit information is sent to the security manager application on the secure manager trusted downgrader work station 24, and processing terminates at step 149.

30 At step 136, the secure manager trusted downgrader workstation 24 (FIG. 1) provides a security label for the data. A user with the appropriate role authorizes the downgrading action. At step 138, the secure manager trusted downgrader workstation 24 associates security rules including a security clearance level for the data object with the

security label. At step 140, the secure manager trusted downgrader workstation 24 binds the security label to the data object forming the secure data object. At step 142, it is determined, after the secure data object reaches the analyst's workstation 26, by the portion of the security integration code 12c on the workstation 26 whether the security label is
5 valid. If the security label is valid processing continues at step 144. Otherwise processing continues at step 148.

At step 144, it is determined whether the user has clearance to receive the requested data object. The determination involves, for example, comparing the user's security clearance level to the security clearance level required to access the data
10 object. If provided in the security rules included in security label, the security integration code 12 performs other checks such as security category, clearance caveats and permitted roles. Other authorizations and handling instructions can also be provided and processed by the security integration code 12. If the analyst has clearance to receive the requested data object, processing continues at step 138 otherwise
15 processing continues at step 132.

At step 146, the Intel workstation's access control mechanism in conjunction with the security integration code 12 allows the user to access the requested data object, and processing terminates at step 149. At step 148, the security label has been determined to be invalid and security label validation failure audit information is sent to the security
20 manager on the secure manager trusted downgrader work station 24, and processing terminates at step 149.

Referring now to FIG. 3, a flow diagram illustrates an exemplary process to launch an application and request a remote data object from the MLS/MLP system 10. The process begins at step 150, after which at step 152 the user, here an Intel analyst, requests
25 that a specific application be launched. It will be appreciated by those of ordinary skill in the art that in addition to allowing access to secure data objects, the security integration code 12 can allow the user to launch and run a secure application. As allowed by the assigned roles, the user can select approved application programs to execute. For example, an air defense operator can launch an application to check on the weapon status for air
30 defense guns and missiles. At step 154, the workstation 26 (FIG. 1) access control mechanism verifies the authority of the analyst to launch application. At step 156, the user requests specific information be retrieved from ML File Server 36, ML DB 22, or explicitly from a remote source (e.g., Intel source 70).

At step 158, it is determined whether the requested data is local to the ML File Server 36 or ML DB 22. If the data is local processing continues at step 162. Otherwise, processing continues at step 160. At step 160, the data is securely requested and retrieved including the security label and handling instructions from a remote source, for example the Intel source 70a (FIG. 1).

At step 162, the request data is returned to security integration code for a mandatory access control check. The security label caveats and handling rules are enforced at this time (as described in more detail in conjunction with FIG. 4).

At step 164 it is determined whether the MLS rules are satisfied. If the MLS rules are satisfied, data is returned to the user at step 162. Otherwise, the MLS security rule checks have failed and audit information is sent to the secure manager trusted downgrader workstation 24 at step 168 and processing resumes at step 152 where additional requests to launch applications are initiated. Only after these checks explicitly grant access, is the data object passed to the application program that made the original request on the analyst's behalf. The Intel operator uses the information to do the analysis and writes the resulting analysis data back out to the database, file server, or sends messages via the network using security labels and the security integration code 12.

The security integration code 12 is non-bypassable (i.e., the security integration code 12 is trusted). This is a MLS/MLP requirement. The security integration code 12 is able to intercept any data requests from the user workstation to the database or data files. The security integration code 12 can be hosted, for example, onto any UNIX platform. The trusted security integration code 12 is interfaced to the underlying trusted operating system.

Referring now to FIG. 4, a flow diagram illustrates an exemplary process for enforcing the security rules in a security label. The process begins at step 170, after which at step 172 the security integration code 12 detects a secure data object and the security label associated with the secure data object in a network transmission. The checks in step 178 and 180 ensure that the requester (e.g., the analyst) is allowed to receive the information.

At step 174 the security integration code 12 verifies whether the security label is valid. The XML specifications (as described in more detail in conjunction with FIGs. 7 and 7A) are used to find out the boundary of the data object and a digital signature. The digital signature is checked to make sure the data object and the security label have not

been modified during transmission. A hashing algorithm and the digital signature algorithm are used as defined in the XML specifications. After verifying the digital signature, the security integration code 12 has the assurance that the security label has not been tampered either during the transit or in storage.

5 At step 176 the security integration code 12 extracts the MLS security rules (also referred to as security rules). It is understood, that the security integration code 12 may not be bypassed by the user to access information from ML DB 22 and ML Server 36. The binding of the security label to the information is described in conjunction with FIG. 6.

10 At step 178, the security integration code 12 applies the security rules to enforce the MLS mandatory access control by determining whether the analyst's access class dominates the access class of the data object. It is determined whether the analyst's security clearance as validated in conjunction with the digital certificate, allows access to the secure data object. In one embodiment, the security label is implemented in XML and is associated with specific data objects including files, portions of files and database
15 objects, and is digitally signed to prevent tampering. When the data object includes classified data, it must be labeled with the highest classification included within that data object. This security label includes a hierarchical level plus a set of non-hierarchical handling instructions (described in conjunction with FIGs. 8 and 8A). This security label is then used by the mandatory access control code (enforced by security integration code
20 12 to determine whether the analyst on the Intel workstation has the proper clearance to access this data. If it is determined that the analyst's access class dominates the access class of the data object processing continues at step 180. Otherwise processing continues at step 184.

25 At step 180, it is determined whether the requested transaction is allowable. A transaction includes reading and writing data objects having different security levels from the application process (as determined from the analyst's logon security level). Downgrading the security level of a data object generally involves multilevel transactions (described in conjunction with FIG. 9). Transactions can also be prohibited by specific handling instructions as provided by caveats in the security label. For some situations, the
30 user of the system is permitted to perform only a certain set of actions. If that is the case, step 180 can enforce this restriction. If the requested transaction is allowable processing continues at step 182. Otherwise processing continues at step 184.

At step 182, the data object is returned to the analyst, and processing resumes at step 172 to detect additional security labels. At step 184, the request for the data object is denied and audit information is sent to the secure manager trusted downgrader workstation 24.

5 Data objects that have been classified in error can be detected by looking through the entire data object for XML security labels. The data object should carry the highest classification security label as aggregated from all the security labels within it. The downgrader workstation can regrade the security label of the data object to the proper aggregation of the security labels contained within it. The security analyst discussed
10 below verifies the new security label to ensure that the correctness. The security analyst also verifies that the higher security level is due to the aggregation of information. If the aggregation causes the total data object at a higher classification, then the proper security level is assigned to the data object.

Now referring to FIG. 5, a flow diagram illustrates an exemplary process to issue a
15 mission execution order (e.g., an order from an air base to an F16 fighter crew) using the MLS/MLP system of FIG. 1. The process begins at step 210, after which at step 212 a message is generated to be transmitted to the mission execution center. At step 214 the analyst requests that the message be downgraded to appropriate security level for Mission Execution Center.

20 Analysts may propose to downgrade a specific security label associated with a specific data object. The data object generated by the analyst is classified at the level that the analyst login session defines. This level may be at a higher level than the mission execution center can receive. The analyst must make sure the content of the data object contains no information higher than the proposed new security label, as the analyst should
25 be in the best position to know this.

In one embodiment, the system requires that a second analyst, with access to a data object, "cosign" the request to downgrade the specific security label. Alternatively, the owner of the data object can downgrade the specific security label of the secure data object (described in conjunction with FIGs 9 and 9A).

30 At step 216, the secure manager trusted downgrader workstation 24 verifies that the data is appropriate for the proposed security level (according to the criteria described in conjunction with FIG. 9). At step 218, it is determined whether the data is appropriate for the proposed security level. If the data is appropriate for the proposed security level, the

secure manager trusted downgrader workstation 24 provides a security label at step 220. Otherwise, downgrading is not possible and audit information is sent to the secure manager trusted downgrader workstation 24 in step 224, and processing terminates at step 226.

- 5 At step 220, the data object with the associated security label (i.e., the secure data object) is returned to the Intel workstation 26. At step 222, the Intel workstation 26 transmits the message including the tasking order to mission execution center 60, and processing terminates at step 226.

 In an alternative embodiment, the system 10 optionally includes a "sniffer"
10 (network protocol monitor, for example Raytheon Company's Silent Runner), operating on the secure manager trusted downgrader workstation 24 for providing additional security management tools for managing the system 10. In a further alternate embodiment, the system 10 includes an automatic communications filter operating on the secure manager trusted downgrader workstation 24 (e.g. Lockheed Martin Corporation's Radiant Mercury
15 system) for automatically sanitizing information transmitted between secured gateways in the network searching for keywords which should not be passed through the gateway.

 Now referring to FIG. 6, an exemplary multilevel secured data object 300 includes a data object 302 (also referred to as an information object 302), a security label 304 and a digital signature 306. The security label is bound to any form of data objects. The security
20 label 304 is embedded with the data object 302. The security label 304 is transported via the secure communications network (local 28 or wide area network 54) to maintain the integrity and trustworthiness of the security label 304.

 The security label 304 can be processed by different operating systems to facilitate interoperability. In one embodiment, XML is used to represent the security
25 label, the intent of the information owner on how to protect the data object, is transmitted within the security label 304 as a set of security rules to the receiving workstation. The security rules included in the security label 304 direct the receiving workstation to perform the clearance checks for access to the data objects and possible modification of the security clearance level of the data objects.

- 30 In processing the security rules, the security integration code 12 compares the user's session security level with the security level included in the XML security label. For example, the analyst's session security level as provided in the analyst's

digital certificate and the security level included in the XML security label 304 are compared with respect to a security dominance relationship. The dominance relationship is described in conjunction with FIGs. 8 and 8A. The security rules can also provide additional handling instructions referred to as caveats. The rules for processing for the caveat handling instructions within the security label are determined prior to use.

For example, the handling instruction can include a rule that content is releasable to Canadian and UK citizens, but not other foreigners. The security integration code ascertains whether the analyst on the Intel workstation is a US, Canadian, or UK citizen. The analyst's citizenship is verified at login time by means of the analyst's digital signature. To handle this type of caveat handling instructions, the security integration code 12 knows the meaning of the handling instruction when the security label is created.

Now referring to FIG. 7 and 7A, an exemplary representation of multiple levels of security in an electronic document includes a plurality of eXtensible Markup Language (XML) tags. The XML model includes a hierarchical document format beginning with the <SecureDocument> container tag 312. The SecureDocument includes multiple labeled elements of the secure document encapsulated within the <SecurityLabel> container. The actual document content is included within the <DataObject> container 318 and may include encrypted text, graphics or a link to an external document. The <DataObject> container 318 may specify encryption characteristics of the secured data. Additional details of the encryption model and the specification of encryption parameters are optionally provided.

Now referring to FIG. 7A, an exemplary XML Security Label data type definition for the Security Labels includes the DataObject 318, SecureDocument 312 and SecurityLabel 314 elements. The DataObject element 318 may include arbitrary data. The SecureDocument element 312 includes one or more SecurityLabels 314. The SecurityLabel includes one or more DataObjects 318. Each SecurityLabel element 314 includes several attributes, here for example, Level, Compartment, HandlingInstruction and Caveat. The Level and Compartment attributes are required and the HandlingInstruction and Caveat attributes are optional.

In the XML example of FIG. 7A, the secure document specification includes one <SecureDocument> container 314 with four secure parts included in a <SecurityLabel>. The secure parts are included in a <DataObject> container. In this example the data parts are not encrypted. It is noted that the document has data objects with multiple levels of security including hierarchical and non-hierarchical components, for example:

1. Security Level: SECRET, Compartment: NOFORN;
2. Security Level: TOP SECRET, Compartments: A, Handling Instruction: Downgrade by the authority of the originator Caveat: Releasable to UK, Japan, and Canada
3. Security Level: Confidential, Compartment: NOFORN; Handling Instruction: Not to be downgraded until Jan 1, 2019; Caveat: Not Releasable to NATO

Specific process instructions included in the XML specifications are performed. For example, "Not to be downgraded until Jan 1, 2019" means the downgrader may not downgrade the data object. "Not releasable to NATO" means the analyst should know that the data object may not be delivered to a network address in Europe (i.e., IPv6 addresses have been divided out by continents. So this check can be processed automatically.)

Now referring to FIGs. 8 and 8A a set of security levels 400 and a set of categories 402 are combined to form a partial ordering 410. The security levels 400 are generally linearly ordered hierarchical components, for example:

Unclassified < CONFIDENTIAL < SECRET < TOP SECRET.

In order to obtain information within the MLS/MLP rules, an analyst must possess an access class whose level is greater than or equal to the level of the access class of the secure data object. Categories 402, for example Nuclear and NATO, are generally non-hierarchical components independent of each other and not ordered. To obtain access to secure data objects, a user must possess an access class whose category set includes all the categories of the access class of the secure data object to be accessed.

Combining the security levels, which form a lattice, and categories forms the partial ordering 410.

Now referring to FIG. 9, a set of authorized transactions 452-458 and a set of unauthorized transactions 460-464 accessing secure data objects in a secret file 442 and an unclassified file 444 are shown. In one embodiment, an analyst executing a pair of

applications on a workstation (represented here by an unclassified process 446 and a secret process 448) can only read an object if the access class of the user dominates the access class of the object. A user can read down the hierarchy as indicated by transactions 454, 456 and 458 but cannot read up the hierarchy as indicated by unauthorized transaction 460.

The user can write up and on the same level as indicated by transaction 452 and 454 but cannot write down as indicated by transaction 462. Because simple security cannot prevent write-down, the process 448 can write data objects into a file whose access class is less than its own for example transaction 462. In the absence of the present invention, it might be possible for the unclassified process 446, to read secret information written in transaction 462. However, the present invention prevents transactions 462 followed by transaction 464 which results in an unauthorized downgrade. An unauthorized downgrade can be prevented, as in step 178 of FIG. 4. An analyst can only write an object if the access class of the analyst is dominated by the access class of the object. The security classification of the data object is higher than the analyst. Hence, whatever the analyst writes, the classification cannot be higher than the security classification of the data object.

Having described the preferred embodiments of the invention, it will now become apparent to one of ordinary skill in the art that other embodiments incorporating their concepts may be used. It is felt therefore that these embodiments should not be limited to disclosed embodiments but rather should be limited only by the spirit and scope of the appended claims. All publications and references cited herein are expressly incorporated herein by reference in their entirety.

What is claimed is:

CLAIMS

- 1 1. A method for providing multilevel security for a data object requested by a
2 workstation user, the method comprising:
3 providing a security label for the data object;
4 associating security rules including a security clearance level for the data object
5 with the security label;
6 binding the security label to the data object;
7 validating the correctness of the security label;
8 associating the user's security clearance level with at least one user certificate;
9 verifying the at least one user certificate; and
10 determining whether the user has clearance to receive the requested data object.
- 1 2. The method of Claim 1 further comprising providing the at least one user
2 certificate on an identification document adapted for securely storing the at least one
3 user certificate.
- 1 3. The method of Claim 2 wherein the identification document is a smart card.
- 1 4. The method of Claim 1 further comprising:
2 detecting the security label in a network packet;
3 extracting the security rules from the security label; and
4 applying the security rules.
- 1 5. The method of Claim 4 wherein applying the rules associated with the security
2 label comprises determining whether the user clearance dominates the data object
3 clearance using the security rules.
- 1 6. The method of Claim 5 wherein detecting the security label comprises:
2 detecting an XML security label data type definition.

1 7. The method of Claim 6 wherein the XML security label data type definition
2 comprises:
3 a level attribute; and
4 a compartment attribute.

1 8. The method of Claim 7 wherein the XML security label data type definition
2 comprises at least one of:
3 a handling instruction attribute; and
4 a caveat attribute.

1 9. The method of Claim 1 wherein the data object comprises at least one of: a
2 record in a database;
3 a view in a database;
4 a specific word;
5 a specific paragraph;
6 a digital image;
7 a specific file; and
8 an electronic representation of digital information.

1 10. The method of Claim 1 wherein binding the security label to the data object
2 comprises:
3 deriving a hash digest from the security label and the data object; and
4 digitally signing the hash digest.

1 11. The method of Claim 10 wherein validating the correctness of the security label
2 for the data object comprises verifying the digital signature.

1 12. The method of Claim 1 further comprising associating the user certificate with
2 at least one of:
3 a security category;
4 a clearance caveat;
5 an authorization; and
6 a permitted role.

- 1 13. The method of Claim 1 wherein the security label includes at least one of:
2 a security clearance level;
3 a security category;
4 a clearance caveat; and
5 a handling instruction.
6
- 1 14. The method of Claim 1 wherein the security label comprises at least one
2 statement in an extensible markup language.
- 1 15. The method of Claim 14 wherein the extensible markup language is XML.
- 1 16. The method of Claim 1 wherein the security label comprises a security
2 clearance level.
- 1 17. The method of Claim 16 further comprising downgrading the security label
2 security clearance level.
- 1 18. The method of Claim 17 wherein the data object is transmitted to a mission
2 execution center.
- 1 19. The method of Claim 1 wherein the data object is located on a remote
2 intelligence source workstation.
- 1 20. A multilevel security system for controlling access to data objects in a secure
2 network comprising:
3 a plurality of security integration code processors coupled to the secure
4 network;
5 a secure manager workstation coupled to one of the plurality of security
6 integration code processors;
7 at least one application workstation coupled to a corresponding one the of the
8 plurality of security integration code processors; and

9 at least one of a multi-level protection database and a multi-level protection
10 server coupled to a corresponding one of the plurality of security integration code
11 processors.

12

1 21. The system of Claim 20 wherein the application workstation is adapted to
2 receive an identification document.

1 22. The system of Claim 21 wherein the identification document comprises a smart
2 card associated with at least one user certificate.

1 23. The system of Claim 22 further comprising an interface to a public key
2 infrastructure (PKI) to verify the at least one user certificate.

1 24. The system of Claim 20 further comprising:
2 a first firewall coupled to a corresponding one of the plurality of security
3 integration code processors;
4 a secure wide area network coupled to the first firewall;
5 an Intel source workstation coupled to the secure wide area network.

6

1 25. The system of Claim 20 further comprising:
2 a first firewall coupled to a corresponding one of the plurality of security
3 integration code processors;
4 a secure wide area network coupled to the first firewall;
5 a mission execution center coupled to the secure wide area network.

1 26. The system of Claim 20 wherein at least one of the plurality of security
2 integration code processors is implemented in a protocol stack in at least one
3 application workstation.

1 27. The system of Claim 20 wherein at least one of the plurality of security
2 integration code processors is implemented in an operating system interface to the
3 network in at least one application workstation.

1 28. The system of Claim 20 wherein the secure network includes an IPSEC
2 protocol.

1 29. The method of Claim 20 further comprising a trusted downgrader workstation
2 coupled to one of the plurality of security integration code processors.

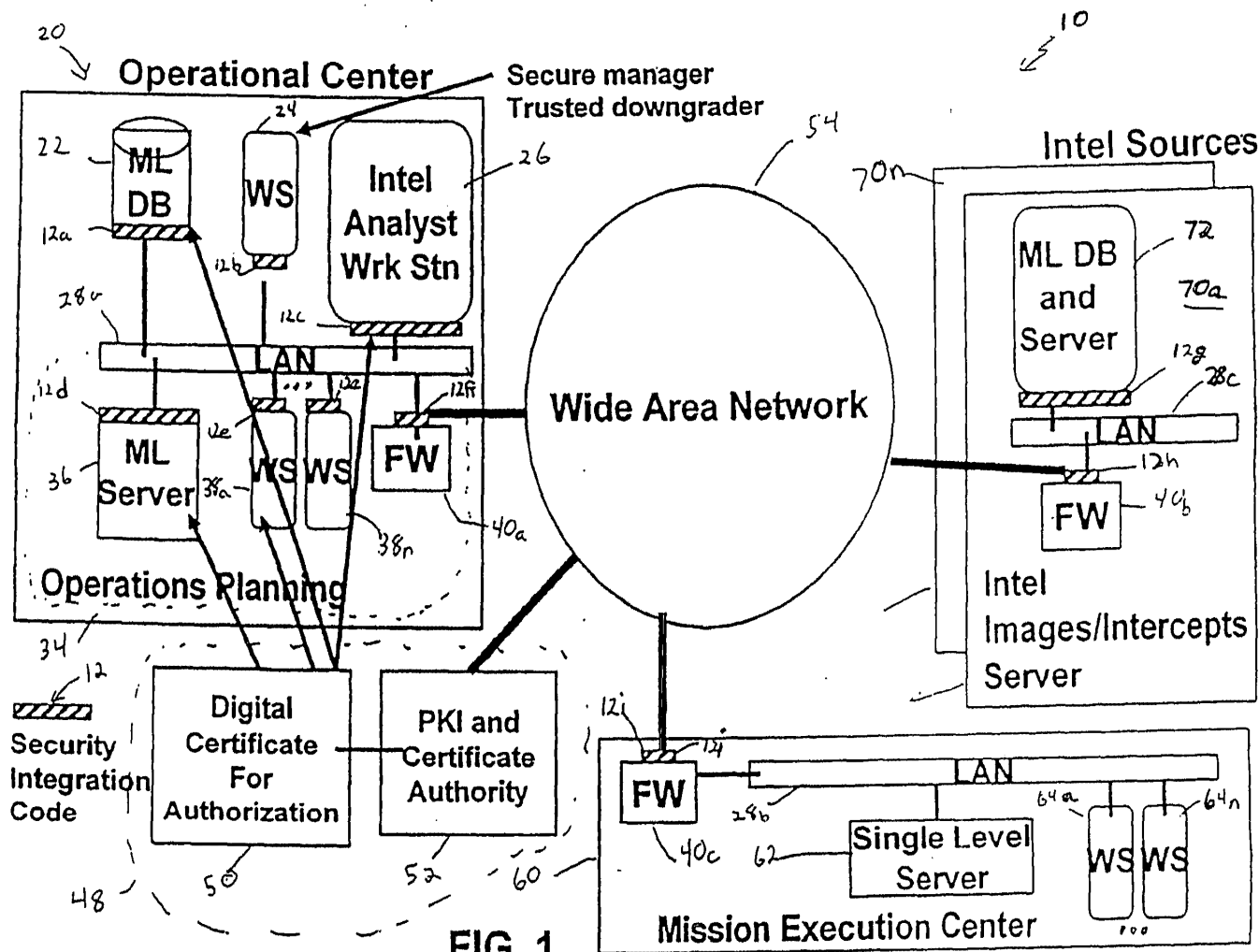
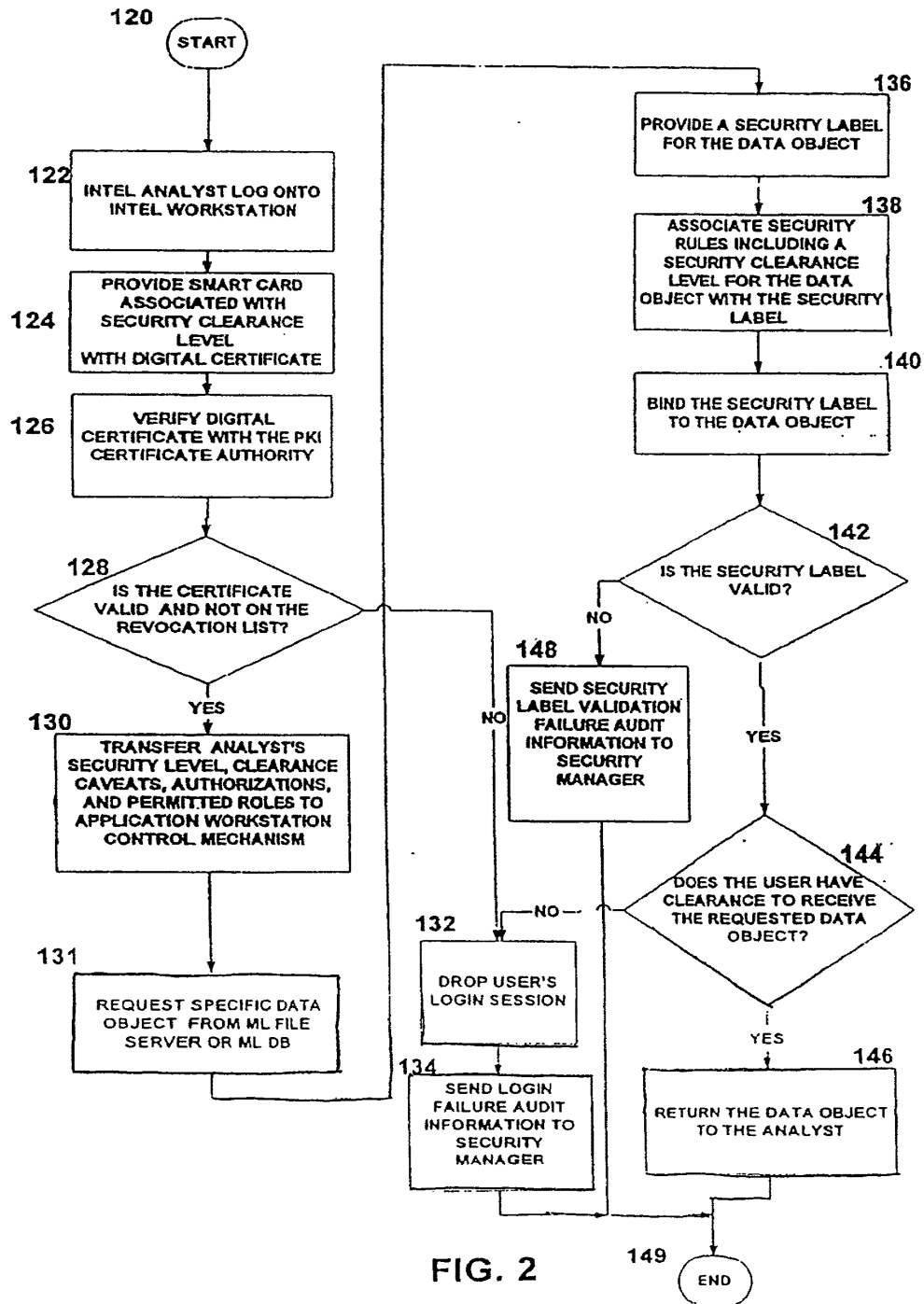
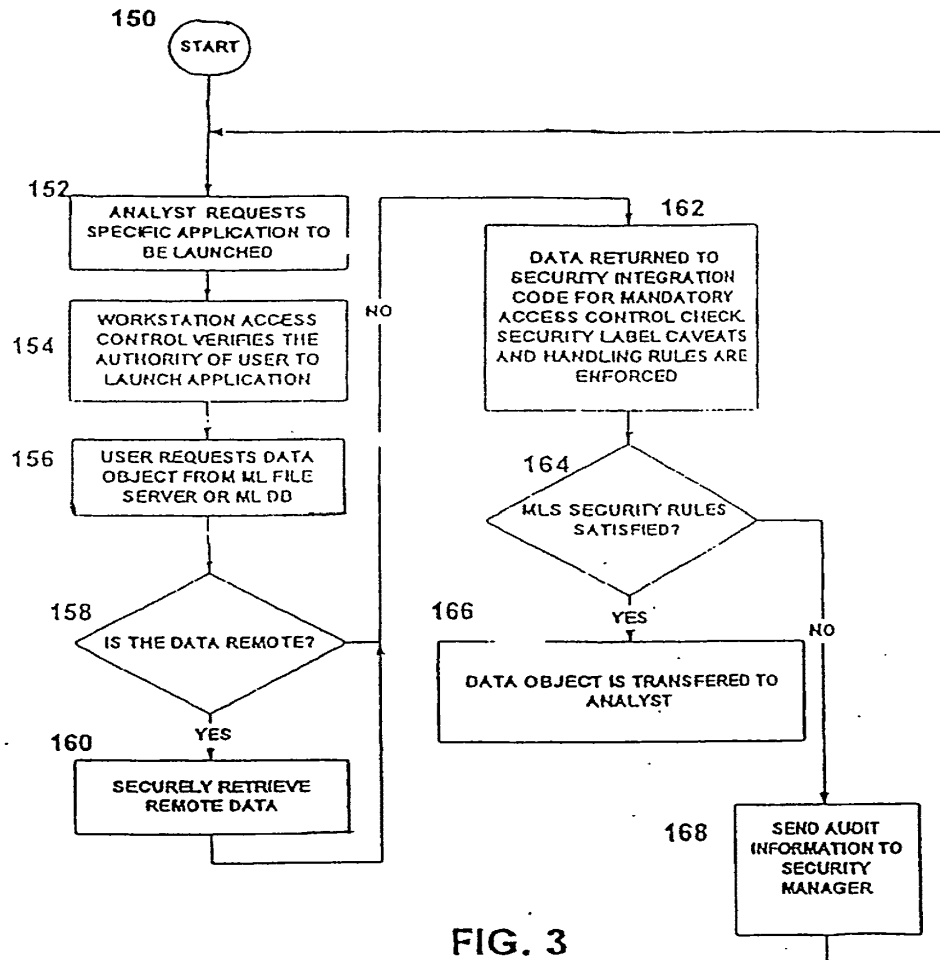


FIG. 1

2/10



3/10



4/10

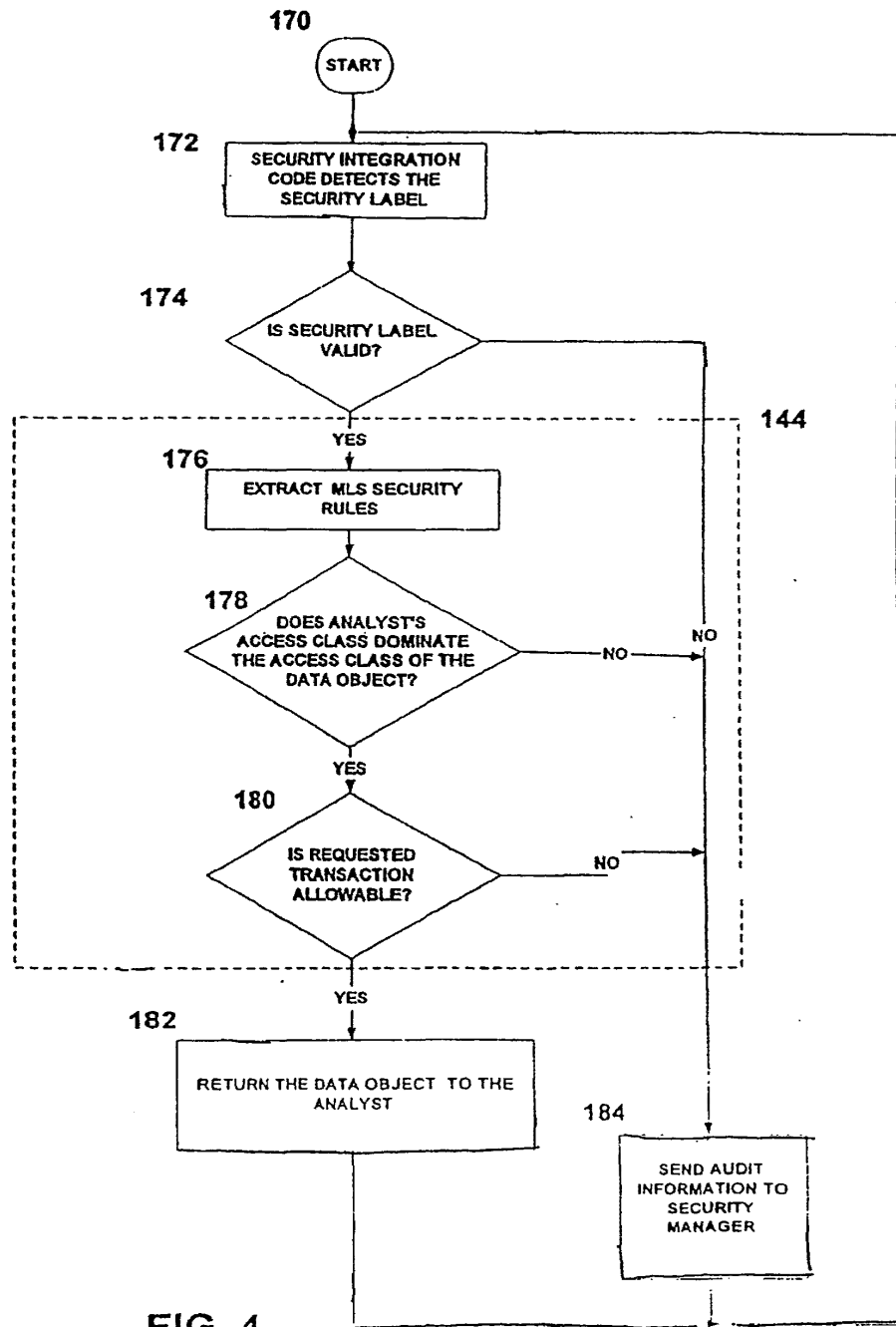


FIG. 4

5/10

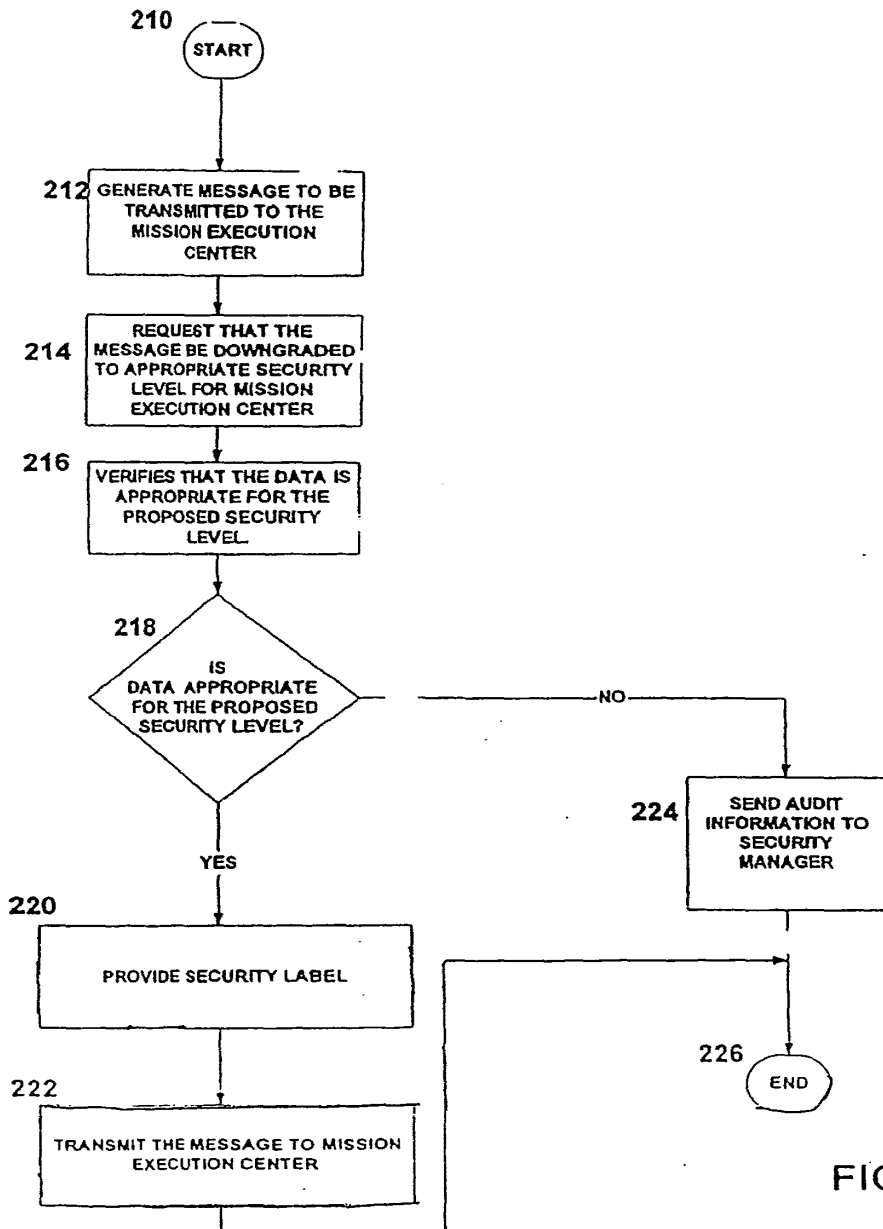


FIG. 5

6/10

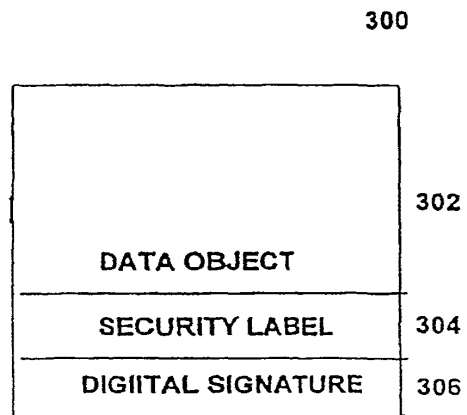


FIG. 6

7/10

<!ELEMENT DataObject (#PCDATA)>
 <!ELEMENT SecureDocument (SecurityLabel+)>
 <!ELEMENT SecurityLabel (DataObject+)>
 <!ATTLIST SecurityLabel
 Level CDATA #REQUIRED
 Compartment (NOFORN | NATO | NUCLEAR | A | B | M | K) #REQUIRED
 HandlingInstruction CDATA #IMPLIED
 Caveat CDATA #IMPLIED
 >

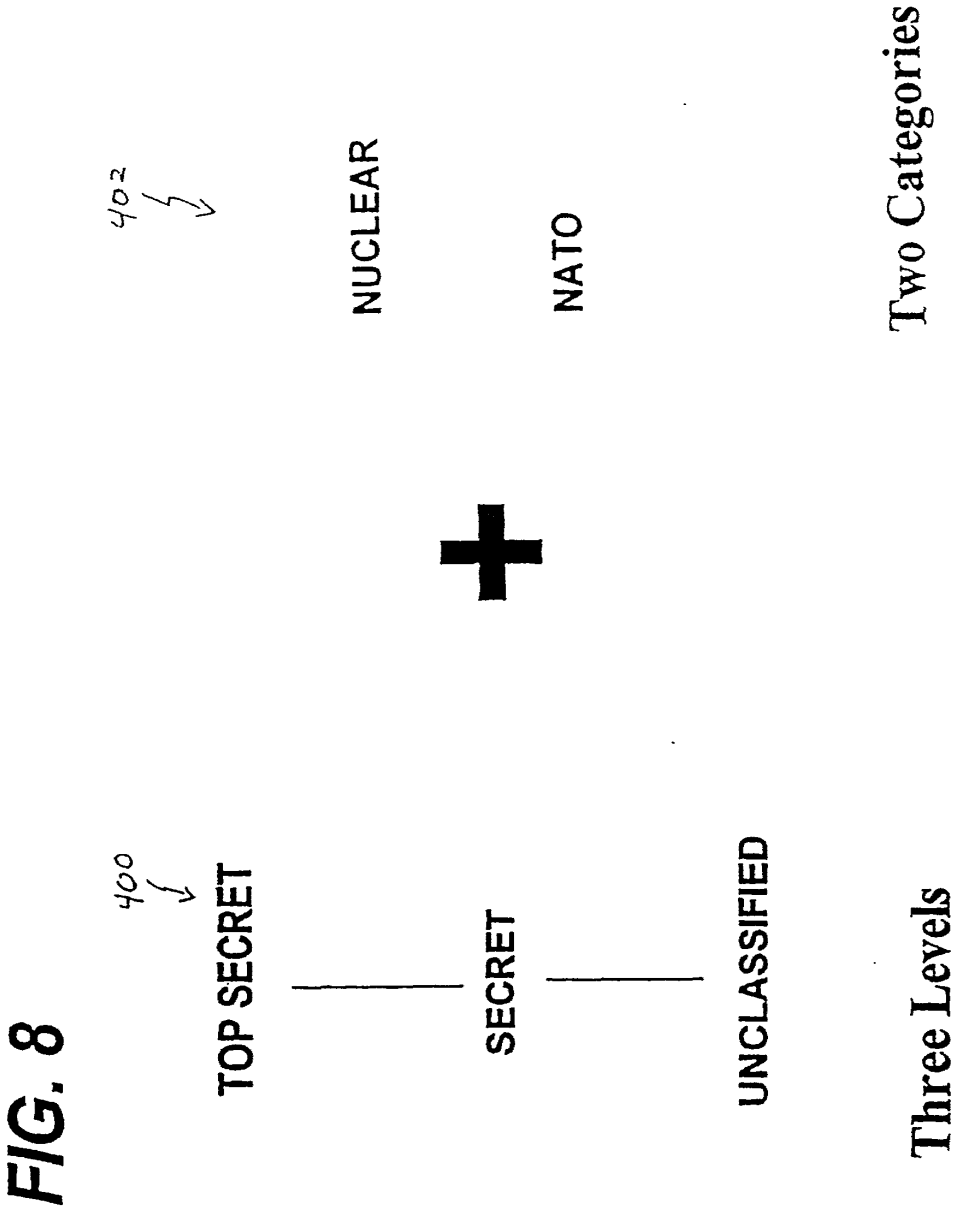
304
↙

FIG. 7

<!DOCTYPE SecureDocument (SecurityLabel.dtd)>
 314 - <SecureDocument> — 312
 <SecurityLabel Level="SECRET" Compartment="NOFORN">
 <DataObject>This is a SECRET NOFORN object</DataObject> — 314a
 </SecurityLabel>
 <SecurityLabel Level="TOP SECRET" Compartment="A"
 HandlingInstruction="Downgrade by the authority of the originator"
 Caveat="Releasable to UK, Japan and Canada">
 <DataObject>This is a TOP SECRET A data object</DataObject>
 </SecurityLabel>
 <SecurityLabel Level="CONFIDENTIAL" Compartment="NOFORN"
 HandlingInstruction="Not to be downgraded until Jan 1, 2019" Caveat="Not.
 Releasable to NATO">
 <DataObject>This is CONFIDENTIAL NOFORN object</DataObject>
 </SecurityLabel>
 <SecurityLabel Level="SECRET" Compartment="NUCLEAR"
 HandlingInstruction="Not Releasable to NATO">
 <DataObject>This is a SECRET NUCLEAR data object</DataObject> — 318b
 </SecurityLabel>
 </SecureDocument>

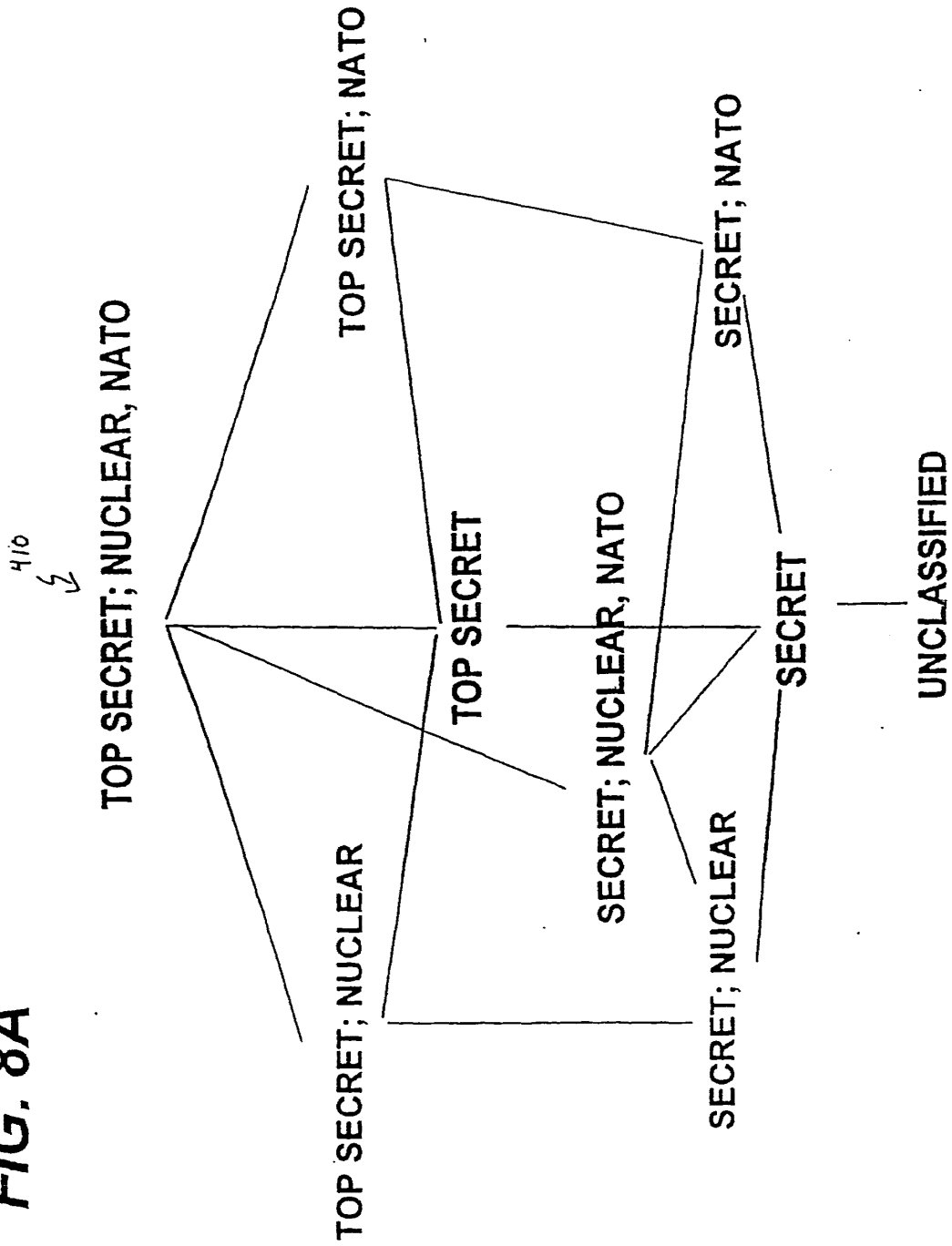
↙ 310

FIG. 7A



9/10

FIG. 8A



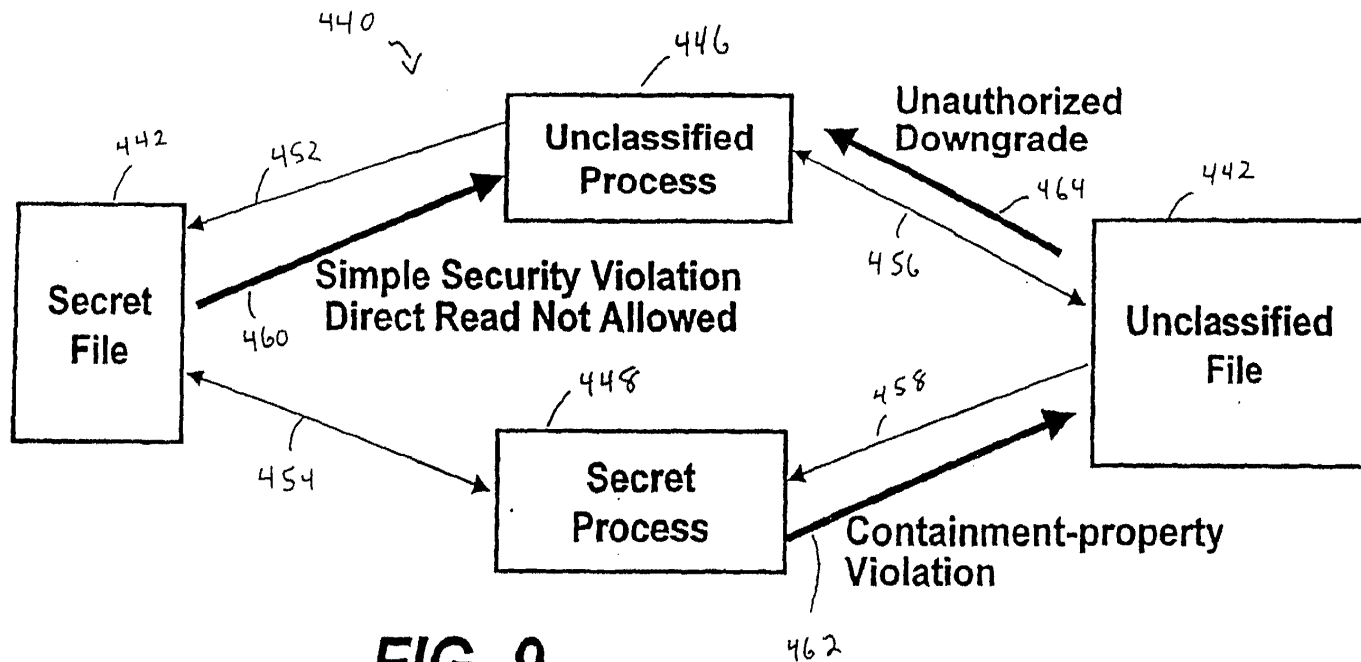


FIG. 9

10/10

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

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
23 October 2003 (23.10.2003)

PCT

(10) International Publication Number
WO 2003/088018 A3

(51) International Patent Classification⁷: G06F 1/00

(21) International Application Number:
PCT/US2003/010751

(22) International Filing Date: 9 April 2003 (09.04.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/372,489 12 April 2002 (12.04.2002) US
Not furnished 1 April 2003 (01.04.2003) US

(71) Applicant: RAYTHEON COMPANY [US/US]; 141
Spring Street, Lexington, MA 02421 (US).

(72) Inventor: KUNG, Kenneth, C.; 19029 Vickie Avenue,
Cerritos, CA 90703 (US).

(74) Agents: DURKEE, Paul, D. et al.; Daly, Crowley & Mof-
ford, LLP, 275 Turnpike Street, Suite 101, Canton, MA
02021 (US).

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

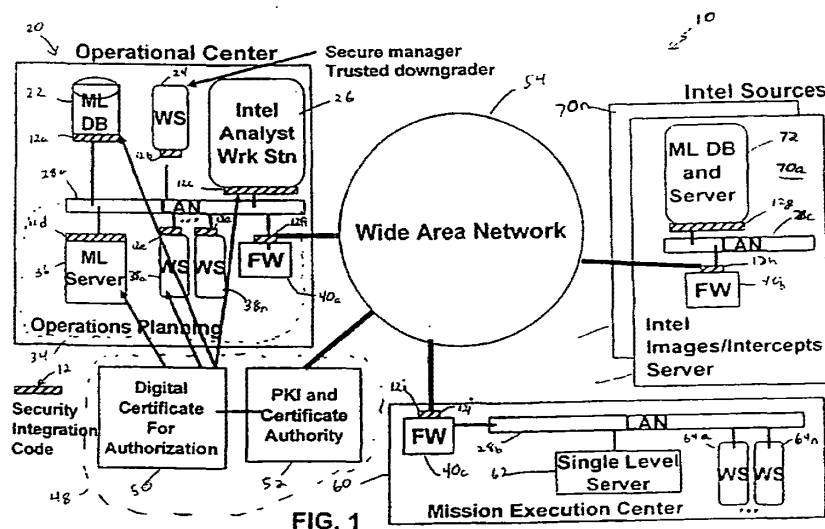
(84) Designated States (*regional*): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,
SE, SI, SK, TR), OAPI patent (BF, BJ,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

Declarations under Rule 4.17:

— as to the identity of the inventor (Rule 4.17(i)) for the fol-
lowing designations AE, AG, AL, AM, AT, AU, AZ, BA, BB,
BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK,
DM, DZ, EC, 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, NI, NO, NZ,
OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM.

[Continued on next page]

(54) Title: SYSTEM AND TECHNIQUES TO BIND INFORMATION OBJECTS TO SECURITY LABELS



(57) Abstract: A method to providing multilevel security for a data object requested by a workstation user includes providing a security label for the data object, associating security rules including a security clearance level for the data object with the security label, binding the security label to the data object, validating the correctness of the security label, associating the user's security clearance level with at least one user certificate, verifying the at least one user certificate, and determining whether the user has clearance to receive the requested data.

WO 2003/088018 A3



TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, 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, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR,

GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations

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:

1 April 2004

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

Internal Application No
PCT/US 03/10751

A. CLASSIFICATION OF SUBJECT MATTER IPC 7 G06F1/00		
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		
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		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SAMESHIMA Y ET AL: "Authorization with security attributes and privilege delegation - Access control beyond the ACL" COMPUTER COMMUNICATIONS, ELSEVIER SCIENCE PUBLISHERS BV, AMSTERDAM, NL, vol. 20, no. 5, 1 July 1997 (1997-07-01), pages 376-384, XP004126692 ISSN: 0140-3664	1,2,4,5, 9,12,13, 16-19
Y	page 377, right-hand column page 378, right-hand column - page 379, left-hand column page 382, right-hand column - page 383; figure 4 ----- -/--	3
☒ 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 14 November 2003		Date of mailing of the international search report 21.01.2004
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 San-Bento Furtado, P

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/US 03/10751

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	SIUDA K: "Security services in telecommunications networks" DIGITAL COMMUNICATIONS, 1988. MAPPING NEW APPLICATIONS ONTO NEW TECHNOLOGIES, 1988 INTERNATIONAL ZURICH SEMINAR ON ZURICH, SWITZERLAND 8-10 MARCH 1988, ZURICH, SWITZERLAND, IEEE, 8 March 1988 (1988-03-08), pages 45-52, XP010000006 ISBN: 3-908265-01-0	3
A	page 50, right-hand column page 51, right-hand column -----	1,2,4,5, 9,12,13, 16-19
A	RUSSELL D., GANGEMI G.: "Computer Security Basics" O'REILLY & ASSOCIATES, INC , 1991 , XP002261456 page 72 - page 77 -----	1-5,9, 12,13, 16-19
A	YESBERG J D ET AL: "QuARC: expressive security mechanisms" NEW SECURITY PARADIGMS WORKSHOP, 1995. PROCEEDINGS LA JOLLA, CA, USA 22-25 AUG. 1995, LOS ALAMITOS, CA, USA, IEEE COMPUT. SOC, US, 22 August 1995 (1995-08-22), pages 34-40, XP010158974 ISBN: 0-8186-7318-4 page 34, right-hand column page 35 - page 36 page 39 -----	1-5,9, 12,13, 16-19
A	GASSER M ET AL: "An architecture for practical delegation in a distributed system" PROCEEDINGS OF THE SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY. OAKLAND, MAY 7 - 9, 1990, LOS ALAMITOS, IEEE COMP. SOC. PRESS, US, vol. SYMP. 11, 7 May 1990 (1990-05-07), pages 20-30, XP010020183 ISBN: 0-8186-2060-9 page 22 - page 23 ----- -/--	1-5,9, 12,13, 16-19

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter 1al Application No
PCT/US 03/10751

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	BRANSTAD M ET AL: "The role of trust in protected mail" PROCEEDINGS OF THE SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY. OAKLAND, MAY 7 - 9, 1990, LOS ALAMITOS, IEEE COMP. SOC. PRESS, US, vol. SYMP. 11, 7 May 1990 (1990-05-07), pages 210-215, XP010020200 ISBN: 0-8186-2060-9 page 211, right-hand column page 214, right-hand column -----	1-5,9, 12,13, 16-19

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

BNSDOCID: <WO_____03088018A3_1_>

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 03/10751

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.:

1-5, 9, 12, 13, 16-19

Remark on Protest

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

Form PCT/ISA/210 (continuation of first sheet (1)) (July 1998)

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

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

1. claims: 1-5,9,12,13,16-19

Multilevel security method of controlling access to data objects by comparing security levels of objects with clearance levels of users.

2. claims: 6-8,14-15

Multilevel security method of controlling access to data objects by comparing security levels of objects with clearance levels of users, using security labels in an extensible markup language to bind security levels to data objects.

3. claims: 10,11

Multilevel security method of controlling access to data objects by comparing security levels of objects with clearance levels of users. Digitally signing the security label of the data object.

4. claims: 20-29

Multilevel security system of controlling access to data objects in a secure network comprising security integration code processors, a secure manager workstation, application workstations and a multi-level protection database or server.

THIS PAGE BLANK (USPTO)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)

PATENT



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No. : 10/798,074 Confirmation No. 5321
Applicant : KOVARIK, JR.
Filed : March 11, 2004
TC/A.U. :
Examiner :

Docket No. : 7162-0110
Customer No. : 39207

PRELIMINARY AMENDMENT

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

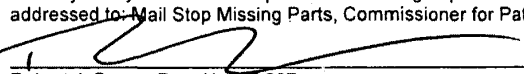
Please enter the following amendment and remarks into the above-identified application prior to Examination thereof.

Amendment to the specification begin on page 2 of this paper.

Remarks begin on page 3 of this paper.

Certificate Under 37 C.F.R. 1.8(a)

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Mail Stop Missing Parts, Commissioner for Patents, Alexandria, VA 22313-1450 on 6/21/04


Robert J. Sacco, Reg. No. 35,667

Amendment to the specification:

Please replace paragraph [0019] with the following amended paragraph:

[0019] Figs. 9A-9H show a series of tables that are useful for understanding how the inventive process can operate in a second example.



REMARKS

Applicants submit that no new matter is entered by this Preliminary Amendment and respectfully requests entry of the Amendment. No fee is believed due. However, should there be any fees relating to this Amendment, please charge such fees to Deposit Account No. 50-2884.

Respectfully submitted,

Date: 6/21/04

Robert J. Sacco
Registration No. 35,667
SACCO & ASSOCIATES, P.A.
Post Office Box 30999
Palm Beach Gardens, FL 33420-0999
561/626-2222



Replacement Sheet
10/798,074
Kovarik

Partially Ordered Set with Transitive Closure Table

POSET	A	B	C	D	dir	exec	del	a	b	c	d	e
A	1	0	0	0	0	0	0	1	1	0	0	0
B	0	1	0	0	0	0	0	1	1	1	0	0
C	0	0	1	0	0	0	0	0	0	1	0	0
D	0	0	0	1	0	0	0	0	1	0	0	1
dir	0	0	0	0	1	0	0	0	0	0	1	1
exec	0	0	0	0	0	1	0	0	0	0	1	1
del	0	0	0	0	0	0	1	0	0	0	0	1
a	0	0	0	0	0	0	0	1	1	0	0	0
b	0	0	0	0	0	0	0	0	1	0	0	0
c	0	0	0	0	0	0	0	0	0	1	0	0
d	0	0	0	0	0	0	0	0	0	0	1	1
e	0	0	0	0	0	0	0	0	0	0	0	1

202

Fig. 2A

	A	B	C	D	dir	exec	del
a	1	1	0	0	0	0	0
b	1	1	0	1	0	0	0
c	0	1	1	0	0	0	0
d	0	0	0	0	1	1	0
e	0	0	0	1	1	1	1

Fig. 2B

Temporal Order Table (TOT)

TOT	A	B	C	D	dir	exec	del
a							
b							
c							
d					1	2	
e				1	2.1	2.2	3

Fig. 3

Process/User Access Table (PUAT)

Usr	A	B	C	D	dir	exec	del
1(1)	0	1	0	2	0	2	1
2(1)	0	1	0	2	0	2	1
3(2)	0	1	0	2	0	2	1
4(1)	0	1	0	2	0	2	1
5(3)	0	1	0	2	0	2	1

Fig. 4A

Temporal Access Table (TAT)

Utr	A	B	C	D	dir	exec	del
1(1)					102	112	
2(1)							
3(2)					111	103	
4(1)							
5(3)							

Fig. 4B

Combinatorial Classification Table (CCT)

CCT	A	B	C	D	dir	exec	del
a	2	2	0	0	0	0	0
b	3	3	0	3	0	0	0
c	0	3	3	0	0	0	0
d	0	0	0	0	3	3	0
e	0	0	0	5	5	5	5

Fig. 5

Replacement Sheet
10/798,074
Kovarik

Fig. 8A

Usr	A	B	C	D	dir	exec	del
1(1)	0	1	0	2	0	2	1
2(1)	0	1	0	2	0	2	1
3(2)	0	1	0	2	0	2	1
4(1)	0	1	0	2	0	2	1
5(3)	0	1	0	2	0	2	1

Fig. 8B

TOT	A	B	C	D	dir	exec	del
a							
b							
c							
d					1	2	
e				1	2.1	2.2	3

Fig. 8C

CCT	A	B	C	D	dir	exec	del
a	2	2	0	0	0	0	0
b	3	3	0	3	0	0	0
c	0	3	3	0	0	0	0
d	0	0	0	0	3	3	0
e	0	0	0	5	5	5	5

Fig. 8D

Usr	A	B	C	D	dir	exec	del
1(1)	0	1	0	2	0	2	1
2(1)	0/1	2	0	2	0	2	1
3(2)	0	1	0	2	0	2	1
4(1)	0	1	0	2	0	2	1
5(3)	0	1	0	2	0	2	1

Fig. 8E

TOT	A	B	C	D	dir	exec	del
a							
b							
c							
d					1	2	
e				1	2.1	2.2	3

Replacement Sheet
10/798,074
Kovarik

Fig. 9A

Usr	A	B	C	D	dir	exec	del
1(1)	0	1	0	2	0	2	1
2(1)	0	1	0	2	0	2	1
3(2)	0	1	0	2	0	2	1
4(1)	0	1	0	2	0	2	1
5(3)	0	1	0	2	0	2	1

Fig. 9B

TOT	A	B	C	D	dir	exec	del
a							
b							
c							
d					1	2	
e				1	2.1	2.2	3

Fig. 9C

CCT	A	B	C	D	dir	exec	del
a	2	2	0	0	0	0	0
b	3	3	0	3	0	0	0
c	0	3	3	0	0	0	0
d	0	0	0	0	3	3	0
e	0	0	0	5	5	5	5

Fig. 9D

Usr	A	B	C	D	dir	exec	del
1(1)	0	1	0	2	0	2	1
2(1)	0	1	0	2	0	2	1
3(2)	0/1	2	0	2	0	2	1
4(1)	0	1	0	2	0	2	1
5(3)	0	1	0	2	0	2	1

Fig. 9E

TOT	A	B	C	D	dir	exec	del
a							
b							
c							
d					1	2	
e				1	2.1	2.2	3

Replacement Sheet
10/798,074
Kovarik

Fig. 9F

CCT	A	B	C	D	dir	exec	del
a	2	2	0	0	0	0	0
b	3	3	0	3	0	0	0
c	0	3	3	0	0	0	0
d	0	0	0	0	3	3	0
e	0	0	0	5	5	5	5

Fig. 9G

Usr	A	B	C	D	dir	exec	del
1(1)	0	1	0	2	0	2	1
2(1)	0	1	0	2	0	2	1
3(2)	0/1	3	0	2/2	0	2	1
4(1)	0	1	0	2	0	2	1
5(3)	0	1	0	2	0	2	1

Fig. 9H

TOT	A	B	C	D	dir	exec	del
a							
b							
c							
d					1	2	
e				1	2.1	2.2	3

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2003

Application or Docket Number

10/798 074

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS	14	
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	14 minus 20 =	*
INDEPENDENT CLAIMS	3 minus 3 =	*
MULTIPLE DEPENDENT CLAIM PRESENT ☐		

* If the difference in column 1 is less than zero, enter "0" in column 2

SMALL ENTITY
TYPE ☐

OR OTHER THAN
SMALL ENTITY

RATE	FEE
BASIC FEE	385.00
XS 9=	
X43=	
+145=	
TOTAL	

RATE	FEE
BASIC FEE	770.00
XS18=	
X86=	
+290=	
TOTAL	770

CLAIMS AS AMENDED - PART II

6-24-04

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total	* 19	Minus ** 20	=
Independent	* 3	Minus *** 3	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM ☐			

SMALL ENTITY

OR OTHER THAN
SMALL ENTITY

RATE	ADDI- TIONAL FEE
XS 9=	
X43=	
+145=	
TOTAL ADDIT. FEE	

RATE	ADDI- TIONAL FEE
XS18=	
X86=	
+290=	
TOTAL ADDIT. FEE	

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total	*	Minus **	=
Independent	*	Minus ***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM ☐			

RATE	ADDI- TIONAL FEE
XS 9=	
X43=	
+145=	
TOTAL ADDIT. FEE	

RATE	ADDI- TIONAL FEE
XS18=	
X86=	
+290=	
TOTAL ADDIT. FEE	

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT C	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total	*	Minus **	=
Independent	*	Minus ***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM ☐			

RATE	ADDI- TIONAL FEE
XS 9=	
X43=	
+145=	
TOTAL ADDIT. FEE	

RATE	ADDI- TIONAL FEE
XS18=	
X86=	
+290=	
TOTAL ADDIT. FEE	

- * If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 - ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."
 - *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."
- The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
10/798,074	03/11/2004	Vincent Joseph Kovarik JR.	7162-0110

CONFIRMATION NO. 5321

39207
 SACCO & ASSOCIATES, PA
 P.O. BOX 30999
 PALM BEACH GARDENS, FL 33420-0999

FORMALITIES LETTER



OC000000012802421

Date Mailed: 05/27/2004

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Filing Date Granted

An application number and filing date have been accorded to this application. The application is informal since it does not comply with the regulations for the reason(s) indicated below. Applicant is given TWO MONTHS from the date of this Notice within which to correct the informalities indicated below. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

The required item(s) identified below must be timely submitted to avoid abandonment:

- Replacement drawings in compliance with 37 CFR 1.84 and 37 CFR 1.121 are required. The drawings submitted are not acceptable because:
 - The drawings have a line quality that is too light to be reproduced (weight of all lines and letters must be heavy enough to permit adequate reproduction) or text that is illegible (reference characters, sheet numbers, and view numbers must be plain and legible) see 37 CFR 1.84(l) and (p)(1)); See Figure(s) 8a-8e; 9a-9j.

Replies should be mailed to: Mail Stop Missing Parts
 Commissioner for Patents
 P.O. Box 1450
 Alexandria VA 22313-1450

*A copy of this notice **MUST** be returned with the reply.*


 Customer Service Center
 Initial Patent Examination Division (703) 308-1202

PART 3 - OFFICE COPY

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL (Only for new nonprovisional applications under 37 CFR 1.53(b))		<table border="1" style="width: 100%; border-collapse: collapse;"><tr><td style="width: 50%;">Attorney Docket No.</td><td>7162-0110</td></tr><tr><td>First Inventor</td><td>KOVARIK, JR.</td></tr><tr><td>Title</td><td>Enforcing Computer Security Utilizing an Adaptive Lattice Mechanism</td></tr><tr><td>Express Mail Label No.</td><td>EV 417207036 US</td></tr></table>	Attorney Docket No.	7162-0110	First Inventor	KOVARIK, JR.	Title	Enforcing Computer Security Utilizing an Adaptive Lattice Mechanism	Express Mail Label No.	EV 417207036 US
Attorney Docket No.	7162-0110									
First Inventor	KOVARIK, JR.									
Title	Enforcing Computer Security Utilizing an Adaptive Lattice Mechanism									
Express Mail Label No.	EV 417207036 US									
APPLICATION ELEMENTS See MPEP chapter 600 concerning utility patent application contents.		ADDRESS TO: Mail Stop Patent Application Commissioner for Patents P.O. Box 1450 Alexandria VA 22313-1450								
1. ☒ Fee Transmittal Form (e.g., PTO/SB/17) (Submit an original and a duplicate for fee processing) 2. ☐ Applicant claims small entity status. See 37 CFR 1.27. 3. ☒ Specification [Total Pages <u>23</u>] (preferred arrangement set forth below) - Descriptive title of the invention - Cross Reference to Related Applications - Statement Regarding Fed sponsored R & D - Reference to sequence listing, a table, or a computer program listing appendix - Background of the Invention - Brief Summary of the Invention - Brief Description of the Drawings (if filed) - Detailed Description - Claim(s) - Abstract of the Disclosure 4. ☒ Drawing(s) (35 U.S.C. 113) [Total Sheets <u>10</u>] 5. Oath or Declaration [Total Sheets <u>2</u>] a. ☒ Newly executed (original or copy) b. ☐ Copy from a prior application (37 CFR 1.63(d)) (for continuation/divisional with Box 18 completed) i. ☐ DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) name in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b). 6. ☒ Application Data Sheet. See 37 CFR 1.76		7. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program (Appendix) 8. Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary) a. ☐ Computer Readable Form (CRF) b. Specification Sequence Listing on: i. ☐ CD-ROM or CD-R (2 copies); or ii. ☐ Paper c. ☐ Statements verifying identity of above copies ACCOMPANYING APPLICATION PARTS 9. ☒ Assignment Papers (cover sheet & document(s)) 10. ☐ 37 CFR 3.73(b) Statement ☐ Power of Attorney (when there is an assignee) 11. ☐ English Translation Document (if applicable) 12. ☒ Information Disclosure ☐ Copies of IDS Citations 13. ☐ Statement (IDS)/PTO-1449 14. ☒ Preliminary Amendment 15. ☐ Return Receipt Postcard (MPEP 503) (Should be specifically itemized) 16. ☐ Certified Copy of Priority Document(s) (if foreign priority is claimed) 17. ☐ Nonpublication Request under 35 U.S.C. 122 (b)(2)(B)(i). Applicant must attach form PTO/SB/35 or its equivalent. 18. ☒ Other: Fee: \$810.....								

18. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:

☐ Continuation

☐ Divisional

☐ Continuation-in-part (CIP)

Prior application No.:

Prior application information: Examiner _____ Art Unit: _____

For CONTINUATION OF DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

19. CORRESPONDENCE ADDRESS

☒ Customer Number: 39207

OR ☐ Correspondence address below

Name	
Address	
City	State
Country	Zip Code
Telephone	Fax

Name (Print/Type)	Robert J. Saee	Registration No. (Attorney/Agent)	35,667
Signature		Date	3/11/04

This collection of information is required by 37 CFR 1.53(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop Patent Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

18851
031104

18851

U.S. PTO

PTO/SB/17 (10-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL
for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27**TOTAL AMOUNT OF PAYMENT** (\$ 810)**Complete if Known**

Application Number	
Filing Date	
First Named Inventor	KOVARIK, JR.
Examiner Name	
Art Unit	
Attorney Docket No.	7162-0110

METHOD OF PAYMENT (check all that apply)☒ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None☒ Deposit Account:

Deposit Account Number

50-2884

Deposit Account Name
Sacco & Associates, P.A.

The Director is authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☒ Credit any overpayments☒ Charge any additional fee(s) or any underpayment of fee(s)☐ Charge fee(s) indicated below, except for the filing fee to the above-identified deposit account.**FEE CALCULATION****1. BASIC FILING FEE**

Large Entity		Small Entity		Fee Description	Fee Paid
Fee Code	Fee (\$)	Fee Code	Fee (\$)		
1001	770	2001	385	Utility filing fee	770
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	
SUBTOTAL (1)					(\$ 770)

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

Total Claims		-20** =		X		=	
Independent Claims		-3** =		X		=	
Multiple Dependent						=	

Large Entity		Small Entity		Fee Description	Fee Paid
Fee Code	Fee (\$)	Fee Code	Fee (\$)		
1202	18	2202	9	Claims in excess of 20	
1201	86	2201	43	Independent claims in excess of 3	
1203	290	2203	145	Multiple dependent claim, if not paid	
1204	86	2204	43	** Reissue independent claims over original patent	
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent	
SUBTOTAL (2)					(\$)

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)**3. ADDITIONAL FEES**

Large Entity Small Entity

Fee Code	Fee (\$)	Fee Code	Fee (\$)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for ex parte reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	40
1809	770	2809	385	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify)

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) (\$ 40)**SUBMITTED BY**

Name (Print/Type) ROBERT J. SACCO

Registration No. 35,667

(Complete if applicable)

Telephone 562-626-2222

Signature

Date

3/11/04

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Express Mail Label:
EV 417207036 US

Express Mail Label: EV417207036US

**ENFORCING COMPUTER SECURITY
UTILIZING AN ADAPTIVE LATTICE MECHANISM**

BACKGROUND OF THE INVENTION

Statement of the Technical Field

[0001] The inventive arrangements relate generally to computer and information security and more particularly to security measures that enforce security based on logical implementation methods.

Description of the Related Art

[0002] Control of access to information and computer system resources is a continuing problem for system, database, and network administrators across the government, military, and private industry. Providing system security in such multi-user environments requires a balance between permitting access to resources necessary to perform the business functions for the enterprise and limiting access. Current security methods fall within two basic categories. These include physical and logical implementation methods.

[0003] Methods for implementing logical security safeguards typically provide access based on a user/group/role identifier and an access control list for the file, database, or system function to be accessed. However, there are a number of serious limitations to such an approach, primarily because control over information access is limited to a simple relational comparison. Significantly, such systems do not enforce security based on patterns of behavior, aggregation of data, or information clustering. Further, conventional systems make use of simple point tests which do not support the ability to look at temporal patterns of access.

[0004] For example, U.S. Patent No. 6,453,418 to Ooki et al. concerns a method for accessing information. The invention addresses some aspects of accessing portions of

{00000949;}

information based on user access authority. However, the invention makes no use of access patterns or temporal activities to control access.

[0005] U.S. Patent No. 6,446,077 to Straube et al. concerns an inherited information propagator for objects. The invention utilizes an inheritance graph to propagate changes in security descriptors to affected objects. The invention focuses on the propagation of security tagging but does not address the process of enforcing the security policy and does not mention aggregation or temporal patterns.

[0006] U.S. Patent No. 6,334,121 to Primeaux et al. concerns a usage pattern based user authenticator. The system utilizes a neural network and a set of rules to track usage patterns and flag suspicious activities. This patent focuses on flagging suspicious activity but does not address enforcement of a security policy based on such flagging.

SUMMARY OF THE INVENTION

[0007] The invention concerns a method for ensuring secure access to a computer system. The method can involve several steps. The method can begin with the step of receiving in the computer system a request from an entity. The entity can be a user or a process and can have a predetermined access authorization level for access to a first base node representing an information type or a computer system function. The computer system determine if the access request completes a prohibited temporal access pattern for the entity. If so, the request is rejected. Otherwise, the system can compare a minimum access level established for the first base node to the predetermined access authorization level assigned to the entity. Thereafter, the system can grant the access request only if the minimum access level for the first base node does not exceed to the predetermined access authorization level. The method can also include the step of denying the request if the minimum access level for the first base node exceeds the predetermined access authorization level assigned to the entity.

[0008] The method can also include logically organizing the computer system in the form of a tree hierarchy having a plurality of leaf nodes and higher-level nodes. A plurality of the base nodes can be defined as comprising respectively a plurality of leaf nodes of the tree hierarchy. Higher-level nodes can be defined as aggregations of the base nodes. Further, the method can include the step of identifying within the hierarchy any higher-level nodes that are aggregations comprising the first base node.

[0009] The method can also include identifying within the hierarchy any nodes that directly or indirectly comprise children of any of the higher-level nodes that are aggregations comprising the first base node. The minimum required entity access level can thereafter be updated for any base nodes that directly or indirectly comprise children of any of the higher-level nodes that are aggregations comprising the first base node.

[0010] For example the updating step can include comparing the entity's predetermined access authorization level against the minimum required access level of the higher-level nodes that are aggregations comprising the first base node. Thereafter,

{00000949;}

a minimum required access level of any the base node that is also a member of any aggregation comprising the first base node can be updated if a minimum required access level for the higher-level node comprising the aggregation has a required access level that is higher than the entity's predetermined access level.

{00000949;}

BRIEF DESCRIPTION OF THE DRAWINGS

- [0011]** Fig. 1 is a representation of data primitives and hierarchical graph that is useful for understanding the invention.
- [0012]** Fig. 2A is an example of a partially ordered set with transitive closure table.
- [0013]** Fig. 3 is an example of a temporal order table.
- [0014]** Fig. 4A is an example of a process/user access table.
- [0015]** Fig. 5 is an example of a combinatorial classification table.
- [0016]** Fig. 6 is a flowchart that is useful for understanding the invention.
- [0017]** Fig. 7 is a flowchart that is useful for understanding the invention.
- [0018]** Figs. 8A-8E show a series of tables that are useful for understanding how the inventive process can operate in one example.
- [0019]** Figs. 9A-9J show a series of tables that are useful for understanding how the inventive process can operate in a second example.
- [0020]** Fig. 10 is a drawing of a computer system that is useful for understanding the implementation of the inventive arrangements.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0021] The invention concerns a method and system for using an adaptive lattice mechanism to enforce computer security. Data and function access security levels form an initial basis for controlling access. These security access primitives can be organized within a partially ordered set (POSET) so as to define a hierarchical, directed graph. The security access primitives can form base nodes in the hierarchical, directed graph. Higher level nodes within the graph represent information aggregation sets and/or temporal patterns of access. Each of the nodes within the graph can have an associated security level representing the mandatory security level for the particular aggregation or pattern. Access authorities are maintained dynamically for each user/process, thereby allowing system objects to have multiple levels of access classification based on historical access by each user.

[0022] Referring now to Fig. 1, a secure computer system can comprise a plurality of object types 102₁-102₄ and system functions 104₁-104₃. The object types can include one or more information types A, B, C, D. Instantiations 106 of object types can include multiple type instances 108 as illustrated. Further, each object type can have a minimum required security access level associated therewith. In Fig. 1, the minimum required security access level for each object type 102₁-102₄ is represented in parenthesis along with the letter identifying the information type. For example, object 102₄ in Fig. 1 is labeled as "D(2)". The number 2 in parenthesis indicates that information type D has a minimum required security access level of two. Any process or user requesting to access any instantiation of object type D must have a security access level greater than or equal to two. Similarly, access to object 102₂, which is shown as B(1), requires a security access level of one or higher.

[0023] The system functions 104₁-104₃ represent functions which can be accessed by a process or user. In Fig. 1, the functions are shown as including directory (dir), execute (exec), and delete (del). However, it should be understood that these are merely intended as some examples of computer system functions, and the invention is not limited to any particular type of computer system function. Similar to the notation

{00000949;}

described above with respect to object types 102₁-102₄, each system function 104₁-104₃ in Fig. 1 is followed by a number in parenthesis. The number represents a minimum security access level required for any process or user to access that particular function. Thus, for example, the "exec" system function labeled exec(2) requires that a process or user possess a security level of at least two in order to access that function.

[0024] The various object types 102₁-102₄ and system functions 104₁-104₃ can be represented in a hierarchical tree graph as shown in Fig. 1. According to one aspect of the invention, the various object types and system functions can be defined as a plurality of leaf or base nodes 110 in the hierarchical tree 100. Further, higher-level nodes 112 can be constructed to represent aggregations of base nodes 110. As illustrated in Fig. 1, higher-level nodes 112 can include aggregations of base nodes 110, as well as higher order aggregations, i.e. aggregations of previously constructed aggregations.

[0025] According to one embodiment of the invention, the hierarchical directed graph of Fig. 1 can be implemented by organizing the object types 102₁-102₄ and system functions 104₁-104₃ within a partially ordered set (POSET). A POSET defines relationships that exist between pairs of elements, e.g. $x \rightarrow R \rightarrow y$ within a set of elements. Within the set of elements, there exists pairs of elements, e.g. m and n, for which no relation R exists. Thus, the set is partially ordered. Consequently, POSETs may have multiple root and leaf nodes in contrast to a tree structure which has a single root node and multiple leaf nodes. Because of the multiplicity of root nodes representing information access and operational functions for which the security operations are to be enforced, the POSET is used to represent the multiplicity of security relationships. Fig. 2A is an example of such a POSET 200 with a transitive closure table 202 that can be produced for the hierarchical tree 100 in Fig. 1.

[0026] Referring again to Fig. 1, it can be seen that relationships can be asserted for temporal access patterns. In this figure the curved arrows labeled T1 denote a temporal ordering between the accesses defined by items 114₁ and 114₂. Thus, for item 114₂, a temporal order is asserted between items 104₁ and 104₂, e.g. $104_1 \rightarrow 104_2$. Thus, node

{00000949;}

d(3) not only identifies an aggregation of the primitive functions denoted by 104_1 and 104_2 but also specifies that an explicit temporal ordering exists in that 104_1 is accessed before 104_2 . So, for the security policy associated with item 114_2 to be activated, not only must both 104_1 and 104_2 be accessed but they must be accessed in the order indicated by the temporal relationship. In addition to specifying a temporal order of access activities for a single node, temporal relations may be subsumed within other nodes through aggregation. This is illustrated by item 114_1 in Figure 1. Item 114_1 has three access items associated with the node, item 102_4 , 114_2 , and 104_3 . As shown on the diagram, a temporal ordering has been identified that specifies $102_4 \rightarrow 114_2 \rightarrow 104_3$. However, item 114_2 is an aggregation of access operations. Thus the operations identified by item 114_2 become subsumed into the overall temporal ordering of item 114_1 and the full temporal order is $102_4 \rightarrow 104_1 \rightarrow 104_2 \rightarrow 104_3$, where item 114_2 in the original temporal order has been replaced by its constituent parts, $104_1 \rightarrow 104_2$.

[0027] Fig. 3 is the Temporal Order Table (TOT) that captures the above relationships. The TOT is useful for capturing the relative temporal order of actions and allows relative or approximate temporal pattern matching to identify hostile actions. So, for access to node d, item 114_2 , the table shows that first the dir operation, item 104_1 , is performed, followed by the exec operation, item 104_2 . This ordering is shown in the row labeled "d" with a numerical ordering of the accesses listed in the columns. Figure 3 further shows that for node e, item 114_1 , the initial access is a data class D, item 102_4 , followed by the constituent elements of node d, item 114_2 , which is the dir, item 104_1 , and exec, item 104_2 , operations. In this case the row labeled "e" stores the order of the accesses using numerical values. In the case of row "e", the inclusion of the access ordering associated with node d, item 114_2 is shown as 2.1 and 2.2 representing the fact that both accesses are grouped as the second item in the temporal ordering for node e, item 114_1 , and that the order for these grouped items is denoted by the second number after the 2.

[0028] Referring now to Fig. 4A, there is shown an example of a Process/User Access Table (PUAT) that can be used in the present invention. The PUAT is a table of access authority that shows the minimum security level that each particular process or

{00000949;}

user is required to have in order to access the object type 102 or system function 104 in Fig. 1. For example, Fig. 3 shows that users 1-5 can be required (at least initially) to possess a security access level of at least one (1) to access information type B. Since users 1-5 in Fig. 4A all have a security access level of at least one (1), this means that all users can, at least initially, access information type B.

[0029] Significantly, however, the PUAT is a dynamic table in which the minimum security level required for a particular process or user to access a particular object type 102 or system function 104 can be changed depending on access history and/or identified temporal patterns. In this way, access authorities are maintained dynamically for each user allowing system objects to have multiple levels of access classification based on historical access by a particular process or user.

[0030] The transitive closure table of the complete set of access operations and aggregate nodes is illustrated in Figure 2A. The transitive closure table is obtained by adding a row and column for each of the aggregate nodes to the table of primitive actions. This yields an n-by-n table where the number of columns and rows are equal and the number of rows and columns is equal to the sum of the number primitive operations and number of aggregation nodes. A subset, item 202, of the transitive closure table of the POSET of Fig. 2A is then used to produce a combinatorial classification table (CCT) which is illustrated in Fig. 5. The CCT is obtained by taking the subset of the transitive closure table, item 202, corresponding to the set of aggregations shown in the columns and the primitive operations shown in the rows. This subset identifies the dependencies between the primitive access operations and the aggregations to which they are associated. This subset of the transitive closure, item 202, is then flipped about its diagonal axis yielding the aggregation items, a through e as the rows and the primitive access operations as the columns, as shown in Fig. 2B. Finally, each row is inspected and for each column containing a 1 entry, the number 1 is replaced with the security access level associated with the aggregation. This yields the final CCT as illustrated in Figure 5.

[0031] A flowchart that is useful for understanding the invention is shown in Figs. 6 and 7. As illustrated therein, the process can begin in step 602 of Fig. 6 by monitoring requests from computer system users and/or processes. Messages are tested in step 604 to determine if they comprise requests to access an information type or system function. If so, then the system continues on to step 606 to determine if the request completes a temporal access pattern for the particular user. If the request does complete a temporal access pattern, this means that the sequence of operations performed matches an identified pattern and is subject to the security access level specified for the that temporal order. If a temporal pattern is completed, the user's access level is compared to the access level required for the requested access action, illustrated in step 607. Note that the temporal ordering of primitive access operations mandates that the operations occur in the order specified for the security policy to be enforced. Thus, in Figure 1, if 104₂ is accessed first followed by item 104₁, the security policy associated with node d, item 114₂, will not be activated because the temporal order was not satisfied. If the access level of the user is not sufficient for the requested action, then the request is rejected in step 608.

[0032] If the request does not complete a temporal access pattern for the particular user or the user's access level is sufficient for the temporal pattern completed, then the system continues on to step 610 and logs the request in the Temporal Access Table (TAT). As shown in Fig. 4B, the Temporal Access Table maintains a history of the primitive operations performed by a user. As a user is granted authorization to perform a primitive access operation, the operation is time-stamped and stored within the TAT. The time stamps are compared against the temporal patterns identified in the Temporal Order Table, Figure 3, to check for matches. Thus, in Fig. 4B user 1 performed a dir operation at time 102 and then requested an exec operation at time 112. Since 112 is after 102, this request would trigger a match in the Temporal Order Table for node d, item 114₂ in Figure 1, and the request would be denied. However, in the case of user 3, the exec operation was performed at time 103 followed by the dir operation at time 111. This pair does not match the defined temporal order and the operations are permitted.

{00000949;}

[0033] In step 612, the computer system makes a determination as to whether the security access level of the user making the request is less than the current minimum required security access level for the specified information type. This determination can be completed by reference to the table in Fig. 4A. If the user does not have authorization for at least the current minimum required security access level, then the request is rejected. Alternatively, if the user does have a sufficiently high security access level then the request is granted in step 616.

[0034] Aggregation nodes 112 are comprised of two or more nodes which may be base nodes 110, other aggregation nodes 112, or a combination of both base and aggregation nodes. Accordingly, such aggregation nodes will often have a higher minimum required security level for permitting access as compared to security levels required for access to participant information types and/or system functions that comprise base nodes 110. This is true because aggregated data is often of a more sensitive nature since it provides greater context and can identify relationships between the various individual information types. Consequently aggregated information will inevitably be of greater interest to unauthorized users and system administrators will naturally wish to impose higher level restrictions on its access.

[0035] Still, it will be appreciated that access to all of the information types or system functions associated with base nodes 110 that are participants in a particular aggregation node is, in many instances, tantamount to directly accessing the aggregation node. Accordingly, it can be desirable to increase a security authorization level necessary for a particular user or process to access certain information types once the user or process has accessed certain other information types. For example, this may be true in those instances where both of the data types are participants in a common aggregation node. In such instances, it can be desirable to increase the required security authorization level for a particular user to access a base node to be at least equal to the security authorization level of an aggregation node to which the base node is a participant.

{00000949;}

[0036] Accordingly, the process can continue in step 702 of Fig. 7 by identifying all higher-level aggregation nodes 112 in which the base node containing the requested information type is a participant. In step 704 the computer system can determine if the minimum required security level for access to identified aggregation nodes is greater than the particular user's authorized security access level. If so, then in step 706 the computer system can identify all base nodes that are also participants in that particular aggregation node. This can be accomplished, for example, by following all paths from the identified aggregation nodes back to all of their corresponding base nodes.

[0037] Once so identified, the minimum required security level for accessing base nodes of the information type that has been already accessed remains the same. However, the minimum required security level for the user to access the other participant base nodes (i.e., other than the originally requested base node) can be updated in step 708. For example, the required minimum security level to access a participant base node can be increased for a particular user to match the minimum required security level for accessing an aggregation node in which the participant base node is a participant.

[0038] The invention can be better understood by considering the following examples which are illustrative of the process.

[0039] Example 1

[0040] Referring to Figs. 1 and 8, consider the case in which access authorization for users 1-5 is established in accordance with PUAT in Fig. 8A. User 2 with access level 1, U2(1) can request access to an object 102₁ of information type A as previously described in relation to step 604. In accordance with step 606, the system consults the TOT (Temporal Order Table) in Fig. 8B and determined that the access request time does not complete a temporal access pattern. Subsequently, the request is logged in the (Temporal Access Table) as provided in step 610. In accordance with step 612 the request is tested to determine if user 2 has a sufficiently high level of access authorization. In this case $U2(1) \geq A(0)$ and therefore access is granted to the requested information type A in accordance with step 616.

{00000949;}

[0041] Thereafter, in step 702 the computer system can identify aggregations with object A using the CCT (Combinatorial Classification Table) in Fig. 8C. In step 704, the system checks to determine if the minimum required security level for accessing the aggregation node 112₁ of type "a" is greater than the user's authorized security access level. In this case, the condition is satisfied since the user's authorized security access level is 1 and the minimum required level to access aggregation node 112₁ of type "a" is equal to 2. Accordingly, the system continues to step 706 and identifies any other base nodes 110 that are part of the aggregation node 112₁ of type "a". In this case, the system identifies information type B as being a participant in the aggregation of type "a".

[0042] Thereafter, in step 708 the PUAT in Fig. 8A is updated such that (1) the minimum security level required for accessing the originally requested base node 110 of information type "A" remains unchanged; and (2) the other participant of the aggregation node 112₁ are updated so that their minimum required security level is increased to equal to the minimum required security level established for the aggregation node "a". This can be expressed as follows: *If $PUAT(i) < CCT(i)$ then $CCT(i) \rightarrow PUAT(i)$* . The result is an updated PUAT table as shown in Fig. 8D.

[0043] The updated table in Fig. 8D shows that for the base node 110 of information type A the minimum security access level continues to be zero. The notation 0/1 for information type A in Fig. 8D indicates that the object has a zero security level and is the first one accessed by User 2. However, with regard to User 2, the minimum security level for accessing an object of information type B in the PUAT of Fig. 8D has been increased to level 2.

[0044] Subsequently, if User 2 with access level 1, U2(1) requests access to an object 102₂ of information type B the system will determine in step 606 that the access request time does not complete a temporal access pattern. This is accomplished by comparing the access time to the TOT in Fig. 8E. The TOT is unchanged from its earlier state in Fig. 8B and therefore the request does not get rejected in step 606. However, in step 612, a check of the updated PUAT of Fig. 8D reveals that the minimum security level required for user 2 to access information of type B is now set to

{00000949;}

level 2. Accordingly, the request is rejected in step 614. This can be expressed as $U2(1) \not\geq A(2)$ therefore deny access.

[0045] Example 2

[0046] Referring to Figs. 1 and 9, consider the case in which access authorization for users 1-5 is established in accordance with PUAT in Fig. 9A. User 3 with access level 2, $U3(2)$ can request access to an object 102_1 of information type A as previously described in relation to step 604. In accordance with step 606, the system consults the TOT (Temporal Order Table) in Fig. 9B and determined that the access request time does not complete a temporal access pattern. Subsequently, the request is logged as provided in step 610. In accordance with step 612 the request is tested to determine if User 3 has a sufficiently high level of access authorization. In this case $U3(2) \geq A(0)$ and therefore access is granted to the requested object 102_1 in accordance with step 616.

[0047] Thereafter, in step 702 the computer system can identify aggregations with object A using the CCT (Combinatorial Classification Table) in Fig. 9C. In step 704, the system checks to determine if the minimum required security level for accessing the aggregation node 112_1 of type "a" is greater than the authorized security access level of user 3. In this case, the condition is not satisfied since the user's authorized security access level is 2 and the minimum required level to access aggregation node 112_1 (i.e., type "a") is equal to 2. Accordingly, the system concludes that the user has an adequate security access level and continues to step 706 where it identifies any other base nodes 110 that are part of the aggregation node 112_1 . In this case, the system identifies 102_2 (information type B) as being a participant in the aggregation.

[0048] Thereafter, in step 708 the PUAT in Fig. 9A is updated such that (1) the minimum security level required for accessing the originally requested base node 110 (information type "A") remains unchanged; and (2) the other participant of the aggregation node 112_1 of type "a" are updated so that their minimum required security level is increased to equal to the minimum required security level established for the aggregation node 112_1 of type "a". This can be expressed as follows: *If* $PUAT(i) <$

{00000949;}

$CCT(i)$ then $CCT(i) \rightarrow PUAT(i)$. The result is an updated PUAT table as shown in Fig. 9D.

[0049] The updated table in Fig. 9D shows that for the base node 102_1 of information type A the minimum security access level continues to be zero for User 3. The notation 0/1 for information type A in Fig. 9D indicates that the object has a zero security level and was the first information type accessed by User 3. However, the minimum security level for accessing an object 102_2 of information type B in the PUAT of Fig. 9D has been increased to level 2.

[0050] Subsequently, if User 3 with access level 2, $U3(2)$ requests access to an object 102_4 of information type D, the computer system will determine in step 606 that the access request time does not complete a temporal access pattern. This is accomplished by comparing the access time to the TOT in Fig. 9E. The TOT is unchanged from its earlier state in Fig. 9B and therefore the request does not get rejected in step 606. In step 612, a check of the updated PUAT of Fig. 9D reveals that the minimum security level required for user 3 to access information of type D is set (as it was initially) at level 2. Accordingly, the request is granted in step 616. This can be expressed as $U3(2) \geq D(2)$ therefore grant access.

[0051] Thereafter, in step 702 the computer system can identify aggregations with the object of information type D using the CCT (Combinatorial Classification Table) in Fig. 9F. In this case node 102_4 (information type D) is a participant in aggregation node 112_2 of type "b". In step 704, the system checks to determine if the minimum required security level for accessing the aggregation node 112_2 is greater than the user's authorized security access level. In this case, the condition is satisfied since the user's authorized security access level is 2 and the minimum required level to access aggregation node 112_2 of type "b" is equal to 3. Accordingly, the system continues to step 706 and identifies any other base nodes 110 that are part of the aggregation node 112_2 of type "b". In this case, the system identifies information types A and B (nodes 102_1 and 102_2) as being a participant in the aggregation of node 112_2 of type "b".

{00000949;}

[0052] Thereafter, in step 708 the PUAT in Fig. 9D is updated such that (1) the minimum security level required for accessing the originally requested base node 102_4 of information type "D" remains unchanged; and (2) the other participant of the aggregation node 112_2 of type "b" are updated so that their minimum required security level is increased to be equal to the minimum required security level established for the aggregation node 112_2 of information type "b". This can be expressed as follows: *If $PUAT(i) < CCT(i)$ then $CCT(i) \rightarrow PUAT(i)$* . The result is an updated PUAT table as shown in Fig. 9G.

[0053] The updated table in Fig. 9G shows that for the base node 102_4 of information type D the minimum security access level continues to be two. The notation 2/2 for information type D in Fig. 9G indicates that the object 102_4 has a security level of 2 and is the second one accessed by User 3. However, with regard to User 3, the minimum security level for accessing an object of information type B in the PUAT of Fig. 9G has been increased to level 3.

[0054] Continuing with the foregoing example, User 3 with access level 2, $U3(2)$ can request access to an object 102_2 of information type B. As illustrated in Fig. 9H, the access request time does not complete a temporal access pattern (step 606). However, in step 612 a comparison is made of the security authorization level for User 3 to the minimum security level required for User 3 to access as specified by the PUAT in Fig. 9G. This test reveals that User 3 (security authorization level 2) does not have a sufficiently high security level to access information type B which now has a minimum required security of 3, at least with respect to requests by user 3. This can be expressed as $U3(2) \nrightarrow B(3)$. Accordingly, the request for access is rejected in step 614.

[0055] The inventive arrangements described herein can be used in conjunction with a wide variety of computer systems. These can include stand-alone computer systems, computer networks or client-server arrangements as shown in Fig. 10. The invention can be integrated within computer application software or implemented as an external component to existing software systems to provide modular accessibility. Further, the invention is not restricted to use with any particular type of software application or

access request from any particular type of entity. Accordingly, to the extent that the invention has been described herein in terms of requests from users or processes, it will be understood by those skilled in the art that the techniques described herein can have much broader application. For example, the invention can be used to provide security for database access, to operating system calls, and/or to identifying hostile patterns of remote access which may be initiated by computer viruses and worms.

[0056] Referring again to Fig. 10, it will be appreciated that the present invention can be realized in software in a centralized fashion in one computer system 1000, or in a distributed fashion where different elements are spread across several interconnected computer systems 1000, 1002. Any kind of computer system or other apparatus adapted for carrying out the methods described herein is suited. A typical implementation can include a general purpose computer system with a computer program that, when being loaded and executed, controls the computer system such that it carries out the methods described herein.

[0057] The present invention also can be embedded in a computer program product, which comprises all the features enabling the implementation of the methods described herein, and which when loaded in a computer system is able to carry out these methods. Computer program in the present context means any expression, in any language, code or notation, of a set of instructions intended to cause a system having an information processing capability to perform a particular function either directly or after either or both of the following: a) conversion to another language, code or notation; b) reproduction in a different material form.

[0058] This invention can be embodied in other forms without departing from the spirit or essential attributes thereof. Accordingly, reference should be made to the following claims, rather than to the foregoing specification, as indicating the scope of the invention.

CLAIMS

We claim:

1. A method for secure access to a computer system, comprising the steps of:

receiving in said computer system a request from an entity with a predetermined access level for access to a first base node representing at least one of an information type and a computer system function;

determining if said access request completes a prohibited temporal access pattern for said entity; and

comparing a minimum access level established for said first base node to said predetermined access level; and

granting said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level.
2. The method according to claim 1, further comprising the step of denying said request if said access request completes a prohibited temporal access pattern for said entity.
3. The method according to claim 1, further comprising the step of denying said request if said minimum access level for said first base node exceeds said predetermined access level for said entity.
4. The method according to claim 1, further comprising the steps of:

logically organizing said computer system in the form of a tree hierarchy having a plurality of leaf nodes and higher-level nodes;

defining a plurality of said base nodes as comprising respectively a plurality of leaf nodes of said tree hierarchy; and

defining said higher-level nodes as aggregations of said base nodes.

{00000949;}

5. The method according to claim 4 further comprising the step of identifying within said hierarchy any higher-level nodes that are aggregations comprising said first base node.

6. The method according to claim 5, further comprising the step of identifying within said hierarchy any nodes that comprise children of any generation of said higher-level nodes that are aggregations comprising said first base node.

7. The method according to claim 6, further comprising the step of updating a minimum required entity access level for any base nodes that comprise children of any generation of said higher-level nodes that are aggregations comprising said first base node.

8. The method according to claim 7, wherein said updating step further comprises the steps of:

comparing said entity's predetermined access level against the minimum required access level of said higher-level nodes that are aggregations comprising said first base node; and

updating a minimum required access level of any said base node that is also a member of any aggregation comprising said first base node if a minimum required access level for said higher-level node comprising said aggregation has a required access level that is higher than said entity's predetermined access level.

9. The method according to claim 1, further comprising the steps of:

comparing said entity's predetermined access level against the minimum required access level of at least one higher-level node that is an aggregation of base nodes including said first base node; and

updating a minimum required access level of any said base node that is also a member of any aggregation comprising said first base node if a minimum required access level for said higher-level node comprising said aggregation has a required access level that is higher than said entity's predetermined access level.

{00000949;}

10. A method for restricting access to a computer system having a plurality of logical base nodes representing at least one of an information type and a computer system function, and a plurality of higher-level nodes arranged together with said base nodes in the form of a tree hierarchy, comprising the steps of:

receiving in said computer system a request from an entity with a predetermined access level for access to a first base node;

determining if said access request completes a prohibited temporal access pattern for said entity; and

comparing a minimum access level established for said first base node to said predetermined access level; and

granting said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level.

11. A secure computer system comprising:

a plurality of logical base nodes representing at least one of an information type and a computer system function;

a plurality of higher-level nodes arranged together with said base nodes in the form of a tree hierarchy;

a computer system interface capable of receiving a request from an entity with a predetermined access level for access to a first base node;

a temporal access table;

processing means programmed for comparing said access request to said temporal access table to determine if said access request completes a prohibited temporal access pattern for said entity, and for comparing a minimum access level established for said first base node to said predetermined access level; and

{00000949;}

wherein said processing means grants said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level.

12. The secure computer system according to claim 11, wherein said processing means denies said request if said access request completes a prohibited temporal access pattern for said entity.

13. The secure computer system according to claim 11, wherein said processing means denies said request if said minimum access level for said first base node exceeds said predetermined access level for said entity.

14. The secure computer system according to claim 11 wherein said higher-level nodes are aggregations of said base nodes.

15. The secure computer system according to claim 14 wherein said processing means identifies within said hierarchy any higher-level nodes that are aggregations comprising said first base node.

16. The secure computer system according to claim 15 wherein said computer processing means identifies within said hierarchy any nodes that comprise children of any generation of said higher-level nodes that are aggregations comprising said first base node.

17. The secure computer system according to claim 16 wherein said processing means updates a minimum required entity access level for any base nodes that comprise children of any generation of said higher-level nodes that are aggregations comprising said first base node.

18. The secure computer system according to claim 17 wherein said processing means compares said entity's predetermined access level against the minimum required access level of said higher-level nodes that are aggregations comprising said first base node; and

{00000949;}

automatically updates a minimum required access level of any said base node that is also a member of any aggregation comprising said first base node if a minimum required access level for said higher-level node comprising said aggregation has a required access level that is higher than said entity's predetermined access level.

19. The secure computer system according to claim 11 wherein said processing means compares said entity's predetermined access level against the minimum required access level of at least one higher-level node that is an aggregation of base nodes including said first base node; and

updates a minimum required access level of any said base node that is also a member of any aggregation comprising said first base node if a minimum required access level for said higher-level node comprising said aggregation has a required access level that is higher than said entity's predetermined access level.

**ENFORCING COMPUTER SECURITY
UTILIZING AN ADAPTIVE LATTICE MECHANISM**

ABSTRACT

Method and apparatus for ensuring secure access to a computer system (1000). The method can begin with the step of receiving in the computer system a request from an entity (using 1002). The entity can have a predetermined access authorization level for access to a first base node (110) representing an information type (102) or a computer system function (104). The system determines if the access request completes a prohibited temporal access pattern for the entity. The system also compares a minimum access level established for the first base node to the predetermined access authorization level assigned to the entity. Thereafter, the system can grant the access request only if the minimum access level for the first base node does not exceed to the predetermined access authorization level.

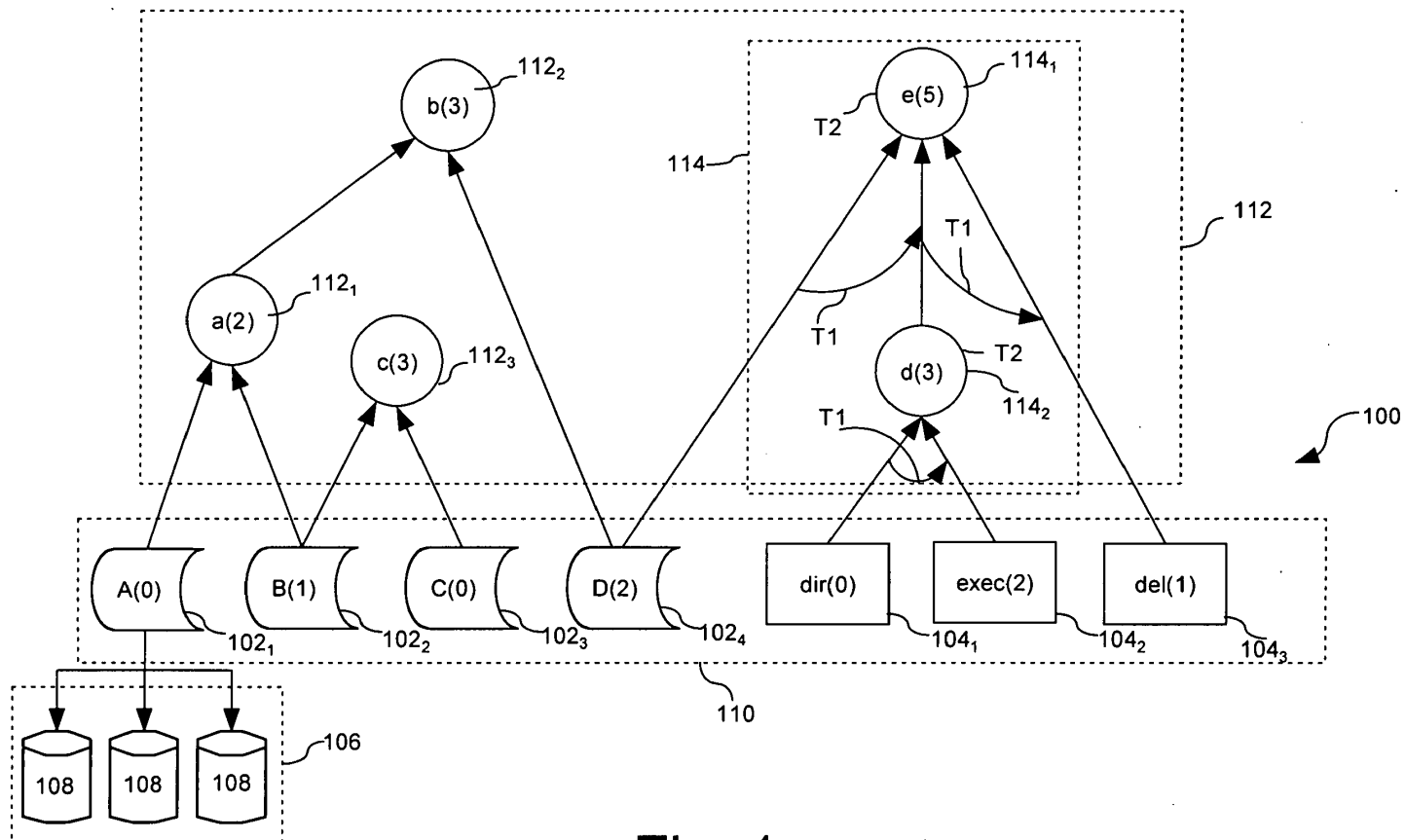


Fig. 1

Partially Ordered Set with Transitive Closure Table

POSET	A	B	C	D	dir	exec	del	a	b	c	d	e
A	1	0	0	0	0	0	0	1	1	0	0	0
B	0	1	0	0	0	0	0	1	1	1	0	0
C	0	0	1	0	0	0	0	0	0	1	0	0
D	0	0	0	1	0	0	0	0	1	0	0	1
dir	0	0	0	0	1	0	0	0	0	0	1	1
exec	0	0	0	0	0	1	0	0	0	0	1	1
del	0	0	0	0	0	0	1	0	0	0	0	1
a	0	0	0	0	0	0	0	1	1	0	0	0
b	0	0	0	0	0	0	0	0	1	0	0	0
c	0	0	0	0	0	0	0	0	0	1	0	0
d	0	0	0	0	0	0	0	0	0	0	1	1
e	0	0	0	0	0	0	0	0	0	0	0	1

Fig. 2A

	A	B	C	D	dir	exec	del
a	1	1	0	0	0	0	0
b	1	1	0	1	0	0	0
c	0	1	1	0	0	0	0
d	0	0	0	0	1	1	0
e	0	0	0	1	1	1	1

Fig. 2B

Temporal Order Table (TOT)

TOT	A	B	C	D	dir	exec	del
a							
b							
c							
d					1	2	
e				1	2.1	2.2	3

Fig. 3

Process/User Access Table (PUAT)

Usr	A	B	C	D	dir	exec	del
1(1)	0	1	0	2	0	2	1
2(1)	0	1	0	2	0	2	1
3(2)	0	1	0	2	0	2	1
4(1)	0	1	0	2	0	2	1
5(3)	0	1	0	2	0	2	1

Fig. 4A

Temporal Access Table (TAT)

Usr	A	B	C	D	dir	exec	del
1(1)					102	112	
2(1)							
3(2)					111	103	
4(1)							
5(3)							

Fig. 4B

Combinatorial Classification Table (CCT)

CCT	A	B	C	D	dir	exec	del
a	2	2	0	0	0	0	0
b	3	3	0	3	0	0	0
c	0	3	3	0	0	0	0
d	0	0	0	0	3	3	0
e	0	0	0	5	5	5	5

Fig. 5

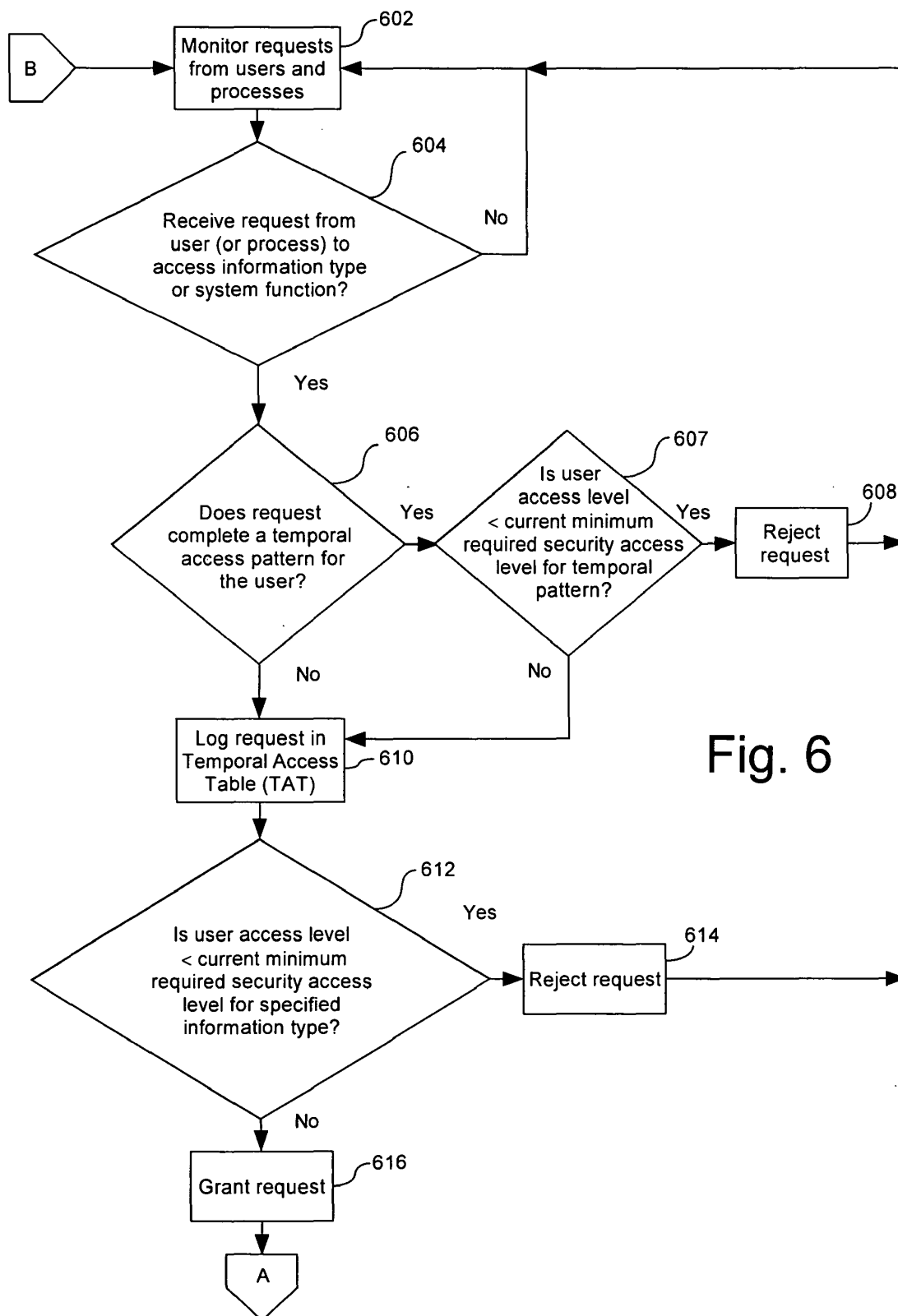


Fig. 6

Fig. 7

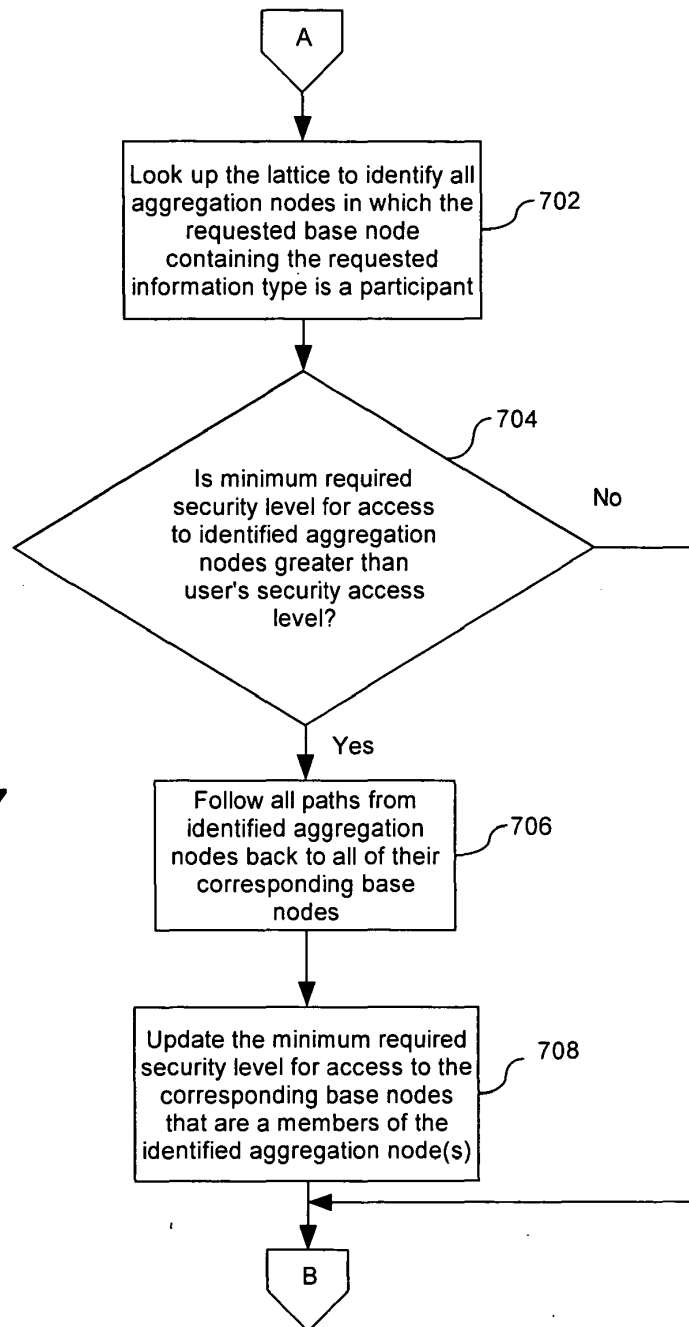


Fig. 8A

Usr	A	B	C	D	dir	exec	del
1(1)	0	1	0	2	0	2	1
2(1)	0	1	0	2	0	2	1
3(2)	0	1	0	2	0	2	1
4(1)	0	1	0	2	0	2	1
5(3)	0	1	0	2	0	2	1

Fig. 8B

TOT	A	B	C	D	dir	exec	del
a							
b							
c							
d					1	2	
e				1	2.1	2.2	3

Fig. 8C

CCT	A	B	C	D	dir	exec	del
a	2	2	0	0	0	0	0
b	3	3	0	3	0	0	0
c	0	3	3	0	0	0	0
d	0	0	0	0	3	3	0
e	0	0	0	5	5	5	5

Fig. 8D

Usr	A	B	C	D	dir	exec	del
1(1)	0	1	0	2	0	2	1
2(1)	0/1	2	0	2	0	2	1
3(2)	0	1	0	2	0	2	1
4(1)	0	1	0	2	0	2	1
5(3)	0	1	0	2	0	2	1

Fig. 8E

TOT	A	B	C	D	dir	exec	del
a							
b							
c							
d					1	2	
e				1	2.1	2.2	3

Fig. 9A

Usr	A	B	C	D	dir	exec	del
1(1)	0	1	0	2	0	2	1
2(1)	0	1	0	2	0	2	1
3(2)	0	1	0	2	0	2	1
4(1)	0	1	0	2	0	2	1
5(3)	0	1	0	2	0	2	1

Fig. 9B

TOT	A	B	C	D	dir	exec	del
a							
b							
c							
d					1	2	
e				1	2.1	2.2	3

Fig. 9C

CCT	A	B	C	D	dir	exec	del
a	2	2	0	0	0	0	0
b	3	3	0	3	0	0	0
c	0	3	3	0	0	0	0
d	0	0	0	0	3	3	0
e	0	0	0	5	5	5	5

Fig. 9D

Usr	A	B	C	D	dir	exec	del
1(1)	0	1	0	2	0	2	1
2(1)	0	1	0	2	0	2	1
3(2)	0/1	2	0	2	0	2	1
4(1)	0	1	0	2	0	2	1
5(3)	0	1	0	2	0	2	1

Fig. 9E

TOT	A	B	C	D	dir	exec	del
a							
b							
c							
d					1	2	
e				1	2.1	2.2	3

Fig. 9F

CCT	A	B	C	D	dir	exec	del
a	2	2	0	0	0	0	0
b	3	3	0	3	0	0	0
c	0	3	3	0	0	0	0
d	0	0	0	0	3	3	0
e	0	0	0	5	5	5	5

Fig. 9G

Usr	A	B	C	D	dir	exec	del
1(1)	0	1	0	2	0	2	1
2(1)	0	1	0	2	0	2	1
3(2)	0/1	3	0	2/2	0	2	1
4(1)	0	1	0	2	0	2	1
5(3)	0	1	0	2	0	2	1

Fig. 9H

TOT	A	B	C	D	dir	exec	del
a							
b							
c							
d					1	2	
e				1	2.1	2.2	3

Fig. 9J

Usr	A	B	C	D	dir	exec	del
1(1)	0	1	0	2	0	2	1
2(1)	0	1	0	2	0	2	1
3(2)	0/1	3	0	2/2	0	2	1
4(1)	0	1	0	2	0	2	1
5(3)	0	1	0	2	0	2	1

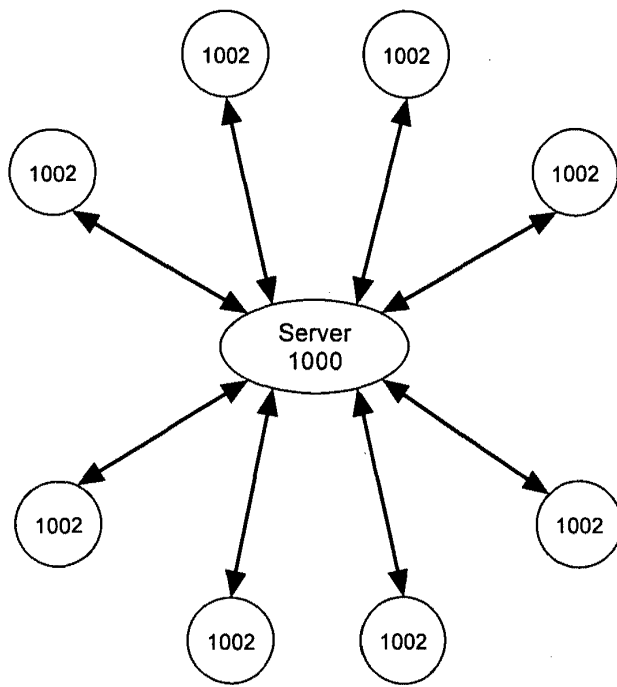


Fig. 10

US

Sacco & Associates, P.A.

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY
(Includes Reference to PCT International Applications)

ATTORNEY DOCKET NUMBER

7162-0110

As a below named inventor, I hereby declare that:

My residence, mailing address and citizenship are as stated below next to my name.

I believe that I am the original and first inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled:

ENFORCING COMPUTER SECURITY UTILIZING AN ADAPTIVE LATTICE MECHANISM

the specification of which (check only one item below):

☒ is attached hereto.

☐ was filed as U.S. Patent Application Serial Number _____
on _____, as amended on _ (if applicable).

☐ was filed as a PCT international application number _____ on
_____, as amended on __ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR §1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. §119(a)-(d) or (f), or §365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or §365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the applications on which priority is claimed:

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?
			☐	☐ YES ☐ NO
			☐	☐ YES ☐ NO
			☐	☐ YES ☐ NO
			☐	☐ YES ☐ NO

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto:

{00001064;}

**Express Mail Label:
EV 417207036 US**

US

Sacco & Associates, P.A.

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (Includes Reference to PCT International Applications)				ATTORNEY DOCKET NUMBER 7162-0110	
I hereby claim the benefit under 35 U.S.C. Sections 120 or 119(e) of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:					
PRIOR U.S. APPLICATIONS OR PCT INTERNATIONAL APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. §120:					
U.S. APPLICATIONS				STATUS (Check One)	
U.S. APPLICATION NUMBER	U.S. FILING DATE		PATENTED	ABANDONED	PENDING
PCT APPLICATIONS DESIGNATING THE U.S.					
PCT APPLICATION NUMBER	PCT FILING DATE	U.S. SERIAL NUMBERS			
POWER OF ATTORNEY: As a named inventor, I hereby appoint registered patent practitioners associated with Customer Number 39207 to prosecute this application and transact all business in the U.S. Patent and Trademark Office connected therewith.					
Send Correspondence to: "Customer Number 39207" Sacco & Associates, P.A. P. O. Box 30999 Palm Beach Gardens, FL 33420-0999			Direct Telephone Calls to: Robert J. Sacco 561-626-2222		
201	FULL NAME OF INVENTOR	FAMILY NAME KOVARIK, Jr.	FIRST GIVEN NAME Vincent	SECOND GIVEN NAME Joseph	
	RESIDENCE & CITIZENSHIP	CITY Melbourne	STATE OR COUNTRY FL	COUNTRY OF CITIZENSHIP US	
	MAILING ADDRESS	MAILING ADDRESS 4497 Pinewood Road	CITY Melbourne	STATE & ZIP CODE/COUNTRY FL 32934-9018	
202	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECOND GIVEN NAME	
	RESIDENCE & CITIZENSHIP	CITY	STATE OR COUNTRY	COUNTRY OF CITIZENSHIP	
	MAILING ADDRESS	MAILING ADDRESS	CITY	STATE & ZIP CODE/COUNTRY	
203	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECOND GIVEN NAME	
	RESIDENCE & CITIZENSHIP	CITY	STATE OR COUNTRY	COUNTRY OF CITIZENSHIP	
	MAILING ADDRESS	MAILING ADDRESS	CITY	STATE & ZIP CODE/COUNTRY	
I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.					
SIGNATURE OF INVENTOR 201		SIGNATURE OF INVENTOR 202		SIGNATURE OF INVENTOR 203	
DATE 3/8/04		DATE		DATE	

{00001064;}

APPLICATION DATA SHEET

(1) Inventor Information

Inventor One Given name: KOVARIK
Family name: Vincent Joseph
Name Suffix: Jr.
Residence: Grant, FL
Mailing Address: 4497 Pinewood Road, Melbourne, FL 32934-9018
Citizenship: US

(2) Correspondence Information

Correspondence Address *39207*

(3) Application Information

Title : ENFORCING COMPUTER SECURITY UTILIZING AN
ADAPTIVE LATTICE MECHANISM

Total No. of Drawing Sheets : 10
Suggested Figure for Publication : 1
Docket Number : 7162-0110
Type of Application : Utility

(4) Representative Information

Representative Information: *39207*
Robert J. Sacco
Registration No. 35,667
Sacco & Associates, P.A.
P.O. Box 30999
Palm Beach Gardens, FL 33420-0999
Telephone: (561) 626-2222
Facsimile: (561)626-2681

(5) Domestic Priority Information

(6) Foreign Application Information

(7) Assignee Information

Assignee name : Harris Corporation
Assignee address : 1025 West NASA Boulevard, Melbourne, FL 32919

{00001271;}

**Express Mail Label:
EV 417207036 US**

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.	:	Filed herewith	Confirmation No.
Applicant	:	KOVARIK, JR.	
Filed	:	Filed herewith	
TC/A.U.	:		
Examiner	:		
Docket No.	:	7162-0110	
Customer No.	:	39207	

**INFORMATION DISCLOSURE STATEMENT
PURSUANT TO 37 CFR 1.97**

Mail Stop: Patent Applications
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

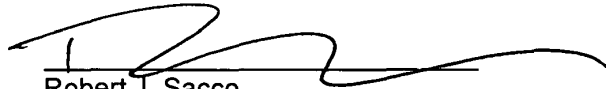
Sir:

This Information Disclosure Statement is being submitted in compliance with 37 CFR 1.97 and 1.98. A list of documents on form PTO 1449 together with a concise explanation or a translation of each non-English language document is enclosed herewith.

This paper is submitted in accordance with 37 CFR 1.97(b) and a fee is not required for consideration of these documents. Please charge any deficiencies to Deposit Acct. No. 50-2884.

Respectfully submitted,

Date: 3/11/04


Robert J. Sacco
Registration No. 35,667
SACCO & ASSOCIATES, P.A.
Post Office Box 30999
Palm Beach Gardens, FL 33420-0999
561/626-2222

{00001273;}

**Express Mail Label:
EV 417207036 US**

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known

Application Number	
Filing Date	
First Named Inventor	KOVARIK
Art Unit	
Examiner Name	
Attorney Docket Number	7162-0110

Sheet	1	of	1
-------	---	----	---

U. S. PATENT DOCUMENTS

[illegible]

FOREIGN PATENT DOCUMENTS

[illegible]

Examiner Signature		Date Considered	
-----------------------	--	--------------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶ Applicant is to place a check-mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, Washington, DC 20231.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Express Mail Label:
EV 417207036 US

PATENT APPLICATION SERIAL NO. _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

03/15/2004 EFLORES 00000030 10798074

01 FC:1001

770.00 OP

PTO-1556.
(5/87)

U.S. Government Printing Office: 2001 — 481-697/59173

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2003

Application or Docket Number

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS	14	
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	14 minus 20 = *	
INDEPENDENT CLAIMS	3 minus 3 = *	
MULTIPLE DEPENDENT CLAIM PRESENT ☐		

* If the difference in column 1 is less than zero, enter "0" in column 2

SMALL ENTITY
TYPE ☐ OR

OTHER THAN SMALL ENTITY

RATE	FEE
BASIC FEE	385.00
X\$ 9=	
X43=	
+145=	
TOTAL	

RATE	FEE
BASIC FEE	770.00
X\$18=	
X86=	
+290=	
TOTAL	770

CLAIMS AS AMENDED - PART II

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total *	Minus **	=
	Independent *	Minus ***	=
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM ☐		

1 - 10 - 11

SMALL ENTITY OR

OTHER THAN SMALL ENTITY

RATE	ADDITIONAL FEE
X\$ 9=	
X43=	
+145=	
TOTAL ADDIT. FEE	

RATE	ADDITIONAL FEE
X\$18=	
X86=	
+290=	
TOTAL ADDIT. FEE	

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total *	Minus **	=
	Independent *	Minus ***	=
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM ☐		

RATE	ADDITIONAL FEE
X\$ 9=	
X43=	
+145=	
TOTAL ADDIT. FEE	

RATE	ADDITIONAL FEE
X\$18=	
X86=	
+290=	
TOTAL ADDIT. FEE	

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT C	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total *	Minus **	=
	Independent *	Minus ***	=
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM ☐		

RATE	ADDITIONAL FEE
X\$ 9=	
X43=	
+145=	
TOTAL ADDIT. FEE	

RATE	ADDITIONAL FEE
X\$18=	
X86=	
+290=	
TOTAL ADDIT. FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL <i>(Only for new nonprovisional applications under 37 CFR 1.53(b))</i>	Attorney Docket No.	7162-0110
	First Inventor	KOVARIK, JR.
	Title	Enforcing Computer Security Utilizing an Adaptive Lattice Mechanism
	Express Mail Label No.	EV 417207036 US

APPLICATION ELEMENTS <i>See MPEP chapter 600 concerning utility patent application contents.</i>	ADDRESS TO: Mail Stop Patent Application Commissioner for Patents P.O. Box 1450 Alexandria VA 22313-1450
--	---

1. ☒ Fee Transmittal Form (e.g., PTO/SB/17)
(Submit an original and a duplicate for fee processing)
2. ☐ Applicant claims small entity status.
See 37 CFR 1.27.
3. ☒ Specification [Total Pages 23]
(preferred arrangement set forth below)
 - Descriptive title of the invention
 - Cross Reference to Related Applications
 - Statement Regarding Fed sponsored R & D
 - Reference to sequence listing, a table, or a computer program listing appendix
 - Background of the Invention
 - Brief Summary of the Invention
 - Brief Description of the Drawings (if filed)
 - Detailed Description
 - Claim(s)
 - Abstract of the Disclosure
4. ☒ Drawing(s) (35 U.S.C. 113) [Total Sheets 10]
5. Oath or Declaration [Total Sheets 2]
 - a. ☒ Newly executed (original or copy)
 - b. ☐ Copy from a prior application (37 CFR 1.63(d))
(for continuation/divisional with Box 18 completed)
 - i. ☐ **DELETION OF INVENTOR(S)**
Signed statement attached deleting inventor(s) name in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. ☒ Application Data Sheet. See 37 CFR 1.76

7. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program (Appendix)
8. Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary)
 - a. ☐ Computer Readable Form (CRF)
 - b. Specification Sequence Listing on:
 - i. ☐ CD-ROM or CD-R (2 copies); or
 - ii. ☐ Paper
 - c. ☐ Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. ☒ Assignment Papers (cover sheet & document(s))
10. ☐ 37 CFR 3.73(b) Statement of Attorney (when there is an assignee) ☐ Power of Attorney
11. ☐ English Translation Document (if applicable)
12. ☒ Information Disclosure Statement (IDS)/PTO-1449 ☐ Copies of IDS Citations
13. ☐ Preliminary Amendment
14. ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
15. ☐ Certified Copy of Priority Document(s)
(if foreign priority is claimed)
16. ☐ Nonpublication Request under 35 U.S.C. 122 (b)(2)(B)(i). Applicant must attach form PTO/SB/35 or its equivalent.
17. ☒ Other: Fee: \$810.....

18. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.:

Prior application information: Examiner _____ Art Unit: _____

For CONTINUATION OF DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

19. CORRESPONDENCE ADDRESS
☒ Customer Number: 39207 OR ☐ Correspondence address below

Name			
Address			
City	State	Zip Code	
Country	Telephone	Fax	

Name (Print/Type)	Robert J. Saee	Registration No. (Attorney/Agent)	35,667
Signature		Date	3/11/04

This collection of information is required by 37 CFR 1.53(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop Patent Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

18351 U.S. PTO
031104

18351 U.S. PTO

PTO/SB/17 (10-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL for FY 2004 Effective 10/01/2003. Patent fees are subject to annual revision.		Complete if Known	
☐ Applicant claims small entity status. See 37 CFR 1.27		Application Number	
		Filing Date	
		First Named Inventor KOVARIK, JR.	
		Examiner Name	
		Art Unit	
TOTAL AMOUNT OF PAYMENT		(\$) 810	
		Attorney Docket No. 7162-0110	

METHOD OF PAYMENT (check all that apply) ☒ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None ☒ Deposit Account: Deposit Account Number: 50-2884 Deposit Account Name: Sacco & Associates, P.A. The Director is authorized to: (check all that apply) ☐ Charge fee(s) indicated below ☒ Credit any overpayments ☒ Charge any additional fee(s) or any underpayment of fee(s) ☐ Charge fee(s) indicated below, except for the filing fee to the above-identified deposit account. FEE CALCULATION 1. BASIC FILING FEE <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Large Entity</th> <th style="text-align: left;">Small Entity</th> <th style="text-align: left;">Fee Description</th> <th style="text-align: right;">Fee Paid</th> </tr> <tr> <th>Fee Code (\$)</th> <th>Fee Code (\$)</th> <th></th> <th></th> </tr> </thead> <tbody> <tr> <td>1001 770</td> <td>2001 385</td> <td>Utility filing fee</td> <td style="text-align: right;">770</td> </tr> <tr> <td>1002 340</td> <td>2002 170</td> <td>Design filing fee</td> <td></td> </tr> <tr> <td>1003 530</td> <td>2003 265</td> <td>Plant filing fee</td> <td></td> </tr> <tr> <td>1004 770</td> <td>2004 385</td> <td>Reissue filing fee</td> <td></td> </tr> <tr> <td>1005 160</td> <td>2005 80</td> <td>Provisional filing fee</td> <td></td> </tr> <tr> <td colspan="3" style="text-align: right;">SUBTOTAL (1)</td> <td style="text-align: right;">(\$) 770</td> </tr> </tbody> </table> 2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Total Claims</th> <th style="text-align: left;">Extra Claims</th> <th style="text-align: left;">Fee from below</th> <th style="text-align: right;">Fee Paid</th> </tr> </thead> <tbody> <tr> <td>Independent Claims</td> <td>-20** =</td> <td>X</td> <td style="text-align: right;"></td> </tr> <tr> <td>Multiple Dependent</td> <td>-3** =</td> <td>X</td> <td style="text-align: right;"></td> </tr> </tbody> </table> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Large Entity</th> <th style="text-align: left;">Small Entity</th> <th style="text-align: left;">Fee Description</th> <th style="text-align: right;">Fee Paid</th> </tr> <tr> <th>Fee Code (\$)</th> <th>Fee Code (\$)</th> <th></th> <th></th> </tr> </thead> <tbody> <tr> <td>1202 18</td> <td>2202 9</td> <td>Claims in excess of 20</td> <td></td> </tr> <tr> <td>1201 86</td> <td>2201 43</td> <td>Independent claims in excess of 3</td> <td></td> </tr> <tr> <td>1203 290</td> <td>2203 145</td> <td>Multiple dependent claim, if not paid</td> <td></td> </tr> <tr> <td>1204 86</td> <td>2204 43</td> <td>** Reissue independent claims over original patent</td> <td></td> </tr> <tr> <td>1205 18</td> <td>2205 9</td> <td>** Reissue claims in excess of 20 and over original patent</td> <td></td> </tr> <tr> <td colspan="3" style="text-align: right;">SUBTOTAL (2)</td> <td style="text-align: right;">(\$)</td> </tr> </tbody> </table> **or number previously paid, if greater; For Reissues, see above	Large Entity	Small Entity	Fee Description	Fee Paid	Fee Code (\$)	Fee Code (\$)			1001 770	2001 385	Utility filing fee	770	1002 340	2002 170	Design filing fee		1003 530	2003 265	Plant filing fee		1004 770	2004 385	Reissue filing fee		1005 160	2005 80	Provisional filing fee		SUBTOTAL (1)			(\$) 770	Total Claims	Extra Claims	Fee from below	Fee Paid	Independent Claims	-20** =	X		Multiple Dependent	-3** =	X		Large Entity	Small Entity	Fee Description	Fee Paid	Fee Code (\$)	Fee Code (\$)			1202 18	2202 9	Claims in excess of 20		1201 86	2201 43	Independent claims in excess of 3		1203 290	2203 145	Multiple dependent claim, if not paid		1204 86	2204 43	** Reissue independent claims over original patent		1205 18	2205 9	** Reissue claims in excess of 20 and over original patent		SUBTOTAL (2)			(\$)	FEE CALCULATION (continued) 3. ADDITIONAL FEES <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Large Entity</th> <th style="text-align: left;">Small Entity</th> <th style="text-align: left;">Fee Description</th> <th style="text-align: right;">Fee Paid</th> </tr> <tr> <th>Fee Code (\$)</th> <th>Fee Code (\$)</th> <th></th> <th></th> </tr> </thead> <tbody> <tr> <td>1051 130</td> <td>2051 65</td> <td>Surcharge - late filing fee or oath</td> <td></td> </tr> <tr> <td>1052 50</td> <td>2052 25</td> <td>Surcharge - late provisional filing fee or cover sheet</td> <td></td> </tr> <tr> <td>1053 130</td> <td>1053 130</td> <td>Non-English specification</td> <td></td> </tr> <tr> <td>1812 2,520</td> <td>1812 2,520</td> <td>For filing a request for ex parte reexamination</td> <td></td> </tr> <tr> <td>1804 920*</td> <td>1804 920*</td> <td>Requesting publication of SIR prior to Examiner action</td> <td></td> </tr> <tr> <td>1805 1,840*</td> <td>1805 1,840*</td> <td>Requesting publication of SIR after Examiner action</td> <td></td> </tr> <tr> <td>1251 110</td> <td>2251 55</td> <td>Extension for reply within first month</td> <td></td> </tr> <tr> <td>1252 420</td> <td>2252 210</td> <td>Extension for reply within second month</td> <td></td> </tr> <tr> <td>1253 950</td> <td>2253 475</td> <td>Extension for reply within third month</td> <td></td> </tr> <tr> <td>1254 1,480</td> <td>2254 740</td> <td>Extension for reply within fourth month</td> <td></td> </tr> <tr> <td>1255 2,010</td> <td>2255 1,005</td> <td>Extension for reply within fifth month</td> <td></td> </tr> <tr> <td>1401 330</td> <td>2401 165</td> <td>Notice of Appeal</td> <td></td> </tr> <tr> <td>1402 330</td> <td>2402 165</td> <td>Filing a brief in support of an appeal</td> <td></td> </tr> <tr> <td>1403 290</td> <td>2403 145</td> <td>Request for oral hearing</td> <td></td> </tr> <tr> <td>1451 1,510</td> <td>1451 1,510</td> <td>Petition to institute a public use proceeding</td> <td></td> </tr> <tr> <td>1452 110</td> <td>2452 55</td> <td>Petition to revive - unavoidable</td> <td></td> </tr> <tr> <td>1453 1,330</td> <td>2453 665</td> <td>Petition to revive - unintentional</td> <td></td> </tr> <tr> <td>1501 1,330</td> <td>2501 665</td> <td>Utility issue fee (or reissue)</td> <td></td> </tr> <tr> <td>1502 480</td> <td>2502 240</td> <td>Design issue fee</td> <td></td> </tr> <tr> <td>1503 640</td> <td>2503 320</td> <td>Plant issue fee</td> <td></td> </tr> <tr> <td>1460 130</td> <td>1460 130</td> <td>Petitions to the Commissioner</td> <td></td> </tr> <tr> <td>1807 50</td> <td>1807 50</td> <td>Processing fee under 37 CFR 1.17(q)</td> <td></td> </tr> <tr> <td>1806 180</td> <td>1806 180</td> <td>Submission of Information Disclosure Stmt</td> <td></td> </tr> <tr> <td>8021 40</td> <td>8021 40</td> <td>Recording each patent assignment per property (times number of properties)</td> <td style="text-align: right;">40</td> </tr> <tr> <td>1809 770</td> <td>2809 385</td> <td>Filing a submission after final rejection (37 CFR 1.129(a))</td> <td></td> </tr> <tr> <td>1810 770</td> <td>2810 385</td> <td>For each additional invention to be examined (37 CFR 1.129(b))</td> <td></td> </tr> <tr> <td>1801 770</td> <td>2801 385</td> <td>Request for Continued Examination (RCE)</td> <td></td> </tr> <tr> <td>1802 900</td> <td>1802 900</td> <td>Request for expedited examination of a design application</td> <td></td> </tr> </tbody> </table> Other fee (specify) _____ *Reduced by Basic Filing Fee Paid SUBTOTAL (3) (\$) 40	Large Entity	Small Entity	Fee Description	Fee Paid	Fee Code (\$)	Fee Code (\$)			1051 130	2051 65	Surcharge - late filing fee or oath		1052 50	2052 25	Surcharge - late provisional filing fee or cover sheet		1053 130	1053 130	Non-English specification		1812 2,520	1812 2,520	For filing a request for ex parte reexamination		1804 920*	1804 920*	Requesting publication of SIR prior to Examiner action		1805 1,840*	1805 1,840*	Requesting publication of SIR after Examiner action		1251 110	2251 55	Extension for reply within first month		1252 420	2252 210	Extension for reply within second month		1253 950	2253 475	Extension for reply within third month		1254 1,480	2254 740	Extension for reply within fourth month		1255 2,010	2255 1,005	Extension for reply within fifth month		1401 330	2401 165	Notice of Appeal		1402 330	2402 165	Filing a brief in support of an appeal		1403 290	2403 145	Request for oral hearing		1451 1,510	1451 1,510	Petition to institute a public use proceeding		1452 110	2452 55	Petition to revive - unavoidable		1453 1,330	2453 665	Petition to revive - unintentional		1501 1,330	2501 665	Utility issue fee (or reissue)		1502 480	2502 240	Design issue fee		1503 640	2503 320	Plant issue fee		1460 130	1460 130	Petitions to the Commissioner		1807 50	1807 50	Processing fee under 37 CFR 1.17(q)		1806 180	1806 180	Submission of Information Disclosure Stmt		8021 40	8021 40	Recording each patent assignment per property (times number of properties)	40	1809 770	2809 385	Filing a submission after final rejection (37 CFR 1.129(a))		1810 770	2810 385	For each additional invention to be examined (37 CFR 1.129(b))		1801 770	2801 385	Request for Continued Examination (RCE)		1802 900	1802 900	Request for expedited examination of a design application	
Large Entity	Small Entity	Fee Description	Fee Paid																																																																																																																																																																																																		
Fee Code (\$)	Fee Code (\$)																																																																																																																																																																																																				
1001 770	2001 385	Utility filing fee	770																																																																																																																																																																																																		
1002 340	2002 170	Design filing fee																																																																																																																																																																																																			
1003 530	2003 265	Plant filing fee																																																																																																																																																																																																			
1004 770	2004 385	Reissue filing fee																																																																																																																																																																																																			
1005 160	2005 80	Provisional filing fee																																																																																																																																																																																																			
SUBTOTAL (1)			(\$) 770																																																																																																																																																																																																		
Total Claims	Extra Claims	Fee from below	Fee Paid																																																																																																																																																																																																		
Independent Claims	-20** =	X																																																																																																																																																																																																			
Multiple Dependent	-3** =	X																																																																																																																																																																																																			
Large Entity	Small Entity	Fee Description	Fee Paid																																																																																																																																																																																																		
Fee Code (\$)	Fee Code (\$)																																																																																																																																																																																																				
1202 18	2202 9	Claims in excess of 20																																																																																																																																																																																																			
1201 86	2201 43	Independent claims in excess of 3																																																																																																																																																																																																			
1203 290	2203 145	Multiple dependent claim, if not paid																																																																																																																																																																																																			
1204 86	2204 43	** Reissue independent claims over original patent																																																																																																																																																																																																			
1205 18	2205 9	** Reissue claims in excess of 20 and over original patent																																																																																																																																																																																																			
SUBTOTAL (2)			(\$)																																																																																																																																																																																																		
Large Entity	Small Entity	Fee Description	Fee Paid																																																																																																																																																																																																		
Fee Code (\$)	Fee Code (\$)																																																																																																																																																																																																				
1051 130	2051 65	Surcharge - late filing fee or oath																																																																																																																																																																																																			
1052 50	2052 25	Surcharge - late provisional filing fee or cover sheet																																																																																																																																																																																																			
1053 130	1053 130	Non-English specification																																																																																																																																																																																																			
1812 2,520	1812 2,520	For filing a request for ex parte reexamination																																																																																																																																																																																																			
1804 920*	1804 920*	Requesting publication of SIR prior to Examiner action																																																																																																																																																																																																			
1805 1,840*	1805 1,840*	Requesting publication of SIR after Examiner action																																																																																																																																																																																																			
1251 110	2251 55	Extension for reply within first month																																																																																																																																																																																																			
1252 420	2252 210	Extension for reply within second month																																																																																																																																																																																																			
1253 950	2253 475	Extension for reply within third month																																																																																																																																																																																																			
1254 1,480	2254 740	Extension for reply within fourth month																																																																																																																																																																																																			
1255 2,010	2255 1,005	Extension for reply within fifth month																																																																																																																																																																																																			
1401 330	2401 165	Notice of Appeal																																																																																																																																																																																																			
1402 330	2402 165	Filing a brief in support of an appeal																																																																																																																																																																																																			
1403 290	2403 145	Request for oral hearing																																																																																																																																																																																																			
1451 1,510	1451 1,510	Petition to institute a public use proceeding																																																																																																																																																																																																			
1452 110	2452 55	Petition to revive - unavoidable																																																																																																																																																																																																			
1453 1,330	2453 665	Petition to revive - unintentional																																																																																																																																																																																																			
1501 1,330	2501 665	Utility issue fee (or reissue)																																																																																																																																																																																																			
1502 480	2502 240	Design issue fee																																																																																																																																																																																																			
1503 640	2503 320	Plant issue fee																																																																																																																																																																																																			
1460 130	1460 130	Petitions to the Commissioner																																																																																																																																																																																																			
1807 50	1807 50	Processing fee under 37 CFR 1.17(q)																																																																																																																																																																																																			
1806 180	1806 180	Submission of Information Disclosure Stmt																																																																																																																																																																																																			
8021 40	8021 40	Recording each patent assignment per property (times number of properties)	40																																																																																																																																																																																																		
1809 770	2809 385	Filing a submission after final rejection (37 CFR 1.129(a))																																																																																																																																																																																																			
1810 770	2810 385	For each additional invention to be examined (37 CFR 1.129(b))																																																																																																																																																																																																			
1801 770	2801 385	Request for Continued Examination (RCE)																																																																																																																																																																																																			
1802 900	1802 900	Request for expedited examination of a design application																																																																																																																																																																																																			

SUBMITTED BY		(Complete if applicable)	
Name (Print/Type)	ROBERT J. SACCO	Registration No. (Attorney/Agent)	35,667
Signature		Telephone	562-626-2222
		Date	3/11/04

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

**Express Mail Label:
EV 417207036 US**