

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-00334	DATE FILED 8/29/2022	U.S. DISTRICT COURT Eastern District of Texas
PLAINTIFF LIONRA TECHNOLOGIES LIMITED		DEFENDANT PALO ALTO NETWORKS, INC.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 7,685,436	3/23/2010	Lionra Technologies Limited
2 8,566,612	10/22/2013	Lionra Technologies Limited
3 7,921,323	4/5/2011	Lionra Technologies Limited
4		
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

EX-1013

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

EX-1013

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

EX-1013



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	REQUEST ID
12/697,112	8566612	2436	16336

PAIR Correspondence Address/Fee Address Change

The following fields have been changed to Customer Number 140558 on 04/22/2016 via Private PAIR in view of the certification copied below that authorized the change.

- Correspondence Address

The address for Customer Number 140558 is:

140558

Davidson, Berquist, Jackson & Gowdey LLP

Harris Corporation

8300 Greensboro Drive

Suite 500

McLean, VA 22102

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

An attorney or Agent of Record registered to practice before the Patent and Trademark Office who has been given power of attorney in this application

Signature:	/Kimani Clark/
Name:	Kimani Clark
Registration Number:	45969



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	REQUEST ID
12/697,112	8566612	2436	16336

PAIR Correspondence Address/Fee Address Change

The following fields have been changed to Customer Number 140558 on 04/22/2016 via Private PAIR in view of the certification copied below that authorized the change.

- Maintenance Fee Address

The address for Customer Number 140558 is:

140558

Davidson, Berquist, Jackson & Gowdey LLP

Harris Corporation

8300 Greensboro Drive

Suite 500

McLean, VA 22102

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

An attorney or Agent of Record registered to practice before the Patent and Trademark Office who has been given power of attorney in this application

Signature:	/Kimani Clark/
Name:	Kimani Clark
Registration Number:	45969



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.
12/697,112	10/22/2013	8566612	2551-0109	1325

42624 7590 10/02/2013
DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

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 0 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 Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

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

John M. Davis, Brentwood, TN;
Richard Takahashi, Phoenix, AZ;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

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)

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.

42624 7590 06/21/2013
DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

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.
12/697,112	01/29/2010	John M. Davis	2551-0109	1325

TITLE OF INVENTION: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1780	\$300	\$0	\$2080	09/23/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
TRAORE, FATOUMATA	2436	713-189000

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 Davidson, Berquist,
2 Jackson & Gowdey
3 LLP

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)

Exelis, Inc.

McLean, VA

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 501860 (enclose an extra copy of this form).

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

- ☐ Applicant certifying micro entity status. See 37 CFR 1.29
- ☐ Applicant asserting small entity status. See 37 CFR 1.27
- ☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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 /Kimani Clark/

Typed or printed name Kimani Clark

Date September 20, 2013

Registration No. 45,969

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.

Electronic Patent Application Fee Transmittal

Application Number:	12697112			
Filing Date:	29-Jan-2010			
Title of Invention:	SYSTEM AND METHOD FOR A SECURE I/O INTERFACE			
First Named Inventor/Applicant Name:	John M. Davis			
Filer:	Kimani Clark			
Attorney Docket Number:	2551-0109			
Filed as Large Entity				
Utility under 35 USC 111(a) 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	1780	1780
Publ. Fee- Early, Voluntary, or Normal	1504	1	300	300
				EX-1013

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				2080

Electronic Acknowledgement Receipt

EFS ID:	16920051
Application Number:	12697112
International Application Number:	
Confirmation Number:	1325
Title of Invention:	SYSTEM AND METHOD FOR A SECURE I/O INTERFACE
First Named Inventor/Applicant Name:	John M. Davis
Customer Number:	42624
Filer:	Kimani Clark
Filer Authorized By:	
Attorney Docket Number:	2551-0109
Receipt Date:	20-SEP-2013
Filing Date:	29-JAN-2010
Time Stamp:	21:44:45
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$2080
RAM confirmation Number	9582
Deposit Account	501860
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part (if appl.)	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	--------------------------	---------------------

1	Issue Fee Payment (PTO-85B)	2551-0109_Issue_Fee_Transmit tal_9-20-13.pdf	130214 4e3017e21916c217b3c99c253616d572cd60f922	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	32007 16ea3313e9fb9177bbc54207b8707cf6ee58c40c	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			162221		
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.					

Notice of Allowability	Application No. 12/697,112	Applicant(s) DAVIS ET AL.	
	Examiner FATOUMATA TRAORE	Art Unit 2436	AIA (First Inventor to File) Status No

-- 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 03/07/2013.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are 30-32 and 34-56. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

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: _____.

Interim copies:

a) ☐ All b) ☐ Some c) ☐ None of the: Interim copies of the priority documents have been 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.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ 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)

1. ☐ Notice of References Cited (PTO-892)	5. ☒ Examiner's Amendment/Comment
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____	6. ☒ Examiner's Statement of Reasons for Allowance
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material	7. ☐ Other _____.
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date <u>05/16/2013</u> .	

/Fatoumata Traore/ Examiner, Art Unit 2436	/David García Cervetti/ Primary Examiner, Art Unit 2436
---	--



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

42624 7590 06/21/2013
DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

EXAMINER

TRAORE, FATOUMATA

ART UNIT

PAPER NUMBER

2436

DATE MAILED: 06/21/2013

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

12/697,112

01/29/2010

John M. Davis

2551-0109

1325

TITLE OF INVENTION: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1780	\$300	\$0	\$2080	09/23/2013

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 ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

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)

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.

42624 7590 06/21/2013
DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

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.
12/697,112	01/29/2010	John M. Davis	2551-0109	1325

TITLE OF INVENTION: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1780	\$300	\$0	\$2080	09/23/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
TRAORE, FATOUMATA	2436	713-189000

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, 1 _____ (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. 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)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

☐ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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.
12/697,112	01/29/2010	John M. Davis	2551-0109	1325

42624 7590 06/21/2013
DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

EXAMINER

TRAORE, FATOUMATA

ART UNIT PAPER NUMBER

2436

DATE MAILED: 06/21/2013

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 0 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 0 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.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

<i>Examiner-Initiated Interview Summary</i>	Application No. 12/697,112	Applicant(s) DAVIS ET AL.	
	Examiner FATOUMATA TRAORE	Art Unit 2436	

All participants (applicant, applicant's representative, PTO personnel):

(1) FATOUMATA TRAORE. (3) ____.

(2) KIMANI CLARK, Reg. No. 45,969. (4) ____.

Date of Interview: 16 May 2013.

Type: ☒ Telephonic ☐ Video Conference
 ☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☐ No.
 If Yes, brief description: ____.

Issues Discussed ☐ 101 ☐ 112 ☐ 102 ☐ 103 ☒ Others
 (For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: 30,33,34 and 40.

Identification of prior art discussed: N/A.

Substance of Interview
 (For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

To expedite prosecution the examiner contacted the applicant representative Kimani Clark Reg. NO. 45,969 to amended independent 30 and 40 such as to include limitations of claim 33 in order to put the application in condition of allowance.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/Fatoumata Traore/ Examiner, Art Unit 2436	
---	--

DETAILED ACTION

1. This is in response to the appeal brief filed 03/07/2013. Claims 1-29 have been cancelled. Claims 30-56 are pending and have been considered below.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Kimani Clark Reg. No. 45,969 on 05/16/2013.

The application has been amended as follows:

Amend Claims 30,33, 34 and 40:

30. (Currently Amended) A security processor to process incoming packets and outgoing packets, the security processor comprising:

a switching system to send the outgoing packets and receive the incoming packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing

packets to the security processor transit one of the plurality of packet engines;

a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;

a signature database; and

an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.

33. (Canceled).

34. (Currently Amended) The security processor of claim 30 ~~33~~ wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines.

40. (Currently Amended) A security processing system comprising:

(a) a security processor comprising:

a switching system to send outgoing packets and to receive incoming packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines;

a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;

a signature database; and

an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database; and a local data bus coupled to the switching system; and (b) a memory coupled to the local data bus.

Allowance

3. Claims 30-32 and 34-56 are allowed.

Examiner's Statement of Reason for allowance

4. The following is an examiner's statement of reasons for allowance:

Narad et al (US 6,157,955 A1) is relates to a general-purpose programmable packet-processing platform for accelerating network infrastructure applications which have been structured so as to separate the stages of classification and action. Network packet classification, execution of actions upon those packets, management of buffer flow, encryption services, and management of Network Interface Controllers are accelerated through the use of a multiplicity of specialized modules. A language interface is defined for specifying both stateless and stateful classification of packets and to associate actions with classification results in order to efficiently utilize these specialized modules.

Krishna et al (US 2003/0014627 A1) is directed toward providing an architecture for a cryptography accelerator chip that allows significant performance improvements over previous prior art designs, wherein the architecture enables

parallel processing of packets through a plurality of cryptography engines and includes a classification engine configured to efficiently process encryption/decryption of data packets.

Ramsey et al (US 7,331,061 B1) is directed to a computer security management system that integrates a firewall with an intrusion detection system (IDS), wherein the firewall and IDS of the present invention can be designed to communicate process or status information and packets with one another in order to facilitate centralized control of the firewall and the IDS and to increase the speed at which packets are passed between a secured computer network and an external network

The prior art of record taken alone or in combination do not teach or render obvious the limitations as recited in independent claims 30 and 40. The cited references, whether alone or in combination fail to disclose or suggest the following limitation : " a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines; a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent

Art Unit: 2436

to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;”

5. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to FATOUMATA TRAORE whose telephone number is (571)270-1685. The examiner can normally be reached on Monday- Friday (every other Friday off) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Philip Chea can be reached on 571 272 3951. 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.

Monday, June 10, 2013

/Fatoumata Traore/
Examiner, Art Unit 2436
/David Garcia Cervetti/
Primary Examiner, Art Unit 2436

Issue Classification 	Application/Control No. 12697112	Applicant(s)/Patent Under Reexamination DAVIS ET AL.
	Examiner FATOUMATA TRAORE	Art Unit 2436

☐ Claims renumbered in the same order as presented by applicant								☐ CPA		☒ T.D.		☐ R.1.47			
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		17		33	23	49								
	2		18	9	34	24	50								
	3		19	4	35	25	51								
	4		20	5	36	10	52								
	5		21	6	37	11	53								
	6		22	7	38	12	54								
	7		23	8	39	22	55								
	8		24	13	40	26	56								
	9		25	14	41										
	10		26	15	42										
	11		27	16	43										
	12		28	17	44										
	13		29	18	45										
	14	1	30	19	46										
	15	2	31	20	47										
	16	3	32	21	48										

/FATOUMATA TRAORE/ Examiner, Art Unit 2436 (Assistant Examiner)	5/17/2013 (Date)	Total Claims Allowed: 26	
/David García Cervetti/ Primary Examiner, Art Unit 2436 (Primary Examiner)	06/16/2013 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 2

Search Notes 	Application/Control No. 12697112	Applicant(s)/Patent Under Reexamination DAVIS ET AL.
	Examiner FATOUMATA TRAORE	Art Unit 2436

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
370	218, 386-389, 468, limited by text search	7/5/2011	FT
713	153-154, 168, 187-189, limited by text search	7/5/2011	FT
726	22-25, limited by text search	7/5/2011	FT

SEARCH NOTES		
Search Notes	Date	Examiner
EAT, google patent and inventors name search performed.	7/5/2011	FT
updated EAST and google search performed.	3/2/2012	FT
updated EAST and google search performed.	5/15/2013	FT

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
370	218, 386-389, 468, limited by text search	5/15/2013	FT
713	153-154, 168, 187-189, limited by text search	5/15/2013	FT
726	22-25, limited by text search	5/15/2013	FT

--	--

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	3	(switch\$3 router) with packet with (classificat\$3 classif\$4) same cryptograph\$3 with (encrypt\$3 decrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 10:35
S2	49	(switch\$3 router) with packet with (classificat\$3 classif\$4) same (cryptograph\$3 encrypt\$3 decrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 10:36
S3	8364	370/389.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 11:27
S4	208	(switch\$3) same (classificat\$3 classif\$4) same (cryptograph\$3 encrypt\$3 decrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 11:28
S5	304	(switch\$3) same (classificat\$3 classif\$4) same (hash\$3 cryptograph\$3 encrypt\$3 decrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 11:28
S6	26	S3 and S5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 11:28
S7	256	packet with (engine classificat\$3 classif\$4) same (secur\$3 cryptograph\$3 encrypt\$3) with (engine core) same (signature intrus\$3 virus wornpattern)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 15:19
S8	14000	370/468.ccls. 370/218.ccls. 370/386-	US-PGPUB;	OR	ON	2011/07/05

		388.ccls. 370/389.ccls.	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			15:21
S9	11	S7 and S8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 15:21
S10	14788	713/153-154.ccls. 713/168.ccls. 713/187-189.ccls. 726/22-25.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 16:11
S11	32	packet with engine same(classificat\$3 classif\$4) same (secur\$3 cryptograph\$3 encrypt\$3) with (engine core) same (signature intrus\$3 virus worn pattern)same detect\$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 16:13
S12	201	packet with engine same(classificat\$3 classif\$4) same (secur\$3 cryptograph\$3 encrypt\$3) with (engine core)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 16:19
S13	35	S12 and (S8 S10)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 16:19
S14	18	("20020066014" "20020108059" "20030014627" "20030196081" "20040010545" "5432950" "5737760" "5892899" "5940626" "6041122" "6049876" "6101255" "6157955" "6788800" "6983366" "7095716" "7493659").PN. OR ("7685436").URPN.	US-PGPUB; USPAT; USOCR	ADJ	ON	2011/07/05 16:25
S15	2	"7685436".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/06 10:59
S16	2	"20100169636".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2011/07/06 11:10

			DERWENT; IBM_TDB			
S17	0	packet with (engine classificat\$3 classif\$4) same pural\$3 same(secur\$3 cryptograph\$3 encrypt\$3) with (engine core)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/06 14:49
S18	0	packet with (engine classificat\$3 classif\$4) same pural\$3 same(secur\$3 cryptograph\$3 encrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/06 14:49
S19	275	packet with (engine classificat\$3 classif\$4) same plural\$3 same(secur\$3 cryptograph\$3 encrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/06 14:49
S20	141	packet with (engine classificat\$3 classif\$4) same plural\$3 same(secur\$3 cryptograph\$3 encrypt\$3) with (engine core)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/06 14:50
S21	2	"7493659".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/06 16:12
S22	2174823	execut\$3 with authenticat\$3 with (boot near2 code bot-code bootcode)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/07 09:40
S23	114	execut\$3 with authenticat\$3 with (boot near2 code bot-code bootcode)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/07 09:40
S24	8	execut\$3 with authenticat\$3 with (boot near2 code bot-code bootcode) same secur\$3 with processor	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/07 09:41
S25	4	"7321061".pn. "6157955".pn.	US-PGPUB; USPAT; USOCR;	OR	ON	2011/07/07 10:24

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S26	1	switching with packet adj (engine classificat\$3) with cryptographic adj (unit engine core)	USPAT	OR	OFF	2012/03/02 10:07
S27	2	"6157955".pn. "20030014627".pn. "7331061".pn.	USPAT	OR	OFF	2012/03/02 10:10
S28	6352	packet with classificat\$3with (rout\$3 switch\$3) with (encrypt\$3 cryptographic)	USPAT	OR	OFF	2012/03/02 12:21
S29	0	packet adj (unit engine device) with classificat\$3 adj (engine unit device)with (rout\$3 switch\$3) with (encrypt\$3 cryptographic)adj (engine device unit)	USPAT	OR	OFF	2012/03/02 12:22
S30	1	packet near7 (unit engine device) with classificat\$3 near7 (engine unit device) with (rout\$3 switch\$3) with (encrypt\$3 cryptographic) near7 (engine device unit)	USPAT	OR	OFF	2012/03/02 12:23
S31	2	packet with(unit engine device) with classificat\$3 with(engine unit device) with (rout\$3 switch\$3) with (encrypt\$3 cryptographic) with (engine device unit)	USPAT	OR	OFF	2012/03/02 12:24
S32	2	packet with classificat\$3 with(engine unit device) with (rout\$3 switch\$3) with (encrypt\$3 cryptographic) with (engine device unit)	USPAT	OR	OFF	2012/03/02 12:27
S33	2	packet with classificat\$3 with (rout\$3 switch\$3) with (encrypt\$3 cryptographic) with (engine device unit)	USPAT	OR	OFF	2012/03/02 12:28
S34	9	packet with classificat\$3 with (rout\$3 switch\$3) with (encrypt\$3 cryptographic)	USPAT	OR	OFF	2012/03/02 12:28
S35	0	packet with classificat\$3 with switch\$3 same cryptographic	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/15 14:34
S36	1362	packet with classificat\$3 with switch\$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/15 14:46
S37	4	packet with classificat\$3 with switch\$3 with (crypto cryptographic security) near3 (device engine core)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/15 14:48

S38	660621	packet sameclassificat\$3 same switch\$3 same (crypto cryptographic security) near3 (device engine core) not S37	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/15 14:57
S39	26	packet same classificat\$3 same switch\$3 same (crypto cryptographic security) near3 (device engine core) not S37	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/15 14:57
S40	0	switch\$3 same (interpos\$3 insert\$3) same classificat\$3 with (crypto cryptotofrahic secur\$3) near3 (device engine core)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/15 15:33
S41	1	switch\$3 same (interpos\$3 insert\$3) same classificat\$3 same(crypto cryptotograhic secur\$3) near3 (device engine core)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/15 15:34
S42	52	switch\$3 same classificat\$3 same(crypto cryptotograhic secur\$3) near3 (device engine core)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/15 15:35
S43	17	("20020083331" "20020144156" "20030088791" "20030145231" "20030177381" "20040083295" "20050193429" "20060253903" "5606668" "5991881" "6499107" "6519703" "6789116" "7007101" "7046680" "7331061" "7562389").PN. OR ("7937761").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2013/05/15 15:38
S44	4808	switch\$3 and classificat\$3 and (crypto cryptotograhic secur\$3) near3 (device engine core)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/15 16:20
S45	10	(switch\$3 and classificat\$3 and (crypto cryptotograhic secur\$3) near3 (device engine core)).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/15 16:20
S46	36981	713/153-154.ccls. 713/168.ccls. 713/187-189.ccls. 726/22-25.ccls. 370/468.ccls. 370/218.ccls. 370/386-	US-PGPUB; USPAT; USOCR;	OR	ON	2013/05/15 16:31

		388.ccls. 370/389.ccls.	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S47	451	S44 and S46	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/15 16:31
S48	0	S46 same packet with (rout\$3 flow\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/15 16:32
S49	11328	S46 and packet with (rout\$3 flow\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/15 16:32
S50	210	S47 and packet with (rout\$3 flow\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/15 16:33
S51	4	"20030014627".pn. "7331061".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/16 17:19

5/ 17/ 2013 8:18:28 AM
C:\ Users\ ftraore\ Documents\ EAST\ Workspaces\ 12697112securityProcessor\ OPacket.wsp

<i>Index of Claims</i> 	Application/Control No. 12697112	Applicant(s)/Patent Under Reexamination DAVIS ET AL.
	Examiner FATOUMATA TRAORE	Art Unit 2436

✓	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	07/05/2011	03/02/2012	05/16/2013					
	1	-	-	-					
	2	-	-	-					
	3	-	-	-					
	4	-	-	-					
	5	-	-	-					
	6	-	-	-					
	7	-	-	-					
	8	-	-	-					
	9	-	-	-					
	10	-	-	-					
	11	-	-	-					
	12	-	-	-					
	13	-	-	-					
	14	-	-	-					
	15	-	-	-					
	16	-	-	-					
	17	-	-	-					
	18	-	-	-					
	19	-	-	-					
	20	-	-	-					
	21	-	-	-					
	22	-	-	-					
	23	-	-	-					
	24	-	-	-					
	25	-	-	-					
	26	-	-	-					
	27	-	-	-					
	28	-	-	-					
	29	-	-	-					
1	30	✓	✓	=					
2	31	✓	✓	=					
3	32	✓	✓	=					
	33	✓	✓	-					
9	34	✓	✓	=					
4	35	✓	✓	=					
5	36	✓	✓	=					

<i>Index of Claims</i> 	Application/Control No. 12697112	Applicant(s)/Patent Under Reexamination DAVIS ET AL.
	Examiner FATOUMATA TRAORE	Art Unit 2436

✓	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	07/05/2011	03/02/2012	05/16/2013															
6	37	✓	✓	=															
7	38	✓	✓	=															
8	39	✓	✓	=															
13	40	✓	✓	=															
14	41	✓	✓	=															
15	42	✓	✓	=															
16	43	✓	✓	=															
17	44	✓	✓	=															
18	45	✓	✓	=															
19	46	✓	✓	=															
20	47	✓	✓	=															
21	48	✓	✓	=															
23	49	✓	✓	=															
24	50	✓	✓	=															
25	51	✓	✓	=															
10	52	✓	✓	=															
11	53	✓	✓	=															
12	54	✓	✓	=															
22	55	✓	✓	=															
26	56	✓	✓	=															

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT APPLICATION OF:

John M. Davis

Application Serial No.: 12/697,112

Application Filing Date: January 29, 2010

Title: **SYSTEM AND METHOD FOR A
SECURE I/O INTERFACE**

Attorney Docket: 2551-0109

Group Art Unit: 2436

Examiner: TRAORE, Fatoumata

Date: February 26, 2013

Confirmation No.: 1325

APPEAL BRIEF PURSUANT TO 37 CFR 41.37

In response to the Final Office action dated March 9, 2012 and Notification of Non-Compliant Appeal Brief dated February 28, 2013, and further to the Notice of Appeal filed September 7, 2012, Applicant hereby submits this brief in support of its appeal.

Real Party in Interest

The name of the real party in interest is Exelis, Inc (formerly ITT Manufacturing Enterprises, Inc.) of Wilmington, Delaware.

Related Appeals and Interferences

No other prior and pending appeals, interferences or judicial proceedings are known to appellant, the appellant's legal representative, or assignee which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status of Claims

Claims 30-56 are pending and rejected. Applicant is appealing the rejection of Claims 30-56.

Status of Amendments

There are no pending amendments filed subsequent to final rejection, thus all amendments have been entered for purposes of this appeal.

Summary of Claimed Subject Matter

The pending claims generally relate to a method and system for connecting a trusted piece of hardware, such as, for example, a personal computer, server, router, cellular phone, or other computing or communication device, to a network using an I/O interface or system that provides improved security for communications received and sent by the trusted hardware. The secure I/O system may perform all security and

network processing to maintain secure communications by the hardware with other devices on internal or external networks. It may also perform the network security processing to be segregated from other processing to ensure safe, protected and efficient system or device operation. The secure I/O system permits off-loading, onto a single system or card, all or substantially all security functions associated with network address translation (NAT), a firewall, intrusion detection/protection system functionality, traffic proxying and encryption from a host or network processor. It may improve the security of communications to and from trusted hardware, improve communication speed, reduce the number of different systems required for secure communications, and reduce the extent of a traffic bottleneck on a bus.

A security processor is provided to process incoming packets and outgoing packets comprising a switching system (208; p. 10, l. 25; Fig. 2) to send the outgoing packets and receive the incoming packets. It also comprises a packet engine (228; p. 11, l. 10; Fig 2.), coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system.

Furthermore, the security processor comprises a cryptographic core (232; p. 11, l. 18; Fig. 2), coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing

for packets received from and sent to the packet engine. The packet engine is interposed between the switching system and the cryptographic core.

The security processor also comprises a signature database (304; p. 30, l. 27; Fig 3.) and an intrusion detection system (302; p. 30, l. 25; Fig. 3) coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.

The independent claims are shown below with reference to the specification and figures.

30. A security processor (104) to process incoming packets and outgoing packets, the security processor comprising:

a switching system (208; p. 10, l. 25; Fig. 2) to send the outgoing packets and receive the incoming packets;

a packet engine (228; p. 11, l. 10; Fig 2.), coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system;

a cryptographic core (232; p. 11, l. 18; Fig. 2), coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;

a signature database (304; p. 30, l. 27; Fig 3.); and

an intrusion detection system (302; p. 30, l. 25; Fig. 3) coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.

40. A security processing system (102) comprising:

(a) a security processor (104) comprising:

a switching system (208; p. 10, l. 25; Fig. 2) to send outgoing packets and to receive incoming packets;

a packet engine (228; p. 11, l. 10; Fig. 2), coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system;

a cryptographic core (232; p. 11, l. 18; Fig. 2), coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;

a signature database (304; p. 30, l. 27; Fig. 3); and

an intrusion detection system (302; p. 30, l. 25; Fig. 3) coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database; and

a local data bus (210) coupled to the switching system; and

(b) a memory (106, 108, 110) coupled to the local data bus.

49. A security processor (104) to connect a trusted network to an un-trusted network for data packet communication, the security processor comprising:

a first interface (114, 118) to couple to the trusted network and to the un-trusted network;

a second interface (128) to couple to a host processor (130);

a switching system (208; p. 10, l. 25; Fig. 2) operable to selectively couple to the first interface or the second interface;

a local data bus (210), coupled to the switching system;

a plurality of packet engines (228; p. 11, l. 10; Fig 2.) coupled to the switching system to handle classification processing for incoming packets received by the plurality of packet engines from the switching system and outgoing packets sent by the plurality of packet engines to the switching system;

a plurality of cryptographic cores (232; p. 11, l. 18; Fig. 2) each coupled to one of the plurality of packet engines to communicate with the switching system via the plurality of packet engines and to provide encryption and decryption processing for packets received from and sent to the plurality of packet engines, wherein the plurality of packet engines are interposed between the switching system and the plurality of cryptographic cores;

a signature database (304; p. 30, l. 27; Fig 3.);

an intrusion detection system (302; p. 30, l. 25; Fig. 3) coupled between the plurality of cryptographic cores and the plurality of packets engine and responsive to at least one packet matching a signature stored in the signature database and

a control processor (212), coupled to the local data bus, to control data packet flow within the security processor.

37 CFR 41.37(c)(1)(vi) Grounds of Rejection to be Reviewed on Appeal.

1. Whether claims 30-56 are patentable in view of the grounds of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-22 of U.S. Patent No. 7,685,436.
2. Whether claims 30-35, 37-44, and 49-53 are patentable under 35 U.S.C. § 103(a) as being unpatentable over *Narad et al.* (U.S. Patent No. 6,157,955) in view of *Krishna et al* (U.S. Publication No. 2003/0014627) in further view of *Ramsey et al.* (U.S. Patent No. 7,331,061).
3. Whether claims 36, 45, and 47 are patentable under 35 U.S.C. § 103(a) as being unpatentable over *Narad* in view of *Krishna* in further view of *Ramsey* and *Savarda et al* (U.S. Publication No. 2003/0196081).
4. Whether claim 46 is patentable under 35 U.S.C. § 103(a) as being unpatentable over *Narad* in view of *Krishna* and *Ramsey*, and further in view of *Savarda* and *Carr et al.* (U.S. Patent No. 6,788,800).

5. Whether claim 48 is patentable under 35 U.S.C. §103(a) as being unpatentable over *Narad* in view of *Krishna* in further view of *Ramsey*, and *Girard* (U.S. Publication No. 2003/0084342).

6. Whether claims 54-56 are patentable under 35 U.S.C. §103(a) as being unpatentable over *Narad* in view of *Krishna* and *Ramsey*, and further in view of *Savarda* and *Wu et al.* (U.S. Patent No. 7,493,659).

Arguments

Fundamental differences between the cited references and the various pending claims include that the cited references do not teach or suggest “the cryptographic core ... receiving...packets from the switching system via the packet engine,” as recited in claim 30. Applicant discusses this limitation and claim 30 in particular, but the arguments apply to all pending claims, whereas similar limitations exist in all currently pending claims.

1. *Narad et al.* does not teach or suggest “a cryptographic core ... receiving...packets from the switching system via the packet engine”

Applicant respectfully traverses the rejections the claims at least because the cited references do not disclose “the cryptographic core ... receiving...packets from the switching system via the packet engine,” as recited, for example, in claim 30. The

Examiner has cited the “packet engine” as being Classification 106 on Figure 2 of *Narad*, the “switching system” as being the Action Code 108 on Figure 2, and the “cryptographic core” as being crypto 112 (Office Action dated March 9, 2012, p. 3). However, there is no specific disclosure of “the cryptographic core ... receiving...packets from the switching system via the packet engine.” That is, there is no transmission of packets from Action Code 108 (alleged switching system) through Classification 106 (alleged packet engine) to Crypto 112 (alleged cryptographic core) in *Narad*. (See Figure 2). Even further, there appears to be no transmission from Classification 106 (alleged packet engine) to Crypto 112 (alleged cryptographic core) in *Narad*. (See col. 8, l. 32 – col. 9, l. 43). As such, there is no disclosure of “the cryptographic core ... receiving...packets from the switching system via the packet engine.”

Narad et al. does not teach or suggest “communicating the outgoing packets to the switching system via the packet engine. . . wherein the packet engine is interposed between the switching system and the cryptographic core,” as recited, for example in claim 30. The Examiner’s Advisory Action rebuttal says that Classification 106 is interposed between Action Code 108 and Crypto 112, (“the packet engine (item 106) is interposed between the switching system (item 108) and the cryptographic core (112)”) but does not say the communication of packets goes from item 108 through 106 to 112, which would be required by the Examiner’s reading of the reference. The Examiner does not contend this because it is not so: as can be seen from Figure 2, there is no disclosure

of packets flowing from 108 to and through 106 to 112. (See also col. 8, l. 32 – col. 9, l. 43).

The Examiner cites that there are “paths the packets can take” (Advisory Action dated August 29, 2012, p. 2) but does not contend this specific required path to be disclosed, nor is it inherent at least because it is not required or necessary (see *Therasense, Inc. v. Becton, Dickinson & Co.*, 593 F.3d 1325 at 1332 (Fed. Cir. 2010)). The Examiner cites a column and a half of text (Advisory Action dated August 29, 2012, p. 2), however, none of that portion of the reference discloses communication of packets from 108 through 106 to 112, nor any transmission from 106 to 112, because it is not disclosed.

2. Narad et al. does not teach or suggest “packets from the switching system via the packet engine”

As mentioned previously, there appears to be no transmission from Classification 106 (alleged packet engine) to Crypto 112 (alleged cryptographic core) in *Narad*. See also col. 8, l. 32 – col. 9, l. 43). The portion cited by the Examiner does not show any transmission of packets from Classification 106 to Crypto 112. As such, there is no disclosure of “packets from the switching system via the packet engine,” as recited, for example, in claim 30.

At least for these reasons, Applicant submits that the pending claims are patentable. In view of the present remarks, the currently pending claims are believed to

be in condition for allowance, and an early and favorable action to that effect is respectfully requested.

CHARGE STATEMENT: Deposit Account No. 501860, order no. 2551-0109.

The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 (missing or insufficiencies only) now or hereafter relative to this application and the resulting Official Document under Rule 20, or credit any overpayment, to our Accounting/ Order Nos. shown above, for which purpose a duplicate copy of this sheet is attached.

This CHARGE STATEMENT does not authorize charge of the issue fee until/unless an issue fee transmittal sheet is filed.

CUSTOMER NUMBER

42624

Respectfully submitted,

By: 

Kimani Clark

Registration No.: 45,969

Davidson Berquist Jackson & Gowdey LLP
4300 Wilson Blvd., 7th Floor, Arlington, Virginia 22203
Main: (703) 894-6400 • FAX: (703) 894-6430

CLAIMS APPENDIX

CLAIMS

The claims are as follows:

1-29. (Canceled)

30. (Previously Presented) A security processor to process incoming packets and outgoing packets, the security processor comprising:

- a switching system to send the outgoing packets and receive the incoming packets;
- a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system;

- a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;

- a signature database; and

- an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.

31. (Previously Presented) The security processor of claim 30 wherein the packet engine is further operable to handle security context management processing for the incoming and outgoing packets.

32. (Previously Presented) The security processor of claim 30 further comprising:

a local data bus coupled to the switching system; and
a modulo engine coupled to the local data bus.

33. (Previously Presented) The security processor of claim 30 wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines.

34. (Previously Presented) The security processor of claim 33 wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines.

35. (Previously Presented) The security processor of claim 32 wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip.

36. (Previously Presented) The security processor of claim 35 further comprising a control processor, coupled to the local data bus, for exception handling of the incoming and outgoing packets.

37. (Previously Presented) The security processor of claim 35 further comprising a key management engine coupled to the local data bus.

38. (Previously Presented) The security processor of claim 35 wherein the security processor handles substantially all security processing for the incoming and outgoing packets.

39. (Previously Presented) The security processor of claim 38 wherein the security processor further handles substantially all network processing for the incoming and outgoing packets.

40. (Previously Presented) A security processing system comprising:

(a) a security processor comprising:

a switching system to send outgoing packets and to receive incoming packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system;

a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;

a signature database; and

an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database; and

a local data bus coupled to the switching system; and

(b) a memory coupled to the local data bus.

41. (Previously Presented) The security processing system of claim 40 further comprising a modulo engine coupled to the local data bus.

42. (Previously Presented) The security processing system of claim 41 further comprising a key management engine coupled to the local data bus.

43. (Previously Presented) The security processing system of claim 40 wherein the memory and the security processor are within the same cryptographic boundary.

44. (Previously Presented) The security processing system of claim 40 wherein the security processor is formed on a single chip.

45. (Previously Presented) The security processing system of claim 40 further comprising:

a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface; and

a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory.

46. (Previously Presented) The security processing system of claim 45 wherein the translator performs steganographic translation of the received data.

47. (Previously Presented) The security processing system of claim 45 wherein the translator performs encryption translation of the received data.

48. (Previously Presented) The security processing system of claim 40 wherein the security processor is operable to (i) execute boot code to load firmware for execution by the security processor and

(ii) authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor.

49. (Previously Presented) A security processor to connect a trusted network to an un-trusted network for data packet communication, the security processor comprising:

- a first interface to couple to the trusted network and to the un-trusted network;
- a second interface to couple to a host processor;
- a switching system operable to selectively couple to the first interface or the second interface;
- a local data bus, coupled to the switching system;
- a plurality of packet engines coupled to the switching system to handle classification processing for incoming packets received by the plurality of packet engines from the switching system and outgoing packets sent by the plurality of packet engines to the switching system;
- a plurality of cryptographic cores each coupled to one of the plurality of packet engines to communicate with the switching system via the plurality of packet engines and to provide encryption and decryption processing for packets received from and sent to the plurality of packet engines, wherein the plurality of packet engines are interposed between the switching system and the plurality of cryptographic cores;
- a signature database;
- an intrusion detection system coupled between the plurality of cryptographic cores and the plurality of packets engine and responsive to at least one packet matching a signature stored in the signature database and
- a control processor, coupled to the local data bus, to control data packet flow within the security processor.

50. (Previously Presented) The security processor of claim 49 wherein the security processor is operable to act as a firewall to deny or accept a data packet and to implement a secure communication channel with another computing device in the untrusted network.

51. (Previously Presented) The security processor of claim 50 wherein the security processor implements data packet security and authentication functions to support the secure communication channel.

52. (Previously Presented) The security processor of claim 30 wherein the packet engine is further operable to add at least one of an IP header or a MAC address to the outgoing packets.

53. (Previously Presented) The security processor of claim 30 wherein the packet engine is further operable to remove an IP header from the incoming packets.

54. (Previously Presented) The security processor of claim 30, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

55. (Previously Presented) The security processing system of claim 40, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

56. (Previously Presented) The security processor of claim 49, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.

Electronic Acknowledgement Receipt

EFS ID:	15139918
Application Number:	12697112
International Application Number:	
Confirmation Number:	1325
Title of Invention:	System and Method For a Secure I/O Interface
First Named Inventor/Applicant Name:	John M. Davis
Customer Number:	42624
Filer:	Kimani Clark
Filer Authorized By:	
Attorney Docket Number:	2551-0109
Receipt Date:	07-MAR-2013
Filing Date:	29-JAN-2010
Time Stamp:	10:37:42
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Appeal Brief Filed	Appeal_Brief_2551-0109_3-7-13.pdf	1459821 2a90a20e5817041327ab57057c3b761486720dccc	no	19

Warnings:

Information:

EX-1013

Palo Alto Networks, Inc. and Fortinet, Inc. v. Lionra Technologies Ltd.

057

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.

New Applications Under 35 U.S.C. 111

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.

National Stage of an International Application under 35 U.S.C. 371

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.

New International Application Filed with the USPTO as a Receiving Office

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.



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.
12/697,112	01/29/2010	John M. Davis	2551-0109	1325
42624	7590	02/28/2013	EXAMINER	
DAVIDSON BERQUIST JACKSON & GOWDEY LLP 4300 WILSON BLVD., 7TH FLOOR ARLINGTON, VA 22203			ART UNIT	PAPER NUMBER

DATE MAILED: 02/28/2013

Please find below and/or attached an Office communication concerning this application or proceeding.

Notification of Non-Compliant Appeal Brief (37 CFR 41.37)	Application No. 12/697,112	Applicant(s) Davis et al	
	Examiner Traore, Fatoumata	Art Unit 2436	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

The Appeal Brief filed on February 26, 2013 is defective for failure to comply with one or more provisions of 37 CFR 41.37(c).

To avoid dismissal of the appeal, applicant must file an amended brief or other appropriate correction (see MPEP 1205.03) within **ONE MONTH or THIRTY DAYS** from the mailing date of this Notification, whichever is longer.

EXTENSIONS OF THIS TIME PERIOD MAY BE GRANTED UNDER 37 CFR 1.136.

1. ☐ The brief does not contain the items required under 37 CFR 41.37(c), or the items are not under the proper heading or in the proper order.
2. ☒ (a) The brief does not contain a concise explanation of the subject matter defined in each of the rejected independent claims, referring to the specification in the Record by page and line number or by paragraph number and to the drawings, if any, by reference characters; and/or (b) the brief fails to identify, for each rejected independent claim and for each dependent claim argued separately that contains a means plus function or step plus function recitation under 35 U.S.C. 112, sixth paragraph, the structure, material, or acts described in the specification as corresponding to each claimed function with reference to the specification in the Record by page and line number or paragraph number, and to the drawings, if any, by reference characters (37 CFR 41.37(c)(1)(iii)).
3. ☐ The brief does not contain a correct copy of the appealed claims as an appendix thereto (37 CFR 41.37(c)(1)(v)).
4. ☒ Other (including any explanation in support of the above items):

Section V Summary of Claimed Subject Matter must identify and map all independent claims separately on appeal to the Specification by page and line number or paragraph(s) number if used in the original specification and/or drawings if any by reference characters. (Claims, 30, 40 and 49).

S. Saunders-Cobb, Paralegal
(571) 272-4665
Q. Gould, Supervisory Paralegal
(571) 272-9797

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT APPLICATION OF:

John M. Davis

Application Serial No.: 12/697,112

Application Filing Date: January 29, 2010

Title: **SYSTEM AND METHOD FOR A
SECURE I/O INTERFACE**

Attorney Docket: 2551-0109

Group Art Unit: 2436

Examiner: TRAORE, Fatoumata

Date: February 26, 2013

Confirmation No.: 1325

APPEAL BRIEF PURSUANT TO 37 CFR 41.37

In response to the Final Office action dated March 9, 2012, and further to the Notice of Appeal filed September 7, 2012, Applicant hereby submits this brief in support of its appeal. Applicant also hereby petitions for and requests a 4 month extension of time to be charged to the Deposit Account listed below.

Real Party in Interest

The name of the real party in interest is Exelis, Inc (formerly ITT Manufacturing Enterprises, Inc.) of Wilmington, Delaware.

Related Appeals and Interferences

No other prior and pending appeals, interferences or judicial proceedings are known to appellant, the appellant's legal representative, or assignee which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status of Claims

Claims 30-56 are pending and rejected. Applicant is appealing the rejection of Claims 30-56.

Status of Amendments

There are no pending amendments filed subsequent to final rejection, thus all amendments have been entered for purposes of this appeal.

Summary of Claimed Subject Matter

The pending claims generally relate to a method and system for connecting a trusted piece of hardware, such as, for example, a personal computer, server, router, cellular phone, or other computing or communication device, to a network using an I/O interface or system that provides improved security for communications received and sent by the trusted hardware. The secure I/O system may perform all security and

network processing to maintain secure communications by the hardware with other devices on internal or external networks. It may also perform the network security processing to be segregated from other processing to ensure safe, protected and efficient system or device operation. The secure I/O system permits off-loading, onto a single system or card, all or substantially all security functions associated with network address translation (NAT), a firewall, intrusion detection/protection system functionality, traffic proxying and encryption from a host or network processor. It may improve the security of communications to and from trusted hardware, improve communication speed, reduce the number of different systems required for secure communications, and reduce the extent of a traffic bottleneck on a bus.

A security processor is provided to process incoming packets and outgoing packets comprising a switching system (208; p. 10, l. 25; Fig. 2) to send the outgoing packets and receive the incoming packets. It also comprises a packet engine (228; p. 11, l. 10; Fig 2.), coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system.

Furthermore, the security processor comprises a cryptographic core (232; p. 11, l. 18; Fig. 2), coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing

for packets received from and sent to the packet engine. The packet engine is interposed between the switching system and the cryptographic core.

The security processor also comprises a signature database (304; p. 30, l. 27; Fig. 3.) and an intrusion detection system (302; p. 30, l. 25; Fig. 3) coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.

37 CFR 41.37(c)(1)(vi) Grounds of Rejection to be Reviewed on Appeal.

1. Whether claims 30-56 are patentable in view of the grounds of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-22 of U.S. Patent No. 7,685,436.
2. Whether claims 30-35, 37-44, and 49-53 are patentable under 35 U.S.C. § 103(a) as being unpatentable over *Narad et al.* (U.S. Patent No. 6,157,955) in view of *Krishna et al.* (U.S. Publication No. 2003/0014627) in further view of *Ramsey et al.* (U.S. Patent No. 7,331,061).
3. Whether claims 36, 45, and 47 are patentable under 35 U.S.C. § 103(a) as being unpatentable over *Narad* in view of *Krishna* in further view of *Ramsey* and *Savarda et al.* (U.S. Publication No. 2003/0196081).

4. Whether claim 46 is patentable under 35 U.S.C. §103(a) as being unpatentable over *Narad* in view of *Krishna* and *Ramsey*, and further in view of *Savarda* and *Carr et al.* (U.S. Patent No. 6,788,800).

5. Whether claim 48 is patentable under 35 U.S.C. §103(a) as being unpatentable over *Narad* in view of *Krishna* in further view of *Ramsey*, and *Girard* (U.S. Publication No. 2003/0084342).

6. Whether claims 54-56 are patentable under 35 U.S.C. §103(a) as being unpatentable over *Narad* in view of *Krishna* and *Ramsey*, and further in view of *Savarda* and *Wu et al.* (U.S. Patent No. 7,493,659).

Arguments

Fundamental differences between the cited references and the various pending claims include that the cited references do not teach or suggest “the cryptographic core ... receiving...packets from the switching system via the packet engine,” as recited in claim 30. Applicant discusses this limitation and claim 30 in particular, but the arguments apply to all pending claims, whereas similar limitations exist in all currently pending claims.

1. *Narad et al.* does not teach or suggest “a cryptographic core ... receiving...packets from the switching system via the packet engine”

Applicant respectfully traverses the rejections the claims at least because the cited references do not disclose “the cryptographic core ... receiving...packets from the switching system via the packet engine,” as recited, for example, in claim 30. The Examiner has cited the “packet engine” as being Classification 106 on Figure 2 of *Narad*, the “switching system” as being the Action Code 108 on Figure 2, and the “cryptographic core” as being crypto 112 (Office Action dated March 9, 2012, p. 3). However, there is no specific disclosure of “the cryptographic core ... receiving...packets from the switching system via the packet engine.” That is, there is no transmission of packets from Action Code 108 (alleged switching system) through Classification 106 (alleged packet engine) to Crypto 112 (alleged cryptographic core) in *Narad*. (See Figure 2). Even further, there appears to be no transmission from Classification 106 (alleged packet engine) to Crypto 112 (alleged cryptographic core) in *Narad*. (See col. 8, l. 32 – col. 9, l. 43). As such, there is no disclosure of “the cryptographic core ... receiving...packets from the switching system via the packet engine.”

Narad et al. does not teach or suggest “communicating the outgoing packets to the switching system via the packet engine. . . wherein the packet engine is interposed between the switching system and the cryptographic core,” as recited, for example in claim 30. The Examiner’s Advisory Action rebuttal says that Classification 106 is

interposed between Action Code 108 and Crypto 112, (“the packet engine (item 106) is interposed between the switching system (item 108) and the cryptographic core (112)”) but does not say the communication of packets goes from item 108 through 106 to 112, which would be required by the Examiner’s reading of the reference. The Examiner does not contend this because it is not so: as can be seen from Figure 2, there is no disclosure of packets flowing from 108 to and through 106 to 112. (See also col. 8, l. 32 – col. 9, l. 43).

The Examiner cites that there are “paths the packets can take” (Advisory Action dated August 29, 2012, p. 2) but does not contend this specific required path to be disclosed, nor is it inherent at least because it is not required or necessary (see *Therasense, Inc. v. Becton, Dickinson & Co.*, 593 F.3d 1325 at 1332 (Fed. Cir. 2010)). The Examiner cites a column and a half of text (Advisory Action dated August 29, 2012, p. 2), however, none of that portion of the reference discloses communication of packets from 108 through 106 to 112, nor any transmission from 106 to 112, because it is not disclosed.

2. *Narad et al.* does not teach or suggest “packets from the switching system via the packet engine”

As mentioned previously, there appears to be no transmission from Classification 106 (alleged packet engine) to Crypto 112 (alleged cryptographic core) in *Narad*. See also col. 8, l. 32 – col. 9, l. 43). The portion cited by the Examiner does not show any

transmission of packets from Classification 106 to Crypto 112. As such, there is no disclosure of “packets from the switching system via the packet engine,” as recited, for example, in claim 30.

At least for these reasons, Applicant submits that the pending claims are patentable. In view of the present remarks, the currently pending claims are believed to be in condition for allowance, and an early and favorable action to that effect is respectfully requested.

CHARGE STATEMENT: Deposit Account No. 501860, order no. **2551-0109**.

The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 (missing or insufficiencies only) now or hereafter relative to this application and the resulting Official Document under Rule 20, or credit any overpayment, to our Accounting/ Order Nos. shown above, for which purpose a duplicate copy of this sheet is attached.

This CHARGE STATEMENT does not authorize charge of the issue fee until/unless an issue fee transmittal sheet is filed.

CUSTOMER NUMBER

42624

Respectfully submitted,

By:



Kimani Clark

Registration No.: 45,969

Davidson Berquist Jackson & Gowdey LLP
4300 Wilson Blvd., 7th Floor, Arlington, Virginia 22203
Main: (703) 894-6400 • FAX: (703) 894-6430

CLAIMS APPENDIX

CLAIMS

The claims are as follows:

1-29. (Canceled)

30. (Previously Presented) A security processor to process incoming packets and outgoing packets, the security processor comprising:

a switching system to send the outgoing packets and receive the incoming packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system;

a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;

a signature database; and

an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.

31. (Previously Presented) The security processor of claim 30 wherein the packet engine is further operable to handle security context management processing for the incoming and outgoing packets.

32. (Previously Presented) The security processor of claim 30 further comprising:

a local data bus coupled to the switching system; and
a modulo engine coupled to the local data bus.

33. (Previously Presented) The security processor of claim 30 wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines.

34. (Previously Presented) The security processor of claim 33 wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines.

35. (Previously Presented) The security processor of claim 32 wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip.

36. (Previously Presented) The security processor of claim 35 further comprising a control processor, coupled to the local data bus, for exception handling of the incoming and outgoing packets.

37. (Previously Presented) The security processor of claim 35 further comprising a key management engine coupled to the local data bus.

38. (Previously Presented) The security processor of claim 35 wherein the security processor handles substantially all security processing for the incoming and outgoing packets.

39. (Previously Presented) The security processor of claim 38 wherein the security processor further handles substantially all network processing for the incoming and outgoing packets.

40. (Previously Presented) A security processing system comprising:

(a) a security processor comprising:

a switching system to send outgoing packets and to receive incoming packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system;

a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;

a signature database; and

an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database; and

a local data bus coupled to the switching system; and

(b) a memory coupled to the local data bus.

41. (Previously Presented) The security processing system of claim 40 further comprising a modulo engine coupled to the local data bus.

42. (Previously Presented) The security processing system of claim 41 further comprising a key management engine coupled to the local data bus.

43. (Previously Presented) The security processing system of claim 40 wherein the memory and the security processor are within the same cryptographic boundary.

44. (Previously Presented) The security processing system of claim 40 wherein the security processor is formed on a single chip.

45. (Previously Presented) The security processing system of claim 40 further comprising:

a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface; and

a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory.

46. (Previously Presented) The security processing system of claim 45 wherein the translator performs steganographic translation of the received data.

47. (Previously Presented) The security processing system of claim 45 wherein the translator performs encryption translation of the received data.

48. (Previously Presented) The security processing system of claim 40 wherein the security processor is operable to (i) execute boot code to load firmware for execution by the security processor and

(ii) authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor.

49. (Previously Presented) A security processor to connect a trusted network to an un-trusted network for data packet communication, the security processor comprising:

- a first interface to couple to the trusted network and to the un-trusted network;
- a second interface to couple to a host processor;
- a switching system operable to selectively couple to the first interface or the second interface;
- a local data bus, coupled to the switching system;
- a plurality of packet engines coupled to the switching system to handle classification processing for incoming packets received by the plurality of packet engines from the switching system and outgoing packets sent by the plurality of packet engines to the switching system;
- a plurality of cryptographic cores each coupled to one of the plurality of packet engines to communicate with the switching system via the plurality of packet engines and to provide encryption and decryption processing for packets received from and sent to the plurality of packet engines, wherein the plurality of packet engines are interposed between the switching system and the plurality of cryptographic cores;
- a signature database;
- an intrusion detection system coupled between the plurality of cryptographic cores and the plurality of packets engine and responsive to at least one packet matching a signature stored in the signature database and
- a control processor, coupled to the local data bus, to control data packet flow within the security processor.

50. (Previously Presented) The security processor of claim 49 wherein the security processor is operable to act as a firewall to deny or accept a data packet and to implement a secure communication channel with another computing device in the untrusted network.

51. (Previously Presented) The security processor of claim 50 wherein the security processor implements data packet security and authentication functions to support the secure communication channel.

52. (Previously Presented) The security processor of claim 30 wherein the packet engine is further operable to add at least one of an IP header or a MAC address to the outgoing packets.

53. (Previously Presented) The security processor of claim 30 wherein the packet engine is further operable to remove an IP header from the incoming packets.

54. (Previously Presented) The security processor of claim 30, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

55. (Previously Presented) The security processing system of claim 40, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

56. (Previously Presented) The security processor of claim 49, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.

Electronic Patent Application Fee Transmittal

Application Number:	12697112			
Filing Date:	29-Jan-2010			
Title of Invention:	System and Method For a Secure I/O Interface			
First Named Inventor/Applicant Name:	John M. Davis			
Filer:	Kimani Clark			
Attorney Docket Number:	2551-0109			
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Filing a brief in support of an appeal	1402	1	630	630
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

EX-1013

Palo Alto Networks, Inc. and Fortinet, Inc. v. Lionra Technologies Ltd.

078

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension - 4 months with \$0 paid	1254	1	2010	2010
Miscellaneous:				
Total in USD (\$)				2640

Electronic Acknowledgement Receipt

EFS ID:	15057470
Application Number:	12697112
International Application Number:	
Confirmation Number:	1325
Title of Invention:	System and Method For a Secure I/O Interface
First Named Inventor/Applicant Name:	John M. Davis
Customer Number:	42624
Filer:	Kimani Clark
Filer Authorized By:	
Attorney Docket Number:	2551-0109
Receipt Date:	26-FEB-2013
Filing Date:	29-JAN-2010
Time Stamp:	17:43:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$2640
RAM confirmation Number	5579
Deposit Account	501860
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part (if appl.)	Pages (if appl.)
		Palo Alto Networks, Inc. and Fortinet, Inc. v. Lionra Technologies Ltd.			

1	Appeal Brief Filed	Appeal_Brief_2551-0109_2-26-13.pdf	1212044 3947269112e58a316f5ab7f5085b60097c17ab0d	no	16
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	31955 d8539f3c8d137d03dae1e15f7fad47366d0d71dc	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			1243999		
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.					

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.

**NOTICE OF APPEAL FROM THE EXAMINER TO
THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Docket Number (Optional)

2551-0109

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" [37 CFR 1.8(a)]

on _____

Signature _____

Typed or printed
name _____In re Application of
DAVIS, John M.Application Number
12/697,112Filed
01/29/2010

For SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

Art Unit
2436Examiner
TRAORE, FatoumataApplicant hereby **appeals** to the Board of Patent Appeals and Interferences from the last decision of the examiner.The fee for this Notice of Appeal is (37 CFR 41.20(b)(1)) \$ 620.00
☐ Applicant claims small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by half, and the resulting fee is: \$ _____

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☒ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 501860.

☐ A petition for an extension of time under 37 CFR 1.136(a) (PTO/SB/22) is enclosed.

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.

I am the

☐ applicant/inventor.

/ Kimani Clark /

Signature

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

Kimani Clark

Typed or printed name

☒ attorney or agent of record. 45,969
Registration number _____

703.894.6400

Telephone number

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34. _____

September 7, 2012

Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 41.31. 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, 1.14 and 41.6. 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.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	12697112			
Filing Date:	29-Jan-2010			
Title of Invention:	System and Method For a Secure I/O Interface			
First Named Inventor/Applicant Name:	John M. Davis			
Filer:	Kimani Clark			
Attorney Docket Number:	2551-0109			
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Notice of appeal	1401	1	620	620
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

EX-1013

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				620

Electronic Acknowledgement Receipt

EFS ID:	13683441
Application Number:	12697112
International Application Number:	
Confirmation Number:	1325
Title of Invention:	System and Method For a Secure I/O Interface
First Named Inventor/Applicant Name:	John M. Davis
Customer Number:	42624
Filer:	Kimani Clark
Filer Authorized By:	
Attorney Docket Number:	2551-0109
Receipt Date:	07-SEP-2012
Filing Date:	29-JAN-2010
Time Stamp:	12:42:51
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$620
RAM confirmation Number	10813
Deposit Account	501860
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part (if appl.)	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	--------------------------	---------------------

1	Notice of Appeal Filed	25510109_Notice_of_Appeal.pdf	247886 314b8fc7126af7c99ca133acdef02b96eed64ac	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	29784 85b319a521ff3ce765c6685a6c8e483c005e8a31	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			277670		
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.					



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.
-----------------	-------------	----------------------	---------------------	------------------

12/697,112

01/29/2010

John M. Davis

2551-0109

1325

42624

7590

08/29/2012

DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

EXAMINER

TRAORE, FATOUMATA

ART UNIT

PAPER NUMBER

2436

MAIL DATE

DELIVERY MODE

08/29/2012

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Advisory Action Before the Filing of an Appeal Brief	Application No. 12/697,112	Applicant(s) DAVIS ET AL.
	Examiner FATOUMATA TRAORE	Art Unit 2436

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 09 August 2012 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

NO NOTICE OF APPEAL FILED

1. ☒ The reply was filed after a final rejection. No Notice of Appeal has been filed. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114 if this is a utility or plant application. Note that RCEs are not permitted in design applications. The reply must be filed within one of the following time periods:

a) ☒ The period for reply expires 5 months from the mailing date of the final rejection.

b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action; or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

c) ☐ A prior Advisory Action was mailed more than 3 months after the mailing date of the final rejection in response to a first after-final reply filed within 2 months of the mailing date of the final rejection. The current period for reply expires _____ months from the mailing date of the prior Advisory Action or SIX MONTHS from the mailing date of the final rejection, whichever is earlier.

Examiner Note: If box 1 is checked, check either box (a), (b) or (c). ONLY CHECK BOX (b) WHEN THIS ADVISORY ACTION IS THE FIRST RESPONSE TO APPLICANT'S FIRST AFTER-FINAL REPLY WHICH WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. ONLY CHECK BOX (c) IN THE LIMITED SITUATION SET FORTH UNDER BOX (c). See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) or (c) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendments filed after a final rejection, but prior to the date of filing a brief, will not be entered because

a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);

b) ☐ They raise the issue of new matter (see NOTE below);

c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or

d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. ☐ Applicant's reply has overcome the following rejection(s): _____.

6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. ☒ For purposes of appeal, the proposed amendment(s): (a) ☐ will not be entered, or (b) ☒ will be entered, and an explanation of how the new or amended claims would be rejected is provided below or appended.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. ☐ The affidavit or other evidence filed after the date of filing the Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:
See Continuation Sheet.

12. ☐ Note the attached Information *Disclosure Statement(s)*. (PTO/SB/08) Paper No(s). _____

13. ☐ Other: _____.

STATUS OF CLAIMS

14. The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: _____.

Claim(s) objected to: _____.

Claim(s) rejected: 30-56.

Claim(s) withdrawn from consideration: _____.

/Philip J Chea/ Supervisory Patent Examiner, Art Unit 2436	/Fatoumata Traore/ Examiner, Art Unit 2436
---	---

Continuation of 11. does NOT place the application in condition for allowance because: Applicant' arguments with respect to "Applicants respectfully traverse the rejections the claims at least because the cited references do not disclose "the cryptographic core ... receiving...packets from the switching system via the packet engine" is not persuasive because: Narad et al teaches in Fig. 2, the packet engine (item 106) is interposed between the switching system (item 108) and the cryptographic core (item 112). Narad et al further teaches col.7, lines 65 to col. 9, line 25, the policy processor (PP) performing switching/routing functions as to forward the packet to the appropriate/proper destination, for example Narad et al teaches "From the PP, there are many paths the packet can take, depending on what the application(s) running on the PP decide is the proper disposition of that packet. It can be transmitted, sent to Crypto, delayed in memory, passed through a Classification Engine again for further processing, or copied from the PE's memory over the PCI bus to the host's memory or to a peer device's memory, using the DMA engine. The PP may also gather statistics on that packet into records in a hash table or in general memory. A pointer to the buffer containing both the packet and data structures describing that packet is passed around among the various modules. The PP may choose to drop a packet, to modify the contents of the packet, or to forward the packet to the AP or to a different network segment over the PCI Bus (e.g. for routing)..

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT Application of:

DAVIS, John M.

Appl. S.N.: 12/697,112

Filing Date: 01/29/2010

Title: **SYSTEM AND METHOD FOR A SECURE
I/O INTERFACE**

Confirmation No.: 1325

Attorney Docket: 2551-0109

Group Art Unit: 2436

Examiner: TRAORE, Fatoumata

Date: August 9, 2012

RESPONSE AFTER FINAL

Hon. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action dated March 9, 2012, Applicants request a two-month extension of time to be charged to the deposit account listed below. Please amend the above-identified application as follows:

Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 9 of this paper.

Application Number 	Application/Control No. 12/697,112	Applicant(s)/Patent under Reexamination DAVIS ET AL.	
Document Code - DISQ		Internal Document – DO NOT MAIL	

TERMINAL DISCLAIMER	☒ APPROVED	☐ DISAPPROVED
Date Filed : 8/9/12	This patent is subject to a Terminal Disclaimer	

Approved/Disapproved by:

Lawana Hixon

U.S. Patent and Trademark Office

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT Application of:	Confirmation No.:	1325
DAVIS, John M.	Attorney Docket:	2551-0109
Appl. S.N.: 12/697,112	Group Art Unit:	2436
Filing Date: 01/29/2010	Examiner:	TRAORE, Fatoumata
Title: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE	Date:	August 9, 2012

RESPONSE AFTER FINAL

Hon. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action dated March 9, 2012, Applicants request a two-month extension of time to be charged to the deposit account listed below. Please amend the above-identified application as follows:

Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 9 of this paper.

CLAIMS

The claims are as follows:

1-29. (Canceled)

30. (Previously Presented) A security processor to process incoming packets and outgoing packets, the security processor comprising:

- a switching system to send the outgoing packets and receive the incoming packets;
- a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system;
- a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;
- a signature database; and
- an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.

31. (Previously Presented) The security processor of claim 30 wherein the packet engine is further operable to handle security context management processing for the incoming and outgoing packets.

32. (Previously Presented) The security processor of claim 30 further comprising:
a local data bus coupled to the switching system; and

a modulo engine coupled to the local data bus.

33. (Previously Presented) The security processor of claim 30 wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines.

34. (Previously Presented) The security processor of claim 33 wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines.

35. (Previously Presented) The security processor of claim 32 wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip.

36. (Previously Presented) The security processor of claim 35 further comprising a control processor, coupled to the local data bus, for exception handling of the incoming and outgoing packets.

37. (Previously Presented) The security processor of claim 35 further comprising a key management engine coupled to the local data bus.

38. (Previously Presented) The security processor of claim 35 wherein the security processor handles substantially all security processing for the incoming and outgoing packets.

Application of: DAVIS, John M.
Serial No.: 12/697,112
Filed: 01/29/2010

39. (Previously Presented) The security processor of claim 38 wherein the security processor further handles substantially all network processing for the incoming and outgoing packets.

40. (Previously Presented) A security processing system comprising:

(a) a security processor comprising:

a switching system to send outgoing packets and to receive incoming packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system;

a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;

a signature database; and

an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database; and

a local data bus coupled to the switching system; and

(b) a memory coupled to the local data bus.

Application of: DAVIS, John M.
Serial No.: 12/697,112
Filed: 01/29/2010

41. (Previously Presented) The security processing system of claim 40 further comprising a modulo engine coupled to the local data bus.
42. (Previously Presented) The security processing system of claim 41 further comprising a key management engine coupled to the local data bus.
43. (Previously Presented) The security processing system of claim 40 wherein the memory and the security processor are within the same cryptographic boundary.
44. (Previously Presented) The security processing system of claim 40 wherein the security processor is formed on a single chip.
45. (Previously Presented) The security processing system of claim 40 further comprising:
a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface; and
a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory.
46. (Previously Presented) The security processing system of claim 45 wherein the translator performs steganographic translation of the received data.
47. (Previously Presented) The security processing system of claim 45 wherein the translator performs encryption translation of the received data.

48. (Previously Presented) The security processing system of claim 40 wherein the security processor is operable to (i) execute boot code to load firmware for execution by the security processor and
(ii) authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor.

49. (Previously Presented) A security processor to connect a trusted network to an untrusted network for data packet communication, the security processor comprising:
a first interface to couple to the trusted network and to the un-trusted network;
a second interface to couple to a host processor;
a switching system operable to selectively couple to the first interface or the second interface;
a local data bus, coupled to the switching system;
a plurality of packet engines coupled to the switching system to handle classification processing for incoming packets received by the plurality of packet engines from the switching system and outgoing packets sent by the plurality of packet engines to the switching system;
a plurality of cryptographic cores each coupled to one of the plurality of packet engines to communicate with the switching system via the plurality of packet engines and to provide encryption and decryption processing for packets received from and sent to the plurality of packet engines, wherein the plurality of packet engines are interposed between the switching system and the plurality of cryptographic cores;
a signature database;
an intrusion detection system coupled between the plurality of cryptographic cores and the plurality of packets engine and responsive to at least one packet matching a signature stored in the signature database and

a control processor, coupled to the local data bus, to control data packet flow within the security processor.

50. (Previously Presented) The security processor of claim 49 wherein the security processor is operable to act as a firewall to deny or accept a data packet and to implement a secure communication channel with another computing device in the untrusted network.

51. (Previously Presented) The security processor of claim 50 wherein the security processor implements data packet security and authentication functions to support the secure communication channel.

52. (Previously Presented) The security processor of claim 30 wherein the packet engine is further operable to add at least one of an IP header or a MAC address to the outgoing packets.

53. (Previously Presented) The security processor of claim 30 wherein the packet engine is further operable to remove an IP header from the incoming packets.

54. (Previously Presented) The security processor of claim 30, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

55. (Previously Presented) The security processing system of claim 40, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

Application of: DAVIS, John M.
Serial No.: 12/697,112
Filed: 01/29/2010

56. (Previously Presented) The security processor of claim 49, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

Application of: DAVIS, John M.
Serial No.: 12/697,112
Filed: 01/29/2010

REMARKS

Favorable reconsideration of this application, in light of the following discussions, is respectfully requested.

Claims 30-56 are pending, and no claims have been amended. In the outstanding Office Action dated March 9, 2012, claims 30-56 were rejected on the grounds of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-22 of U.S. Patent No. 7,685,436.

The Examiner also rejected claims 30-35, 37-44, and 49-53 under 35 U.S.C. § 103(a) as unpatentable over *Narad et al.* (U.S. Patent No. 6,157,955) in view of *Krishna et al.* (U.S. Publication No. 2003/0014627) in further view of *Ramsey et al.* (U.S. Patent No. 7,331,061). The Examiner also rejected claims 36, 45, and 47 under 35 U.S.C. § 103(a) as being unpatentable over *Narad* in view of *Krishna* in further view of *Ramsey* and *Savarda et al.* (U.S. Publication No. 2003/0196081). The Examiner also rejected claim 46 under 35 U.S.C. § 103(a) as being unpatentable over *Narad* in view of *Krishna* and *Ramsey*, and further in view of *Savarda* and *Carr et al.* (U.S. Patent No. 6,788,800). The Examiner also rejected claim 48 under 35 U.S.C. § 103(a) as being unpatentable over *Narad* in view of *Krishna* in further view of *Ramsey*, and *Girard* (U.S. Publication No. 2003/0084342). The Examiner also rejected claims 54-56 under 35 U.S.C. § 103(a) as being unpatentable over *Narad* in view of *Krishna* and *Ramsey*, and further in view of *Savarda* and *Wu et al.* (U.S. Patent No. 7,493,659).

Applicants have submitted a Terminal Disclaimer to obviate the double patenting rejection.

Applicants respectfully traverse the rejections the claims at least because the cited references do not disclose “the cryptographic core ... receiving...packets from the

Application of: DAVIS, John M.
Serial No.: 12/697,112
Filed: 01/29/2010

switching system via the packet engine.” The Examiner has cited the “packet engine” as being Classification 106 on figure 2 of *Narad*, the “switching system” as being the Action Code 108 on Figure 2, and the “cryptographic core” as being crypto 112 (Office Action p. 3). However, there is no specific disclosure of “the cryptographic core ... receiving...packets from the switching system via the packet engine.” That is, there is no transmission of packets from Action Code 108 (alleged switching system) through Classification 106 (alleged packet engine) to Crypto 112 (alleged cryptographic core) in *Narad*. Even further, there appears to be no transmission from Classification 106 (alleged packet engine) to Crypto 112 (alleged cryptographic core) in *Narad*. (See Col. 8, l. 32 – col. 9, l. 43). As such, there is no disclosure of “the cryptographic core ... receiving...packets from the switching system via the packet engine.”

Consequently, in view of the present amendment and in light of the above discussions, the outstanding grounds for rejection are believed to have been overcome and the pending claims are in condition for allowance. An early and favorable action to that effect is respectfully requested.

CHARGE STATEMENT: Deposit Account No. 501860, order no. **2551-0109**.

The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 (missing or insufficiencies only) now or hereafter relative to this application and the resulting Official Document under Rule 20, or credit any overpayment, to our Accounting/ Order Nos. shown above, for which purpose a duplicate copy of this sheet is attached.

This CHARGE STATEMENT does not authorize charge of the issue fee until/unless an issue fee transmittal sheet is filed.

CUSTOMER NUMBER

42624

Respectfully submitted,

By: / Kimani Clark /
Kimani Clark
Registration No.: 45,969

Application of: DAVIS, John M.
Serial No.: 12/697,112
Filed: 01/29/2010

Davidson Berquist Jackson & Gowdey LLP
4300 Wilson Blvd., 7th Floor, Arlington, Virginia 22203
Main: (703) 894-6400 • FAX: (703) 894-6430

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT Application of:

DAVIS, John M.

Appl. S.N.: 12/697,112

Filing Date: January 29, 2010

Title: **SYSTEM AND METHOD FOR A SECURE
I/O INTERFACE**

Confirmation No.: 1325

Attorney Docket: 2551-0109

Group Art Unit: 2436

Examiner: TRAORE, Fatoumata

Date: August 9, 2012

**TERMINAL DISCLAIMER
(By Attorney)**

Hon. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The **Owner**, EXELIS INC., of 100 percent interest in the instant application hereby disclaims the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **reference patent** No. 7,685,436 as the term of said prior patent is defined in 35 U.S.C. 154 and 173, and as the term of said **reference patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **reference patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

The undersigned petitioner, an attorney of record, is hereby acting for the **Owner**.

Atty. Sig.: / Kimani Clark /

Name: Kimani Clark

Date: August 9, 2012

☒ Terminal disclaimer fee under 37 CFR 1.20(d) is enclosed.

*Attorney and client: Please note on that other file and also this application file not to assign either separately in view of this disclaimer.

Electronic Patent Application Fee Transmittal

Application Number:	12697112			
Filing Date:	29-Jan-2010			
Title of Invention:	System and Method For a Secure I/O Interface			
First Named Inventor/Applicant Name:	John M. Davis			
Filer:	Kimani Clark			
Attorney Docket Number:	2551-0109			
Filed as Large Entity				
Utility under 35 USC 111(a) 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:				
Extension-of-Time:				
Extension - 2 months with \$0 paid	1252	1	560	560 EX-1013

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Statutory or terminal disclaimer	1814	1	160	160
Total in USD (\$)				720

Electronic Acknowledgement Receipt

EFS ID:	13462230
Application Number:	12697112
International Application Number:	
Confirmation Number:	1325
Title of Invention:	System and Method For a Secure I/O Interface
First Named Inventor/Applicant Name:	John M. Davis
Customer Number:	42624
Filer:	Kimani Clark
Filer Authorized By:	
Attorney Docket Number:	2551-0109
Receipt Date:	09-AUG-2012
Filing Date:	29-JAN-2010
Time Stamp:	17:36:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$720
RAM confirmation Number	4523
Deposit Account	501860
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part (if appl.)	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	--------------------------	---------------------

1	Amendment After Final	25510109_Response_After_Final.pdf	66627 e7bf2b2bdf9b019f140a2c2c9660d406d8811c14	no	1
Warnings:					
Information:					
2	Claims	25510109_Claims.pdf	51320 e3fd14f07c2a51d5d904c8d5e6e866f0a9cc9482	no	7
Warnings:					
Information:					
3	Applicant Arguments/Remarks Made in an Amendment	25510109_Remarks.pdf	171344 21ba053b9cf2f3afeebba0d25e1b60e07ff34bb6	no	3
Warnings:					
Information:					
4	Terminal Disclaimer Filed	25510109_Terminal_Disclaimer.pdf	77102 1deb65b57870a54631d9892f2b70b9da578530d3	no	1
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	31658 357dcfae550e956a592367cbdbbc596351988642	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			398051		
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.					

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 12/697,112		Filing Date 01/29/2010		☐ 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), (l), 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(j))	minus 20 =	*	X \$	=	OR	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))										
			TOTAL			TOTAL				
* If the difference in column 1 is less than zero, enter "0" in column 2.										
APPLICATION AS AMENDED – PART II										
(Column 1)			(Column 2)			SMALL ENTITY OR		OTHER THAN SMALL ENTITY		
AMENDMENT	08/09/2012	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	* 27	Minus	** 27	=	0		X \$60=	0	
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	=	0		X \$250=	0	
☐ Application Size Fee (37 CFR 1.16(s))										
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))										
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0	
(Column 1)			(Column 2)			SMALL ENTITY OR		OTHER THAN SMALL ENTITY		
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 \$	=		
	Independent (37 CFR 1.16(h))	*	Minus	***	=		X \$	=		
☐ Application Size Fee (37 CFR 1.16(s))										
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))										
					TOTAL ADD'L FEE		OR	TOTAL ADD'L 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.										

Legal Instrument Examiner:
/PATSY ZIMMERMAN/

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

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.
-----------------	-------------	----------------------	---------------------	------------------

12/697,112

01/29/2010

John M. Davis

2551-0109

1325

42624

7590

03/09/2012

DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

EXAMINER

TRAORE, FATOUMATA

ART UNIT

PAPER NUMBER

2436

MAIL DATE

DELIVERY MODE

03/09/2012

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 12/697,112	Applicant(s) DAVIS ET AL.	
	Examiner FATOUMATA TRAORE	Art Unit 2436	

-- 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 12 December 2011.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
- 4) ☐ 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

- 5) ☒ Claim(s) 30-56 is/are pending in the application.
- 5a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 6) ☐ Claim(s) ____ is/are allowed.
- 7) ☒ Claim(s) 30-56 is/are rejected.
- 8) ☐ Claim(s) ____ is/are objected to.
- 9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 10) ☐ The specification is objected to by the Examiner.
- 11) ☒ The drawing(s) filed on 29 January 2010 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).
- 12) ☐ 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

- 13) ☐ 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 ____. | 6) ☐ Other: ____. |

DETAILED ACTION

1. This is in response to amendments filed 12/12/2011. Claims 1-29 have been cancelled. Claims 30-56 are pending and have been considered below.

Priority

2. This application is a continuation of and claim priority to US patent application 10/903,785 filed 07/30/2004 now U.S. Patent No. 7,685,436 and claiming Priority from Provisional Application 60507976 filed 10/02/2003.

Oath/Declaration

3. The oath filed on 01/29/2010 complies with all the requirements set forth in MPEP 602 and therefore is accepted.

Drawings

4. The drawings filed on 01/29/2010 are accepted.

Specification

5. The specification filed on 01/29/2010 is accepted.

Response to Arguments

6. Applicant's arguments filed 12/12/2011 have been fully considered but they are not persuasive. Applicant arguments see remarks page with respect to "Narad et al. does not teach or suggest "communicating the outgoing packets to the switching system via the packet engine..., wherein the packet engine is interposed between the switching system and the cryptographic core," as recited, for example in claim 30. In Narad et al., the cited Classification Engine (CE) 106 is not interposed between the Crypto 112 and whatever the Examiner appears to consider the

switching system. (See Figure 2). Also, it is not clear what the Examiner specifically considers to be the switching system” is not persuasive because :

Narad et al teaches in Fig. 2, the packet engine (item 106) is interposed between the switching system (item 108) and the cryptographic core (item 112). Narad et al further teaches col.7, lines 65 to col. 9, line 25, the policy processor (PP) performing switching/routing functions as to forward the packet to the appropriate/proper destination, for example Narad et al teaches “From the PP, there are many paths the packet can take, depending on what the application(s) running on the PP decide is the proper disposition of that packet. It can be transmitted, sent to Crypto, delayed in memory, passed through a Classification Engine again for further processing, or copied from the PE's memory over the PCI bus to the host's memory or to a peer device's memory, using the DMA engine. The PP may also gather statistics on that packet into records in a hash table or in general memory. A pointer to the buffer containing both the packet and data structures describing that packet is passed around among the various modules. The PP may choose to drop a packet, to modify the contents of the packet, or to forward the packet to the AP or to a different network segment over the PCI Bus (e.g. for routing.)

7. Applicant with respect to double patenting rejecting have been considered, the examiner acknowledged the filing of the terminal Disclaimer (TD), however the examiner that the TD has not been approved. Applicant is required to refile a new TD to comply with all the requirements set forth in 35 USC 154 and 173.

Double Patenting

8. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

9. Claims 30-56 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1- 22 of U.S. Patent No. 7,685,436. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-22 of US patent No. 7,685,436 contain every element of claims 30-56 of the present application. A comparison of the claims languages has been provided below for applicant review.

US 7,685,236	US 12/697,112
1. A security processor to process incoming packets and outgoing packets, the security processor comprising: a switching system to send the outgoing packets and receive the incoming packets; a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming packets and outgoing packets to the	30. A security processor to process incoming packets and outgoing packets, the security processor comprising: a switching system to send the outgoing packets and receive the incoming packets; a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system;

security processor transit one of the plurality of packet engines, and wherein the incoming packets and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines an egress path within the security processor upon exit from a corresponding cryptographic core; a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core; a signature database; and an intrusion detection system coupled	a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;
--	---

between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database. 2. The security processor of claim 1 wherein the packet engine is further operable to handle security context management processing for the incoming and outgoing packets. 3. The security processor of claim 1 further comprising: a local data bus coupled to the switching system; and a modulo engine coupled to the local data bus.	a signature database; and an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database. 31. The security processor of claim 30 wherein the packet engine is further operable to handle security context management processing for the incoming and outgoing packets. 32. The security processor of claim 30 further comprising: a local data bus coupled to the switching system; and a modulo engine coupled to the local data bus. 33. The security processor of claim 30 wherein
---	--

4. The security processor of claim 3 wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip. 5. The security processor of claim 4 further comprising a control processor, coupled to the local data bus, for exception handling of the incoming and outgoing packets. 6. The security processor of claim 4 further comprising a key management engine coupled to the local data bus.	the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines. 34. The security processor of claim 33 wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines. 35. The security processor of claim 32 wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip. 36. The security processor of claim 35 further comprising a control processor, coupled to the local data bus, for exception handling of the incoming and outgoing packets.
---	---

7. The security processor of claim 4 wherein the security processor handles substantially all security processing for the incoming and outgoing packets. 8. The security processor of claim 7 wherein the security processor further handles substantially all network processing for the incoming and outgoing packets. 9. The security processor of claim 1 wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the	37. The security processor of claim 35 further comprising a key management engine coupled to the local data bus. 38. The security processor of claim 35 wherein the security processor handles substantially all security processing for the incoming and outgoing packets. 39. The security processor of claim 38 wherein the security processor further handles substantially all network processing for the incoming and outgoing packets. 40. A security processing system comprising: (a) a security processor comprising: a switching system to send outgoing packets and to receive incoming packets; a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system; a
---	---

plurality of packet engines. 10. The security processor of claim 1 wherein the packet engine is further operable to add at least one of an IP header or a MAC address to the outgoing packets. 11. The security processor of claim 1 wherein the packet engine is further operable to remove an IP header from the incoming packets. 12. The security processor of claim 1, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet. 13. A security processing system comprising: (a) a security processor comprising: a switching system to send	cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core; a signature database; and an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database; and a local data bus coupled to the switching system; and (b) a memory coupled to the local data bus. 41. The security processing system of claim 40 further comprising a modulo engine coupled to the local data bus. 42. The security processing system of claim 41
--	--

outgoing packets and to receive incoming packets; a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines, and wherein the incoming and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines an egress path within the security processor upon exit from a corresponding cryptographic core; a cryptographic core, coupled to the packet engine and receiving the incoming packets from the	further comprising a key management engine coupled to the local data bus. 43. The security processing system of claim 40 wherein the memory and the security processor are within the same cryptographic boundary. 44. The security processing system of claim 40 wherein the security processor is formed on a single chip. 45. The security processing system of claim 40 further comprising: a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface; and a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory. 46. The security processing system of claim 45 wherein the translator performs steganographic translation of the received data.
---	--

switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core; a signature database; and an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database; and a local data bus coupled to the switching system; and (b) a memory coupled to the local data bus. 14. The security processing system of claim 13 further comprising a modulo engine coupled to the local data bus.	47. The security processing system of claim 45 wherein the translator performs encryption translation of the received data. 48. The security processing system of claim 40 wherein the security processor is operable to (i) execute boot code to load firmware for execution by the security processor and (ii) authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor. 49. A security processor to connect a trusted network to an un-trusted network for data packet communication, the security processor comprising: a first interface to couple to the trusted network and to the un-trusted network; a second interface to couple to a host processor; a switching system operable to selectively couple to the first interface or the second interface; a local data bus, coupled to the switching system; a plurality of packet engines coupled to the switching system to
---	--

15. The security processing system of claim 14 further comprising a key management engine coupled to the local data bus. 16. The security processing system of claim 13 wherein the memory and the security processor are within the same cryptographic boundary. 17. The security processing system of claim 13 wherein the security processor is formed on a single chip. 18. The security processing system of claim 13 further comprising: a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface; and a translator coupled to the memory interface to perform translation of data received by the memory	handle classification processing for incoming packets received by the plurality of packet engines from the switching system and outgoing packets sent by the plurality of packet engines to the switching system; a plurality of cryptographic cores each coupled to one of the plurality of packet engines to communicate with the switching system via the plurality of packet engines and to provide encryption and decryption processing for packets received from and sent to the plurality of packet engines, wherein the plurality of packet engines are interposed between the switching system and the plurality of cryptographic cores; a signature database; an intrusion detection system coupled between the plurality of cryptographic cores and the plurality of packets engine and responsive to at least one packet matching a signature stored in the signature database and a control processor, coupled to the local data bus, to control data
---	---

interface from the memory. 19. The security processing system of claim 18 wherein the translator performs steganographic translation of the received data. 20. The security processing system of claim 18 wherein the translator performs encryption translation of the received data. 21. The security processing system of claim 13 wherein the security processor is operable to (i) execute boot code to load firmware for execution by the security processor and (ii) authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor.	packet flow within the security processor. 50. The security processor of claim 49 wherein the security processor is operable to act as a firewall to deny or accept a data packet and to implement a secure communication channel with another computing device in the untrusted network. 51. The security processor of claim 50 wherein the security processor implements data packet security and authentication functions to support the secure communication channel. 52. The security processor of claim 30 wherein the packet engine is further operable to add at least one of an IP header or a MAC address to the outgoing packets. 53. The security processor of claim 30 wherein the packet engine is further operable to remove an IP header from the incoming packets. 54. The security processor of claim 30,
---	---

22. The security processing system of claim 13, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.	wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet. 55. The security processing system of claim 40, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet. 56. The security processor of claim 49, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.
--	--

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2436

11. Claims 30-35, 37-44 and 49-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narad et al US 6,157,955 A1 in view of Krishna et al US 2003/0014627 A1 in further view of Ramsey et al US 7,331,061 B1

Claims 30, 40 and 49: Narad et al teaches A security processor to connect a trusted network to an un-trusted network for data packet communication, the security processor comprising:

- i. a plurality of packet engines coupled to the switching system to handle classification processing for incoming packets received by the plurality of packet engines from the switching system and outgoing packets sent by the plurality of packet engines to the switching system (**col. 6 :line55 to col.7 :line, col.7 :lines 63-67 to col.8 :lines 30-65, Fig. 2-4; Each Ethernet MAC receives packets into buffers addressed by buffer points obtained from a producer-consumer ring and then passes the buffer to a Classification Engine for processing. There are four Classification Engines 208, 212, 238, and 242 which are microprogrammed processors optimized for the predicate analysis associated with packet filtering**);
- ii. a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed

between the switching system and the cryptographic core (**alternatively the action code 108 may choose to send the packet to the attached cryptographic processor (Crypto) 246 for encryption, decryption compression, decompression, security key management, parsing of IPSEC headers, or other associated functions**) (column 8, line 67 to column 9, line 25);;

- iii. a signature database(**col.14 :lines 20-67, hash table**);
- iv. a memory coupled to the local data bus(**col. 7: lines 15-20, A large parity-protected synchronous DRAM (SDRAM) buffer memory is provided, along with a PCI interface that is used for communication with the host (AP) and potentially for peer-to-peer communication among Policy Engines, e.g. for applications which route and switch**).

Narad et al fails to teach first interface, a second interface, a plurality of cryptographic cores nor an intrusion detection system coupled between the plurality of cryptographic cores and the plurality of packets engine and responsive to at least one packet matching a signature stored in the signature database and

Krishna et al teaches similar concept, which further teaches :

a plurality of cryptographic core(**paragraph [0039], Fig.2 item 214, packet are distributed to a plurality of cryptographic engine with corresponding security associations**).

Therefore, it would have been obvious for one ordinary skill in the art at the time of the invention to modify the teaching of Narad et al with the addition feature of Krishna et al

in order to provide an architecture for a cryptography accelerator chip that allows significant performance improvements over previous prior art designs, as suggested by Krishna et al (paragraph [0010]).

The combined disclosure fails to teach, first interface, a second interface, an intrusion detection system coupled between the plurality of cryptographic cores and the plurality of packets engine and responsive to at least one packet matching a signature stored in the signature database.

Ramsey et al teaches similar concept, which further teaches:

- v. a first interface to couple to the trusted network and to the un-trusted network(**Fig.3, items 265, 270, col. 12:lines 11-13, The firewall 225 can limit access between an external or unsecured network 265 and a secured network 270 in order to prevent intrusion**);
- vi. a second interface to couple to a host processor (**Fig. 3, item 260**);
- vii. a switching system operable to selectively couple to the first interface or the second interface (**Figs. 3, item 215**);
- viii. a local data bus, coupled to the switching system(**Figs. 3, item 230**);
- ix. a control processor, coupled to the local data bus, to control data packet flow within the security processor(**Figs. 3. item 260, The integrated firewall and IDS system 215 can be connected to a controller 260**);

an intrusion detection system coupled between the plurality of cryptographic cores and the plurality of packets engine and responsive to at least one packet

matching a signature stored in the signature database (**col.15 :lines 5-30, col.18 :lines 25-40, Fig. 4, items 425-435, Fig. 5, items 538-542, the IDS can employ one or more signatures to determine whether a data packet can pass through the intrusion detection system. The IDS can also reject, accept or deny a packet based upon the comparison with the one or more signatures.**)

Therefore, it would have been obvious for one ordinary skill in the art at the time of the invention to modify the combination with the addition feature of Ramsey et al in order to provide centralized control of the firewall, the IDS, and the AVS which can increase the speed at which packets are passed between a secured computer network and an external network, as suggested by Ramsey et al (col. 3 :lines25-40).

Claim 31: The combination further teaches wherein the packet engine is further operable to handle security context management processing for the incoming and outgoing packets (**Narad et al, col.6 :lines 40-65**).

Claims 32 and 41: The combination further teaches that the security processor comprises:

- i. A local data bus coupled to the switching system (**Narad et al, col.7, lines 40-50, PCI-to-PCI Bridges 312 controls child PCI bus 332 which provides the Application Processor 302 with connection to standard I/O devices through local I/O 314 and optionally to PCI expansion slots 316 into which additional PCI devices can be connected**); and
- ii. A modulo engine coupled to the local data bus (**Narad et al, Fig. 2., item 110**).

Claim 33: The combination further teaches wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines (**Narad et al col. 6 : line 55 to col.7 :line, col.7 :lines 63-67 to col.8 :lines 30-65, Fig. 2-4; There are four Classification Engines 208, 212, 238, and 242 which are microprogrammed processors optimized for the predicate analysis associated with packet filtering**)

Claim 34: The combination further teaches wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines (**Krishna et al, paragraph [0039], Fig.2 item 214, packet are distributed to a plurality of cryptographic engine with corresponding security associations**).

Claims 35 and 44: The combination further teaches wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip(**Narad et al, Fig. 2, items 106, 110 and 112**).

Claims 37 and 42: The combination further teaches that the security processor further comprises a key management engine coupled to the local data bus (**Narad et al, column 7, lines 1-5**).

Claim 38: The combination further teaches wherein the security processor handles substantially all security processing for the incoming and outgoing packets(**Narad et al, col. 7, lines 1-5**).

Claim 39: (The combination further teaches wherein the security processor further handles substantially all network processing for the incoming and outgoing packets (Narad et al, col.6 :lines 40-65).

Claims 43: The combination further teaches wherein the memory and the security processor are within the same cryptographic boundary (Narad et al, col.7, lines 30-50 and Fig. 4, PCI-to-PCI Bridges 312 controls child PCI bus 332 which provides the Application Processor 302 with connection to standard I/O devices through local I/O 314 and optionally to PCI expansion slots 316 into which additional PCI devices can be connected).

Claim 50: The combination further teaches wherein the security processor is operable to act as a firewall to deny or accept a data packet and to implement a secure communication channel with another computing device in the un-trusted network (Narad et al, column 13 lines 25-58).

Claim 51: The combination further teaches wherein the security processor implements data packet security and authentication functions to support the secure communication channel (Narad et al, column 13, lines 25-58).

Claim 52: The combination further teaches wherein the packet engine is further operable to add at least one of an IP header or MAC address to the outgoing packets (Narad et al, column 20, lines 50-67).

Claim 53: The combination further teaches wherein the packet engine is further operable to remove at least one of an IP header from the incoming packets (Narad et al, column 20, lines 50-67).

2. Claims 36, 45 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narad et al US 6,157,955 A1 in view of Krishna et al US 2003/0014627 A1 in further view of Ramsey et al US 7,331,061 B1 and Savarda et al US 2003/0196081.

Claim 36: The combination fails to teach a control processor coupled to the local data bus, for exception handling of the incoming and outgoing packets. However, Savarda et al teaches similar concepts, which further teaches a control processor coupled to the local data bus, for exception handling of the incoming and outgoing packets (**paragraph [0031], The packet inspection/outbound policy module 108 may be configured with multiplexing circuitry to integrate the outbound and inbound packet streams into a single stream for pipeline processing in the packet co-processor 100. In addition, the packet inspection and or outbound policy module 108 may be further configured to inspect packet-objects to ensure their integrity**) .

Therefore, it would have been obvious for one ordinary skill in the art at the time of the invention to modify the combination with the addition feature of Savarda et al in order to maintain system integrity, as suggested by Savarda et al .

Claim 45: The combination further discloses:

a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface (**Narad et al, col. 7: lines 15-20, A large parity-protected synchronous DRAM (SDRAM) buffer memory is provided, along with a PCI interface that is used for communication with the**

host (AP) and potentially for peer-to-peer communication among Policy Engines, e.g. for applications which route and switch));

The combination fails to teach a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory. However, Savarda et al discloses a system for processing a packet object using multiple pipelined processing modules, which further discloses

a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory (**the SAD contains parameter information about each SA. Such parameters may include the security protocol algorithms and keys for Authentication Header (AH) or Encapsulating Security Payload (ESP) security protocols, sequence numbers, protocol mode, and SA lifetime. For outbound packets, the SPD is consulted to determine if IPSec processing is required and/or if other processing or discarding of the packet is to be performed. If IPSec is required, then the outbound SAD is searched for an existing SA that matches the packet profile**) (paragraphs [0004], [0009], [0024], and [0026]).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a translator. One would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

Claim 47: The combination further discloses that the translator performs encryption translation of the received data (**Savarda et al, the cryptographic chip may perform the encryption, decryption, and/or authentication transforms as required. After**

completion of the cryptographic operations, the system processor may further process the packet to finish any remaining IPSec transforms, paragraphs [0007], 0026] and Fig.6).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt received data. One would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

12. Claim 46 is rejected under 35 U.S.C. 103(a) as being unpatentable over Narad et al US 6,157,955 A1 in view of Krishna et al US 2003/0014627 A1 and of Ramsey et al US 7,331,061 B1 in further view of Savarda et al US 2003/0196081 and Carr et al US 6,788,800.

Claim 46: The combination fails to teach a translator performing steganographic translation of the received data. However, Carr et al discloses a similar concept, which further discloses a step of performing steganographic translation of the received data (col.1 :lines 38-49, it also steganographically embeds security data into product).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combination such as to perform steganographic translation. One would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

13. Claim 48 is rejected under 35 U.S.C. 103(a) as being unpatentable over Narad et al US 6,157,955 A1 in view of Krishna et al US 2003/0014627 A1 in further view of Ramsey et al US 7,331,061 B1 and Girard (US 2003/0084342 A1).

Claim 48: The combination fails to teach wherein the security processor is operable to (i) execute boot code to load firmware for execution by the security processor and (ii) authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor.

Girard teaches similar concepts, which further teaches:

- i. execute boot code to load firmware for execution by the security processor(see paragraphs [0043], [0047], [0053]) and
- ii. authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor (**paragraphs [0043], [0047], [0053], The authentication stack enables boot code that is to be downloaded from a boot server to be authenticated prior to control being passed to the operating system of the booting computer system).**

Therefore, it would have been obvious for one ordinary skill in the art at the time of the invention to modify the combination with the addition feature of Girard in order to improve authentication for remote management of a computer system, as suggested by Girard paragraph [0014].

14. Claims 54-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narad et al US 6,157,955 A1 in view of Krishna et al US 2003/0014627 A1 in further view of Ramsey et al US 7,331,061 B1 and Wu et al US 7,493,659.

Claims 54, 55 and 56: The combination fails to teach wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

Wu et al teaches similar concept, which further teaches wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet (**Wu et al column 5, lines 43-67**).

Therefore, it would have been obvious for one ordinary skill in the art at the time of the invention to modify the combination with the addition feature of Girard in order to accurately detect various intrusions hidden in high-speed network traffic, as suggested by Wu et al col. 2, lines 5-10.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

15. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Friday, March 02, 2012

/Fatoumata Traore/

Examiner, Art Unit 2436

/Nasser Moazzami/

Supervisory Patent Examiner, Art Unit 2436

Search Notes 	Application/Control No. 12697112	Applicant(s)/Patent Under Reexamination DAVIS ET AL.
	Examiner FATOUMATA TRAORE	Art Unit 2436

SEARCHED			
Class	Subclass	Date	Examiner
370	218, 386-389, 468, limited by text search	7/5/2011	FT
713	153-154, 168, 187-189, limited by text search	7/5/2011	FT
726	22-25, limited by text search	7/5/2011	FT

SEARCH NOTES		
Search Notes	Date	Examiner
EAT, google patent and inventors name search performed.	7/5/2011	FT
updated EAST and google search performed.	3/2/2012	FT

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	6352	packet with classificat\$3with (rout\$3 switch\$3) with (encrypt\$3 cryptographic)	USPAT	OR	OFF	2012/03/02 12:21
L3	0	packet adj (unit engine device) with classificat\$3 adj (engine unit device)with (rout\$3 switch\$3) with (encrypt\$3 cryptographic)adj (engine device unit)	USPAT	OR	OFF	2012/03/02 12:22
L4	1	packet near7 (unit engine device) with classificat\$3 near7 (engine unit device) with (rout\$3 switch\$3) with (encrypt\$3 cryptographic) near7 (engine device unit)	USPAT	OR	OFF	2012/03/02 12:23
L5	2	packet with(unit engine device) with classificat\$3 with(engine unit device) with (rout\$3 switch\$3) with (encrypt\$3 cryptographic) with (engine device unit)	USPAT	OR	OFF	2012/03/02 12:24
L6	2	packet with classificat\$3 with(engine unit device) with (rout\$3 switch\$3) with (encrypt\$3 cryptographic) with (engine device unit)	USPAT	OR	OFF	2012/03/02 12:27
L7	2	packet with classificat\$3 with (rout\$3 switch\$3) with (encrypt\$3 cryptographic) with (engine device unit)	USPAT	OR	OFF	2012/03/02 12:28
L8	9	packet with classificat\$3 with (rout\$3 switch\$3) with (encrypt\$3 cryptographic)	USPAT	OR	OFF	2012/03/02 12:28
S1	3	(switch\$3 router) with packet with (classificat\$3 classif\$4) same cryptograph\$3 with (encrypt\$3 decrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 10:35
S2	49	(switch\$3 router) with packet with (classificat\$3 classif\$4) same (cryptograph\$3 encrypt\$3 decrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 10:36
S3	8364	370/389.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 11:27

S4	208	(switch\$3) same (classificat\$3 classif\$4) same (cryptograph\$3 encrypt\$3 decrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 11:28
S5	304	(switch\$3) same (classificat\$3 classif\$4) same (hash\$3 cryptograph\$3 encrypt\$3 decrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 11:28
S6	26	S3 and S5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 11:28
S7	256	packet with (engine classificat\$3 classif\$4) same (secur\$3 cryptograph\$3 encrypt\$3) with (engine core) same (signature intrus\$3 virus wornpattern)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 15:19
S8	14000	370/468.ccls. 370/218.ccls. 370/386- 388.ccls. 370/389.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 15:21
S9	11	S7 and S8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 15:21
S10	14788	713/153-154.ccls. 713/168.ccls. 713/187-189.ccls. 726/22-25.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 16:11
S11	32	packet with engine same(classificat\$3 classif\$4) same (secur\$3 cryptograph\$3 encrypt\$3) with (engine core) same (signature intrus\$3 virus worn pattern)same detect\$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 16:13
S12	201	packet with engine same(classificat\$3 classif\$4) same (secur\$3 cryptograph\$3 encrypt\$3) with (engine core)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2011/07/05 16:19

			DERWENT; IBM_TDB			
S13	35	S12 and (S8 S10)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 16:19
S14	18	("20020066014" "20020108059" "20030014627" "20030196081" "20040010545" "5432950" "5737760" "5892899" "5940626" "6041122" "6049876" "6101255" "6157955" "6788800" "6983366" "7095716" "7493659").PN. OR ("7685436").URPN.	US-PGPUB; USPAT; USOCR	ADJ	ON	2011/07/05 16:25
S15	2	"7685436".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/06 10:59
S16	2	"20100169636".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/06 11:10
S17	0	packet with (engine classificat\$3 classif\$4) same plural\$3 same(secur\$3 cryptograph\$3 encrypt\$3) with (engine core)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/06 14:49
S18	0	packet with (engine classificat\$3 classif\$4) same plural\$3 same(secur\$3 cryptograph\$3 encrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/06 14:49
S19	275	packet with (engine classificat\$3 classif\$4) same plural\$3 same(secur\$3 cryptograph\$3 encrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/06 14:49
S20	141	packet with (engine classificat\$3 classif\$4) same plural\$3 same(secur\$3 cryptograph\$3 encrypt\$3) with (engine core)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/06 14:50
S21	2	"7493659".pn.	US-PGPUB; USPAT;	OR	ON	2011/07/06 16:12

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S22	2174823	execut\$3 with authenticat\$3 with (boot near2 code bot-code bootcode)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/07 09:40
S23	114	execut\$3 with authenticat\$3 with (boot near2 code bot-code bootcode)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/07 09:40
S24	8	execut\$3 with authenticat\$3 with (boot near2 code bot-code bootcode) same secur\$3 with processor	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/07 09:41
S25	4	"7321061".pn. "6157955".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/07 10:24
S26	1	switching with packet adj (engine classificat\$3) with cryptographic adj (unit engine core)	USPAT	OR	OFF	2012/03/02 10:07
S27	2	"6157955".pn. "20030014627".pn. "7331061".pn.	USPAT	OR	OFF	2012/03/02 10:10

3/ 2/ 2012 12:36:41 PM
C:\ Users\ ftraore\ Documents\ EAST\ Workspaces\ 12697112securityProcessor\ OPacket.wsp

<i>Index of Claims</i> 	Application/Control No. 12697112	Applicant(s)/Patent Under Reexamination DAVIS ET AL.
	Examiner FATOUMATA TRAORE	Art Unit 2436

✓	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	07/05/2011	03/02/2012						
	1	-	-						
	2	-	-						
	3	-	-						
	4	-	-						
	5	-	-						
	6	-	-						
	7	-	-						
	8	-	-						
	9	-	-						
	10	-	-						
	11	-	-						
	12	-	-						
	13	-	-						
	14	-	-						
	15	-	-						
	16	-	-						
	17	-	-						
	18	-	-						
	19	-	-						
	20	-	-						
	21	-	-						
	22	-	-						
	23	-	-						
	24	-	-						
	25	-	-						
	26	-	-						
	27	-	-						
	28	-	-						
	29	-	-						
	30	✓	✓						
	31	✓	✓						
	32	✓	✓						
	33	✓	✓						
	34	✓	✓						
	35	✓	✓						
	36	✓	✓						

<i>Index of Claims</i> 	Application/Control No. 12697112	Applicant(s)/Patent Under Reexamination DAVIS ET AL.
	Examiner FATOUMATA TRAORE	Art Unit 2436

✓	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	07/05/2011	03/02/2012												
	37	✓	✓												
	38	✓	✓												
	39	✓	✓												
	40	✓	✓												
	41	✓	✓												
	42	✓	✓												
	43	✓	✓												
	44	✓	✓												
	45	✓	✓												
	46	✓	✓												
	47	✓	✓												
	48	✓	✓												
	49	✓	✓												
	50	✓	✓												
	51	✓	✓												
	52	✓	✓												
	53	✓	✓												
	54	✓	✓												
	55	✓	✓												
	56	✓	✓												

Application Number 	Application/Control No. 12/697,112	Applicant(s)/Patent under Reexamination DAVIS ET AL.	
Document Code - DISQ		Internal Document – DO NOT MAIL	

TERMINAL DISCLAIMER	☐ APPROVED	☒ DISAPPROVED
Date Filed : 12/12/11	This patent is subject to a Terminal Disclaimer	

Approved/Disapproved by:

The language 35 USC 154 to 156 and 173 is unclear and the statues do not cover the same rights, it should be 35 USC 154 and 173.

Lawana Hixon

U.S. Patent and Trademark Office

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT Application of:

DAVIS, John M.

Appl. S.N.: 12/697,112

Filing Date: January 29, 2010

Title: **SYSTEM AND METHOD FOR A SECURE
I/O INTERFACE**

Confirmation No.: 1325

Attorney Docket: 2551-0109

Group Art Unit: 2436

Examiner: TRAORE, Fatoumata

Date: December 12, 2011

RESPONSE

Hon. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action dated July 15, 2011, Applicant respectfully requests a two-month extension of time to be charged to the Deposit Account list below and also submits the following response.

The pending Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 9 of this paper.

Application of: DAVIS, John M.
Serial No.: 12/697,112
Filed: January 29, 2010
Reply to Office Action of July 15, 2011

CLAIMS

Please amend the claims as follows:

1-29. (Canceled)

30. (Previously Presented) A security processor to process incoming packets and outgoing packets, the security processor comprising:

- a switching system to send the outgoing packets and receive the incoming packets;

- a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system;

- a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;

- a signature database; and

- an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.

31. (Previously Presented) The security processor of claim 30 wherein the packet engine is further operable to handle security context management processing for the incoming and outgoing packets.

Application of: DAVIS, John M.
Serial No.: 12/697,112
Filed: January 29, 2010
Reply to Office Action of July 15, 2011

32. (Previously Presented) The security processor of claim 30 further comprising:
a local data bus coupled to the switching system; and
a modulo engine coupled to the local data bus.

33. (Previously Presented) The security processor of claim 30 wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines.

34. (Previously Presented) The security processor of claim 33 wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines.

35. (Previously Presented) The security processor of claim 32 wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip.

36. (Previously Presented) The security processor of claim 35 further comprising a control processor, coupled to the local data bus, for exception handling of the incoming and outgoing packets.

37. (Previously Presented) The security processor of claim 35 further comprising a key management engine coupled to the local data bus.

Application of: DAVIS, John M.
Serial No.: 12/697,112
Filed: January 29, 2010
Reply to Office Action of July 15, 2011

38. (Previously Presented) The security processor of claim 35 wherein the security processor handles substantially all security processing for the incoming and outgoing packets.

39. (Previously Presented) The security processor of claim 38 wherein the security processor further handles substantially all network processing for the incoming and outgoing packets.

40. (Previously Presented) A security processing system comprising:

(a) a security processor comprising:

a switching system to send outgoing packets and to receive incoming packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system;

a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;

a signature database; and

Application of: DAVIS, John M.
Serial No.: 12/697,112
Filed: January 29, 2010
Reply to Office Action of July 15, 2011

an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database; and

a local data bus coupled to the switching system; and

(b) a memory coupled to the local data bus.

41. (Previously Presented) The security processing system of claim 40 further comprising a modulo engine coupled to the local data bus.

42. (Previously Presented) The security processing system of claim 41 further comprising a key management engine coupled to the local data bus.

43. (Previously Presented) The security processing system of claim 40 wherein the memory and the security processor are within the same cryptographic boundary.

44. (Previously Presented) The security processing system of claim 40 wherein the security processor is formed on a single chip.

45. (Previously Presented) The security processing system of claim 40 further comprising:

a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface; and

a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory.

Application of: DAVIS, John M.
Serial No.: 12/697,112
Filed: January 29, 2010
Reply to Office Action of July 15, 2011

46. (Previously Presented) The security processing system of claim 45 wherein the translator performs steganographic translation of the received data.

47. (Previously Presented) The security processing system of claim 45 wherein the translator performs encryption translation of the received data.

48. (Previously Presented) The security processing system of claim 40 wherein the security processor is operable to (i) execute boot code to load firmware for execution by the security processor and
(ii) authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor.

49. (Previously Presented) A security processor to connect a trusted network to an un-trusted network for data packet communication, the security processor comprising:

- a first interface to couple to the trusted network and to the un-trusted network;

- a second interface to couple to a host processor;

- a switching system operable to selectively couple to the first interface or the second interface;

- a local data bus, coupled to the switching system;

- a plurality of packet engines coupled to the switching system to handle classification processing for incoming packets received by the plurality of packet engines from the switching system and outgoing packets sent by the plurality of packet engines to the switching system;

- a plurality of cryptographic cores each coupled to one of the plurality of packet engines to communicate with the switching system via the plurality of packet engines and

Application of: DAVIS, John M.
Serial No.: 12/697,112
Filed: January 29, 2010
Reply to Office Action of July 15, 2011

to provide encryption and decryption processing for packets received from and sent to the plurality of packet engines, wherein the plurality of packet engines are interposed between the switching system and the plurality of cryptographic cores;

a signature database;

an intrusion detection system coupled between the plurality of cryptographic cores and the plurality of packets engine and responsive to at least one packet matching a signature stored in the signature database and

a control processor, coupled to the local data bus, to control data packet flow within the security processor.

50. (Previously Presented) The security processor of claim 49 wherein the security processor is operable to act as a firewall to deny or accept a data packet and to implement a secure communication channel with another computing device in the untrusted network.

51. (Previously Presented) The security processor of claim 50 wherein the security processor implements data packet security and authentication functions to support the secure communication channel.

52. (Previously Presented) The security processor of claim 30 wherein the packet engine is further operable to add at least one of an IP header or a MAC address to the outgoing packets.

53. (Previously Presented) The security processor of claim 30 wherein the packet engine is further operable to remove an IP header from the incoming packets.

Application of: DAVIS, John M.
Serial No.: 12/697,112
Filed: January 29, 2010
Reply to Office Action of July 15, 2011

54. (Previously Presented) The security processor of claim 30, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

55. (Previously Presented) The security processing system of claim 40, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

56. (Previously Presented) The security processor of claim 49, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

Application of: DAVIS, John M.
Serial No.: 12/697,112
Filed: January 29, 2010
Reply to Office Action of July 15, 2011

REMARKS/ARGUMENTS

Favorable reconsideration of this application, in light of the following discussions, is respectfully requested.

Claims 1-29 have been cancelled, claims 30-56 are pending, and no claims have been amended. In the outstanding Office Action dated July 15, 2011, claims 30-56 were rejected on the grounds of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-22 of U.S. Patent No. 7,685,436. The Examiner also rejected claims 30-35, 37-44, and 49-53 under 35 U.S.C. § 103(a) as unpatentable over *Narad et al.* (U.S. Patent No. 6,157,955) in view of *Krishna et al.* (U.S. Publication No. 2003/0014627) in further view of *Ramsey et al.* (U.S. Patent No. 7,331,061). The Examiner also rejected claims 36, 45, and 47 under 35 U.S.C. § 103(a) as being unpatentable over *Narad* in view of *Krishna* in further view of *Ramsey* and *Savarda et al.* (U.S. Publication No. 2003/0196081). The Examiner also rejected claim 46 under 35 U.S.C. § 103(a) as being unpatentable over *Narad* in view of *Krishna* and *Ramsey*, and further in view of *Savarda* and *Carr et al.* (U.S. Patent No. 6,788,800). The Examiner also rejected claim 48 under 35 U.S.C. § 103(a) as being unpatentable over *Narad* in view of *Krishna* in further view of *Ramsey*, and *Girard* (U.S. Publication No. 2003/0084342). The Examiner also rejected claims 54-56 under 35 U.S.C. § 103(a) as being unpatentable

Application of: DAVIS, John M.
Serial No.: 12/697,112
Filed: January 29, 2010
Reply to Office Action of July 15, 2011

over *Narad* in view of *Krishna* in further view of *Ramsey*, and *Wu et al.* (U.S. Patent No. 7,493,659).

Applicant has filed a Terminal Disclaimer herewith to obviate the nonstatutory obviousness rejections.

Narad et al. does not teach or suggest “communicating the outgoing packets to the switching system via the packet engine. . . wherein the packet engine is interposed between the switching system and the cryptographic core,” as recited, for example in claim 30. In *Narad et al.*, the cited Classification Engine (CE) 106 is not interposed between the Crypto 112 and whatever the Examiner appears to consider the switching system. (See Figure 2). Also, it is not clear what the Examiner specifically considers to be the switching system. Applicants submit that the claims are in condition for allowance, but if this or any other rejection is to be maintained, Applicants respectfully request that the Examiner cite what is considered to be the switching system with specific components of the cited reference with respect to specific claim limitations for clarity, pursuant to 37 C.F.R. 1.104(c)(2) and M.P.E.P. 707.07(i). The other cited references are not contended to have this limitation.

At least for these reasons, Applicants submit that claims 30-56 are patentable. In view of the present remarks, the currently pending claims are believed to be in condition for allowance, and an early and favorable action to that effect is respectfully requested.

Application of: DAVIS, John M.
Serial No.: 12/697,112
Filed: January 29, 2010
Reply to Office Action of July 15, 2011

CHARGE STATEMENT: Deposit Account No. 501860, order no. 2551-0109.

The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 (missing or insufficiencies only) now or hereafter relative to this application and the resulting Official Document under Rule 20, or credit any overpayment, to our Accounting/ Order Nos. shown above, for which purpose a duplicate copy of this sheet is attached.

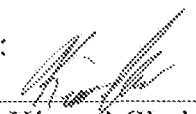
This CHARGE STATEMENT does not authorize charge of the issue fee until/unless an issue fee transmittal sheet is filed.

CUSTOMER NUMBER

42624

Respectfully submitted,

By:



Kimani Clark

Registration No.: 45,969

Davidson Berquist Jackson & Gowdey LLP
4300 Wilson Blvd., 7th Floor, Arlington, Virginia 22203
Main: (703) 894-6400 • FAX: (703) 894-6430

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT Application of:

DAVIS, John M.

Appl. S.N.: 12/697,112

Filing Date: January 29, 2010

Title: **SYSTEM AND METHOD FOR A SECURE
I/O INTERFACE**

Confirmation No.: 1325

Attorney Docket: 2551-0109

Group Art Unit: 2436

Examiner: TRAORE, Fatoumata

Date: December 12, 2011

**TERMINAL DISCLAIMER
(By Attorney)**

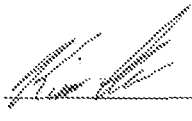
Hon. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The **Owner**, ITT Corporation, of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term **prior patent No. 7,685,436** (to which said **Owner** also has legal title) as the term of said **prior patent** is defined in 35 U.S.C. 154 to 156 and 173, and as the term of said **prior patent** is presently shortened (if at all) by any terminal disclaimer. The **Owner** hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the **Owner** does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 to 156 and 173 of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later: expires for failure to pay a maintenance fee; is held unenforceable; is found invalid by a court of competent jurisdiction; is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321; has all claims canceled by a reexamination certificate; is reissued; or is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

The undersigned petitioner, an attorney of record, is hereby acting for the **Owner**.

Atty. Sig.: 

Name: Kimani Clark

Date: December 6, 2011

☒ Terminal disclaimer fee under 37 CFR 1.20(d) is enclosed.

*Attorney and client: Please note on that other file and also this application file not to assign either separately in view of this disclaimer.

Electronic Patent Application Fee Transmittal

Application Number:	12697112			
Filing Date:	29-Jan-2010			
Title of Invention:	System and Method For a Secure I/O Interface			
First Named Inventor/Applicant Name:	John M. Davis			
Filer:	Kimani Clark			
Attorney Docket Number:	2551-0109			
Filed as Large Entity				
Utility under 35 USC 111(a) 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:				
Extension-of-Time:				
Extension - 2 months with \$0 paid	1252	1	560	EX-1013 ⁵⁶⁰

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Statutory or terminal disclaimer	1814	1	160	160
Total in USD (\$)				720

Electronic Acknowledgement Receipt

EFS ID:	11599163
Application Number:	12697112
International Application Number:	
Confirmation Number:	1325
Title of Invention:	System and Method For a Secure I/O Interface
First Named Inventor/Applicant Name:	John M. Davis
Customer Number:	42624
Filer:	Kimani Clark
Filer Authorized By:	
Attorney Docket Number:	2551-0109
Receipt Date:	12-DEC-2011
Filing Date:	29-JAN-2010
Time Stamp:	18:45:56
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$720
RAM confirmation Number	6095
Deposit Account	501860
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part (if appl.)	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	--------------------------	---------------------

1	Amendment/Req. Reconsideration-After Non-Final Reject	Response_2551-0109_12-9-11. pdf	24042 1b7636df98983b19af1298ac78ffd5a81b161643	no	1
Warnings:					
Information:					
2	Claims	Claims_2551-0109_12-9-11.pdf	268588 6b0c7029ff189f3c584f2821e26053761e9eaea6	no	7
Warnings:					
Information:					
3	Applicant Arguments/Remarks Made in an Amendment	Remarks_2551-0109_12-9-11. pdf	471268 6e6cb058693e814d781d0d39346536731dc8da5e	no	3
Warnings:					
Information:					
4	Terminal Disclaimer Filed	Terminal_Disclaimer_2551-010 9_12-9-11.pdf	612664 11e815ca81991ac07b11cc8f89b51bfe73e8f59d	no	1
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	31659 60899c8970ef87c9326bf1b12e353208200a606d	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			1408221		
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.					

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 12/697,112		Filing Date 01/29/2010		☐ To be Mailed	
---	--	--	--	--	---	--	----------------------------------	--	---------------------------------------	--

APPLICATION AS FILED – PART I					OTHER THAN				
(Column 1)		(Column 2)		SMALL ENTITY ☐		OR		SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	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), (l), 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(j))	minus 20 =	*	X \$	=	OR	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))									
			TOTAL			TOTAL			

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II					OTHER THAN						
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR		SMALL ENTITY	
AMENDMENT	12/12/2011	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(i))	* 27	Minus	** 27	= 0	X \$	=	OR	X \$60=	0	
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X \$	=	OR	X \$250=	0	
	☐ Application Size Fee (37 CFR 1.16(s))										
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR			
					TOTAL ADD'L FEE			OR	TOTAL ADD'L FEE	0	

(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR		SMALL ENTITY	
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	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))							OR			
					TOTAL ADD'L FEE			OR	TOTAL ADD'L 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.

Legal Instrument Examiner:
/BRENDA TURNER/

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

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.
-----------------	-------------	----------------------	---------------------	------------------

12/697,112

01/29/2010

John M. Davis

2551-0109

1325

42624

7590

07/15/2011

DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

EXAMINER

TRAORE, FATOUMATA

ART UNIT

PAPER NUMBER

2436

MAIL DATE

DELIVERY MODE

07/15/2011

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 12/697,112	Applicant(s) DAVIS ET AL.	
	Examiner FATOUMATA TRAORE	Art Unit 2436	

-- 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 01/29/2010.
- 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) 30-56 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) 30-56 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 29 January 2010 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 Draftperson'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 _____ | 6) ☐ Other: _____ |

DETAILED ACTION

1. This is in response to the original filing and preliminary amendments of January 29 , 2010. Claims 1-29 have been cancelled. Claims 30-56 have been added. Claims 30-56 are pending and have been considered below.

Priority

2. This application is a continuation of and claim priority to US patent application 10/903,785 filed 07/30/2004 now U.S. Patent No. 7,685,436 and claiming Priority from Provisional Application 60507976 filed 10/02/2003.

Oath/Declaration

3. The oath filed on 01/29/2010 complies with all the requirements set forth in MPEP 602 and therefore is accepted.

Drawings

4. The drawings filed on 01/29/2010 are accepted.

Specification

5. The specification filed on 01/29/2010 is accepted.

Double Patenting

6. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

7. Claims 30-56 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1- 22 of U.S. Patent No. 7,685,436. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-22 of US patent No. 7,685,436 contain every element of claims 30-56 of the present application. A comparison of the claims languages has been provided below for applicant review.

US 7,685,236	US 12/697,112
1. A security processor to process incoming packets and outgoing packets, the security processor comprising: a switching system to send the outgoing packets and receive the incoming packets; a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the	30. A security processor to process incoming packets and outgoing packets, the security processor comprising: a switching system to send the outgoing packets and receive the incoming packets; a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system;

incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines, and wherein the incoming packets and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines an egress path within the security processor upon exit from a corresponding cryptographic core; a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core; a signature database; and	a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core; a signature database; and
--	---

an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database. 2. The security processor of claim 1 wherein the packet engine is further operable to handle security context management processing for the incoming and outgoing packets. 3. The security processor of claim 1 further comprising: a local data bus coupled to the switching system; and a modulo engine coupled to the local data bus.	an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database. 31. The security processor of claim 30 wherein the packet engine is further operable to handle security context management processing for the incoming and outgoing packets. 32. The security processor of claim 30 further comprising: a local data bus coupled to the switching system; and a modulo engine coupled to the local data bus. 33. The security processor of claim 30 wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming
---	---

4. The security processor of claim 3 wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip. 5. The security processor of claim 4 further comprising a control processor, coupled to the local data bus, for exception handling of the incoming and outgoing packets. 6. The security processor of claim 4 further comprising a key management engine coupled	and outgoing packets to the security processor transit one of the plurality of packet engines. 34. The security processor of claim 33 wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines. 35. The security processor of claim 32 wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip. 36. The security processor of claim 35 further comprising a control processor, coupled to the local data bus, for exception handling of the incoming and outgoing packets. 37. The security processor of claim 35 further comprising a key management engine coupled
--	--

to the local data bus. 7. The security processor of claim 4 wherein the security processor handles substantially all security processing for the incoming and outgoing packets. 8. The security processor of claim 7 wherein the security processor further handles substantially all network processing for the incoming and outgoing packets. 9. The security processor of claim 1 wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of	to the local data bus. 38. The security processor of claim 35 wherein the security processor handles substantially all security processing for the incoming and outgoing packets. 39. The security processor of claim 38 wherein the security processor further handles substantially all network processing for the incoming and outgoing packets. 40. A security processing system comprising: (a) a security processor comprising: a switching system to send outgoing packets and to receive incoming packets; a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system; a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet
---	--

cryptographic cores after transiting one of the plurality of packet engines. 10. The security processor of claim 1 wherein the packet engine is further operable to add at least one of an IP header or a MAC address to the outgoing packets. 11. The security processor of claim 1 wherein the packet engine is further operable to remove an IP header from the incoming packets. 12. The security processor of claim 1, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet. 13. A security processing system comprising: (a) a security processor	engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core; a signature database; and an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database; and a local data bus coupled to the switching system; and (b) a memory coupled to the local data bus. 41. The security processing system of claim 40 further comprising a modulo engine coupled to the local data bus. 42. The security processing system of claim 41 further comprising a key management engine coupled to the local data bus. 43. The security processing system of claim 40
---	---

comprising: a switching system to send outgoing packets and to receive incoming packets; a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines, and wherein the incoming and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines an egress path within the security processor upon exit from a corresponding cryptographic core; a cryptographic core, coupled to the packet engine and	wherein the memory and the security processor are within the same cryptographic boundary. 44. The security processing system of claim 40 wherein the security processor is formed on a single chip. 45. The security processing system of claim 40 further comprising: a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface; and a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory. 46. The security processing system of claim 45 wherein the translator performs steganographic translation of the received data. 47. The security processing system of claim 45 wherein the translator performs encryption translation of the received data. 48. The security processing system of claim 40
--	---

receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core; a signature database; and an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database; and a local data bus coupled to the switching system; and (b) a memory coupled to the local data bus. 14. The security processing system of claim 13 further comprising a modulo engine coupled to the local data bus.	wherein the security processor is operable to (i) execute boot code to load firmware for execution by the security processor and (ii) authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor. 49. A security processor to connect a trusted network to an un-trusted network for data packet communication, the security processor comprising: a first interface to couple to the trusted network and to the un-trusted network; a second interface to couple to a host processor; a switching system operable to selectively couple to the first interface or the second interface; a local data bus, coupled to the switching system; a plurality of packet engines coupled to the switching system to handle classification processing for incoming packets received by the plurality of packet engines from the switching system and outgoing packets sent by the plurality of packet
---	---

15. The security processing system of claim 14 further comprising a key management engine coupled to the local data bus. 16. The security processing system of claim 13 wherein the memory and the security processor are within the same cryptographic boundary. 17. The security processing system of claim 13 wherein the security processor is formed on a single chip. 18. The security processing system of claim 13 further comprising: a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface; and a translator coupled to the memory interface to perform translation of	engines to the switching system; a plurality of cryptographic cores each coupled to one of the plurality of packet engines to communicate with the switching system via the plurality of packet engines and to provide encryption and decryption processing for packets received from and sent to the plurality of packet engines, wherein the plurality of packet engines are interposed between the switching system and the plurality of cryptographic cores; a signature database; an intrusion detection system coupled between the plurality of cryptographic cores and the plurality of packets engine and responsive to at least one packet matching a signature stored in the signature database and a control processor, coupled to the local data bus, to control data packet flow within the security processor. 50. The security processor of claim 49 wherein the security processor is operable to act as a firewall to deny or accept a data packet and to
---	--

data received by the memory interface from the memory. 19. The security processing system of claim 18 wherein the translator performs steganographic translation of the received data. 20. The security processing system of claim 18 wherein the translator performs encryption translation of the received data. 21. The security processing system of claim 13 wherein the security processor is operable to (i) execute boot code to load firmware for execution by the security processor and (ii) authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor.	implement a secure communication channel with another computing device in the untrusted network. 51. The security processor of claim 50 wherein the security processor implements data packet security and authentication functions to support the secure communication channel. 52. The security processor of claim 30 wherein the packet engine is further operable to add at least one of an IP header or a MAC address to the outgoing packets. 53. The security processor of claim 30 wherein the packet engine is further operable to remove an IP header from the incoming packets. 54. The security processor of claim 30, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet. 55. The security processing system of claim 40, wherein the at least one packet matching
---	--

22. The security processing system of claim 13, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.	the signature stored in the signature database comprises a plain text packet. 56. The security processor of claim 49, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.
--	---

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 30-35, 37-44 and 49-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narad et al US 6,157,955 A1 in view of Krishna et al US 2003/0014627 A1 in further view of Ramsey et al US 7,331,061 B1

Claims 30, 40 and 49: Narad et al teaches A security processor to connect a trusted network to an un-trusted network for data packet communication, the security processor comprising:

- i. a plurality of packet engines coupled to the switching system to handle classification processing for incoming packets received by the plurality of packet engines from the switching system and outgoing packets sent by the plurality of packet engines to the switching system (**col. 6 :line55 to col.7 :line, col.7 :lines 63-67 to col.8 :lines 30-65, Fig. 2-4; Each Ethernet MAC receives packets into buffers addressed by buffer points obtained from a producer-consumer ring and then passes the buffer to a Classification Engine for processing. There are four Classification Engines 208, 212, 238, and 242 which are microprogrammed processors optimized for the predicate analysis associated with packet filtering**);
- ii. a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core (**core (alternatively the action code 108 may choose to send the packet to the attached cryptographic processor (Crypto) 246 for encryption, decryption compression, decompression, security key management, parsing of IPSEC headers, or other associated functions) (column 8, line 67 to column 9, line 25)**);
- iii. a signature database(**col.14 :lines 20-67, hash table**);

- iv. a memory coupled to the local data bus(**col. 7: lines 15-20, A large parity-protected synchronous DRAM (SDRAM) buffer memory is provided, along with a PCI interface that is used for communication with the host (AP) and potentially for peer-to-peer communication among Policy Engines, e.g. for applications which route and switch).**

Narad et al fails to teach first interface, a second interface, a plurality of cryptographic cores nor an intrusion detection system coupled between the plurality of cryptographic cores and the plurality of packets engine and responsive to at least one packet matching a signature stored in the signature database and

Krishna et al teaches similar concept, which further teaches :

- a plurality of cryptographic core(**paragraph [0039], Fig.2 item 214, packet are distributed to a plurality of cryptographic engine with corresponding security associations).**

Therefore, it would have been obvious for one ordinary skill in the art at the time of the invention to modify the teaching of Narad et al with the addition feature of Krishna et al in order to provide an architecture for a cryptography accelerator chip that allows significant performance improvements over previous prior art designs, as suggested by Krishna et al (:paragraph [0010]).

The combined disclosure fails to teach, first interface, a second interface, an intrusion detection system coupled between the plurality of cryptographic cores and the plurality of packets engine and responsive to at least one packet matching a signature stored in the signature database.

Ramsey et al teaches similar concept, which further teaches:

- v. a first interface to couple to the trusted network and to the un-trusted network(**Fig.3, items 265, 270, col. 12:lines 11-13, The firewall 225 can limit access between an external or unsecured network 265 and a secured network 270 in order to prevent intrusion**);
 - vi. a second interface to couple to a host processor (**Fig. 3, item 260**);
 - vii. a switching system operable to selectively couple to the first interface or the second interface (**Figs. 3, item 215**);
 - viii. a local data bus, coupled to the switching system(**Figs. 3, item 230**);
 - ix. a control processor, coupled to the local data bus, to control data packet flow within the security processor(**Figs. 3. item 260, The integrated firewall and IDS system 215 can be connected to a controller 260**);
- an intrusion detection system coupled between the plurality of cryptographic cores and the plurality of packets engine and responsive to at least one packet matching a signature stored in the signature database (**col.15 :lines 5-30, col.18 :lines 25-40, Fig. 4, items 425-435, Fig. 5, items 538-542, the IDS can employ one or more signatures to determine whether a data packet can pass through the intrusion detection system. The IDS can also reject, accept or deny a packet based upon the comparison with the one or more signatures.**)

Therefore, it would have been obvious for one ordinary skill in the art at the time of the invention to modify the combination with the addition feature of Ramsey et al in order to

provide centralized control of the firewall, the IDS, and the AVS which can increase the speed at which packets are passed between a secured computer network and an external network, as suggested by Ramsey et al (col. 3 :lines25-40).

Claim 31: The combination further teaches wherein the packet engine is further operable to handle security context management processing for the incoming and outgoing packets (**Narad et al, col.6 :lines 40-65**).

Claims 32 and 41: The combination further teaches that the security processor comprises:

- i. A local data bus coupled to the switching system (**Narad et al, col.7, lines 40-50, PCI-to-PCI Bridges 312 controls child PCI bus 332 which provides the Application Processor 302 with connection to standard I/O devices through local I/O 314 and optionally to PCI expansion slots 316 into which additional PCI devices can be connected**); and
- ii. A modulo engine coupled to the local data bus (**Narad et al, Fig. 2., item 110**).

Claim 33: The combination further teaches wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines (**Narad et al col. 6 : line 55 to col.7 :line, col.7 :lines 63-67 to col.8 :lines 30-65, Fig. 2-4; There are four Classification Engines 208, 212, 238, and 242 which are microprogrammed processors optimized for the predicate analysis associated with packet filtering**)

Claim 34: The combination further teaches wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and

substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines (**Krishna et al, paragraph [0039], Fig.2 item 214, packet are distributed to a plurality of cryptographic engine with corresponding security associations**).

Claims 35 and 44: The combination further teaches wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip(**Narad et al, Fig. 2, items 106, 110 and 112**).

Claims 37 and 42: The combination further teaches that the security processor further comprises a key management engine coupled to the local data bus (**Narad et al, column 7, lines 1-5**).

Claim 38: The combination further teaches wherein the security processor handles substantially all security processing for the incoming and outgoing packets(**Narad et al, col. 7, lines 1-5**).

Claim 39: (The combination further teaches wherein the security processor further handles substantially all network processing for the incoming and outgoing packets (**Narad et al, col.6 :lines 40-65**).

Claims 43: The combination further teaches wherein the memory and the security processor are within the same cryptographic boundary (**Narad et al, col.7, lines 30-50 and Fig. 4, PCI-to-PCI Bridges 312 controls child PCI bus 332 which provides the Application Processor 302 with connection to standard I/O devices through local I/O**

314 and optionally to PCI expansion slots 316 into which additional PCI devices can be connected).

Claim 50: The combination further teaches wherein the security processor is operable to act as a firewall to deny or accept a data packet and to implement a secure communication channel with another computing device in the un-trusted network (**Narad et al, column 13 lines 25-58**).

Claim 51: The combination further teaches wherein the security processor implements data packet security and authentication functions to support the secure communication channel (**Narad et al, column 13, lines 25-58**).

Claim 52: The combination further teaches wherein the packet engine is further operable to add at least one of an IP header or MAC address to the outgoing packets (**Narad et al, column 20, lines 50-67**).

Claim 53: The combination further teaches wherein the packet engine is further operable to remove at least one of an IP header from the incoming packets (**Narad et al, column 20, lines 50-67**).

10. Claims 36, 45 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narad et al US 6,157,955 A1 in view of Krishna et al US 2003/0014627 A1 in further view of Ramsey et al US 7,331,061 B1 and Savarda et al US 2003/0196081.

Claim 36: The combination fails to teach a control processor coupled to the local data bus, for exception handling of the incoming and outgoing packets. However, Savarda et al teaches similar concepts, which further teaches a control processor coupled to the local

data bus, for exception handling of the incoming and outgoing packets (**paragraph [0031], The packet inspection/outbound policy module 108 may be configured with multiplexing circuitry to integrate the outbound and inbound packet streams into a single stream for pipeline processing in the packet co-processor 100. In addition, the packet inspection and or outbound policy module 108 may be further configured to inspect packet-objects to ensure their integrity**) .

Therefore, it would have been obvious for one ordinary skill in the art at the time of the invention to modify the combination with the addition feature of Savarda et al in order to maintain system integrity, as suggested by Savarda et al .

Claim 45: The combination further discloses:

a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface (**Narad et al, col. 7: lines 15-20, A large parity-protected synchronous DRAM (SDRAM) buffer memory is provided, along with a PCI interface that is used for communication with the host (AP) and potentially for peer-to-peer communication among Policy Engines, e.g. for applications which route and switch**));

The combination fails to teach a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory. However, Savarda et al discloses a system for processing a packet object using multiple pipelined processing modules, which further discloses

a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory (**the SAD contains**

parameter information about each SA. Such parameters may include the security protocol algorithms and keys for Authentication Header (AH) or Encapsulating Security Payload (ESP) security protocols, sequence numbers, protocol mode, and SA lifetime. For outbound packets, the SPD is consulted to determine if IPSec processing is required and/or if other processing or discarding of the packet is to be performed. If IPSec is required, then the outbound SAD is searched for an existing SA that matches the packet profile) (paragraphs [0004], [0009], [0024], and [0026]).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a translator. One would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

***Claim 47:* The combination further discloses that the translator performs encryption translation of the received data (Savarda et al, the cryptographic chip may perform the encryption, decryption, and/or authentication transforms as required. After completion of the cryptographic operations, the system processor may further process the packet to finish any remaining IPSec transforms, paragraphs [0007], 0026] and Fig.6).**

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt received data. One would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

Art Unit: 2436

11. Claim 46 is rejected under 35 U.S.C. 103(a) as being unpatentable over Narad et al US 6,157,955 A1 in view of Krishna et al US 2003/0014627 A1 and of Ramsey et al US 7,331,061 B1 in further view of Savarda et al US 2003/0196081 and Carr et al US 6,788,800.

Claim 46: The combination fails to teach a translator performing steganographic translation of the received data. However, Carr et al discloses a similar concept, which further discloses a step of performing steganographic translation of the received data (**col.1 :lines 38-49, it also steganographically embeds security data into product**). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combination such as to perform steganographic translation. One would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

12. Claim 48 is rejected under 35 U.S.C. 103(a) as being unpatentable over Narad et al US 6,157,955 A1 in view of Krishna et al US 2003/0014627 A1 in further view of Ramsey et al US 7,331,061 B1 and Girard (US 2003/0084342 A1).

Claim 48: The combination fails to teach wherein the security processor is operable to (i) execute boot code to load firmware for execution by the security processor and (ii) authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor.

Girard teaches similar concepts, which further teaches:

- i. execute boot code to load firmware for execution by the security processor(see paragraphs [0043], [0047], [0053]) and

- ii. authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor (**paragraphs [0043], [0047], [0053], The authentication stack enables boot code that is to be downloaded from a boot server to be authenticated prior to control being passed to the operating system of the booting computer system).**

Therefore, it would have been obvious for one ordinary skill in the art at the time of the invention to modify the combination with the addition feature of Girard in order to improve authentication for remote management of a computer system, as suggested by Girard paragraph [0014].

13. Claims 54-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narad et al US 6,157,955 A1 in view of Krishna et al US 2003/0014627 A1 in further view of Ramsey et al US 7,331,061 B1 and Wu et al US 7,493,659.

Claims 54, 55 and 56: The combination fails to teach wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet. Wu et al teaches similar concept, which further teaches wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet (**Wu et al column 5, lines 43-67**).

Therefore, it would have been obvious for one ordinary skill in the art at the time of the invention to modify the combination with the addition feature of Girard in order to accurately detect various intrusions hidden in high-speed network traffic, as suggested by Wu et al col. 2, lines 5-10.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

Thursday, July 07, 2011

/Fatoumata Traore/

Examiner, Art Unit 2436

Notice of References Cited	Application/Control No. 12/697,112		Applicant(s)/Patent Under Reexamination DAVIS ET AL.	
	Examiner FATOUMATA TRAORE		Art Unit 2436	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,157,955	12-2000	Narad et al.	709/228
*	B	US-2003/0014627	01-2003	Krishna et al.	713/153
*	C	US-7,331,061	02-2008	Ramsey et al.	726/23
*	D	US-2003/0196081	10-2003	Savarda et al.	713/153
*	E	US-6,788,800	09-2004	Carr et al.	382/100
*	F	US-2003/0084342	05-2003	Girard, Luke E.	713/201
*	G	US-7,493,659	02-2009	Wu et al.	726/26
	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.

<i>Index of Claims</i> 	Application/Control No. 12697112	Applicant(s)/Patent Under Reexamination DAVIS ET AL.
	Examiner FATOUMATA TRAORE	Art Unit 2436

✓	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	07/05/2011							
	1	-							
	2	-							
	3	-							
	4	-							
	5	-							
	6	-							
	7	-							
	8	-							
	9	-							
	10	-							
	11	-							
	12	-							
	13	-							
	14	-							
	15	-							
	16	-							
	17	-							
	18	-							
	19	-							
	20	-							
	21	-							
	22	-							
	23	-							
	24	-							
	25	-							
	26	-							
	27	-							
	28	-							
	29	-							
	30	✓							
	31	✓							
	32	✓							
	33	✓							
	34	✓							
	35	✓							
	36	✓							

<i>Index of Claims</i> 	Application/Control No. 12697112	Applicant(s)/Patent Under Reexamination DAVIS ET AL.
	Examiner FATOUMATA TRAORE	Art Unit 2436

✓	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	07/05/2011							
	37	✓							
	38	✓							
	39	✓							
	40	✓							
	41	✓							
	42	✓							
	43	✓							
	44	✓							
	45	✓							
	46	✓							
	47	✓							
	48	✓							
	49	✓							
	50	✓							
	51	✓							
	52	✓							
	53	✓							
	54	✓							
	55	✓							
	56	✓							

Search Notes 	Application/Control No. 12697112	Applicant(s)/Patent Under Reexamination DAVIS ET AL.
	Examiner FATOUMATA TRAORE	Art Unit 2436

SEARCHED			
Class	Subclass	Date	Examiner
370	218, 386-389, 468, limited by text search	7/5/2011	FT
713	153-154, 168, 187-189, limited by text search	7/5/2011	FT
726	22-25, limited by text search	7/5/2011	FT

SEARCH NOTES		
Search Notes	Date	Examiner
EAT, google patent and inventors name search performed.	7/5/2011	FT

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L4	2174823	execut\$3 with authentica\$3 with (boot near2 code bot- code bootcode)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/07 09:40
L5	114	execut\$3 with authentica\$3 with (boot near2 code bot- code bootcode)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/07 09:40
L6	8	execut\$3 with authentica\$3 with (boot near2 code bot- code bootcode) same secur\$3 with processor	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/07 09:41
L7	4	"7321061".pn. "6157955".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/07 10:24
S1	3	(switch\$3 router) with packet with (classificat \$3 classif\$4) same cryptograph\$3 with (encrypt\$3 decrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 10:35
S2	49	(switch\$3 router) with packet with (classificat \$3 classif\$4) same (cryptograph\$3 encrypt \$3 decrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 10:36
S3	8364	370/389.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 11:27

S4	208	(switch\$3) same (classificat\$3 classif\$4) same (cryptograph\$3 encrypt\$3 decrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 11:28
S5	304	(switch\$3) same (classificat\$3 classif\$4) same (hash\$3 cryptograph\$3 encrypt \$3 decrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 11:28
S6	26	S3 and S5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 11:28
S7	256	packet with (engine classificat\$3 classif\$4) same (secur\$3 cryptograph\$3 encrypt \$3) with (engine core) same (signature intrus \$3 virus wornpattern)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 15:19
S8	14000	370/468.ccls. 370/218. ccls. 370/386-388.ccls. 370/389.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 15:21
S9	11	S7 and S8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 15:21
S10	14788	713/153-154.ccls. 713/168.ccls. 713/187- 189.ccls. 726/22-25. ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 16:11
S11	32	packet with engine same(classificat\$3 classif\$4) same (secur \$3 cryptograph\$3 encrypt\$3) with (engine core) same (signature intrus\$3 virus worn pattern) same detect\$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 16:13

S12	201	packet with engine same(classificat\$3 classif\$4) same (secur\$3 cryptograph\$3 encrypt\$3) with (engine core)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 16:19
S13	35	S12 and (S8 S10)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/05 16:19
S14	18	("20020066014" "20020108059" "20030014627" "20030196081" "20040010545" "5432950" "5737760" "5892899" "5940626" "6041122" "6049876" "6101255" "6157955" "6788800" "6983366" "7095716" "7493659").PN. OR ("7685436").URPN.	US-PGPUB; USPAT; USOCR	ADJ	ON	2011/07/05 16:25
S15	2	"7685436".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/06 10:59
S16	2	"20100169636".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/06 11:10
S17	0	packet with (engine classificat\$3 classif\$4) same pural\$3 same (secur\$3 cryptograph\$3 encrypt\$3) with (engine core)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/06 14:49
S18	0	packet with (engine classificat\$3 classif\$4) same pural\$3 same (secur\$3 cryptograph\$3 encrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/06 14:49

S19	275	packet with (engine classificat\$3 classif\$4) same plural\$3 same (secur\$3 cryptograph \$3 encrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/06 14:49
S20	141	packet with (engine classificat\$3 classif\$4) same plural\$3 same (secur\$3 cryptograph \$3 encrypt\$3) with (engine core)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/06 14:50
S21	2	"7493659".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/06 16:12

7/ 7/ 2011 11:08:15 AM



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. 1325

SERIAL NUMBER 12/697,112	FILING or 371(c) DATE 01/29/2010 RULE	CLASS 713	GROUP ART UNIT 2436	ATTORNEY DOCKET NO. 2551-0109	
APPLICANTS John M. Davis, Brentwood, TN; Richard Takahashi, Phoenix, AZ; ** CONTINUING DATA ***** This application is a CON of 10/903,785 07/30/2004 PAT 7,685,436 which claims benefit of 60/507,976 10/02/2003 ** FOREIGN APPLICATIONS ***** ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** 03/01/2010					
Foreign Priority claimed ☐ Yes ☒ No 35 USC 119(a-d) conditions met ☐ Yes ☒ No Verified and /FATOUMATA TRAORE/ Acknowledged Examiner's Signature	☐ Met after Allowance FT Initials	STATE OR COUNTRY TN	SHEETS DRAWINGS 10	TOTAL CLAIMS 27	INDEPENDENT CLAIMS 3
ADDRESS DAVIDSON BERQUIST JACKSON & GOWDEY LLP 4300 WILSON BLVD., 7TH FLOOR ARLINGTON, VA 22203 UNITED STATES					
TITLE System and Method For a Secure I/O Interface					
FILING FEE RECEIVED 1454	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		



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	ATTY. DOCKET NO./TITLE
12/697,112	01/29/2010	John M. Davis	2551-0109

CONFIRMATION NO. 1325

PUBLICATION NOTICE

42624

DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203



OC000000042381526

Title:System and Method For a Secure I/O Interface

Publication No.US-2010-0169636-A1

Publication Date:07/01/2010

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <http://pair.uspto.gov/>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



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	TOT CLAIMS	IND CLAIMS
12/697,112	01/29/2010	2115	1454	2551-0109	27	3

CONFIRMATION NO. 1325

42624

DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

UPDATED FILING RECEIPT



Date Mailed: 03/23/2010

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 submit a written request for a Filing Receipt Correction. 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)

John M. Davis, Brentwood, TN;
Richard Takahashi, Phoenix, AZ;

Power of Attorney: The patent practitioners associated with Customer Number 42624

Domestic Priority data as claimed by applicant

This application is a CON of 10/903,785 07/30/2004 PAT 7,685,436
which claims benefit of 60/507,976 10/02/2003

Foreign Applications

If Required, Foreign Filing License Granted: 03/01/2010

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/697,112**

Projected Publication Date: 07/01/2010

Non-Publication Request: No

Early Publication Request: No

Title

System and Method For a Secure I/O Interface

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).

FACSIMILE TRANSMISSION

RECEIVED
CENTRAL FAX CENTER

MAR 11 2010

To: United States Patent and Trademark Office

Facsimile No.: (571) 273-8300

From: Davidson Berquist Jackson & Gowdey, LLP

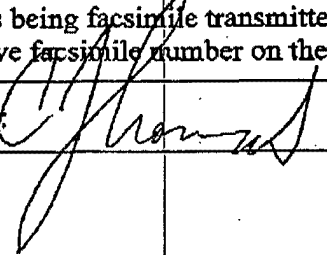
No. of Pages (including this page): 4

**IF YOU DO NOT RECEIVE CLEARLY ALL PAGES, PLEASE CONTACT US
IMMEDIATELY BY TELEPHONE AT (703) 894-6400.****USPTO: PLEASE ACKNOWLEDGE CLEAR RECEIPT OF ALL PAGES INDICATED
ABOVE BY FAXING THIS PAGE BACK TO (703) 894-6430**

In re PATENT APPLICATION OF:	Attorney Docket: 2551-0109
DAVIS, John M. et al.	Group Art Unit: 2431
Application Serial No.: 12/697,112	Examiner: Unassigned
Application Filing Date: January 29, 2010	Date: March 11, 2010
Title: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE	Confirmation No.: 1325

Name(s) of paper(s) being transmitted:

- Reply to Notice to File Missing Parts of Nonprovisional Application
- Notice to File Missing Parts of Nonprovisional Application (copy)

CERTIFICATE OF FACSIMILE TRANSMISSION			
I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office at the above facsimile number on the date shown below.			
Name:	Chris J. Thomas	Signature: 	Date: 03-11-10

CUSTOMER NUMBER

42624

DAVIDSON BERQUIST JACKSON & GOWDEY, LLP
4300 WILSON BLVD., 7TH FLOOR, ARLINGTON, VA 22203
703.894.6400 (main) • 703.894.6430 (Fax)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED
CENTRAL EXAM CENTER

MAR 11 2010

In re PATENT APPLICATION OF:

DAVIS, John M. et al.

Application Serial No.: 12/697,112

Application Filing Date: January 29, 2010

Title: SYSTEM AND METHOD FOR A SECURE
I/O INTERFACE

Attorney Docket: 2551-0109

Group Art Unit: 2431

Examiner: Unassigned

Date: March 11, 2010

Confirmation No.: 1325

RESPONSE TO NOTICE TO FILE MISSING PARTS
OF NONPROVISIONAL APPLICATIONMail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the *Notice to File Missing Parts of Nonprovisional Application* dated March 2, 2010, attached please find the following documents which complete the filing of the above-identified patent application.

- ☒ Notice to File Missing Parts of Nonprovisional Application (copy)
- ☒ Please charge Deposit Account No. 501860, Order No. 2551-0109 in the amount of \$364 to cover the additional claim fees for a non-small entity.

Our Deposit Account No.: 501860

Our Order No. (Client-Matter No.): 2551-0109

CHARGE STATEMENT: The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 (missing or insufficiencies only) now or hereafter relative to this application and the resulting Official document under Rule 20, or credit any overpayment, to our Account/Order Nos. (or Attorney Docket No.) shown in the heading hereof for which purpose a duplicate copy of this paper is attached.

This Charge Statement does not authorize charge of the issue fee until/unless an issue fee transmittal form is filed.

CUSTOMER NUMBER
42624

Respectfully submitted,


Kimani Clark

Registration No.: 45,969

Davidson Berquist Jackson & Gowdey LLP
4300 Wilson Blvd., 7th Floor
Arlington, VA 22203
Phone 703.894.6400/Fax 703.894.6430

RECEIVED
CENTRAL FAX CENTER
MAR 11 2010

COPY



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address COMMISSIONER FOR PATENTS
P.O. Box 1480
Alexandria, Virginia 22304-1480
703/292-2000

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/697,112	01/29/2010	John M. Davis	2551-0109

CONFIRMATION NO. 1325

42624

DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

RECEIVED

FORMALITIES LETTER

MAR 3 2010



0000000040361950

DAVIDSON BERQUIST

Date Mailed: 03/02/2010 DJ

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given TWO MONTHS from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- Additional claim fees of \$364 as a non-small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is \$364 for a non-small entity

- Total additional claim fee(s) for this application is \$364
- \$364 for 7 total claims over 20.

03/12/2010 HMARZ11 00000019 501860 12697112

01 FC:1202 364.00 DA

page 1 of 2

COPY

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
<https://portal.uspto.gov/authenticate/AuthenticateUserLocalEPE.html>

For more information about EFS-Web please call the USPTO Electronic Business Center at 1-866-217-9197 or
visit our website at <http://www.uspto.gov/ebc>.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/Ilvuong/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

page 2 of 2

FACSIMILE TRANSMISSION

RECEIVED
CENTRAL FAX CENTER

MAR 11 2010

To: United States Patent and Trademark Office

Facsimile No.: (571) 273-8300

From: Davidson Berquist Jackson & Gowdey, LLP

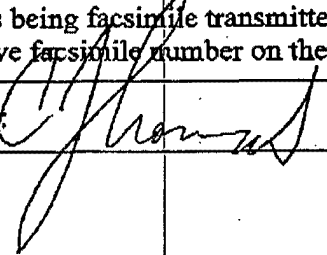
No. of Pages (including this page): 4

**IF YOU DO NOT RECEIVE CLEARLY ALL PAGES, PLEASE CONTACT US
IMMEDIATELY BY TELEPHONE AT (703) 894-6400.****USPTO: PLEASE ACKNOWLEDGE CLEAR RECEIPT OF ALL PAGES INDICATED
ABOVE BY FAXING THIS PAGE BACK TO (703) 894-6430**

In re PATENT APPLICATION OF:	Attorney Docket: 2551-0109
DAVIS, John M. et al.	Group Art Unit: 2431
Application Serial No.: 12/697,112	Examiner: Unassigned
Application Filing Date: January 29, 2010	Date: March 11, 2010
Title: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE	Confirmation No.: 1325

Name(s) of paper(s) being transmitted:

- Reply to Notice to File Missing Parts of Nonprovisional Application
- Notice to File Missing Parts of Nonprovisional Application (copy)

CERTIFICATE OF FACSIMILE TRANSMISSION			
I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office at the above facsimile number on the date shown below.			
Name:	Chris J. Thomas	Signature: 	Date: 03-11-10

CUSTOMER NUMBER

42624

DAVIDSON BERQUIST JACKSON & GOWDEY, LLP
4300 WILSON BLVD., 7TH FLOOR, ARLINGTON, VA 22203
703.894.6400 (main) • 703.894.6430 (Fax)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED
CENTRAL EXAMINER

MAR 11 2010

In re PATENT APPLICATION OF:

DAVIS, John M. et al.

Application Serial No.: 12/697,112

Application Filing Date: January 29, 2010

Title: SYSTEM AND METHOD FOR A SECURE
I/O INTERFACE

Attorney Docket: 2551-0109

Group Art Unit: 2431

Examiner: Unassigned

Date: March 11, 2010

Confirmation No.: 1325

RESPONSE TO NOTICE TO FILE MISSING PARTS
OF NONPROVISIONAL APPLICATIONMail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the *Notice to File Missing Parts of Nonprovisional Application* dated March 2, 2010, attached please find the following documents which complete the filing of the above-identified patent application.

- ☒ Notice to File Missing Parts of Nonprovisional Application (copy)
- ☒ Please charge Deposit Account No. 501860, Order No. 2551-0109 in the amount of \$364 to cover the additional claim fees for a non-small entity.

Our Deposit Account No.: 501860

Our Order No. (Client-Matter No.): 2551-0109

CHARGE STATEMENT: The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 (missing or insufficiencies only) now or hereafter relative to this application and the resulting Official document under Rule 20, or credit any overpayment, to our Account/Order Nos. (or Attorney Docket No.) shown in the heading hereof for which purpose a duplicate copy of this paper is attached.

This Charge Statement does not authorize charge of the issue fee until/unless an issue fee transmittal form is filed.

CUSTOMER NUMBER
42624

Respectfully submitted,


Kimani Clark

Registration No.: 45,969

Davidson Berquist Jackson & Gowdey LLP
4300 Wilson Blvd., 7th Floor
Arlington, VA 22203
Phone 703.894.6400/Fax 703.894.6430

RECEIVED
CENTRAL FAX CENTER
MAR 11 2010

COPY



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address COMMISSIONER FOR PATENTS
P.O. Box 1480
Alexandria, Virginia 22304-1480
703/292-2000

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/697,112	01/29/2010	John M. Davis	2551-0109

CONFIRMATION NO. 1325

42624

DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

RECEIVED

FORMALITIES LETTER

MAR 3 2010



0000000040361950

DAVIDSON BERQUIST

Date Mailed: 03/02/2010 DJ

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given TWO MONTHS from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- Additional claim fees of \$364 as a non-small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is \$364 for a non-small entity

- Total additional claim fee(s) for this application is \$364
- \$364 for 7 total claims over 20.

03/12/2010 HMARZ11 00000019 501860 12697112

01 FC:1202 364.00 DA

page 1 of 2

COPY

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
<https://portal.uspto.gov/authenticate/AuthenticateUserLocalEPE.html>

For more information about EFS-Web please call the USPTO Electronic Business Center at 1-866-217-9197 or
visit our website at <http://www.uspto.gov/ebc>.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/Ilvuong/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

page 2 of 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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/697,112	01/29/2010	John M. Davis	2551-0109

CONFIRMATION NO. 1325

FORMALITIES LETTER

42624
DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203



Date Mailed: 03/02/2010

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given TWO MONTHS from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- Additional claim fees of **\$364** as a non-small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **\$364** for a non-small entity

- Total additional claim fee(s) for this application is **\$364**
 - **\$364** for 7 total claims over 20.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
<https://portal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html>

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at <http://www.uspto.gov/ebc>.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/llvuong/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



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	TOT CLAIMS	IND CLAIMS
12/697,112	01/29/2010	2431	1090	2551-0109	27	3

CONFIRMATION NO. 1325

42624

DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

FILING RECEIPT



OC000000040361989

Date Mailed: 03/02/2010

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 submit a written request for a Filing Receipt Correction. 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)

John M. Davis, Brentwood, TN;
Richard Takahashi, Phoenix, AZ;

Power of Attorney: The patent practitioners associated with Customer Number 42624

Domestic Priority data as claimed by applicant

This application is a CON of 10/903,785 07/30/2004
which claims benefit of 60/507,976 10/02/2003

Foreign Applications

If Required, Foreign Filing License Granted: 03/01/2010

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/697,112**

Projected Publication Date: 06/10/2010

Non-Publication Request: No

Early Publication Request: No

Title

System and Method For a Secure I/O Interface

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).



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	ATTY. DOCKET NO./TITLE
12/697,112	01/29/2010	John M. Davis	2551-0109

42624
DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

CONFIRMATION NO. 1325
POA ACCEPTANCE LETTER



Date Mailed: 03/02/2010

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 01/29/2010.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/ttu/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT APPLICATION OF:	Confirmation No.: Unassigned
DAVIS, John M. et al.	Atty. Dkt.: 2551-0109
Application No.: New Application	Art Unit: Unassigned
Filing Date: Herewith	Examiner: Unassigned
Title: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE	Date: January 29, 2010

PRELIMINARY AMENDMENT

Hon. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Please preliminarily amend the subject application as follows prior to fee calculation
and examination:

Amendments to the specification begin on page 2.

Amendments to the claims are reflected in the listing of the claims which begins on
page 3.

Remarks begin on page 8 .

Application of: DAVIS, John M. et al.
Atty Docket: 2551-0109
Application S.N.: New Application
Page 2 of 8

AMENDMENTS TO THE SPECIFICATION

Please replace the title on line 3 and the immediately following paragraph that begins on line 5 with the following rewritten title and paragraph:

“This application is a continuation of and claims benefit to U.S. Patent Application No. 10/903,785, filed on July 30, 2004, which is a non-provisional application claiming benefit under 35 U.S.C. sec. 119(e) of U.S. Provisional Application Serial No. 60/507,976, filed October 2, 2003 ~~10/02/2003 (titled SYSTEM AND METHOD FOR A SECURE I/O INTERFACE by John M. Davis et al.’ attorney docket no. 4224-25PRV)~~, both of which are ~~[[is]]~~ incorporated by reference herein.”

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

1-29. (Canceled)

30. (New) A security processor to process incoming packets and outgoing packets, the security processor comprising:

- a switching system to send the outgoing packets and receive the incoming packets;
- a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system;
- a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;
- a signature database; and
- an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.

31. (New) The security processor of claim 30 wherein the packet engine is further operable to handle security context management processing for the incoming and outgoing packets.

32. (New) The security processor of claim 30 further comprising:

- a local data bus coupled to the switching system; and
- a modulo engine coupled to the local data bus.

33. (New) The security processor of claim 30 wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines.

34. (New) The security processor of claim 33 wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines.
35. (New) The security processor of claim 32 wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip.
36. (New) The security processor of claim 35 further comprising a control processor, coupled to the local data bus, for exception handling of the incoming and outgoing packets.
37. (New) The security processor of claim 35 further comprising a key management engine coupled to the local data bus.
38. (New) The security processor of claim 35 wherein the security processor handles substantially all security processing for the incoming and outgoing packets.
39. (New) The security processor of claim 38 wherein the security processor further handles substantially all network processing for the incoming and outgoing packets.
40. (New) A security processing system comprising:
 (a) a security processor comprising:
 a switching system to send outgoing packets and to receive incoming packets;
 a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system;
 a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the

outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;

a signature database; and

an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database; and

a local data bus coupled to the switching system; and

(b) a memory coupled to the local data bus.

41. (New) The security processing system of claim 40 further comprising a modulo engine coupled to the local data bus.

42. (New) The security processing system of claim 41 further comprising a key management engine coupled to the local data bus.

43. (New) The security processing system of claim 40 wherein the memory and the security processor are within the same cryptographic boundary.

44. (New) The security processing system of claim 40 wherein the security processor is formed on a single chip.

45. (New) The security processing system of claim 40 further comprising:

a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface; and

a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory.

46. (New) The security processing system of claim 45 wherein the translator performs steganographic translation of the received data.

47. (New) The security processing system of claim 45 wherein the translator performs encryption translation of the received data.

48. (New) The security processing system of claim 40 wherein the security processor is operable to (i) execute boot code to load firmware for execution by the security processor and (ii) authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor.

49. (New) A security processor to connect a trusted network to an un-trusted network for data packet communication, the security processor comprising:

- a first interface to couple to the trusted network and to the un-trusted network;
- a second interface to couple to a host processor;
- a switching system operable to selectively couple to the first interface or the second interface;
- a local data bus, coupled to the switching system;
- a plurality of packet engines coupled to the switching system to handle classification processing for incoming packets received by the plurality of packet engines from the switching system and outgoing packets sent by the plurality of packet engines to the switching system;
- a plurality of cryptographic cores each coupled to one of the plurality of packet engines to communicate with the switching system via the plurality of packet engines and to provide encryption and decryption processing for packets received from and sent to the plurality of packet engines, wherein the plurality of packet engines are interposed between the switching system and the plurality of cryptographic cores;
- a signature database;
- an intrusion detection system coupled between the plurality of cryptographic cores and the plurality of packets engine and responsive to at least one packet matching a signature stored in the signature database and

a control processor, coupled to the local data bus, to control data packet flow within the security processor.

50. (New) The security processor of claim 49 wherein the security processor is operable to act as a firewall to deny or accept a data packet and to implement a secure communication channel with another computing device in the untrusted network.

51. (New) The security processor of claim 50 wherein the security processor implements data packet security and authentication functions to support the secure communication channel.

52. (New) The security processor of claim 30 wherein the packet engine is further operable to add at least one of an IP header or a MAC address to the outgoing packets.

53. (New) The security processor of claim 30 wherein the packet engine is further operable to remove an IP header from the incoming packets.

54. (New) The security processor of claim 30, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

55. (New) The security processing system of claim 40, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

56. (New) The security processor of claim 49, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

Electronic Patent Application Fee Transmittal

Application Number:				
Filing Date:				
Title of Invention:	System and Method For a Secure I/O Interface			
First Named Inventor/Applicant Name:	John M. Davis			
Filer:	Kimani Clark			
Attorney Docket Number:	2551-0109			
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Utility application filing	1011	1	330	330
Utility Search Fee	1111	1	540	540
Utility Examination Fee	1311	1	220	220
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

EX-1013

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1090

Electronic Acknowledgement Receipt

EFS ID:	6915681
Application Number:	12697112
International Application Number:	
Confirmation Number:	1325
Title of Invention:	System and Method For a Secure I/O Interface
First Named Inventor/Applicant Name:	John M. Davis
Customer Number:	42624
Filer:	Kimani Clark
Filer Authorized By:	
Attorney Docket Number:	2551-0109
Receipt Date:	29-JAN-2010
Filing Date:	
Time Stamp:	19:35:51
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 1090
RAM confirmation Number	13918
Deposit Account	501860
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part (if appl.)	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	--------------------------	---------------------

1	Specification	Spec_01-29-10_2551-0109.pdf	1870163	no	35
			a36e8c6face3bebb87176627e282e46e485cfed7		
Warnings:					
Information:					
2	Claims	Claims_01-29-10_2551-0109.pdf	166100	no	5
			5d518a0c2d2327588a9c7df4519ffdd443f9a937		
Warnings:					
Information:					
3	Abstract	Abstract_01-29-10_2551-0109.pdf	21438	no	1
			3973cedb294497a491ddfc1fb6c6ead737455b03		
Warnings:					
Information:					
4	Drawings-only black and white line drawings	Drawings_01-29-10_2551-0109.pdf	178193	no	10
			f5f561e17e0795d394c57d603a48e2d3e06b5ed8		
Warnings:					
Information:					
5	Oath or Declaration filed	Dec_01-29-10_2551-0109.pdf	109230	no	2
			32219dc3bcfa65d5251aaec03ed1244afa8db1868		
Warnings:					
Information:					
6	Applicant Arguments/Remarks Made in an Amendment	PA_Remarks_2551-0109_1-29-10.pdf	102819	no	1
			713e3aca98ea79557bea4f36eeFeb9991b12104c		
Warnings:					
Information:					
7	Power of Attorney	POA_Change_2551-0109_1-29-10.pdf	389692	no	6
			9775b6f11a541b7eb3f49b56c1e51badfdfe1634		
Warnings:					
Information:					
8	Preliminary Amendment	Prelim_Amend_2551-0109_1-29-10.pdf	66382	no	1
			3b601ad415f78b014754e5dd3a3884f313bb75c		
Warnings:					
Information:					
9	Specification	PA_Spec_2551-0109_1-29-10.pdf	67755	no	1
			353ef2370552659cd24fa82e854b9cdfaf54bf0f2		
Warnings:					
Information:					

EX-1013

10	Claims	PA_Claims_2551-0109_1-29-10.pdf	576077 038ddfdc4ba162de5a707dbf9f89f061d3417cc7	no	5
Warnings:					
Information:					
11	Fee Worksheet (PTO-875)	fee-info.pdf	32437 567fa26628aebff53535f3b6a0bb5162ed2bd7ec	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			3580286		
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.					

SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

Related Application

5 This application is a non-provisional application claiming benefit under 35 U.S.C. sec. 119(e) of U.S. Provisional Application Serial No. 60/507,976, filed 10/02/2003 (titled SYSTEM AND METHOD FOR A SECURE I/O INTERFACE by John M. Davis et al.; attorney docket no. 4224-25PRV), which is incorporated by reference herein.

Field of the Invention

10 The present invention relates in general to data communications, and particularly to secure cryptographic communications, and more particularly to a secure input/output (I/O) interface system for a computing device such as, for example, a host
15 computer communicating using internet protocol (IP) data packets or other datagrams.

Background of the Invention

20 Trusted internal computer networks are typically protected from un-trusted external computer networks by routers or other gateway systems that provide different types of firewall functionality. Security processing performed by related systems may also provide additional protection. For example, a computer in the internal network may establish a virtual private network (VPN) session with a computer in the external network. The host processor of the computer or a dedicated security processor coupled
25 to the router or other gateway system typically performs the security processing necessary to support the VPN. In addition, a dedicated network processor may be coupled to the security processor and/or the host processor to handle network packet processing functions.

30 Network interface cards (NIC) often provide a computer's physical connection to its trusted internal network. More specifically, a NIC connects a personal computer,

server or workstation to a local area network (LAN) and has two primary interfaces: the network interface and the host bus interface. NICs are typically low-cost ASIC-based products designed for simple buffering and data transfer.

It is desired that communications to and from a trusted computer be secure and
5 that communication speeds be improved. However, providing firewall, network processing and security functionalities in different systems, which are often made by different manufacturers, provides increased opportunities for snooping or other techniques that may permit an unauthorized person to gain access to ongoing communications or to discover key or other security data when it is exchanged between
10 subsystems. For example, if certain security functions associated with securing communications over a NIC are handled by the computer's host processor and/or by other computers on the internal network, then the communications may be more easily attacked or otherwise accessed or interfered with by an unauthorized person, who may attempt to exploit easier snooping access or other vulnerabilities presented by the
15 processing of security functions by a host processor or another server on the network.

The use of different systems to perform different portions of security and network processing also requires additional processing and interfaces for coordinating communications processing between the systems. Such additional processing and interfaces increase processing demands, which limits communication speed and
20 increases the size of the chips and systems necessary to implement secure communications.

As a specific example, when using a separate security processor and I/O card connected to a backplane bus of a host, input encrypted data is typically transferred using direct memory access (DMA) from the I/O card, under control of the host, to
25 memory coupled to the host. Then, the data is transferred by DMA from the memory via the host to the security processor. After the data is decrypted, and possibly a public key generated, the data is transferred by DMA from the security processor to memory again via the host. Finally, the decrypted data is transferred by DMA from the memory to the I/O card for output to another destination. This large number of data transfers

creates a bottleneck on the backplane bus, which includes multiple data transactions, many interrupts, and heavy usage of memory to store the data.

The use of secure communications in broadband networks will increasingly require high-speed security and network processing. Further, the use of portable
5 devices that securely connect to networks will require smaller chip and system sizes that can meet security and networking processing demands while at the same time retaining easy portability. In light of the foregoing, there is a general need for a secure I/O interface system and method that improve the security of communications to and from
10 trusted hardware, improve communication speed, reduce the number of different systems required for secure communications, and reduce the extent of the bottleneck on the backplane bus.

Brief Description of the Drawings

15 The invention is pointed out with particularity in the appended claims. However, for a more complete understanding of the present invention, reference is now made to the following figures, wherein like reference numbers refer to similar items throughout the figures:

FIG. 1 illustrates a simplified functional block diagram of a system architecture
20 suitable for use in implementing embodiments of a security processing system and method in accordance with an embodiment of the present invention;

FIG. 2 illustrates a high-level simplified functional block diagram of a security processor in accordance with an embodiment of the present invention;

FIG. 3 illustrates a more-detailed functional block diagram of a network
25 intrusion detection system used in a portion of the security processor of FIG. 2 in accordance with an embodiment of the present invention;

FIG. 4 illustrates a simplified flow diagram of packet flow in the security processor of FIG. 2;

FIG. 5 illustrates a data representation convention used herein;

FIG. 6 is a block diagram illustrating the GDMA block, which incorporates an EDMA block, in accordance with an embodiment of the present invention;

FIG. 7 is a block diagram illustrating the EDMA block in accordance with an embodiment of the present invention;

5 FIG. 8 is a block diagram illustrating the ER block in accordance with an embodiment of the present invention;

FIG. 9 is a block diagram illustrating the OPC interfaces in accordance with an embodiment of the present invention;

10 FIG. 10 is an internal block diagram illustrating the OPC in accordance with an embodiment of the present invention;

FIG. 11 is a block diagram illustrating the relationship of the ER block to the cryptographic core and memory in accordance with an embodiment of the present invention; and

15 FIG. 12 is a block diagram illustrating the relationship between the ER block, the EDMA block, the cryptographic core, and memory in accordance with an embodiment of the present invention.

The exemplification set out herein illustrates an embodiment of the invention in one form, and such exemplification is not intended to be construed as limiting in any manner.

20

Detailed Description of the Drawings

The following description and the drawings illustrate specific embodiments of the invention sufficiently to enable those skilled in the art to practice it. Other embodiments may incorporate structural, logical, electrical, process and other changes. Examples merely typify possible variations. Individual components and functions are optional unless explicitly required, and the sequence of operations may vary. Portions and features of some embodiments may be included in or substituted for those of others. The scope of the invention encompasses the full ambit of the claims and all available equivalents.

25

The present invention is described and claimed herein primarily with reference to the processing of "packets". However, as used herein, it is intended that the term "packet" or "packets" have the meaning and scope of the more generic term "datagram" or "datagrams."

5 In one embodiment, the present invention provides, among other things, a system and method for connecting a trusted piece of hardware, such as, for example, a personal computer, server, router, personal digital assistant (PDA), cellular phone, network-enabled device or other computing or communication device, to a network using an I/O interface or system that provides improved security for all or substantially
10 all communications received and sent by the trusted hardware. The secure I/O system preferably may perform all security and network processing necessary to maintain secure communications by the hardware with other devices on internal or external networks. Alternatively, it may perform the network security processing essential to be segregated from other processing to ensure safe (i.e., protected) and efficient system or
15 device operation. For example, the secure I/O system permits establishing a VPN with a computer on an external network. The VPN may be established using, for example, the standard IPsec internet protocol security, as described in "Request for Comment" (RFC) 2401, 2402 and 2406, which are incorporated herein by reference.

 The secure I/O system of the present invention permits performing all or
20 substantially all network processing functions and off-loads all or substantially all security functions associated with network address translation (NAT), the providing of a firewall, intrusion detection/protection system functionality, traffic proxying, and encryption from a host or network processor onto a single system or card, for example a NIC. This card may be inserted into each of the servers and other computers connected
25 on an internal network.

 The security processing performed by the secure I/O system typically may include encryption, decryption, signing and verification of packets at, for example, 100 megabits per second full duplex and greater speeds. For example, the secure I/O system of the present invention may provide wire speed performance, for example, of about 2-3

gigabits per second firewall and VPN throughput. The secure I/O system may simplify the deployment of security solutions on open platforms and appliances.

The elements that implement the various embodiments of the present invention are described below, in some cases at an architectural level. Many elements may be
5 configured using well-known structures. The functionality and processes herein are described in such a manner to enable one of ordinary skill in the art to implement the functionality and processes within the architecture.

FIG. 1 illustrates a simplified functional block diagram of a system architecture suitable for use in implementing a security processing system and method in accordance
10 with an embodiment of the present invention. Architecture 100 includes security processing system 102 comprising security processor 104, which may consolidate the processing of discrete or consolidated security functions and maintain the relationships and integrity of the stored security context and other information in memories 106, 108, and 110. Memories 106, 108 and 110 are coupled to security processor 104. Memories
15 106, 108 and 110 store, for example, cryptographic keys and other data used in security functions by security processor 104, and also store security associations and connection entries used in maintaining multiple security sessions with other computers. Memories 106, 108 and 110 also may be used to buffer inbound or outbound data packets awaiting security processing by security processor 104. Memory 108 may be used to support
20 classification processing by security processor 104.

Security processing system 102 is preferably contained within cryptographic boundary 112 and provides a secure I/O interface for computing or communications hardware as described above. Cryptographic boundary 112 preferably complies with Federal Information Processing Standards Publication (FIPS PUB) 140-2 titled
25 "Security Requirements for Cryptographic Modules", issued May 25, 2001, by National Institute of Standards and Technology (NIST), which is incorporated by reference herein.

Security processing system 102 may be coupled to internal network 116 by I/O interface 114 and to external network 120 by I/O interface 118. Interfaces 114 and 118

may perform physical (PHY) layer processing to convert a digital bit stream to or from an analog or photonic signal for transmission over a physical medium such as, for example, copper wire pairs, co-axial cable, fiber or air. Interfaces 114 and 118 are, for example, streaming data interfaces such as a Packet-Over-SONET Physical-Layer
5 Three (POS/PHY3) type streaming interface, although 10/100 megabit (Mb) Ethernet, 1 Gigabit (Gb) Ethernet, UTOPIA, LX SPI-4 and other interface types may be suitable. By routing all or substantially all I/O to and from host processor 130 and/or internal network 116 through security processing system 102, host processor 130 and internal network 116 are substantially protected against unauthorized access or other security
10 breaches, protecting the security information integrity, and providing processing and storage efficiency from information consolidation.

IP data packets are received from and transmitted to external network 120 and internal network 116 over interfaces 114 and 118. In other embodiments, security processing system 102 may include a number of additional interfaces to internal or
15 external networks. Security processor 104 performs, for example, routing of data packets from external network 120 to appropriate destinations in internal network 116 and handles IPSec processing for both inbound and outbound data packets. Security processor 104 preferably handles all network and security processing functions for the data packets to provide the most secure I/O interface. However, in alternative
20 embodiments, certain selected networking and/or security functions may be handled by other processors such as, for example, host processor 130. Examples of network and security processing systems and methods, and related communications interfaces and protocols, suitable for implementation in and with security processing system 102 are described in U.S. patent applications serial no. 09/880,701 (entitled "METHOD AND
25 SYSTEM FOR HIGH-SPEED PROCESSING IPSEC SECURITY PROTOCOL PACKETS" filed by Lee P. Noehring et al. on June 13, 2001) and serial no. 10/160,330 (entitled "SYSTEM AND METHOD FOR MANAGING SECURITY PACKET PROCESSING" filed by Lee P. Noehring et al. on May 30, 2002), which applications are incorporated by reference herein.

Security processing system 102 may process packets delivered from internal or external networks 116 or 120 or from host processor 130. System 102 may, for example, handle thousands of separate IPSec tunnels at various packet sizes from 64 bytes and higher at a throughput of, for example, about 300 Mb per second or greater.

5 System 102 may handle transport or tunnel mode IPSec.

Other computing devices may be coupled to external network 120. For example, user devices 122 and 124 may correspond to devices that may establish secure communication sessions with host processor 130 or another device on internal network 116. User device 124 may be protected using a secure I/O interface 126, which may be
10 a hardware system similar to security processing system 102. User device 122 may use only its host processor and software to process secure communications through external network 120.

Security processor 104 may handle both so-called fast path and slow path processing functions. Fast path functions include time-sensitive processing such as, for
15 example, packet classification, modification and forwarding, and slow path functions include, for example, system management and alarm functions and time-insensitive packet processing functions such as route calculation, unknown address resolution, firewall rule management, and routing table management. Packet classification generally involves matching information from an incoming packet to a table of
20 connection entries (which may include state and context elements, and relations to encryption associations) stored in, for example, memory 106 or 108.

Security processing system 102 may be implemented, for example, as a stand-alone system box or as a card such as, for example, a NIC, that connects to a slot in the motherboard of a host system. Security processing system 102 may be coupled to host
25 processor 130 using host bridge or interface 128. Host processor 130 may be coupled to hard drive 132, digital content input device 134, and authentication input device 136. Hard drive 132 may store, for example, a software application that communicates with the application program interface (API) of security processing system 102. Security

processor 104 may send security-related information and data as requested to host processor 130, and may switch its I/O ports as requested by host processor 130.

Host bridge 128 may couple security processor to host processor 130 of, for example, a personal computer, server, or other computing or communications device.

5 Host bridge 128 may be, for example, a peripheral component interconnect (PCI) interface, and in one embodiment, may be a 32 bit, 66 MHz PCI interface.

Authentication input device 136 may be, for example, a physical key or token, a smart card, or a biometric identification sensor. Authentication input device 136 may enable the authentication of a user attempting to access host processor 130.

10 Authentication input device 136 may be directly attached, for example, to a serial, network, or EEPROM interface of host processor 130 using a physically segregated or covered transmission channel. Authentication input device 136 may act as a mechanism for enabling or modifying the functions of security processor 104, or as an information-loading mechanism, used for example in loading keys, uncovering keys, or
15 modifying rules for device operation.

Digital content input device 134 may be, for example, a CD-ROM, portable storage device, or keyboard and provides digital data such as program code or security data to host processor 130.

Security processor 104 may provide the first inspection of incoming data from
20 external network 120 to determine, for example, if the data is encrypted or in plain text form, and the type of security processing required, as may be determined by reading the header or other content of incoming data packets, and to set up a secure channel or process to handle the data, as may be requested for a security policy.

Security processing system 102 may include a unique identification (ID) number
25 stored on a chip containing security processor 104 or stored in encrypted form in, for example, memory 110. Security processing system 102 may perform protected key generation in hardware, and protected keys are preferably never output from security processor 104 in plain text form.

Security processing system 102 may also serve as a trusted hardware device to authenticate another hardware security token connected on, for example, a common network. Security processing system 102 may be authenticated using authentication input device 136 and may provide the cryptographic processing for such authentication.

- 5 Security processing system 102 may communicate verification or other information regarding the authentication status of input device 136 to host processor 130.

By performing all or most security and networking processing for I/O communications to host processor 130 in security processing system 102, a large proportion, for example, of greater than about 50-90 percent of VPN and firewall I/O
10 data loops may be handled in security processing system 102 without intervention by host processor 130. In addition, all or most security and network exception processing may be handled by security processing system 102.

Security Processor

- 15 FIG. 2 illustrates a high-level simplified functional block diagram of security processor 104 in accordance with an embodiment of the present invention. In other embodiments of the present invention, other security processor configurations may be used in the system architecture of FIG. 1. Security processor 104 is preferably, though not necessarily, formed on a single chip.

- 20 Streaming interface 200 may be coupled for input and output to physical I/O interfaces 114 and 118 and supports fast path data flow to security processor 104. Host interface 206 may be coupled to physical host bridge 128 and supports slow path data flow and system management by host processor 130. Host interface 206 may be coupled to DMA interface 204. Both streaming interface 200 and DMA interface 204
25 may be coupled to switching system 208. Although only a single streaming and DMA interface are illustrated, more than one interface of each type may be used. For example, in one embodiment, streaming interface 200 may comprise three 10/100 Ethernet interfaces, and DMA interface 204 may comprise two DMA interfaces. Switching system 208 may be used to provide a switching mechanism to route packets

and data to and from any of the I/O interfaces of security processor 104 and local data bus 210.

Local data bus 210 may be coupled to DMA interface 204 and operate under control of local bus controller 222. Local memory interface 202 may be coupled to
5 local data bus 210 and may couple security processor 104 to memories 106, 108, and 110, which are typically provided on one or more separate chips although operating portions of memories 106, 108 and/or 110 may be provided on-chip with security processor 104. In other embodiments, more than one local data bus 210 may be used.

Local memory interface 202, and DMA interface 204 may be used, for example,
10 by packet engines 228 to access memories 106 and 108 for classification processing and by control processor 212 for accessing firmware 214. Memory 106 may be, for example, a DDR SDRAM, and memory 108 may be, for example, an SRAM. Memory 106 may be made available to control processor 212 for operating system and code storage (for example, for firewall and internet key exchange (IKE) functionality, routing
15 and network address translation (NAT) information, and firewall table entries). Memory 106 may be made available to packet engine 228 for access to specific firewall information, and stored security policies and associations. Memory 106 may be made available to cryptographic core 232 to store security association and key information. Memory 106 may also be made accessible via host interface 206 to host processor 130.
20 Alternatively, a portion or all of the security association data may be stored in a memory, for example an SRAM (not shown), on-chip in security processor 104.

Memory 108 may be made available to both control processor 212 and each packet engine 228. Memory 108 may be used to aid in rapid lookups supporting packet engine 228 in classification and forwarding decisions. Memory 110 may be, for
25 example, flash memory to provide non-volatile storage, for example, for boot memory and certain key storage. The boot code used to load firmware for execution by security processor 104 may optionally be authenticated using a mechanism internal to security processor 104 prior to its operation.

Switching system 208 may provide a flexible I/O system that allows packet processing engines or packet engines 228 to communicate high-speed data with several different types of interfaces including, for example, streaming interface 200 and direct memory access (DMA) interface 204. A non-limiting example of a switching system and method that are suitable for use with the present invention is described in U.S. patent application serial no. 10/172,814 (entitled FLEXIBLE I/O INTERFACE AND METHOD FOR PROVIDING A COMMON INTERFACE TO A PROCESSING CORE, filed by Swaroop Adusumilli et al. on June 12, 2002), which is hereby incorporated by reference. Alternatively, switching system 208 may be implemented using conventional switches. Switching system 208 may provide a common bus interface to packet engines 228.

More specifically, switching system 208 may arbitrate between streaming and DMA interfaces to provide a common interface for packet engines 228 to permit communication of differing types of data over a plurality of bus types that implement different bus protocols and/or standards. The use of switching system 208 with DMA interface 204 may permit packets and other data to be routed using direct memory access among control processor 212, each of packet engines 228, and external memory such as memories 106 and 108. In one embodiment, individual packets may be routed within security processing system 102 using DMA.

Switching system 208 may select the I/O port or interface, including host interface 206, to use for data packets based on the results of cryptographic or other security or network processing. For example, packets classified for forwarding to another destination after a security operation (such as encryption or new connection validation) could be directed to the proper egress port, while packet data requiring host inspection (such as IKE messages, or exception or initial packets for firewall classification) could be redirected to DMA interface 204. In contrast to prior systems that rely on external bus interfaces to re-direct packet traffic to varying packet processing devices, the present invention may permit simplifying or collapsing the schema and protocols used, for example, in firewall, routing, NAT and IPsec

processing with the result that lookups, transforms, and other application activity are more efficient. Prior systems typically require context labeling or other data envelopment or tagging to manage packet workflow among varying processing devices.

Switching system 208 may also include the ability to perform packet spanning.

5 Spanning generally refers to a capability in managing network data flow that duplicates a selected traffic flow through an additional port for analysis by a traffic analyzer or intrusion detection system. The term “spanning” includes within its meaning, but is not necessarily limited to, functionality associated with the use of switched port analysis (often designated by the acronym “SPAN”). Unlike the all-or-nothing port duplication
10 capabilities of typical existing network switches having a SPAN capability, the spanning function of switching system 208 may selectively identify flows of traffic and then stream duplicate packets or other datagrams via DMA interface 204 to control processor 212 or to, for example, another integral MIPS or associated control processor (not shown) that may be included in security processor 104.

15 Typical data traffic that will not be spanned (i.e., non-spanned traffic) flows from one of packet engines 228 to, for example, an output packet cache (OPC). The OPC is an intermediate buffer to switching system 208 for outgoing packet traffic that will leave security processor 104 through DMA interface 204 or streaming interface 200. FIG. 9 is a block diagram illustrating the OPC interfaces.

20 At the OPC, this outgoing packet traffic may be placed on an active list (for example, a list of 64-byte memory structures residing in the OPC) for transmission out of interface 204 or 200 (for example, a PDMA or GMII interface). The OPC may be implemented, for example, as an embedded memory structure or in external memory and may be coupled between a packet engine 228 and one of the external interfaces of
25 security processor 104. The use of the spanning feature is preferably configurable and may be selected by the system or operator. This feature is preferably implemented primarily using the OPC. FIG. 10 is an internal block diagram illustrating the OPC.

More specifically, the OPC may include an output packet buffer (OPB) memory (e.g., a RAM) for buffering output data, and a buffer control block (BCB). The BCB is

typically a set of pointers stored in memory that each refer to memory locations of the output data. The BCB may maintain metadata such as, for example, start-of-packet, end-of-packet, error, sequence number, pointer to next BCB in chain, and other metadata. The BCB is preferably used to manage the active lists and the free list for the
5 linked-list allocation scheme. When logically dictated during the operation of security processor 104 such as, for example, in the case of a five-tuple match result from a lookup engine, a NIDS engine match to packet type, or particular TCP state, or some other pattern within a datagram that is of interest to the system operator, a control bit or flag (sometimes referred to as a “SPAN bit” herein) may be set or some other
10 notification may be sent by packet engine 228 to notify the BCB for packet data that is transiting the OPB memory, including the output device or interface that will be used. When a packet that will not be spanned (i.e., a “non-span packet”) is stored in the OPC, a “DONE” flag, for example, is set to zero for each such non-span packet, and each non-span packet may be queued for egress out through an appropriate interface (i.e.,
15 streaming interface 200 or DMA interface 204).

After the memory pointed to by the BCB is drained (i.e., data is read or outputted out of that location into another location), the BCB “DONE” flag may be set to allow the memory to be overwritten. Alternatively, another method may be used to move output buffer data from the “active list” to the “free list”. When a spanned packet
20 is sent to the OPC from packet engine 228, a separate bit may be set (this separate bit is referred to herein as a “SPAN” bit). The SPAN bit may be used to initiate alteration of the behavior of the OPC. The packet may be streamed out through the original targeted egress interface (e.g., streaming interface 200 or data interface 204), but before releasing the data memory area pointed to by the BCB, the data may be drained out via
25 a designated interface, for example DMA interface 204 to control processor 212 or to host processor 130. After such a packet is successfully duplicated using DMA interface 204, the BCB may be set to free the memory to be overwritten as described above.

In an alternate embodiment, the BCB or some other memory control mechanism could maintain an active list and a free list and place the active data blocks of OPB

memory (i.e., re-map the pointers) from the active list to the free list when the packet data is streamed out. When the SPAN bit is set, the data would first be streamed to the alternate interface (such as, for example, DMA interface 204) in addition to its primary target output interface prior to moving the data blocks to the free list. After spanned
5 data has been drained to control processor 212 or host processor 130, the spanned data is available to other processors or systems for any desired subsequent actions such as, for example, logging, analysis for intrusion detection, or transcription.

The foregoing approach may be particularly useful for network intrusion detection functions. When one of the defined actions for a certain packet traffic type is
10 to log the packet, the above approach permits security processor 104 to act substantially as an in-line tap, which permits selectively duplicating streams of data that may be of interest based on specific pre-selected criteria. When NIDS 302 returns a potential signature match to one of packet engines 228, and that packet engine 228 is able to verify that the potential signature match is a true positive match, packet engine 228 may
15 set the SPAN bit for that packet so that it is duplicated to control processor 212 and/or host processor 130 as discussed above. This verification may, for example, be based on the protocol of the packet or other appropriate criteria. Control processor 212 and/or host processor 130, as is applicable, may then run further analysis on the packet or the packet stream, and/or may forward it to a centralized IDS collector for enterprise
20 intrusion detection.

Alternatively, the packet or packet stream may be re-directed or duplicated to host processor 130 for further processing. Such processing may include, for example, upper-layer cross-packet analysis, packet normalization, data mangling, or other operations. The packet may be forwarded out through the appropriate interface (e.g.,
25 streaming interface 200 or DMA interface 204) after such post-analysis or post-processing.

Packet engines 228 may each be coupled to a cryptographic core 232. Packet engines 228 may each comprise microprocessors customized for packet operations such as, for example, packet processing and classification. Examples of packet engines

suitable for use with the present invention are described in detail in U.S. patent application serial no. 09/880,701 (entitled "METHOD AND SYSTEM FOR HIGH-SPEED PROCESSING IPSEC SECURITY PROTOCOL PACKETS" filed by Lee P. Noehring et al. on June 13, 2001), which is incorporated by reference herein. Each
5 packet engine 228 may, for example, process packets needing initial NAT processing and firewall table entry setup, process packets corresponding to existing NAT and firewall tables, and process IPsec packets.

More specifically, each packet engine 228 may perform hash table lookups to a firewall connection table entry, which may contain state information, a rule to be
10 applied to a packet, optional security association information, routing information (for example, for MAC overlay), and any application level gateway (ALG) packet mangling to be done.

For outbound IPsec traffic, each packet engine 228 may provide a pointer to security association data for an IP packet, load a security association database entry into
15 a local buffer located on or off-chip, construct and add an outer IP header and IPsec header, perform lifetime checks, and update an associated security association database (SAD) entry (for example, the sequence number and byte count).

For inbound IPsec traffic, each packet engine 228 may locate an associated SAD entry by using a security policy index (SPI) number from the IPsec header or by
20 an SAD address provided by the classification of the destination address, protocol and SPI. In order to use the SPI number, IKE firmware 214 may define the inbound SPI number from the API provided for security processor 104 during security association establishment. Packet engine 228 may then load the SAD entry into a local buffer, perform anti-replay checks and lifetime checks, and then update the SAD entry. Each
25 cryptographic core 232 may remove tunnel IP headers, ESP or AH headers, and ESP trailers. The packet may then optionally be redirected through packet engine 228 for a firewall connection table lookup.

Packet engines 228 in FIG. 2 represent one or more packet engines that may be provided in parallel in security processor 104. The optional presence of additional packet engines 228 is indicated in FIG. 2 by ellipsis 229.

Input and output buffers 236 and 240 may be provided to couple each packet engine 228 to switching system 208. Buffers 236 and 240 may be, for example, FIFO buffers. In one embodiment, each of output buffers 240 may read control data prepended to the data payload as an in-band instruction set that determines the distribution direction or interface of the packet by switching system 208. Input and output buffers 236 and 240 may each have a size of, for example, 16-32 kilobytes (KB). An alternative is to have a direct control interface provided to couple each packet engine 228 to switching system 208, for out-of-band signaling of the packet data distribution direction. Roughly stating the foregoing in another way, instructions may be sent either from a packet engine 228 to switching system 208 either in-band, as prepended control words, or out-of-band, via a discrete control channel.

Packet engines 228 may be interconnected at the packet level for passing a packet and associated context information to other functional blocks or to each other for specific processing. In parallel operation, the individual packet engines 228 may each independently process discrete packets and forward the packets to other devices, such as cryptographic processing cores or switches. Two or more microprocessors could, for example, be serialized to perform discrete functional tasks as the packet transits from one functional block to another. Packet engines 228, in conjunction with cryptographic cores 232 and under the common control of control processor 212, may perform, for example, firewall lookup and statistics, IPSec and secure sockets layer (SSL) processing, quality of service (QoS), traffic management, and public key processing. Packet engines 228 may be programmable through registers (not shown), which may be configured by an external driver or initialization program. Each packet engine 228 may perform any needed datagram modification prior to sending a packet out from security processor 104. For example, packet engine 228 may write a MAC destination address to a packet as it streams out of processor 104.

In one embodiment, all incoming packets to security processor 104 may be initially processed by one of packet engines 228. Each packet engine 228 may classify the packet based upon a lookup table result and then may apply a variety of operations including, for example, forwarding with necessary transform parameters to
5 cryptographic core 232, or forwarding to control processor 212 for application level processing. Such operations may further include overwriting portions of the packet with new data such as, for example, the media access control (MAC) header for forwarding and the IP header for NAT, and may also include dropping the packet, or passing the packet through security processor 104 to an egress interface, such as, for
10 example, streaming interface 200, unchanged.

Cryptographic cores 232 may provide security processing to perform, for example, IPSec and/or SSL processing. Each cryptographic core 232 may provide high-speed fixed function encryption and authentication hash processing for packet data. Each cryptographic core 232 may receive instructions and key address
15 information affixed to a packet for applying appropriate transforms. Examples of cryptographic cores 232 suitable for use with the present invention are described in the following U.S. patent applications, all of which are incorporated herein by reference: serial no. 10/144,004 (entitled "SINGLE-PASS CRYPTOGRAPHIC PROCESSOR AND METHOD" filed by Satish N. Anand et al. on May 13, 2002); serial no.
20 10/144,332 (entitled "SECURITY ASSOCIATION DATA CACHE AND STRUCTURE" filed by Satish N. Anand et al. on May 13, 2002); serial no. 10/144,195 (entitled "APPARATUS AND METHOD FOR A HASH PROCESSING SYSTEM USING MULTIPLE HASH STORAGE AREAS" filed by Satish N. Anand on May 13, 2002); and serial no. 10/144,197 (entitled "APPARATUS AND METHOD FOR A
25 HASH PROCESSING SYSTEM USING INTEGRATED MESSAGE DIGEST AND SECURE HASH ARCHITECTURES" filed by Satish N. Anand on May 13, 2002).

It should be noted that each cryptographic core 232 is preferably accessible only through a corresponding packet engine 228. Alternatively, several packet engines 228 may access a single cryptographic core in a round robin or other arbitrated flow

mechanism. Accordingly, all or substantially all packet and data flow may return to the corresponding packet engine 228 from cryptographic core 232 prior to output from security processor 104. Also, in a preferred embodiment according to the present invention, all I/O data to security processor 104 transits one of cryptographic cores 232
5 whether or not the data needs encryption/decryption or other security processing. After exiting cryptographic core 232, a packet may be assigned its distribution directions (for example, to a destination of one of several streaming interfaces 200 or control processor 212) by packet engine 228 for distribution through switching system 208.

Streaming interface 200, switching system 208, packet engines 228 and
10 cryptographic cores 232 may provide fast path data flow for security processing system 102. This fast path data flow may provide both firewall and virtual private network (VPN) functionality along with network intrusion detection functionality as described further below. Control processor 212 and firmware 214 may provide all or substantially all control for these firewall, VPN and network intrusion functions.

15 Initial packets for a data flow may transit from packet engine 228 and cryptographic core 232 to control processor 212 for an initial classification. Control processor 212 may perform firewall, NAT, and routing classification for the packet, and further may create a connection table and hash entry in memory 106 for use by packet engine 228 on subsequent packets in the data flow. This may include the building of
20 more than one connection table entry, depending on the application. Examples of this include preemptively constructing inbound and outbound entries, as well as a data channel entry for certain protocols. Control processor 212 may also trigger IKE processing as a result of the classification of the initial packet.

The connection table entries above provide a mechanism that allows the
25 acceleration of security operations, such as firewall or NAT decision processing for packets. Connection entries may have a relationship (for example, one-to-one or many-to-one) to IPSec SAD entries in support of IPSec operations as a result of classification.

Control processor 212 may provide control plane operations for security processing system 102 and may run an embedded operating system or simple task

scheduler to handle complex packet applications such as, for example, firewall and intrusion detection system applications, a TCP/IP stack including routing functions, and support applications such as IKE and user interfaces for configuration, for example, from host processor 130. The use of control processor 212 in the foregoing manner
5 may permit the complete containment of all key generation, public key and symmetric key encryption and decryption processing within the hardware of security processing system 102 and within cryptographic boundary 112. Control processor 212 allows the flexibility of general purpose processing for non-real-time, demand-driven or OS-based applications to be executed.

10 Modulo/expo engine 216 may be coupled to local data bus 210 to provide processing for streaming and modular exponentiation. Control processor 212 may provide public key macro acceleration by providing pre-processing for modulo/expo engine 216, which would permit host processor 130 to request high-level public key acceleration calls that are handled completely by security processing system 102.
15 Modulo/expo engine 216 may be made accessible to control processor 212 and also host processor 130. The interconnectivity of operations that may be provided by control processor 212, specifically the providing of key management functions, modulo/expo engine operation and local access to encrypted/protected memory, allows security processor 104 to keep all unprotected cryptographic keys and operations within the
20 boundary of security processor 104. In other embodiments, a dedicated key management processor (not shown), which may be coupled to local data bus 210, and associated firmware may be integrated and made accessible to modulo/expo engine 216 in addition to or even in the absence of control processor 212.

Firmware 214 may be executed by control processor 212 and may provide
25 operating system software and other software to provide IKE and other functions and additional functions known to one of skill in the art. Control processor 212 may be, for example, a general purpose processor such as a 32-bit RISC processor. Other types of processors may also be used. Other software stored as part of firmware 214 may be used to permit control processor 212 to provide VPN, firewall, intrusion

detection/prevention, and SSL protocol communications, virus protection, digital rights management, content filtering, access control, verifying of application integrity, and management of public key infrastructure (PKI) exchanges.

Additional software stored as part of firmware 214 may permit a wide variety of data analysis functions including, for example, packet analysis, pattern matching, or other data analysis. Statistics may be generated by such functions and/or other functions and the results communicated to host processor 130 or another device (not shown) for central data collection of activity on devices coupled to internal network 116.

Firmware 214 may include control plane software that runs on control processor 212. The control plane software may communicate with the data plane software using a set of application program interfaces (APIs) and a message-based protocol. The data plane software may include forwarding software responsible for performing high-speed packet processing that handles the data plane steady-state portion of networking applications, such as, for example, IP packet forwarding protocols. The functionalities provided by security processing system 102 may be changed and/or updated by updating firmware 214. Such updating may be done, for example, as new industry or government security standards are developed or modified. Also, the resources devoted to each of the security and networking processing functions may be customized for each host computing device or by the location of a device on a network, for example a location at either a gateway or at an edge of the network.

Security processor 104 may include random number generator (RNG) 218 and timers, universal asynchronous receiver/transmitter (UART), and general purpose I/O 220 coupled to local data bus 210. RNG 218 may be a true digital random-number generator. RNG 218 may be made available to control processor 212 and also to host processor 130. Timers 220 may operate most operations in the core of security processor 104 and may run, for example, at a frequency of about 150 MHz. A separate reference clock (not shown) may be coupled to control processor 212, which may be bridged to the security processor 104 core, and run, for example, at about 250 MHz.

Security processor 104 optionally may include anti-tamper system 224. Anti-tamper system is controlled by control processor 212 and may include detection circuits for voltage, temperature and physical probing forms of tampering. More specifically, anti-tamper system 224 may comprise hardware tamper circuits and firmware routines to check the integrity or health of stored flash content. The firmware routines may check the general integrity or health of the flash content using, for example, both DES-MAC or AES-MAC security methods or other hashing and authentication techniques. Anti-tamper system 224 may be implemented as a network of detection circuits tied to a fail-safe fault collector (not shown).

Translator 226, which may be, for example, a steganography translator or another memory obfuscation device or encryption translator, such as an encryption filter, may optionally be coupled to local memory interface 202 to use known steganographic or encryption techniques, as applicable to the type of device 226 used, in the writing and reading of security keys and other data to and from memories 106, 108 and/or 110. For example, an encryption key of, for example, about 112 bits may be distributed in an SRAM memory 108 in a data block size of, for example, about 100,000 bits and only be retrievable from memory 108 using a translation algorithm implemented in software in translator 226.

Encrypted Memory System

A hardware encryption path may be included between local data bus 210 and a memory controller block in security processor 104. This path may consist of two main components: (i) an encryption DMA block (EDMA) that may be a write-only path between a local host and off-chip memory (e.g., memory 106) for securely storing SA (security association) keying material; and (ii) an "ER" block that may be a read path from the memory controller block to the block from which a calling function is originating (for example, a cryptographic function running in cryptographic core 232 that uses SA keys for IPSec processing). The hardware encryption path as described herein may in general be useful with any off-chip memory, including for example,

memory 106, 108, or 110. FIG. 12 is a block diagram illustrating the relationship in this embodiment between the ER block, the EDMA block, cryptographic core 232, and memory. The division of memory access shown could be physical (block connection) or logical (access to targeted address ranges that are encrypted).

5 The EDMA block may consist of several blocks including an AES encryption block (e.g., 18-round AES with a 64-bit block size), an address expansion block, a control block, and a configuration block. The EDMA may sit between DMA interface 204 and an "AHB master block" (see FIGs. 6 and 7), which is coupled to the memory controller block (as discussed in more detail below). As discussed in more detail below
10 and as illustrated in the figures, the AHB may be an internal AMBA host for the chip. AMBA refers to the Advanced Microcontroller Bus Architecture.

 The EDMA block monitors signals from, for example, DMA interface 204 to determine if the current write request from DMA interface 204 to the AHB master block is, for example, for an IPsec SA, and/or SSL SA, or for a transfer which does not
15 contain any SA data. This distinction may be controlled by two control bits in a control word associated with DMA interface 204 and used for each transfer. If the transfer is for an IPsec SA, the EDMA logic may hold off the request going to the AHB master block until the AES block is ready e.g., when the initial 10 rounds of AES processing are complete). The AES block may use the SA source address and an internally
20 generated key (K) to complete the initial 10 rounds. On completion of the 10 rounds, 64-bits, for example, of Cipher Text 0 (CT₀) will be produced, and the write request will be allowed to pass to the AHB master block. The AHB master block will assert its read signal and the first 8 bytes of data (a Basic Command Word [BCW], which is control data not needing confidentiality protection) will be allowed to transfer as
25 cleartext. On each of the remaining transfers, the AES block will step one round of the AES algorithm per each transfer, and the data will be XOR'ed with CT_n (n=0...8) to produce a value EDMA_K [Data_n] (n=0...8) for a total transfer of 80-bytes, of which 72 bytes are encrypted. The EDMA preferably will not encrypt any transfer where the source address equals the destination address.

The ER block may provide a path from memory 106 (e.g., off-chip SA DDR) to cryptographic core 232 for decrypting SA's that are located within memory 106. The ER block may consist of several blocks including an AES encryption block (e.g., 18-round, 64-bit AES), an address expansion block, a variable FIFO, a control block, and a configuration block. The ER block may be located between the calling functional block (e.g., cryptographic core 232 or another block) and memory 106. The ER block may be read-only, or it may be read-write, if necessary to, for example, copy back state information. FIG. 11 is a block diagram illustrating the relationship in this embodiment of the ER block to the cryptographic core and memory.

The ER block may monitor the calling functional block's request signals to memory 106. If the request is a read, the ER block will hold off the completion of the read by de-asserting its ready signal ("*ER_rdy*") to a memory arbiter until the AES block is ready (i.e., when the initial 10 rounds of the AES algorithm are complete). The memory arbiter (e.g., a RAM arbiter) brokers access requests from the requestors of memory (e.g., a MIPS processor, one of packet engines 228, or cryptographic core 232). Signal *ER_rdy* may be transmitted to the memory controller (see the "CRA" block in Fig. 12) from the EDMA or the ER control element.

The AES block may use the SA source address provided from the interface to cryptographic core 232 and the K key to complete the initial 10 rounds of the AES algorithm. On completion of the 10 rounds, 64-bits of Cipher Text 0 (CT0) will be produced and the ready signal (*ER_rdy*) may be asserted allowing the read request to pass to the memory arbiter. The memory arbiter will assert its data ready signal and the first 8-bytes of data (the BCW) will be allowed to transfer in the clear. On each of the remaining transfers, the AES block will step one round of the 64-bit AES algorithm per transfer, and the data will be XOR'ed with CT_n ($n=0\dots8$) to produce values $E1_K[Data_n]$ ($n=0\dots8$) for a total transfer of 80 bytes, of which 72 bytes are decrypted. More generally, the ER block may decrypt or encrypt to arbitrary offsets per each read or write request, intermingling data stored in the clear with data stored in an encrypted form so as to make a clear text delivery to the calling functional block.

Now discussing an encrypted hardware path according to the present invention in more detail, an encrypted memory system may be implemented as a multi-block system tasked with the selective encryption of memory structures to protect data that may reside in off-chip memory (e.g., memory 106, 108, or 110, as mentioned above) 5 from use by anything other than the intended block and/or logic that resides in the system itself. It is particularly useful in encryption devices and applications such as with the IP Security protocol where one wishes to achieve FIPS 140-2 level 2 or similar levels of protection for data and process contents.

The specific embodiment of the present invention discussed here preferably has 10 two primary blocks. First, the EDMA block may provide logic and a protected path from, for example, a host general purpose DMA interface to the memory controller. This is the path over which the encrypted data may be written to memory. The utility of the EDMA block is to provide a method of inserting data into memory, encrypting it enroute. Second, the ER block may provide a fast decryption path for data read from 15 external memory. The ER block is accessible only to trusted requestor blocks within the chip, making retrieval and decryption of certain protected memory data discriminatory, based on purposeful hardware design. An encryption key K may be used for encryption and decryption of the externally stored data. K is preferably internally generated at initialization and not visible nor accessible outside the system.

20 ***Data Representation Conventions***

FIG. 5 illustrates the data representation convention used herein for purposes of explanation. Other conventions may be used in different embodiments. Throughout the description herein, all data vectors and one-dimensional data structures are represented with the Most Significant Bit (MSb) in the leftmost position and the Least Significant 25 Bit (LSb) in the rightmost position. All two-dimensional data structures are represented with the MSb in the upper leftmost position and the LSb in the lower rightmost position.

EDMA Block (GDMA to Off-Chip Memory)

The EDMA block may provide a write-only path between a local host or other data generating device and the off-chip memory for securely storing protected information, such as SA keying material. It may consist of several blocks that include
5 an N round B block AES encrypt (where B is the width of the memory interface), address expansion, control, and configuration. An AES algorithm of 128-bit key size is typically used though other key sizes may be used with the appropriate adjustment in key expansion rounds. Likewise, some other streaming or block cipher may be used in an alternate implementation. The EDMA block sits between the interface from the data
10 path and the bus to the memory controller. In one implementation the EDMA may be located between the "GDMA" block and the "AHB" block (see FIGs. 6-8). The GDMA (general purpose DMA) block may interface the internal or external host to the AHB. The AHB master is the mechanism for the functional block (e.g., the GDMA block or packet DMA [PDMA]) to take control of the bus for signalling and data transmission.
15 Alternatively, in a multi-path (parallelizing) design, the EDMA block could be located between the GDMA Slice0 (gda_slice0) and the GDMA multiplexer (mux) as illustrated in FIG. 6.

The EDMA block monitors the incoming data bus (e.g., GDMA signals) to determine if the current write request is protected data or a transfer which does not
20 contain any protected data. This distinction may be controlled by signaling, for example, two control bits in a GDMA control word for each transfer. The signaling may also determine whether or not there is an offset to the beginning of encryption, allowing a block-sized multiple of clear text to precede the encrypted data in a single transaction. If the transfer is to be encrypted, for instance for an IPSec SA, the EDMA
25 logic will hold off the request going to the AHB Master until the AES is ready, that is when the initial 10 rounds of AES are complete, and the block multiple clear text offset is reached, if it exists. The AES block will use the incoming data's Source Address (M) and K key to complete the initial 10 rounds. On completion of the 10 rounds, B bits of Cipher Text 0 (CT0) will be produced and the write request will be allowed to pass to

the AHB Master. The AHB Master (in this example) will assert its read signal and the first 8-bytes of data will be allowed to transfer. On each of the remaining transfers the AES block will step one round of the AES algorithm per transfer and the data will be XOR'ed with CT_n ($n=0\dots i$) to produce $E_K[Data_n]$ for a total transfer of $n \times 8$ bytes being encrypted. The EDMA block will not encrypt any transfer where the source address equals the destination address. A more detailed block diagram is illustrated in FIG. 7. The sections below describe each of these blocks in more detail.

RND_{mix}

The RND_{mix} value will be initialized during the boot-up sequence as a 64-bit (or block size) random or pseudo-random number and then written to the EDMA RND_{mix} register. The RND_{mix} will be XOR'd with the cipher text XOR data and then be sent to the EDMA mux, providing additional mix protection to mitigate the weakness of "to 000 or FFF" writes to memory.

AES64 Encryption Block

The AES block preferably uses a reduced block size, 64-bit block AES (128-bit key) algorithm as defined in the Appendix to this application (AES64 Specification). Although the embodiment of the present invention is discussed in the context of this specific AES algorithm, one of skill in the art will recognize that other algorithms (e.g., other than AES) may be used in other embodiments. Although in the Appendix the number of rounds for the AES algorithm is defined as 10, for the EDMA or ER blocks the AES64 may be extended to support an $10+n$ round cipher, as determined by the size of the encrypted data transaction. For more detail, see the following table:

PreAdd	
round 1	SubBytes
round 1	ShiftRows

	round 1	MixColumn
	round 1	AddKey
	...	
5	round n	SubBytes
	round n	ShiftRows
	round n	(No MixColumn On Last Round)
	round n	AddKey
10		

The output of rounds 11 through n will produce CT_0 through CT_n which will be used to XOR with the eight byte blocks (for a 64-bit memory width) of the data transaction being written to off-chip memory. An initial, block multiple amount of data may be allowed to pass in the clear prior to the active encryption, based on any offset
15 programmed into the transaction signaling.

EDMA Address Expansion Block

The address expansion block takes n_m -bits of address data together with some amount of K data and produces block-sized bits of address expansion data for input to
20 the AES block. The address expansion block may use S-Box and E-Box functions to accomplish the expansion, though other substitution or expansion algorithms may be used as long as they introduce sufficient variability. The address is typically expanded through the E-Box or some other expansion function. Some mixing bits are selected from K and run through a number of S-Box's or some other substitution function to
25 produce data that will be XOR'd with the expanded address seed from the E-Box. The output from the XOR is then appended to the address (or data that is address dependant) to form a block-sized amount of output ($ax_data[B:0]$). In more detail, in formula form: $ax_data[B:0] = \{gdma_EDMA_amemory[m_i:0], X_i[(B-m_i:0)]\}$

ER Block (Cryptographic Core to/from Security Association (SA) Memory)

The ER block (e.g., for a four-channel slice) provides a read-only (e.g., IPSec) path from off-chip memory to the functional block or device reading the memory, for example, in the case where cryptographic core 232 would need to decrypt SA's that are located within off-chip memory. It may consist of several blocks that include an n-round, B-bit AES encrypt, address expansion, variable FIFO, control, and configuration. The ER block may be located between the memory-consuming function (e.g., cryptographic core 232) and off-chip memory as illustrated in more detail in FIG. 8. Multiple function blocks or devices may have their own or a shared ER block to memory.

The ER block monitors the calling block's request signals to the off-chip memory. If the request is a read, the ER block will hold off the completion of the read by de-asserting its ready signal (*ER_rdy*) to a memory arbiter until the AES block is ready (i.e., when the initial 10 rounds of AES64 are complete). The AES block will use the memory Source Address provided from the cryptographic core interface and the K key to complete the initial 10 rounds of AES64. On completion of the 10 rounds, 64 bits of Cipher Text 0 (CT0) will be produced and the ready signal (*ER_rdy*) will be asserted allowing the read request to pass to the memory arbiter. The memory Arbiter will assert its data ready signal and the data will be allowed to transfer. If an offset is included in the request signal, then a block multiple of data may precede the decrypted information in the clear. On each of the remaining transfers the AES block will step one round of the AES algorithm per transfer and the data will be XOR'ed with CT_n (n=0...8) to produce E1_K[Data_n] for a total transfer of 8 x n bytes being decrypted.

Host Configuration Interface (I/F)

A host configuration interface provides read/write access to local configuration and status registers.

RND_{mix}

The RND_{mix} value will be initialized during the boot-up sequence as a 64-bit (or block size) random or pseudo-random number and then be written to the EDMA RND_{mix} register. The RND_{mix} will be XOR'd with the cipher text XOR data and then be sent to the EDMA mux, providing additional mix protection to mitigate the weakness of "to 000 or FFF" writes to memory.

AES Encryption Block

The AES block preferably uses a reduced-block size, 64-bit AES algorithm as defined in the Appendix to this application (AES Specification). Although the discussion in the Appendix defines the number of rounds as 10, for the ER block the AES block is able to support a 10+n round cipher, where n represents the number of bus width blocks of memory to be retrieved.

ER Address Expansion Block

The ER address expansion block may be implemented in the same way as the EDMA address expansion block.

Network Intrusion Detection System

FIG. 3 illustrates a more-detailed functional block diagram of a network intrusion detection system that may be used in a portion of security processor 104 in accordance with an embodiment of the present invention. FIG. 3 illustrates, for example, three packet engines 228 in parallel and each connected to a cryptographic core 232.

Network intrusion detection system (NIDS) 302 has taps 303 that may couple to the input/output of each of packet engine 228 and cryptographic core 232 pair. Signature database 304 is a defined set of patterns stored in on and/or off-chip memory.

NIDS 302 attempts to match parts of the data stream (for example, the header, payload, or trailer) against the stored set of patterns.

According to the present invention, by passing all I/O traffic to host processor 130 and/or internal network 116 through security processing system 102, and including
5 NIDS 302 within system 102, undesirable intrusions may be detected in-line with such I/O traffic, such as, for example, it passes through an NIC. By being in-line in this manner, intrusions identified by NIDS 302 may be stopped in the I/O traffic flow and any further related improper intrusion prevented from passing to host processor 130 and/or internal network 116.

10 Each computer or computing device (not shown) connected, for example, to internal network 116 may be protected by security processing system 102, such as, for example, using an NIC containing security processing system 102 for all I/O traffic for each device. Each such distributed NIC may communicate with a central server (not shown) connected to internal network 116 to accumulate performance, security,
15 network processing and other data related to activities reported by each such security processing system 102. Additionally, such accumulated data may be processed and/or analyzed by the central server and then new or modified control signals sent to all, or a selected portion, of the security processing systems 102 of each device on internal network 116.

20 Having a tap on each of the input and output paths to each cryptographic core 232 permits the capture of clear text packets either before or after encryption, depending on whether the packets are inbound or outbound. Thus, signature matching may be done on clear text data. NIDS 302 may flag a packet as having a potential signature match to a pattern in signature database 304. The flagged packet may either be dropped
25 (and the flow of subsequent packets in the same data flow stopped) or continue to its next destination, with a logging report to host processor 130 in either case indicating the status of the packet. Also, in addition to being sent to its next destination, the flagged packet may be redirected or duplicated and receive further slow path processing by control processor 212. The logging report may be used to form an audit trail for

collective or heuristic analysis and future packet inspection by a centralized intrusion detection system or other process or device. If a packet has been identified as undesirable, intrusion prevention may be provided by dropping related future packets in packet engines 228.

5 NIDS 302 may be coupled to a separate control channel 305 coupled back to one or more, and preferably all, of packet engines 228. Control channel 305 is a special path to send packets that have been flagged by NIDS 302 to the control plane on local data bus 210 (and then optionally on to host processor 130) for logging or other administrative tasks, including, for example, providing data for use by a network administrator in managing and improving network intrusion detection and prevention by
10 security processing system 102.

 Flagging of a packet or a packet data structure may be done by setting a bit flag in a control word corresponding to the packet. By examining this bit flag for a packet, control processor 212 may direct the packet to a certain location for logging. Results
15 from packet classification performed by each packet engine 228 (for example, to determine that the packet is network file system (NFS) traffic) may be used to select from one of many rules sets or signature sets in signature database 304.

 Based on comparisons to the selected rules or signature sets, control channel 305 may indicate one or more types of initial potential intrusion violations associated with a
20 packet. After indicating flagged packets to one or more of packet engines 228 through control channel 305, each packet engine 228 may further classify the packet by comparison to the one or more types of other potential intrusion violations provided for the packet by control channel 305, and use information from prior classification processing for the packet by the packet engine 228 to narrow or eliminate the set of
25 potential intrusion violations.

Packet/Data Flow

FIG. 4 illustrates a simplified flow diagram of typical packet or data flow for one embodiment of security processing system 102. Each packet engine 228 may

comprise a packet processor and a classification engine. Circles 404 and 406 generally correspond to the functionality provided by the classification engine and the packet processor, and such functionality is referred to herein as classification engine 404 and packet processor 406.

5 Classification engine 404 may provide lookup and decision logic for, among other things, security policy database (SPD) lookup, firewall connection table lookup, NAT table lookup, routing, and limited application level gateway (ALG) rule application and data mangling. Any or all of the foregoing classification engine functions may be subsumed in a single connection table entry. Once an initial data flow
10 is defined, the foregoing classification engine functions may be made integral to the data flow.

 Packet flow through security processing system 102 typically begins when a packet enters switching system 208 via one of streaming interfaces 200 or DMA
15 interfaces 204. Each packet may be inserted into an active list waiting for the next available packet engine 228. The same active list may be an insertion path for control processor 212 to direct packet traffic into a packet engine 228. Regardless of destination, whether, for example, it is to streaming interface 200, host interface 206, control processor 212, or a loop through a packet engine 228, all packet data preferably flows to a packet engine 228 and then to a corresponding cryptographic core 232.
20 Tagging of the packet upon ingress to the packet engine 228 may determine the egress path from cryptographic core 232. More specifically, the incoming and outgoing packets may be provided with a tag upon ingress to one of packet engines 228 and the tag may be used to determine the egress path upon exit from the corresponding cryptographic core 232.

25 Classification hash lookup data and a detailed connection flow table and security policy/association data may be stored, for example, in memory 106. Upon receiving a packet, packet engine 228 may find a match in the connection table, fetch the connection information (including SAD information as appropriate), and apply the appropriate rules and transforms. This may include forwarding the packet to control

processor 212. If no match is found in the connection table, then the packet is preferably forwarded to control processor 212.

Outbound packets may be buffered after transit through packet engine 228 and cryptographic core 232 for sending out to streaming interface 200 or to host interface 206. Outbound packets may have made a single trip through packet engine 228 and core 232, may have made a second trip through packet engine 228 and core 232 after prior processing by control processor 212, or may have made a second trip through packet engine 228 for firewall inspection following decryption in cryptographic core 232.

Initial packets needing classification to create a NAT lookup table entry and/or firewall connection table entry may be forwarded to control processor 212 for processing, then back to classification engine 404, and then to packet processor 406 prior to output from security processor 104 (unless dropped in accordance with the firewall rules in effect). If such initial packets also need IPSec processing, they may be forwarded to packet engine 228 after initial processing by control processor 212, then back to an egress interface.

For packets that are already in an existing data flow, for example, already having connection table entries or NAT global mapping in existence, a successful lookup may result in a direct forwarding to packet processor 406 for modification, and then classification by classification engine 404 for egress from security processor 104. Outbound IPSec packets in an existing flow transit to packet engine 228 and cryptographic core 232 after egress classification and firewall packet processing. Inbound IPSec packets in an existing flow are forwarded to packet engine 228 and cryptographic core 232, then to the classification engine 404 and packet processor 406 for SPD validation, routing, and optionally, firewall and NAT processing prior to egress.

APPENDIX

5 An APPENDIX is included at the end of this application, which is incorporated by reference in full herein. The APPENDIX describes the AES64 algorithm referenced above. The APPENDIX presents information regarding a specific algorithm and is not intended to be limiting in any way. Other implementations of the present invention may be made.

10

CONCLUSION

By the foregoing description, an improved secure I/O interface system and method have been described. The system and method may improve the security of communications to and from trusted hardware, improve communication speed, reduce the number of different systems required for secure communications, and reduce the extent of the bottleneck on the backplane bus.

20 The foregoing description of specific embodiments reveals the general nature of the invention sufficiently that others can, by applying current knowledge, readily modify and/or adapt it for various applications without departing from the generic concept. Therefore, such adaptations and modifications are within the meaning and range of equivalents of the disclosed embodiments. The phraseology or terminology employed herein is for the purpose of description and not of limitation. Accordingly, the invention embraces all such alternatives, modifications, equivalents and variations as fall within the spirit and scope of the appended claims.

25

CLAIMS

What is claimed is:

- 5 1. A security processor to process incoming and outgoing packets, the security processor comprising:
- a switching system to send and receive packets;
- a packet engine, coupled to the switching system, to handle classification processing for the incoming and outgoing packets; and
- 10 a cryptographic core, coupled to the packet engine, to provide encryption and decryption processing for packets received from the packet engine.
2. The security processor of claim 1 wherein the packet engine is further operable to handle security context management processing for the incoming and
- 15 outgoing packets.
3. The security processor of claim 1 further comprising:
- a local data bus coupled to the switching system; and
- a modulo engine coupled to the local data bus.
- 20 4. The security processor of claim 1 wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines.
- 25 5. The security processor of claim 4 wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines.

6. The security processor of claim 4 wherein the incoming and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines the egress path within the security processor upon exit from the
5 corresponding one of the plurality of cryptographic cores.

7. The security processor of claim 3 wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip.

10 8. The security processor of claim 7 further comprising a control processor, coupled to the local data bus, for exception handling of the incoming and outgoing packets.

9. The security processor of claim 7 further comprising a key management
15 engine coupled to the local data bus.

10. The security processor of claim 1 further comprising an intrusion detection system coupled between the cryptographic core and the packet engine.

20 11. The security processor of claim 7 wherein the security processor handles substantially all security processing for the incoming and outgoing packets.

12. The security processor of claim 11 wherein the security processor further handles substantially all network processing for the incoming and outgoing packets.
25

13. The security processor of claim 1 further comprising an intrusion detection system coupled between the cryptographic core and the packet engine.

14. A security processing system comprising:
(a) a security processor comprising:
a switching system to send outgoing and to receive incoming packets;
a packet engine, coupled to the switching system, to handle classification
5 processing for the incoming and outgoing packets;
a cryptographic core, coupled to the packet engine, to provide encryption
and decryption processing for packets received from the packet engine; and
a local data bus coupled to the switching system; and
(b) a memory coupled to the local data bus.

10

15. The security processing system of claim 14 further comprising a modulo
engine coupled to the local data bus.

16. The security processing system of claim 15 further comprising a key
15 management engine coupled to the local data bus.

17. The security processing system of claim 14 wherein the memory and the
security processor are within the same cryptographic boundary.

20 18. The security processing system of claim 14 wherein the security
processor is formed on a single chip.

19. The security processing system of claim 14 further comprising:
a memory interface coupled to the local data bus, wherein the memory is
25 coupled to the local data bus using the memory interface; and
a translator coupled to the memory interface to perform translation of data
received by the memory interface from the memory.

20. The security processing system of claim 19 wherein the translator performs steganographic translation of the received data.

21. The security processing system of claim 19 wherein the translator
5 performs encryption translation of the received data.

22. The security processing system of claim 14 wherein the security processor is operable to (i) execute boot code to load firmware for execution by the security processor and (ii) authenticate the boot code using a mechanism internal to the
10 security processor prior to operation of the security processor.

23. A security processor to connect a trusted network to an un-trusted network for data packet communication, the security processor comprising:

a first interface to couple to the trusted network and to the un-trusted network;
15 a second interface to couple to a host processor;
a switching system operable to selectively couple to the first interface or the second interface;
a local data bus, coupled to the switching system;
a plurality of packet engines coupled to the switching system;
20 a plurality of cryptographic cores each coupled to one of the plurality of packet engines; and
a control processor, coupled to the local data bus, to control data packet flow within the security processor.

24. The security processor of claim 23 wherein the security processor is operable to act as a firewall to deny or accept a data packet and to implement a secure communication channel with another computing device in the un-trusted network.

25. The security processor of claim 24 wherein the security processor implements data packet security and authentication functions to support the secure communication channel.

5 26. A communication system comprising:
a trusted network; and
a secure interface coupled to the trusted network to carry all incoming and outgoing communications of the trusted network, wherein the secure interface comprises a security processor to handle substantially all security processing for the
10 incoming and outgoing communications.

27. The communication system of claim 26 wherein the security processor performs substantially all network processing for data packet communications traveling to and from the trusted network.

15 28. The communication system of claim 27 wherein the secure interface handles substantially all security processing for the incoming and outgoing communications.

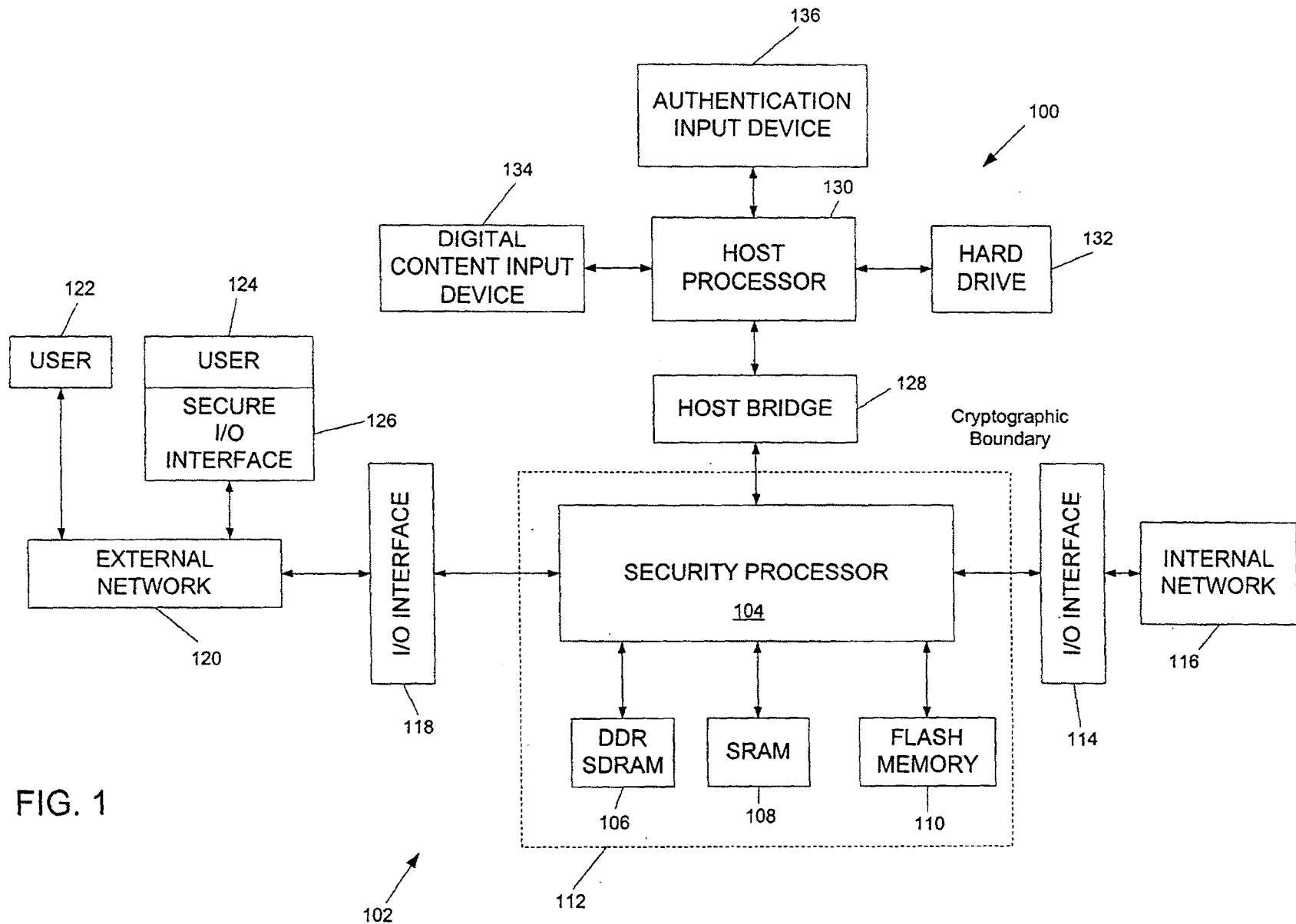
20 29. The communication system of claim 28 wherein the information security processing comprises IPSec processing.

25

SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

Abstract

5 A security processor performs all or substantially all security and network processing to provide a secure I/O interface system to protect computing hardware from unauthorized access or attack. The security processor sends and receives all incoming and outgoing data packets for a host device and includes a packet engine, coupled to a local data bus, to process the incoming and outgoing packets. The processor further
10 comprises a cryptographic core coupled to the packet engine to provide encryption and decryption processing for packets processed by the packet engine. The packet engine also handles classification processing for the incoming and outgoing packets. A modulo engine may be coupled to the local data bus.



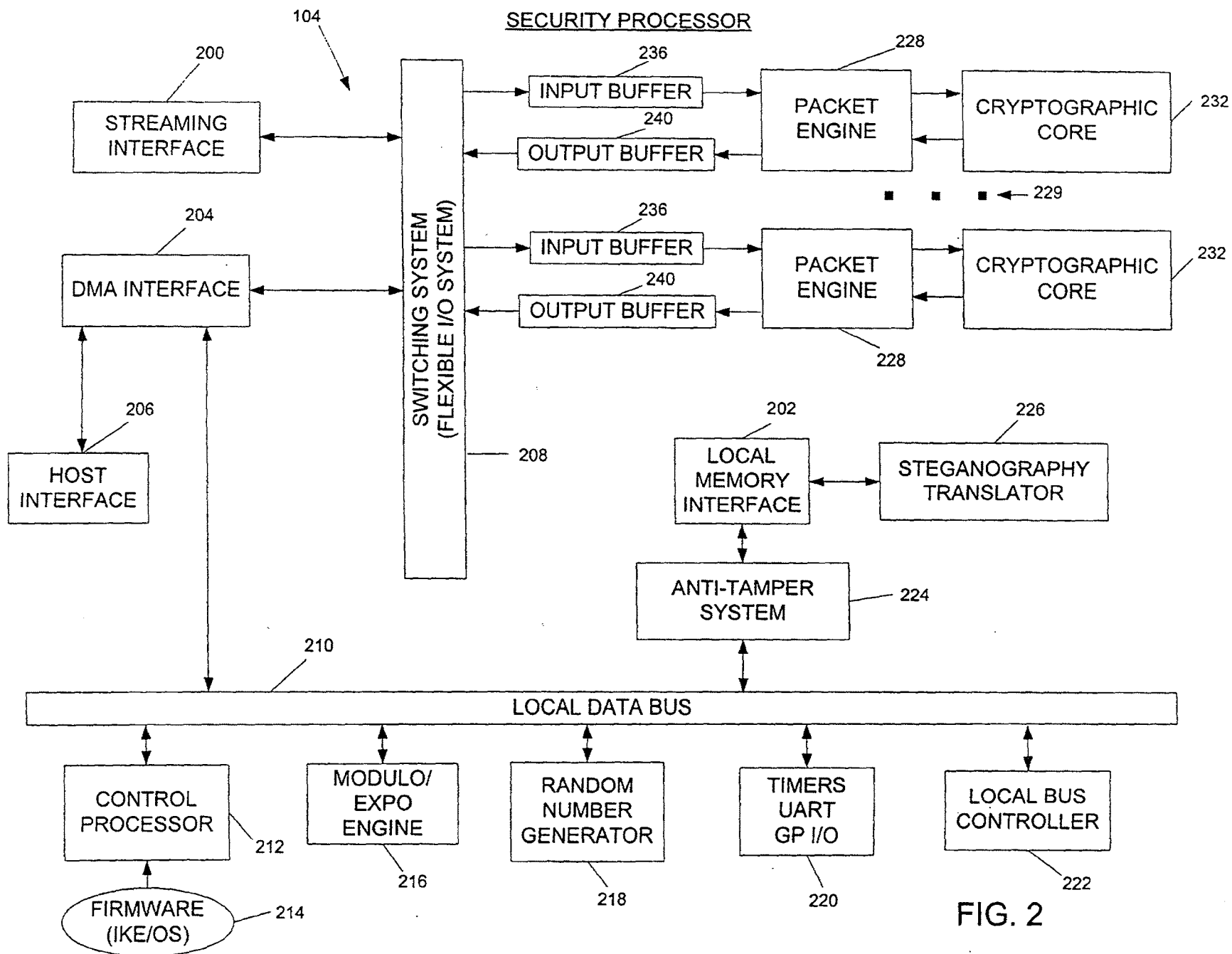


FIG. 2

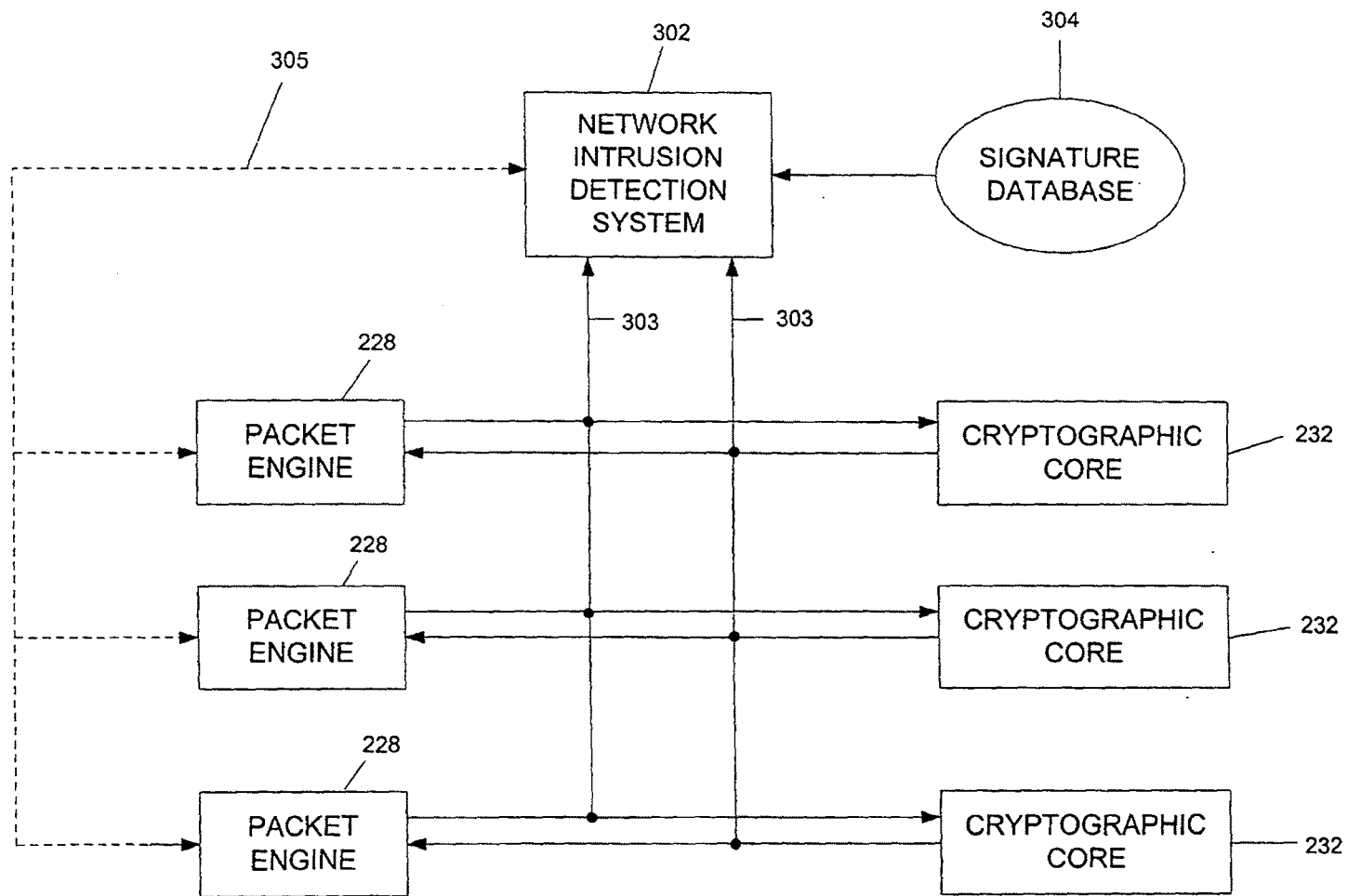


FIG. 3

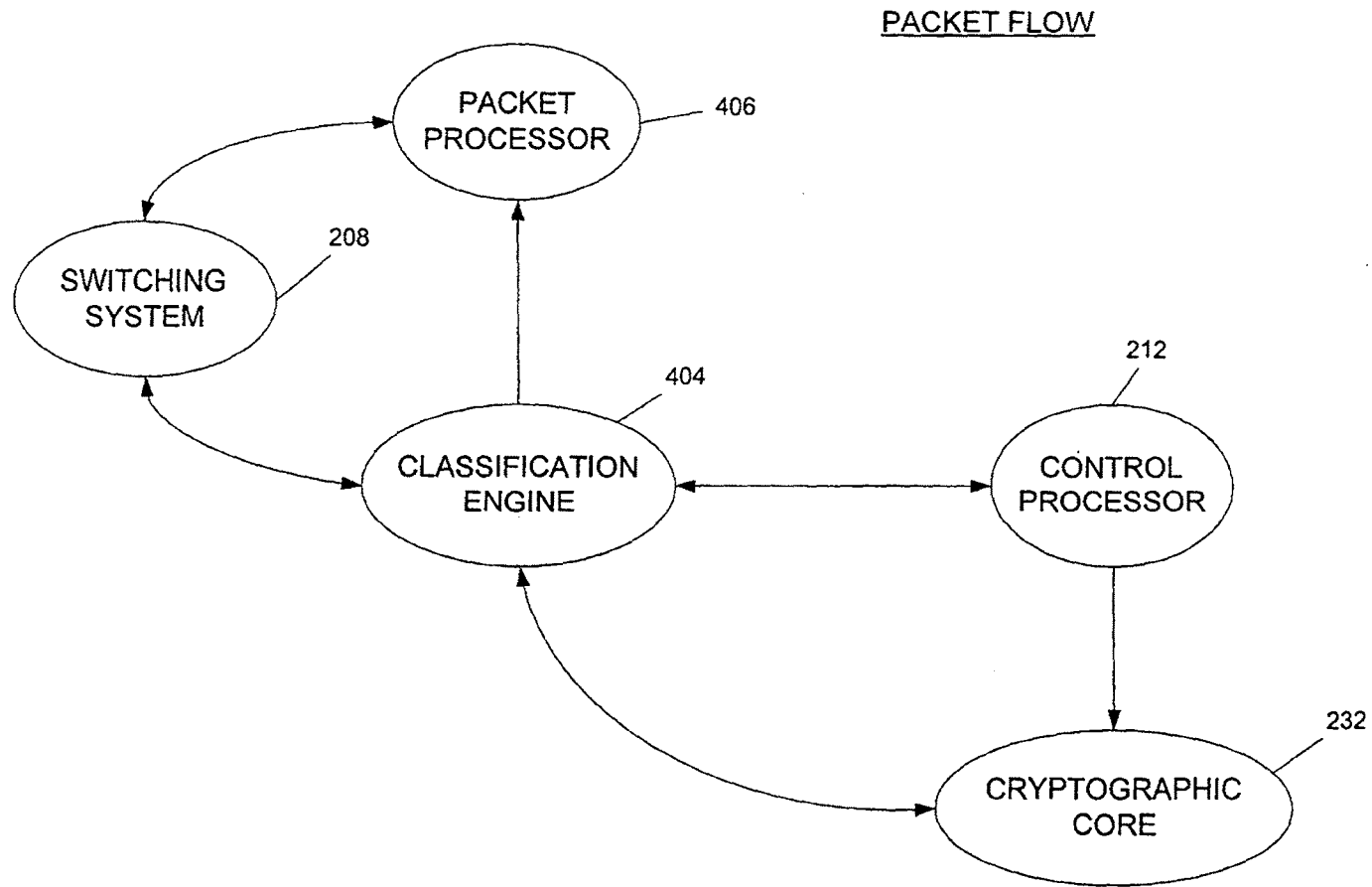


FIG. 4

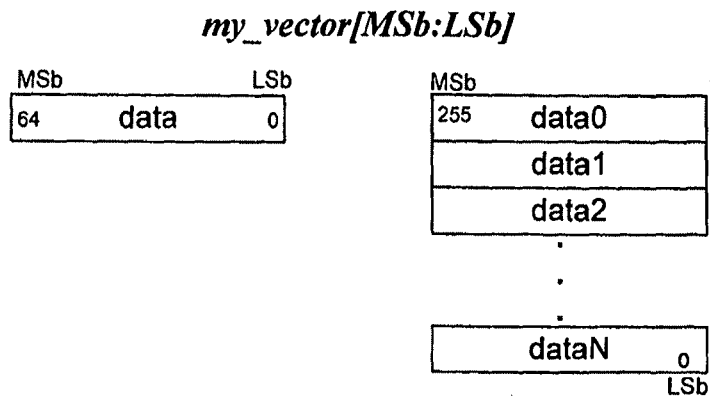


FIG. 5

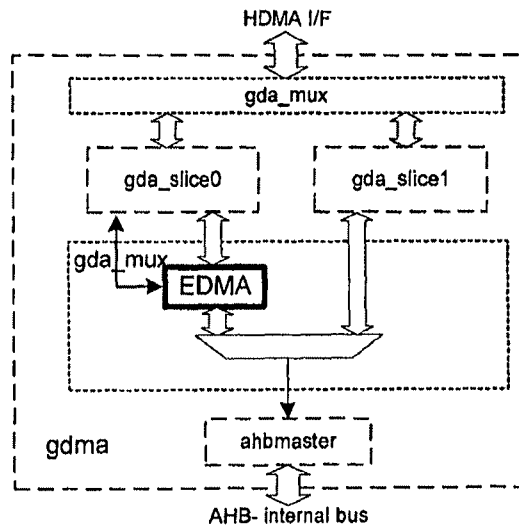


FIG. 6

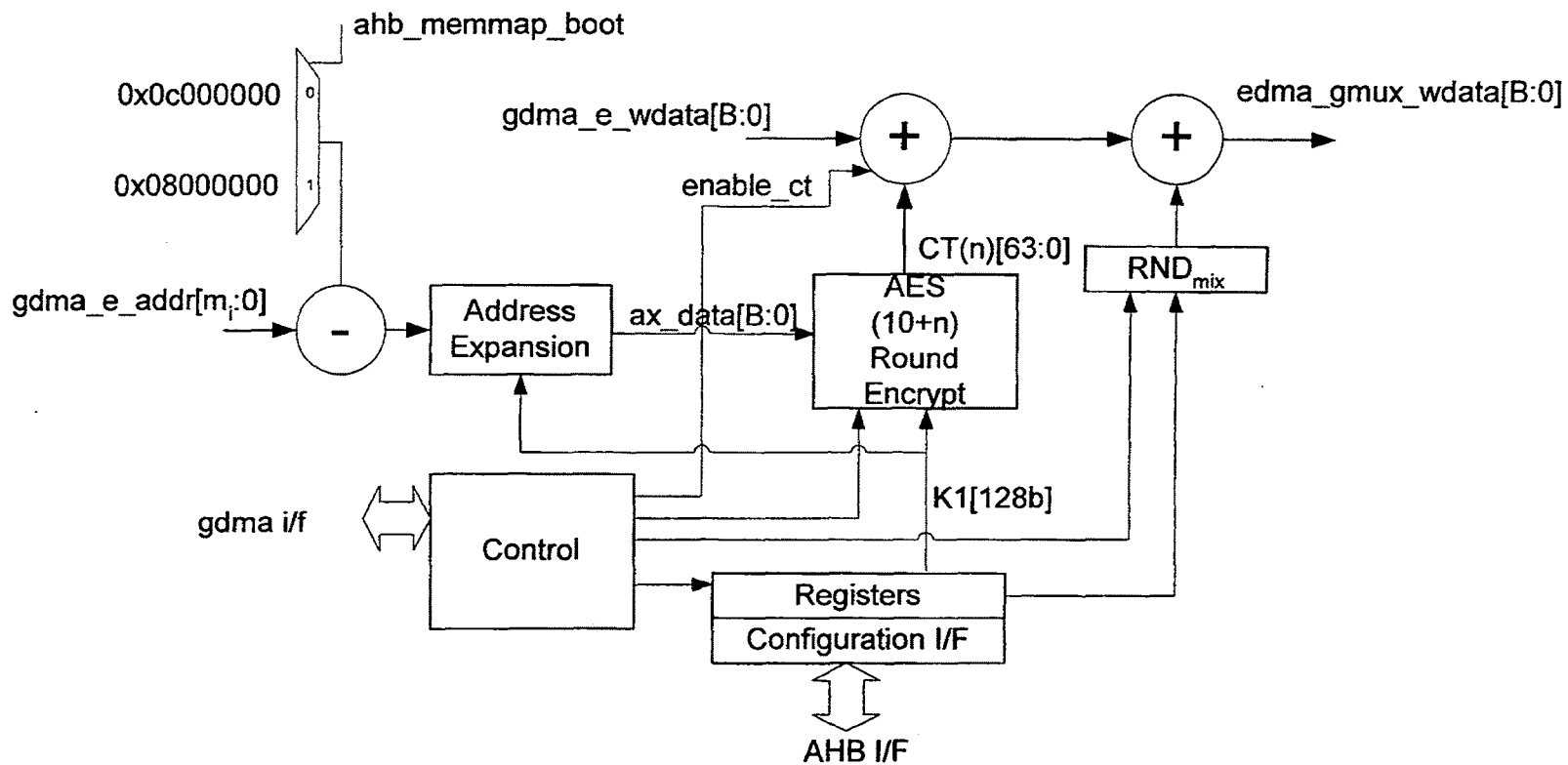


FIG. 7

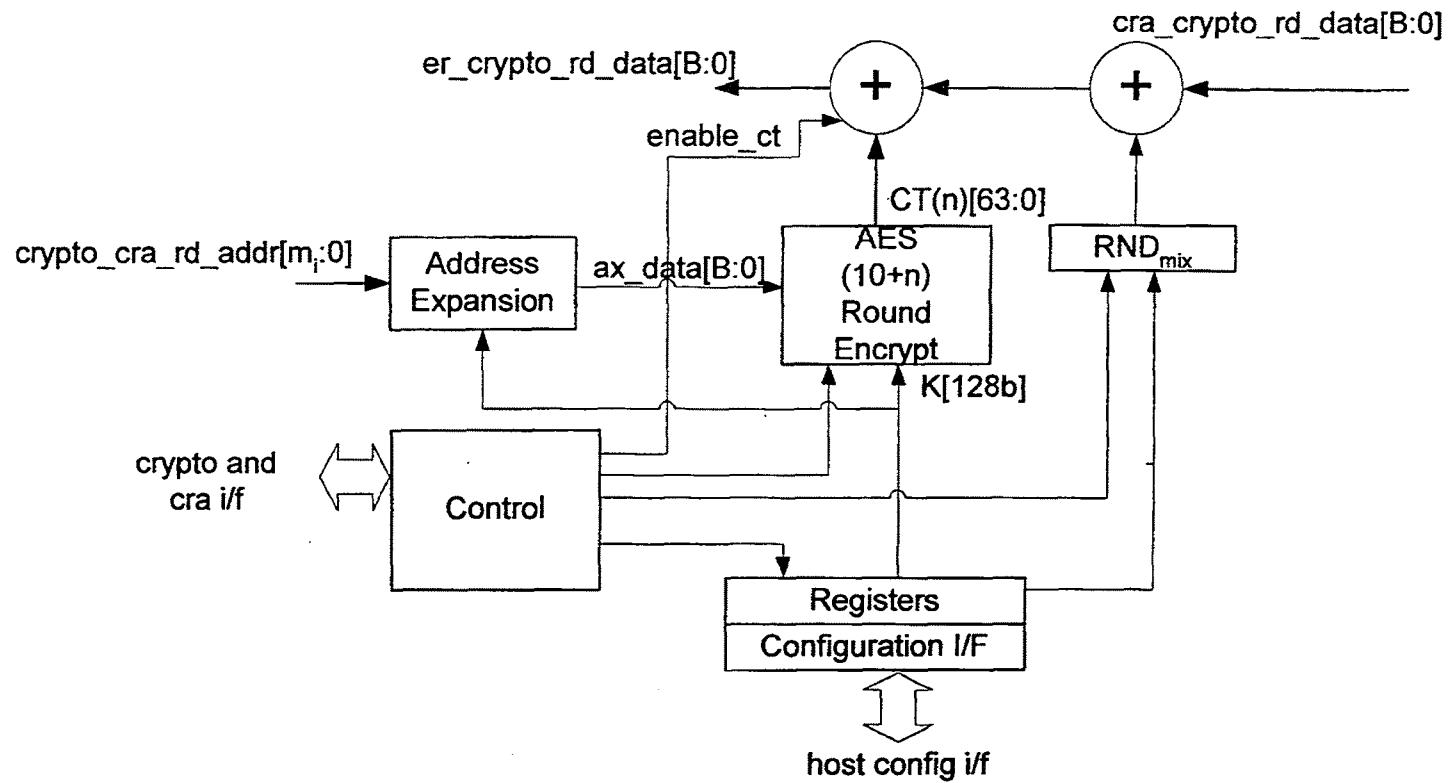


FIG. 8

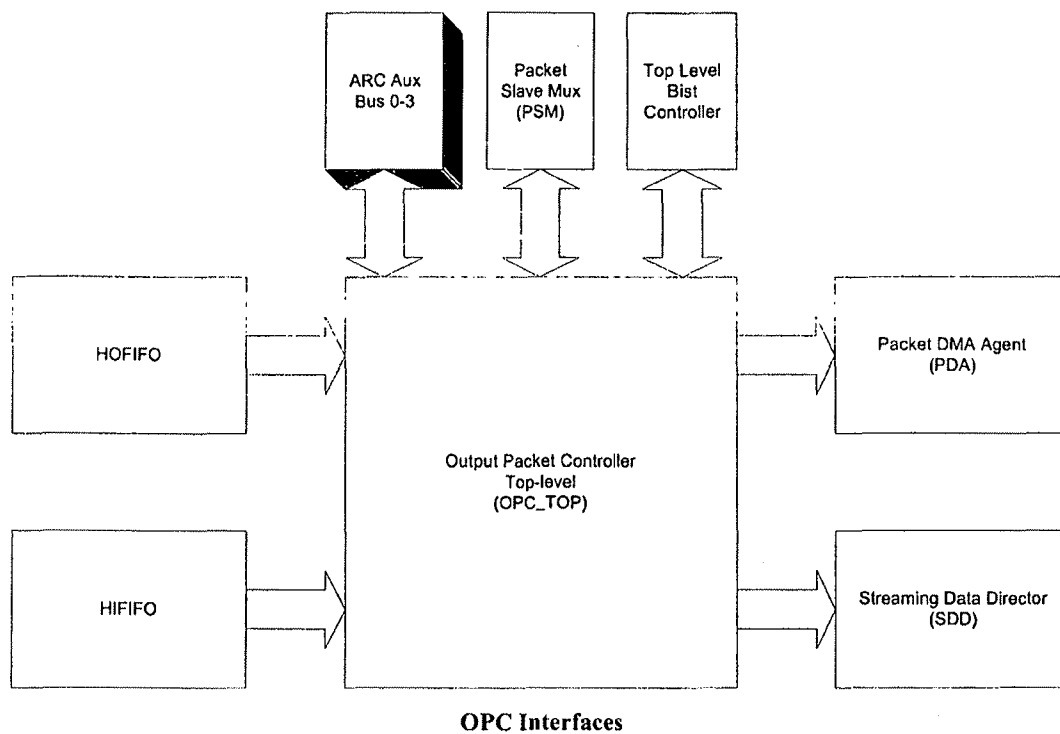
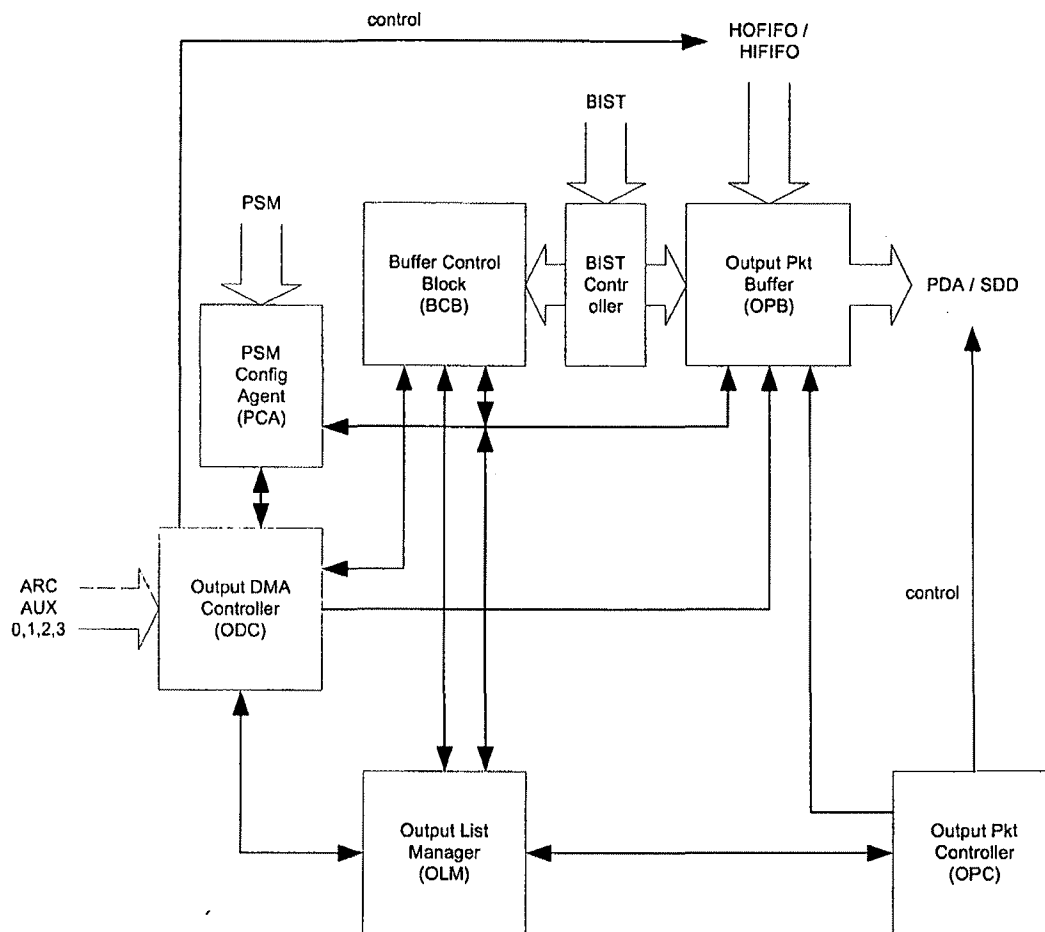


FIG. 9



OPC Internal Block Diagram

Notation:

PDA=Packet DMA Agent, forwards packets to host or connected entity via DMA.

SDD=Streaming Data Director. The SDD transfers packets to Streaming IO (e.g. GMII, PL-3, etc).

PCA= PSM Config Agent module enables host access to some of the OLM registers, and it contains a few configuration registers itself. Also, the PSM can access the OPB and the BCB RAMs (allowing host access).

FIG. 10

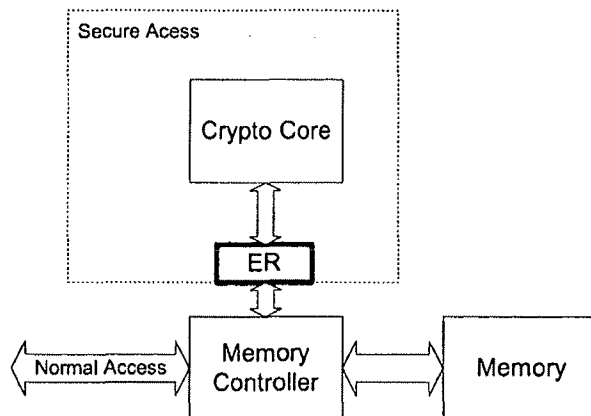


FIG. 11

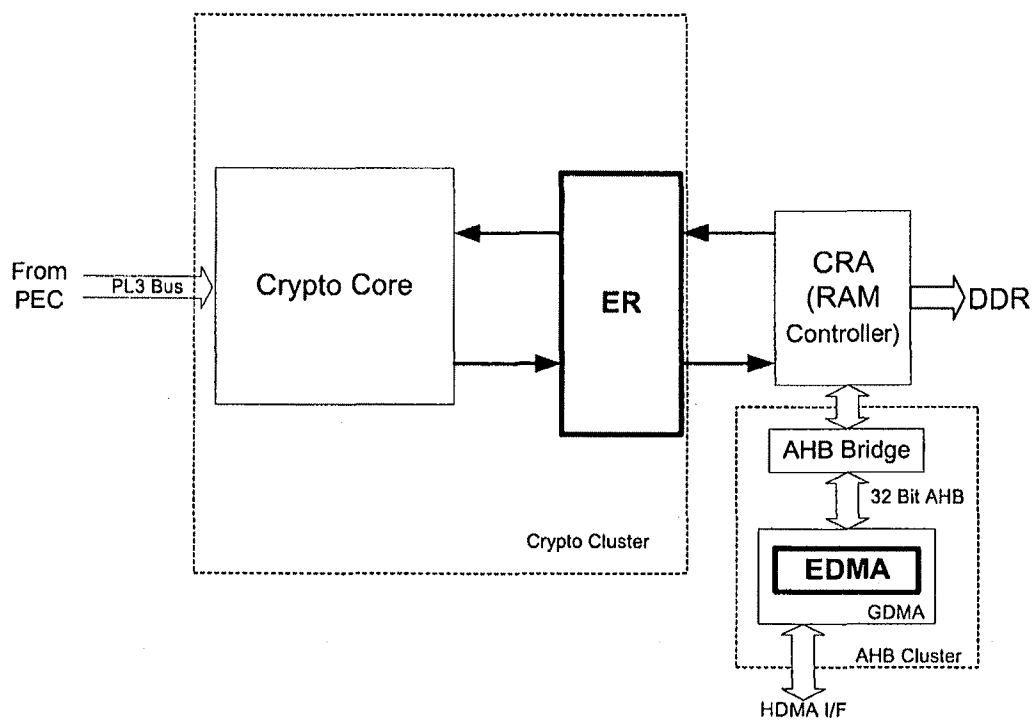


FIG. 12

F&L Form - PTO/SB/01

United States Patent Application
 Attorney Docket No.: 4224-25US (044.0003)
 First Named Inventor: John M. Davis



COMBINED DECLARATION AND POWER OF ATTORNEY FOR A UNITED STATES PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, mailing address, and country of citizenship are stated below next to my full name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter, which is claimed and for which a patent is sought on the invention entitled:

SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

the specification of which:

- ☐ is attached hereto;
☒ was filed on July 30, 2004 and assigned U.S. application serial no. or PCT application no. 10/903,785;
☐ and was 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 specifically referred to above, if any.

I hereby acknowledge the duty to disclose information which is material to patentability as defined by 37 C.F.R. § 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. 119 or 365 of any foreign application(s) for patent, inventor's or plant breeders rights certificate(s), listed below and have also identified below, any foreign application for patent, inventor's or plant breeders rights certificate(s), or of any PCT international application having a filing date before that of the application of which priority is claimed:

<u>Foreign Application No.</u>	<u>Country</u>	<u>Foreign Filing Date</u>
--------------------------------	----------------	----------------------------

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States Provisional applications listed below:

<u>Application No.</u>	<u>Filing Date</u>
60/507,976	10/02/2003

I hereby claim the benefit under 35 U.S.C. 120 of 365 of any United States application(s) or of any PCT international application designating the United States of America, listed below:

Page 1 of 2

PAGE 5/8 * RCVD AT 11/22/2004 12:30:49 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/1 * DNIS:7464060 * CSID:4803855061 * DURATION (mm-ss):03-04

EX-1013

Palo Alto Networks, Inc. and Fortinet, Inc. v. Lionra Technologies Ltd.

279

BEST AVAILABLE COPY

IF&L Form - PTO/SB/01

U.S. Parent Application
or PCT Parent No.

Country

Foreign Filing Date

As a named inventor I hereby also appoint the practitioner(s) associated with Ingrassia Fisher & Lorenz, PC, Customer Number 29906 to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

I hereby declare that all statements made herein of my own knowledge are true and that all statements 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 18 U.S.C. 1001 and that willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole or First Inventor: John M. Davis
 Signature of Sole or First Inventor: [Signature] Date: 11/9/04
 Residence City: Brentwood Residence State: TN
 Residence Country: USA Citizenship: USA
 Home or Business Post Office Address 1016 Highland Rd.
 City: Brentwood State: TN Zip Code: 37027

Full Name of Second Joint Inventor: Richard Takahashi
 Signature of Second Joint Inventor: [Signature] Date: Nov 9, 2004
 Residence City: Phoenix Residence State: AZ
 Residence Country: USA Citizenship: USA
 Home or Business Post Office Address 14033 So. 35th Place
 City: Phoenix State: AZ Zip Code: 85044

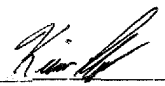
Application of: DAVIS, John M. et al.
Atty Docket: 2551-0109
Application S.N.: New Application
Page 8 of 8

REMARKS

The preliminary amendments made herein are to add priority data to the specification and insert revised claims. Claims 1-29 are canceled and 30-56 are pending. No new matter has been added through these amendments.

An early action on the merits is respectfully requested.

CHARGE STATEMENT: Deposit Account No. 501860, order no. (client-matter no.) 2551-0109 .
The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 (<u>missing or insufficiencies only</u>) now or hereafter relative to this application and the resulting Official Document under Rule 20, or credit any overpayment, to our Accounting/ Order Nos. shown above, for which purpose a <u>duplicate</u> copy of this sheet is attached
This CHARGE STATEMENT <u>does not authorize</u> charge of the <u>issue fee</u> until/unless an <u>issue fee transmittal sheet</u> is filed.

CUSTOMER NUMBER 42624	Respectfully submitted, By:  Kimani Clark Registration No.: 45,969
Davidson Berquist Jackson & Gowdey LLP 4300 Wilson Blvd., 7th Floor, Arlington, Virginia 22203 Main: (703) 894-6400 • FAX: (703) 894-6430	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT APPLICATION OF:

Confirmation No.: Unassigned

DAVIS, John M. et al.

Atty. Dkt.: 2551-0109

Application No.: New Application

Art Unit: Unassigned

Filing Date: Herewith

Examiner: Unassigned

Title: **SYSTEM AND METHOD FOR A SECURE
I/O INTERFACE**

Date: January 29, 2010

Change in Power of Attorney and Mailing Address

Hon. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Pursuant to 37 C.F.R. §1.63 (d)(4), attached is a copy of the change of power of attorney executed in the parent patent application. Please address all correspondence for the current continuation patent application to customer number 42624.

CHARGE STATEMENT: Deposit Account No. 501860, order no. **2551-0109**.

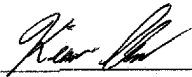
The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 (missing or insufficiencies only) now or hereafter relative to this application and the resulting Official Document under Rule 20, or credit any overpayment, to our Accounting/ Order Nos. shown above, for which purpose a duplicate copy of this sheet is attached.

This CHARGE STATEMENT does not authorize charge of the issue fee until/unless an issue fee transmittal sheet is filed.

CUSTOMER NUMBER

42624

Respectfully submitted,

By: 

Kimani Clark

Registration No.: 45,969

Davidson Berquist Jackson & Gowdey LLP
4300 Wilson Blvd., 7th Floor, Arlington, Virginia 22203
Main: (703) 894-6400 • FAX: (703) 894-6430



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	ATTY. DOCKET NO./TITLE
10/903,785	07/30/2004	John M. Davis	4224-25 US (044.0003)

CONFIRMATION NO. 4954

POWER OF ATTORNEY NOTICE

29906
INGRASSIA FISHER & LORENZ, P.C.
7150 E. CAMELBACK, STE. 325
SCOTTSDALE, AZ 85251



Date Mailed: 11/20/2007

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/08/2007.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/rmohamed/

Office of Initial Patent Examination (571) 272-4000 or 1-800-PTO-9199



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	ATTY. DOCKET NO./TITLE
10/903,785	07/30/2004	John M. Davis	2551-0032

42624

DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

CONFIRMATION NO. 4954

POA ACCEPTANCE LETTER



OC000000026769365

Date Mailed: 11/20/2007

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/08/2007.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/rmohamed/

Office of Initial Patent Examination (571) 272-4000 or 1-800-PTO-9199

Best Available Copy

DAVIDSON BERQUIST

Fax: 7038946430

Nov 8 2007 16:10

P. 01

RECEIVED
CENTRAL FAX CENTER

NOV 08 2007

FACSIMILE TRANSMISSION

To: United States Patent and Trademark Office

Facsimile No.: (571) 273-8300

From: Davidson Berquist Jackson & Gowdey, LLP

No. of Pages (including this page): 3

IF YOU DO NOT RECEIVE CLEARLY ALL PAGES, PLEASE CONTACT US
IMMEDIATELY BY TELEPHONE AT (703) 894-6400.**USPTO:** PLEASE ACKNOWLEDGE CLEAR RECEIPT OF ALL PAGES INDICATED
ABOVE BY FAXING THIS PAGE BACK TO (703) 894-6430

In re Patent Application of:	Attorney Docket No.: 2551-0032
DAVIS, John et al.	Group Art Unit: 2136
Application Serial No. 10/903,785	Confirmation No.: 4954
Filing date: July 30, 2004	Examiner: Traore, Fatoumata
Title: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE	Date: November 8, 2007

Name(s) of paper(s) being transmitted:

- Executed General Power of Attorney
- Statement Under 37 CFR 3.73(B)

CERTIFICATE OF FACSIMILE TRANSMISSION			
I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office at the above facsimile number on the date shown below.			
Name:	Sarah Lanning	Signature: <i>Sarah Lanning</i>	Date: 11/08/2007

CUSTOMER NUMBER

42624

DAVIDSON BERQUIST JACKSON & GOWDEY, LLP
4300 WILSON BLVD., 7TH FLOOR, ARLINGTON, VA 22203
703.894.6400 (main) • 703.894.6430 (Fax)

PAGE 1/3 * RCVD AT 11/8/2007 3:04:54 PM [Eastern Standard Time] * SVR:USPTO-EFAXRF-2/2 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):01:40

EX-1013

Palo Alto Networks, Inc. and Fortinet, Inc. v. Lionra Technologies Ltd.

285

Best Available Copy

DAVIDSON BERQUIST

Fax: 7038946430

Nov 8 2007 16:10

P. 02

RECEIVED
CENTRAL FAX CENTER

NOV 08 2007

STATEMENT UNDER 37 CFR 3.73(B)

Applicant / Patent Owner: DAVIS, John et al.

Docket No. 2551-0032

Application No. / Patent No. 10/903,785

Filed / Issued Date: July 30, 2004

Entitled: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

Assignee: ITT MANUFACTURING ENTERPRISES, INC.

A Corporation

(Name of assignee)

(Type of Assignee: corporation, partnership, university, government agency, etc.)

States that it is:

1. ☒ the assignee of the entire right, title, and interest; or
2. ☐ an assignee of less than the entire right, title and interest.
(The extent (by percentage) of its ownership interest is %)

in the patent application / patent identified above by virtue of either:

- A. ☐ An assignment from the inventor(s) of the patent application / patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

OR

- B. ☒ A chain of title from the inventor(s), of the patent application / patent identified above, to the current assignee shown below:

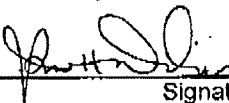
1.	From: <u>Inventors</u> To: <u>Corrent Corporation</u> The document was recorded in the United States Patent and Trademark Office at Reel <u>015256</u> Frame <u>0889</u> , or for which a copy thereof is attached.
2.	From: <u>Corrent Corporation</u> To: <u>ITT Manufacturing Enterprises, Inc.</u> The document was recorded in the United States Patent and Trademark Office at Reel <u>020056</u> Frame <u>0483</u> , or for which a copy thereof is attached.
3.	From: _____ To: _____ The document was recorded in the United States Patent and Trademark Office at Reel _____ Frame _____, or for which a copy thereof is attached.

- ☐ Additional documents in the chain of title are listed on a supplemental sheet.
- ☐ Copies of assignments or other documents in the chain of title are attached.

As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[Note: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, if the assignment is to be recorded in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.


Signature

J. Scott Davidson

Printed or Typed Name

Attorney, Registration No. 33,489

Title: _____

November 8, 2007

Date

703-894-6401

Telephone Number

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

POWER OF ATTORNEY,
CORRESPONDENCE ADDRESS
AND REVOCATION OF PRIOR POWERSRECEIVED
CENTRAL FAX CENTER

NOV 08 2007

Hon. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Revocation: I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

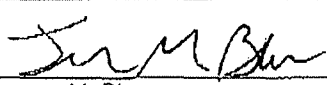
Power of Attorney: I hereby appoint the practitioners associated with customer number **42624**, individually and collectively, as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

I authorize Davidson Berquist Jackson & Gowdey, LLP to delete names/numbers of persons no longer with the Firm and to act and rely on instructions from and communicate directly with the entity who first sent this case to them and by whom I hereby declare that I have consented after full disclosure to be represented unless/until I instruct Davidson Berquist Jackson & Gowdey, LLP in writing to the contrary.

Correspondence Address: Please recognize or change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to the address associated with Customer Number **42624**.

*Assignee Name and Address:*ITT MANUFACTURING ENTERPRISES, INC.
1105 North Market Street, Suite 1217
Wilmington, DE 19801

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record			
The individual whose signature and title is supplied below is authorized to act on behalf of the assignee			
Signature		Date	11/5/07
Name	Thomas M. Blasey	Telephone	703-790-6314
Title	Assistant Secretary		

Date: 01/29/10

Approved for use through 7/31/2006. 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.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 12/697112		
APPLICATION AS FILED – PART I							
(Column 1)		(Column 2)		SMALL ENTITY		OR	
OTHER THAN SMALL ENTITY							
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)	
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A		N/A	330	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A		N/A	540	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A		N/A	220	
TOTAL CLAIMS (37 CFR 1.16(i))	27	minus 20 = 7	x\$26		x\$52	364	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	minus 3 = *	x\$110		x\$220		
APPLICATION SIZE FEE (37 CFR 1.16(s))			If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$260 (\$130 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR				
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))			195		390		
			TOTAL		TOTAL	1454	
* If the difference in column 1 is less than zero, enter "0" in column 2.							
APPLICATION AS AMENDED – PART II							
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY	
OTHER THAN SMALL ENTITY						OR	
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	Minus **	=	X =		X =	
	Independent (37 CFR 1.16(h))	Minus ***	=	X =		X =	
	Application Size Fee (37 CFR 1.16(s))			N/A		N/A	
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))			TOTAL ADD'T FEE		TOTAL ADD'T FEE	
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY	
OTHER THAN SMALL ENTITY						OR	
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	Minus **	=	X =		X =	
	Independent (37 CFR 1.16(h))	Minus ***	=	X =		X =	
	Application Size Fee (37 CFR 1.16(s))			N/A		N/A	
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))			TOTAL ADD'T FEE		TOTAL ADD'T 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.							

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.

EX-1013

Palo Alto Networks, Inc. and Fortinet, Inc. v. Lionra Technologies Ltd.

288